ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1811)
CURSO DE CIÊNCIAS MILITARES

João Pedro Castro Brum Silva Gomes

AS VULNERABILIDADES CRIADAS PELA CONDUÇÃO DE CELULARES NAS OPERAÇÕES DO PELOTÃO DE EXPLORADORES

Resende
2021

João Pedro Castro Brum Silva Gomes

AS VULNERABILIDADES CRIADAS PELA CONDUÇÃO DE CELULARES NAS OPERAÇÕES DO PELOTÃO DE EXPLORADORES

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Orientador: Cap Anderson Streit de Faria

Resende
2021

João Pedro Castro Brum Silva Gomes

AS VULNERABILIDADES CRIADAS PELA CONDUÇÃO DE CELULARES NAS OPERAÇÕES DO PELOTÃO DE EXPLORADORES

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Aprovado em_____ de _____ de 2021.

Banca examinadora:

_____
ANDERSON STREIT DE FARIA - Cap Cav
Orientador

_____
JASSON EGGRES PANDO - Cap Cav
Avaliador

_____
FILIPE GUEDES MAICÁ - 1º Ten Cav
Avaliador

Resende
2021

Dedico este trabalho à minha família, em especial ao meu pai Paulo Filho, companheiro, conselheiro incansável, exemplo de pai, fonte de inspiração militar e amigo leal.

AGRADECIMENTOS

Agradeço primeiramente a Deus, Senhor dos Exércitos e fonte de minha temperança e fé, que sempre esteve ao meu lado nos momentos de indecisão, incerteza, dificuldade e desafio.

Agradeço também à minha família, meu pai, Paulo, mãe, Angelita, e irmã, Maria Eduarda, que de longe acompanharam meus dias de alegria e de incerteza fazendo-se presentes de alma e sustendo-me no cumprimento desta missão.

Sou obrigado a retribuir meus amigos e camaradas de arma, sempre presentes em minha vida, que, vivendo as dificuldades e sorrindo às felicidades dos desafios vencidos, me mantêm firme no caminho que sigo.

Por fim, aos meus orientadores, Capitão Streit e Tenente Henkes, pelo esforço, dedicação e lealdade dispendidos a mim e a este trabalho. Sem o auxílio e conselhos dos senhores, este trabalho não seria viável.

RESUMO

AS VULNERABILIDADES CRIADAS PELA CONDUÇÃO DE CELULARES NAS OPERAÇÕES DO PELOTÃO DE EXPLORADORES

AUTOR: João Pedro Castro Brum Silva Gomes
ORIENTADOR: Anderson Streit de Faria

O mundo atual é marcado pela velocidade das comunicações pessoais. Os aparelhos celulares surgiram encurtando distâncias e agilizando o envio e recebimento de dados. Militares de todo mundo buscaram adaptar-se a essa nova realidade, utilizando as facilidades dos *smartphones* para melhorarem seus trabalhos de coordenação e controle. Entretanto, a velocidade desta mudança não foi acompanhada pela constante preocupação com a proteção dos dados e com a contrainteligência. Tal fato é demonstrado tanto em exercícios militares, em que aplicativos de celular foram utilizados para localizar tropas adversárias no terreno, quanto em situações reais, como os ataques eletrônicos e cibernéticos a tropas ucranianas, durante a anexação da Crimeia em 2014. Essa realidade nos leva a pensar o quão preparado o Exército Brasileiro está para enfrentá-la. O berço da oficialidade brasileira é a Academia Militar das Agulhas Negras. Por essa razão, cabe entender como esses jovens percebem o uso do celular por militares para que se tenha uma ideia clara da mentalidade de contrainteligência dos futuros oficiais. Concomitantemente a isso, é necessário expor as consequências do mau uso de um aparelho celular para as tropas nacionais. O trabalho presente teve por escopo o estudo das vulnerabilidades criadas pela condução de celulares em operações do pelotão de exploradores, uma vez que os militares deste pelotão realizam operações em prol de escalões superiores e normalmente convivem lado a lado com os meios mais nobres do Exército Brasileiro.

Palavras-chave: Exploradores, Celular, Contrainteligência.

ABSTRACT

THE VULNERABILITIES CREATED BY THE CONDUCTION OF CELLPHONES DURING SCOUT PLATOONS OPERATIONS

AUTHOR: João Pedro Castro Brum Silva Gomes
ADVISOR: Anderson Streit de Faria

Today's world is marked by the great speed of personal communication. Cellphone devices shortened distances and sped up the exchange of data. Military personnel around the world have tried to adapt to this new reality, using its functionalities to enhance command and control decisions. However, the speed of this change was not followed by the constant precaution with data protection, nor by counterintelligence. This fact is shown either in military exercises, in which smartphone applications were used to find adversary troops on the field, or in real situations, like electronic and cybernetic attacks against Ukrainian troops, during the Crimea crises of 2014. This reality invites us to think about how prepared the Brazilian Army is to face these new threats. The origin of the Brazilian Army officiality stands in the Academia Militar das Agulhas Negras. This is the reason why we shall understand how young cadets perceive the use of cellphones, to have a clear view of how developed the counterintelligence mentality of these men is. At the same time, it is necessary to expose the consequences of the uncareful use of a cellphone for the national troops. This study used the Scout' Platoon, once the men of this group operate for higher ranks and usually stay side by side with the most important means of Brazilian Army.

Keywords: Explorers, Cellphone, Counterintelligence

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

AMAN	Academia Militar das Agulhas Negras
BIB	Batalhão de Infantaria Blindado
CMT	Comandante
EB	Exército Brasileiro
ESC SP	Escalão superior
FA	Forças Armadas
GPS	*Global Position System*
MC	Manual de campanha
OM	Organização Militar
P	Página
PEL	Pelotão
RCB	Regimento de Cavalaria Blindado
RCC	Regimento de Carros de Combate
%	Porcentagem

SUMÁRIO

1 INTRODUÇÃO

A sociedade mundial passou por uma rápida transformação nas últimas décadas. Atualmente, o conhecimento, a criação e a capacidade de disseminação de informações são essenciais para o sucesso das organizações. O conhecimento passou a ser um dos ativos mais importantes, devendo ser protegido e explorado. (BELL, 1973)

Nesta sociedade do conhecimento, avanços tecnológicos acompanharam a necessidade crescente de acessar a informação rapidamente. Alguns destes avanços tornaram-se extremamente populares e parte do cotidiano de todos, inclusive de militares. O celular é um exemplo de nova tecnologia que se tornou companheira diária dos militares e será o objeto de estudo principal deste trabalho.

É possível observar que grande parte dos membros do Exército Brasileiro utilizam seus aparelhos celulares como instrumento de trabalho. Grupos em redes sociais deixaram o canal de comunicação mais amplo e rápido. Consulta a documentos de trabalho podem ser feitos em qualquer lugar. Blocos de anotação estão sendo gradativamente substituídos por blocos de notas digitais.

Essa evolução tecnológica também é percebida em operações militares. Nos conflitos armados modernos, a informação é necessária de maneira muito mais rápida e detalhada. Tal demanda exige aparelhos e equipamentos modernos que facilitem o trabalho de comando e controle, de alta conectividade e praticidade. O celular conectado à *internet*, então, aparece como um suposto substituto para um equipamento militar com essas funcionalidades.

No campo tático, um importante elemento de inteligência e de obtenção de informações essenciais para a decisão do comandante é o pelotão de exploradores. Alinhando isso ao exponencial aumento de uso de aparelhos celulares pelas tropas militares convém problematizar: Os celulares conduzidos pelos militares em operação do pelotão de exploradores podem ser utilizados como fonte de dados pelo inimigo?

Cabe ressaltar que o trabalho se propõe a relacionar diversas áreas de concentração. A fim de analisar o problema apresentado, abordar-se-á as áreas de cibernética, Contrainteligência e emprego tático do pelotão de exploradores.

Existem, na doutrina do Exército Brasileiro, diversos manuais que discorrem sobre a necessidade de negar informações ao inimigo. Como exemplo, o caderno de instrução EB70-MC-10.220, sobre contrainteligência. Contudo, o Exército carece de publicações doutrinárias

específicas ou atualizadas que relacionem as medidas de Contrainteligência com o uso de celulares.

Em razão dessa carência, vislumbra-se como sendo de interesse da Força Terrestre que se faça uma pesquisa sobre a aplicabilidade dos fundamentos da Contrainteligência e da segurança da informação no contexto atual de grande popularização do uso do celular.

As tropas de cavalaria do Exército Brasileiro têm como característica fundamental as suas comunicações amplas e flexíveis. Assim, o celular, que facilita, agiliza e flexibiliza as comunicações pode passar a impressão de ser uma ferramenta de extrema valia, especialmente em missões que requerem uma atuação extremamente decentralizada, como a do pelotão de exploradores.

Dessa premissa, também cabe pesquisar como o comprometimento dos dados dos celulares de um pelotão de exploradores pode prejudicar a missão do próprio pelotão ou até mesmo da força ou escalão dentro do qual ele está inserido.

O problema do vazamento de informações de celulares é posto em evidência quando identificamos as diversas formas que ela pode ocorrer. Alguns exemplos são as análises de conteúdo, as técnicas de localização eletrônica, as análises de tráfego de mensagens pela guerra eletrônica e cibernética inimiga ou até pela simples exploração de vulnerabilidades em aplicações instaladas, para a qual não se requer tropas especializadas.

A pesquisa, a partir do exposto, justifica-se por colaborar com a criação de possíveis procedimentos e hábitos relativos à condução de celulares em operações militares. Assim, acredita-se ser possível apontar maneiras para se aumentar a segurança orgânica dos militares bem como estudar as possíveis medidas de proteção eletrônica necessárias para impedir o comprometimento de missões pela ação da Inteligência, Guerra Eletrônica e Cibernética inimiga nos celulares de militares de nossas tropas.

Para tanto, este trabalho é dividido em cinco capítulos. Na introdução, apresentam-se os antecedentes históricos que levaram ao problema e a motivação deste trabalho. Em seguida, no referencial teórico, apresenta-se a doutrina brasileira de Contrainteligência. Neste capítulo, é feita uma pesquisa bibliográfica, principalmente no manual EB70-MC-10.220 (BRASIL, 2019), em que os conceitos e definições da contrainteligência são evidenciados e correlacionados com a armazenagem de dados nos celulares. Também neste capítulo, é feita uma pesquisa histórica e documental sobre como tropas militares pelo mundo foram expostas, em razão do mal uso de aparelhos celulares. O capítulo finaliza-se com um estudo da doutrina nacional sobre o pelotão de exploradores. São apresentadas suas características, missões e possibilidades.

No referencial metodológico, é realizada, apresentada e discutida uma pesquisa de campo, com o objetivo de entender a conjuntura atual do Exército com relação ao uso de celulares pessoais. Esta pesquisa busca compreender qual é a relação entre os futuros oficiais do Exército Brasileiro e os seus celulares. Juntamente com a pesquisa de campo, uma avaliação sistemática dos principais aplicativos busca apontar quais são as permissões mais requeridas por aplicativo comuns.

No capítulo 4, discussão dos resultados, apresenta-se o pelotão de exploradores, e como a negligência no uso de celulares pode gerar vulnerabilidades facilmente exploráveis pelo inimigo. Também busca-se apresentar as missões do pelotão, bem como as consequências do mal uso do celular em cada uma delas.

Por fim, o trabalho se encerra com uma conclusão, que traz as medidas de proteção propostas para que as deficiências na segurança eletrônica e cibernéticas dos celulares sejam minimizadas.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Apresentar as possíveis vulnerabilidades dos celulares que podem ser exploradas pela inteligência inimiga em operações típicas do pelotão de exploradores, concluindo sobre possíveis propostas para a mitigação dessas vulnerabilidades.

1.1.2 Objetivos específicos

Mapear deficiências na segurança dos celulares, possivelmente conduzidos pelo pelotão de exploradores, por meio de lições aprendidas e casos históricos;

Identificar se existe uma mentalidade de contrainteligência e de preservação de dados dos celulares dos futuros oficiais da linha de ensino militar bélica;

Identificar as possíveis consequências da exploração das vulnerabilidades dos celulares conduzidos por um pelotão de exploradores e

Propor procedimentos e hábitos que contribuam para a redução das vulnerabilidades apresentadas pelo celular.

2 REFERENCIAL TEÓRICO

2.1 SEGURANÇA DA INFORMAÇÃO E CONTRAINTELIGÊNCIA

Para este trabalho, cabe realizar uma revisão da literatura referente a segurança informacional e contrainteligência. Nenhum sistema do mundo será completamente seguro (AMAN, 2018, p. 1). Cabe ao comandante de fração buscar, a todo instante, formas e ferramentas que minimizem a aquisição de dados pelo inimigo em operações militares. Tais ações caracterizam a prática da contrainteligência.

Existem algumas estratégias que auxiliam a proteção da informação no ambiente cibernético, ambiente foco deste trabalho. Citam-se o privilégio mínimo, a defesa em profundidade, o ponto de estrangulamento, a simplicidade e a segurança através da obscuridade. (AMAN, 2018, p 10)

Quanto mais pessoas ou mais programas têm acesso a uma informação, maior a probabilidade desta informação ser utilizada ou vazada de maneira indevida. É neste princípio que se baseia a segurança do privilégio mínimo. Portanto, é interessante, em termos de segurança da informação, que o menor número de pessoas e programas tenha acesso a informação.

A defesa em profundidade estabelece que os dados devem ser protegidos por mais de um sistema. Assim, para que eles sejam acessados pelo inimigo, mais de uma defesa deve ser rompida. O ponto de estrangulamento, utilizado juntamente com a defesa em profundidade, garante que o acesso aquela informação seja único. Assim, o controle da disponibilidade da informação fica mais simples, contribuindo para a sua confidencialidade.

A simplicidade, como visto, também é forma de proteger a informação. Defesas muito complexas são mais propensas a falhas que podem ser exploradas. Por fim, existe a segurança por obscuridade. Esta se faz pela não divulgação da existência de uma informação.

É importante ressaltar que toda segurança é tão forte quanto for seu elo mais fraco. (AMAN, 2018, p.12) e que com o crescente número de informações contidas em um celular, esse aparelho pode vir a ser o novo elo mais fraco da segurança orgânica da tropa brasileira.

A Contrainteligência, segundo a doutrina brasileira, tem a função de prevenir, detectar, identificar, avaliar, obstruir, explorar e neutralizar a atuação da Inteligência inimiga, bem como negar as ações que ameacem a salvaguarda de dados e conhecimentos que a Força tenha o interesse de preservar. (BRASIL, 2019, p. 1-1).

A doutrina brasileira exposta no manual EB70-MC-10.220 não esgota os meios pelos quais se pratica a contrainteligência em campanha. Isso porque ela deve ser sempre aplicada, independentemente do meio de comunicação ou situação em que a tropa se encontre. Com as novas tecnologias, e com o crescente uso diário do celular pelos militares do Exército Brasileiro, é urgente que se aponte como o celular pode ser utilizado pela força inimiga para aquisição de dados.

As ações de contrainteligência orientam-se pelo levantamento das deficiências na segurança, bem como pelo mapeamento dos ativos do Exército a serem protegidos e pelas ameaças reais ou potenciais às quais os ativos estão expostos. (BRASIL, 2019, p.1-2)

Já se têm, pela doutrina nacional, mapeados os ativos a serem protegidos. Um deles é a segurança orgânica, que elenca os recursos materiais, recursos humanos, áreas e instalações e a informação como importantes recursos a serem protegidos. Celulares, como será exposto neste trabalho, carregam informações e dados sobre recursos humanos, materiais e áreas sensíveis.

2.2 DEFESA CIBERNÉTICA

2.2.1 A atuação do comandante na redução de vulnerabilidades

> No futuro, guerras não serão disputadas apenas por soldados com armas ou por aviões que lançam bombas. Elas também serão combatidas com o clique de um mouse, por todo mundo (SINGER, 2017, p.12, apud CLAYTON, 2011)

Como percebido pelos especialistas citados, a questão da segurança do ciberespaço já ocupa importante espaço nas discussões das Forças Armadas do mundo. Além dos computadores, já robustecidos e amplamente utilizados pelos exércitos modernos, celulares são cada vez mais utilizados pelos soldados. Com estes aparelhos, as comunicações foram agilizadas e individualizadas. Dados passaram a ser armazenados e transmitidos a todo instante. Estes dados existentes nos celulares de militares, por serem riquíssimos em informação, tornam-se ativos a serem protegidos pela segurança da informação e pela Contrainteligência.

A discussão sobre como reduzir as vulnerabilidades em um pelotão de exploradores passa pelo do conceito de ameaça. segundo a doutrina brasileira:

> Ameaça é a conjunção de ator, motivação e capacidade de realizar ação hostil, real ou potencial, com possibilidade de, por intermédio da exploração de deficiências, comprometer as informações, afetar o material, o pessoal e seus valores, bem como as áreas e instalações, podendo causar danos ao Exército (BRASIL, 2019, p. 2-1).

O presente trabalho objetiva contribuir para a redução das vulnerabilidades criadas pelo porte de celulares no pelotão de exploradores. Vulnerabilidades são, por sua vez, deficiências que, ao serem exploradas pelas ameaças podem causar incidentes de segurança (BRASIL, 2019, p.2-1)

Restaria, ao comandante de pelotão de exploradores, agir de duas formas distintas para eliminar vulnerabilidades: reduzir ameaças ou mitigar deficiências.

A redução de ameaças está acima do nível do tenente comandante de pelotão. Tal redução necessitaria, conforme manual citado, neutralização do ator inimigo, atuando à retaguarda profunda das linhas inimigas no ambiente cibernético, retirando sua capacidade de agir e recorrendo à desestruturação de imensas infraestruturas de comunicações, ou a destruição da motivação do inimigo de combater. Ambas as linhas de ação são inviáveis, taticamente, para serem realizadas por um pelotão de exploradores.

Assim, cabe ao comandante de pelotão, reduzir as vulnerabilidades atuando nas deficiências de sua tropa. Portanto, este trabalho pode contribuir para os trabalhos de contrainteligência previstos no manual EB70-MC-10.220, que prevê como um dos fatores orientadores da Contrainteligência a realização do levantamento das deficiências da segurança. (BRASIL, 2019, p.1-2)

2.2.2 As vulnerabilidades existentes em aplicativos

No ambiente cibernético, segundo SINGER (2017, p.51), existem três modos pelos quais o inimigo pode se manifestar: pelo furto de dados, uso indevido de credenciais e sequestro de recursos. Qualquer exploração de uma dessas três situações adversas pode causar muitos danos.

O furto de dados pode revelar dados operacionais de uma tropa, bem como os meios de que dispõe. O uso indevido de credenciais pode mudar ou destruir dados importantes. E, por fim, o sequestro de recursos pode levar ao fim das comunicações, bem como à divulgação de produtos da operação psicológica inimiga.

Quando se analisa a exploração cibernética aplicada aos celulares, é possível observar a presença de outro fator complicador da segurança: as aplicações. Estas são *softwares* que aumentam ou complementam as funcionalidades de um aparelho celular. Atualmente, existem cerca de 8.9 milhões de aplicativos disponíveis para serem baixados (KOETSIER, 2020). Isso gera abrigo para milhares de aplicativos possivelmente maliciosos e voltados para a aquisição de dados dos celulares.

Esse risco é apontado por Singer (2017, p. 54). Segundo ele, também se podem criar vulnerabilidades caso as aplicações sejam mal configuradas. Também há vulnerabilidades na grande complexidade dos aplicativos e *softwares* presentes nos celulares. A simplicidade é um dos princípios da segurança da informação. (AMAN, 2018, p 10) Assim, os complexos arranjos de códigos dos aplicativos, por muitas vezes, deixam brechas, que podem ser exploradas por atacantes ou inimigos.

Essas aplicações apontadas por Singer gerem seus acessos a dados por meio de permissões. Permissões são os privilégios de acesso que cada aplicativo requer. Podem variar de acesso a câmera, localização de GPS, acesso ao microfone, acesso aos arquivos do sistema, controle do fluxo de dados e outros.

Estas permissões normalmente são autorizadas pelo próprio usuário do aplicativo. Isso cria uma deficiência na segurança dos usuários desatentos, uma vez que o excesso de permissões vai de encontro ao conceito de privilégio mínimo, outra estratégia de segurança cibernética. (AMAN, 2018, p 10) Isso dá a oportunidade ao inimigo ou força adversa para explorar os dados de um celular sem precisar recorrer a métodos complexos de guerra cibernética.

2.3 ANÁLISE HISTÓRICA

Tal exploração cibernética, sem escalação de privilégios de aplicativos, já pode ser percebida dentro do campo militar. Diversas notícias trazem à tona a realidade de que tropas bem adestradas ainda não conhecem os riscos causados pela condução de aparelhos celulares em operações ou exercícios.

As deficiências de segurança surgidas na condução do celular podem ser divididas em dois grupos. O primeiro grupo é caracterizado pela exploração cibernética dos *softwares* que adicionam ou complementam as funcionalidades de um celular, conhecidos como aplicações ou aplicativos. O segundo grupo decorre da exploração eletrônica, realizada por tropas especializadas em guerra eletrônica, por meio de monitoramento de redes e ataques direcionados ao sinal de celular.

2.3.1 Lições aprendidas com casos de exploração cibernética

Como as funcionalidades dos aplicativos são das mais variadas, aplicações necessitam armazenar dados sobre seus usuários. E são estes os dados que podem servir de fonte de informação para terceiros.

Para demonstrar como dados sensíveis para a segurança orgânica são armazenados e expostos pelos aplicativos, recorre-se ao método de pesquisa histórico. Uma notícia[1] do final de 2019 mostra um exercício militar conjunto entre Noruega e Estados Unidos da América. Durante esse exercício, as instalações sigilosas da Noruega foram localizadas. Para isso, os americanos tiraram proveito de informações disponíveis a todos os usuários na aplicação "Tinder".

Esta é uma aplicação de relacionamentos que dá a opção de mostrar aos usuários da rede sua distância em relação ao outro. Nessa situação, militares noruegueses possuíam a aplicação em seus celulares e, por essa razão, estavam mapeados dentro da rede interna do aplicativo.

Os soldados americanos, aproveitando-se disso, observaram quais eram as distâncias entre eles e os usuários noruegueses que encontravam. Por meio de uma simples triangulação das distâncias encontradas pelos aplicativos, puderam localizar as tropas norueguesas.

Apesar de se tratar de um exercício, não é uma extrapolação imaginar que aplicativos como estes podem ser usados em operações reais, caso não haja uma diretriz rígida e rigorosa do escalão superior quanto a condução e uso dos celulares pelas tropas.

Cabe salientar que a informação da localização das tropas norueguesas estava disponível na rede pois a aplicação "Tinder" possuía a permissão de reconhecer, armazenar e divulgar a localização GPS daqueles aparelhos celulares.

A desatenção com as permissões dadas a aplicações também causou o vazamento de plantas de aquartelamentos americanos no Afeganistão. Segundo noticiado pela BBC[2], a rede social Strava coletava informações sobre a geolocalização de soldados enquanto faziam seu treinamento físico.

Como corriam portando o celular, foram lançadas, na plataforma, as plantas, localização de entradas e saídas, áreas restritas e outras informações sobre áreas e instalações americanas no Afeganistão – cabe lembrar áreas e instalações militares são um dos ativos mapeados que deve ser protegido pela contrainteligência para a manutenção da segurança orgânica.

---

[1] Notícia vinculada pelo blog CONTRADITORIUM, Disponível em https://contraditorium.com/2020/01/07/facar-amor-ou-faca-guerra-como-o-tinder-derrotou-uma-tropa-inimiga/, acesso em 27 de maio de 2020

[2] Disponível em https://www.bbc.com/news/technology-42853072, acesso em 27 de maio de 2020

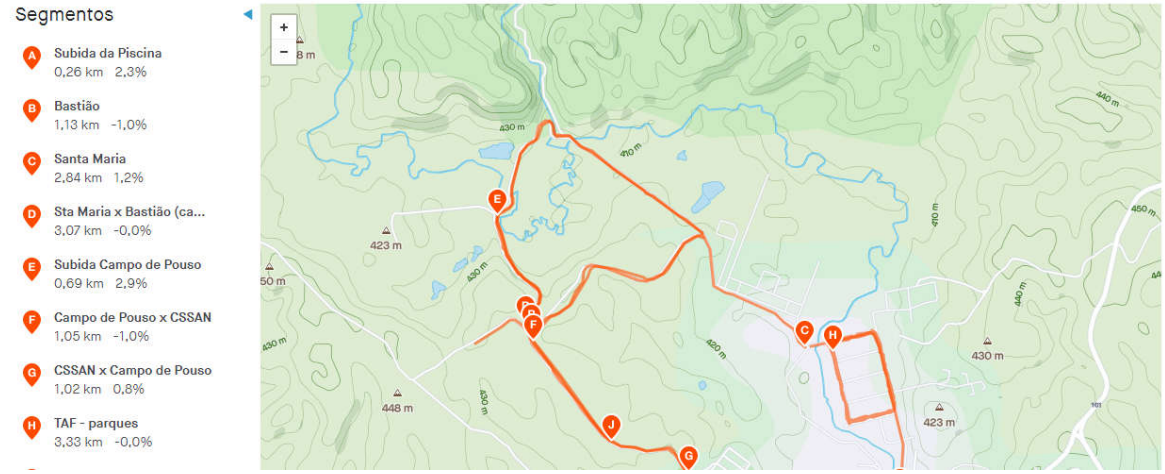
Figura 1 – Base norteamericana no Afeganistão exposta pela aplicação “Strava”

Fonte: BBC, 2018

Notícias como esta levam à seguinte reflexão: se tropas de países e exércitos desenvolvidos, que atualmente estão em campanha e operações de guerra mundo afora, negligenciam a segurança portando celulares, as tropas brasileiras estão cientes e preparadas para este risco?

Assim, pode-se, da mesma forma, analisar os dados fornecidos por aplicativos no Brasil. O aplicativo Strava, por exemplo, tem em seu banco de dados um mapa detalhado, com áreas do campo de instrução da AMAN iluminados, devido ao uso deste aplicativo no interior da Academia.

Figura 2: Áreas do campo de instrução da AMAN iluminadas pelo "strava"



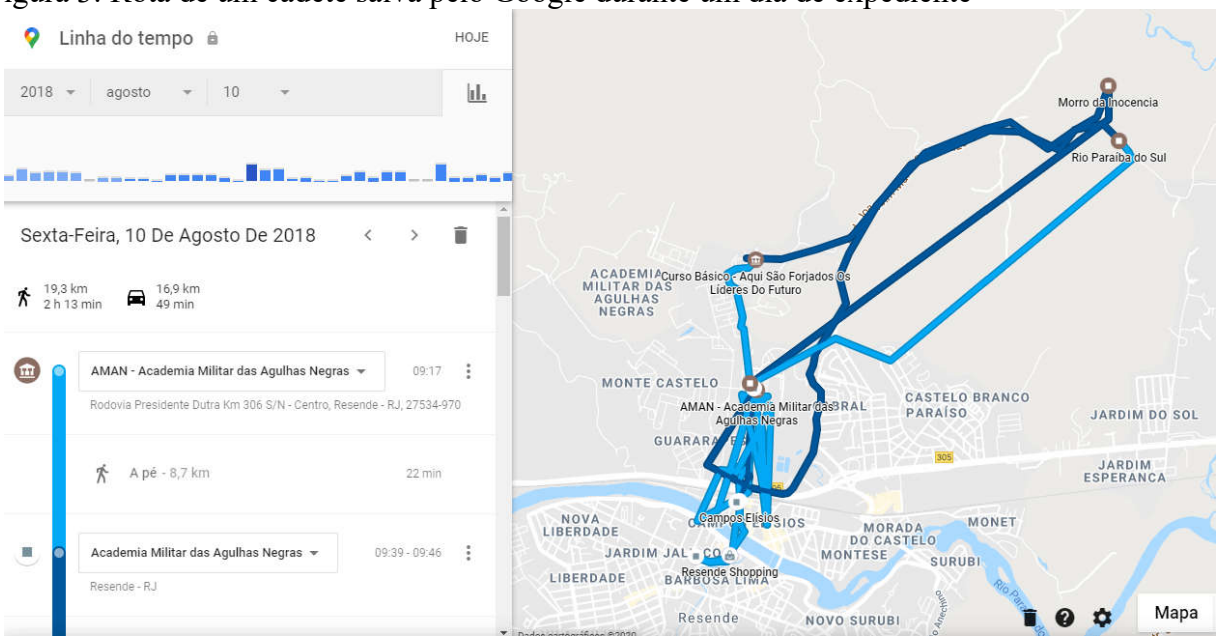
Fonte: Autor 2021

Além da aplicação Strava, outros aplicativos que atuam de maneira latente no aparelho celular podem gerar dados úteis ao inimigo ou a força adversa. O Google é um segundo exemplo disto. Das palavras de Gary Mcgraw, especialista em cibersegurança, depreende-se que o Google uma das ferramentas mais valiosas do arsenal dos atacantes:

> Você deseja furtar algo e precisa saber quem é o diretor de desenvolvimento? No passado, você enviaria James Bond para seduzir a recepcionista do RH e, então, esgueirar-se para dentro dos arquivos, enquanto ela dormia após uma noite de martinis e sexo. Agora, isso é mais tedioso. Apenas digite o nome em um site de busca na internet e você pode obter tudo. (SINGER, 2017, p 71, apud, MCGRAW, 2011)

Quando se troca o desejo de furtar dados de um produto qualquer pelo desejo de furtar dados militares, percebe-se como é vulnerável a segurança orgânica de toda uma tropa. Um exemplo disto é a vulnerabilidade criada pelo Google quando este aplicativo tem a permissão de coletar dados sobre a atividade física e localização GPS de seus usuários.

Figura 3: Rota de um cadete salva pelo Google durante um dia de expediente



Fonte: Autor, 2021

Se, em ambiente de paz, tais dados são gerados e armazenados nos celulares de militares, tem-se uma deficiência na segurança. Em tempos de conflito, tais dados já existentes podem ser utilizados pelo inimigo para a aquisição de localização de áreas de treinamento e estudo de técnicas militares nacionais. Além disso, sem a devida atenção, dados novos, em períodos de litígio, podem ser utilizados pelo inimigo a fim de se obter informações de campanha da Força Terrestre

A falta de conhecimento sobre as vulnerabilidades que podem ser criadas a partir de celulares pode levar a consequências graves para a segurança orgânica do pelotão de exploradores. Aplicativos maliciosos com permissões indevidas podem realizar *exploits* (códigos que exploram as vulnerabilidades em sistemas eletrônicos) para obterem informações tanto do aparelho (como sua localização) quanto do usuário (seus dados pessoais).

A exploração via aplicativos maliciosos já foi feita em combates modernos. Segundo noticiado pela agência de notícias Reuters[3], um grupo de *hackers* russos utilizou um *malware* implantado em dispositivos *android* de tropas ucranianas para localizá-las e destruí-las por fogo de artilharia.

2.3.2 Lições aprendidas com casos de exploração eletrônica

A exploração cibernética ocorre pela utilização de aplicativos maliciosos ou mal configurados pelos seus usuários. Já a exploração eletrônica necessita de maior infraestrutura de comunicações

Apesar de tropas especializadas serem necessárias para o mapeamento eletromagnético de celulares, ou para o uso destes como receptáculos e pontos de difusão de propaganda inimiga, já se tem notícias do uso da guerra eletrônica em celulares no mundo. Assim, é preciso lembrar que um dos objetivos da contrainteligência é também a neutralização da ação psicológica hostil do inimigo, bem como a desinformação. (BRASIL, 2019, p. 1-3)

Um exemplo ocorreu durante os conflitos entre Ucrânia e Rússia na península da Crimeia. Segundo noticiado[4], celulares de soldados ucranianos receberam mensagens que continham contraordens e mensagens voltadas para o impacto psicológico.

Segundo o *site* de notícias Associated Press[5], membros da resistência ucraniana recebiam em seus celulares particulares mensagens de desestímulo ao combate e de terror psicológico. Alguns exemplos de mensagens recebidas são: “Soldado ucraniano, eles encontrarão seus corpos quando a neve derreter” ou então “Existem 1054 suicídios nas Forças Armadas da Ucrânia. Quer ser o próximo?”

Não bastasse a operação psicológica, russos monitoravam as redes de celulares do campo de batalha. Manipulando o sistema de mensagens, verificavam os locais aos quais mensagens chegavam e saiam de aparelhos celulares e, assim, por diversas vezes, localizavam tropas de resistência. Tais ações foram apontadas também pelo relatório da OTAN escrito por Kenneth Geers.

---

[3] Disponível em: https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU, Acesso em 18 de out de 2020

[4] Disponível em: https://www.businessinsider.com/russians-use-creepy-text-messages-scare-ukrainians-changing-warfare-2018-8, acesso em 27 de maio de 2020

[5] Disponível em: https://apnews.com/article/9a564a5f64e847d1a50938035ea64b8f, acesso em 18 de outubro de 2020. Traduções nossas

> A inteligência de sinais russa (SIGINT), incluindo a espionagem cibernética, permitiu planejamentos de operações de combate muito eficientes contra o exército ucraniano. Fogos de artilharia podem ser ajustados com base na localização extraída de telefones celulares. (GEERS, KENNETH, 2015, tradução nossa)[6]

2.4 PELOTÃO DE EXPLORADORES

O pelotão de exploradores é a tropa que confere agilidade e consciência situacional às unidades blindadas. É utilizado para aumentar a gama de informações que o comandante necessita para decidir. Devido às suas características, possui grande mobilidade e proporciona a economia de meios para seus comandantes (BRASIL, 2002, p. 1-2)

Esta fração do Exército Brasileiro é subordinada, normalmente, à subunidade de comando e apoio de regimentos de carros de combate, regimentos de cavalaria blindados e a batalhões de infantaria blindados. E, por isso, cumpre missões em proveito dessas unidades, garantindo que as forças blindadas, meios mais nobres da Força Terrestre, sejam empregados com segurança e eficiência.

O pelotão é composto por seis viaturas leves, com cada uma a 4 homens. (Nas unidades de cavalaria, adiciona-se mais um rádio operador e um soldado explorador por viatura, totalizando 36 homens por pelotão). (BRASIL, 2002, p. 1-3).

Figura 4: Composição do pelotão de exploradores

	Viatura	Pessoal
GP CMDO		1º Ten (Cmt Pel)
		Sd Exp (At Lç Gr 40mm)
		Sd Exp (Mot VBL)
		Cb Exp (At Lç Roj / Rd Op)
		2º Sgt (Adj Pel)
		Sd Exp (At Lç Gr 40mm)
		Sd Exp (Mot VBL)
		Cb Exp (At Lç Roj / Rd Op)
1º GEXP		3º Sgt (Cmt GE)
		Sd Exp (At Lç Gr 40mm)
		Sd Exp (Mot VBL)
		Sd Exp (At Lç Roj / Rd Op)
		Cb Aux (Cmt 2ª Pa)
		Sd Exp (At Lç Gr 40mm)
		Sd Exp (Mot VBL)
		Sd Exp (At Lç Roj / Rd Op)
2º GEXP		3º Sgt (Cmt GE)
		Sd Exp (At Lç Gr 40mm)
		Sd Exp (Mot VBL)
		Sd Exp (At Lç Roj / Rd Op)
		CB Aux (Cmt 2ª Pa)
		Sd Exp (At Lç Gr 40mm)
		Sd Exp (Mot VBL)
		Sd Exp (At Lç Roj / Rd Op)

Fonte: BRASIL, 2014, p. 6

[6] No original: Russian signals intelligence (SIGINT), including cyber espionage, has allowed for very effective combat operations planning against the Ukrainian army. Artillery fire can be adjusted based on location data gleaned from mobile phones

Como o pelotão é composto por seis viaturas leves, a comunicação entre elas é fundamental.

> Uma das características das frações de reconhecimento é dispor de "Comunicações amplas e flexíveis". Tal flexibilidade permite ao Cmt Pel comandar e controlar seus subordinados, sem, no entanto, restringir sua capacidade de manobra. (BRASIL, 2002, p. 1-14)

Uma ferramenta como o celular, pelas suas características, pode, à primeira vista, parecer extremamente útil. Contudo, além de não ser meio de comunicação previsto na doutrina brasileira, a simples condução do aparelho gera vulnerabilidades que serão exploradas neste trabalho.

2.4.1 O pelotão de exploradores em operações de guerra

O pelotão de exploradores é uma fração extremamente versátil. Como é subordinado aos RCC, RCB e BIB, trabalha em proveito de unidades com os meios mais nobres do EB. Por esse motivo, as suas falhas de segurança podem gerar repercussões extremamente graves para suas unidades e escalões enquadrantes. Neste trabalho, estudaremos caso a caso as possíveis deficiências e vulnerabilidades das missões típicas do pelotão, criadas a partir da condução de celulares.

Umas das missões típicas do pelotão é a de executar missões de reconhecimento. As missões de reconhecimento têm a finalidade de informar ao comandante da unidade os Elementos Essenciais de Inteligência solicitados por ele ou pelo seu Estado Maior. (BRASIL, 2002, p. 3-1) O pelotão é capaz de reconhecer até dois eixos, zonas de até dois quilômetros de frente, cursos d'água ou itinerários.

Outra operação característica do pelotão é o reconhecimento e preparação inicial de uma zona de reunião de sua unidade. Segundo o caderno de instrução pelotão de exploradores (2002, p. 4-1), a zona de reunião é o local onde a tropa se reagrupa e se prepara para futuras operações, conduzindo as atividades de ressuprimento, alimentação, manutenção ou repouso.

O pelotão de exploradores também é apto a escoltar comboios, protegendo as viaturas que realizam as atividades logísticas. Nessas missões, existe grande dificuldade em se enfrentar emboscadas bem planejadas e, por isso, o comandante do comboio deve prever a possibilidade de ser emboscado. (BRASIL, 2002, p. 4-19)

Por fim, mas não esgotando a ampla diversidade de missões do pelotão de exploradores, tem-se o controle de estradas. Para isso, atua mobiliando pontos de controle e bloqueio de estradas, isolado ou em reforço a outras tropas, para controlar o movimento ao longo de um eixo específico.

3 REFERENCIAL METODOLÓGICO

O trabalho realizou, majoritariamente, os métodos de pesquisa histórico e indutivo. Assim, juntamente com a análise histórica das notícias apresentadas durante o referencial teórico, foi apresentada uma análise estatística sobre a consciência dos futuros oficiais, em formação na Academia Militar das Agulhas Negras

Segundo o manual EB70-MC-10.220:

> Desenvolver a mentalidade de Contrainteligência é um objetivo que deve ser buscado de forma permanente. A conscientização do público interno contribui para reduzir as deficiências e dificultar a atuação das ameaças (BRASIL, 2019, p. 1-5)

Como, segundo a doutrina, faz parte da contrainteligência identificar as ameaças existentes, (BRASIL, 2019, p. 4-1) realizou-se uma pesquisa de campo na AMAN para avaliar-se a mentalidade de contrainteligência dos futuros oficiais.

3.1 TIPO DE PESQUISA

A pesquisa utilizada neste trabalho é do tipo mista, utilizando dados quantitativos e qualitativos para a solução do problema apresentado. Para isso, a pesquisa apresentou 4 fases. Na primeira fase, fez-se uma pesquisa documental sobre casos históricos de aplicativos celulares que expuseram tropas militares em campanha.

Em sua segunda fase, outra pesquisa documental fora realizada, levantando-se quais são os principais aplicativos presentes nos celulares brasileiros. Nesta fase, também se realizou uma análise sistemática dos aplicativos mais comuns, avaliando quais eram as permissões às quais os celulares dos cadetes estavam expostos.

Determinados quais eram estes aplicativos, iniciou-se a terceira fase. Fez-se uma pesquisa de campo, de caráter quantitativo, com os cadetes da AMAN, a fim de verificar se os aplicativos mais comuns, segundo as fontes pesquisadas, estavam também presentes em celulares desses militares. A pesquisa também foi utilizada para avaliar o nível de consciência dos cadetes quanto ao uso seguro de celular e controle de permissões de aplicativos.

Por fim, realizou-se a integração de todos os dados. Assim, o trabalho objetiva mapear as lições aprendidas com exércitos do mundo sobre o uso dos celulares, identificar quais são os

aplicativos e suas permissões mais comuns na AMAN e relacionar ambas as linhas de pesquisa com possíveis consequências para as operações de um pelotão de exploradores.

3.1.1 Avaliação sistemática dos aplicativos

Foi feita uma avaliação sistemática dos seguintes aplicativos: WhatsApp, Google, Instagram, aplicações de e-mail, Aplicações de Banco (BB, Nubank e Santander), Facebook, Garmin Connect, Waze, CamScanner, Strava, Tinder e o jogo Pokémon GO.

Estes aplicativos foram escolhidos pela sua aparente credibilidade e popularidade entre os cadetes. Na avaliação sistemática, levantou-se quais as permissões que cada aplicativo requer.

Como já apresentado, aplicativos recolhem informações e dados dos aparelhos celulares. Em referencial metodológico, fez-se um repositório de lições aprendidas e expôs-se como os aplicativos podem vulnerabilizar uma tropa. Para trazer essa problemática à realidade brasileira, pesquisou-se quais eram os aplicativos mais utilizados pelos brasileiros (EXAME, 2020)[7], quais possuíam vulnerabilidades já conhecidas (Tinder e Pokémon Go) (TILGHMAN, 2016)[8] e quais eram populares entre os cadetes (AUTOR, 2021).

Contatou-se que esses aplicativos requeriam, conforme a tabela 1, em que o "X" representa a solicitação do aplicativo para ter acesso àquela permissão, os seguintes requisitos: acesso à câmera do celular, a localização do dispositivo por GPS, acesso ao microfone do celular, acesso ao armazenamento dos dados armazenados no dispositivo, acesso à lista de contatos do dispositivo, acesso ao telefone, acesso ao registro de ligações do celular, o monitoramento da atividade física realizada com o celular e o acesso às mensagens SMS do celular.

Tabela 1: Relação entre aplicações e permissões por elas solicitadas após o download

Permissões / Aplicações	Câ-mera	Localiza-ção	Micro-fone	Acesso aos dados	Conta-tos	Telefo-ne	Sensor de Atividade físcia	Registro de ligaçoes	SMS
Aplicação de bancos	x	x		x	x	x			
CamScanner	x			x					

[7] Disponível em: https://exame.com/tecnologia/saiba-quais-foram-os-aplicativos-mais-baixados-no-brasil-e-no-mundo/, Acesso em 10 de novembro de 2020

[8] Disponível em: https://www.militarytimes.com/news/your-military/2016/08/12/the-pentagon-has-banned-pokemon-go-from-official-military-phones/, Acesso em 10 de novembro de 2020

Permissões/ Aplicações	Câ-mera	Localiza-ção	Micro-fone	Acesso aos dados	Conta-tos	Telefo-ne	Sensor de Atividade física	Registro de ligaçoes	SMS
E-mail	x	x	x	x	x				
Facebok	x	x	x	x	x	x			
Garmin Connect	x	x		x	x	x		x	x
Pokémon Go	x	x		x	x		x		
Strava		x		x	x				
Tinder	x	x		x		x			
Waze	x	x	x	x	x	x			
WhatsApp	x	x	x	x	x	x		x	x

Fonte: Autor 2021

3.1.2 Questionário sobre o uso de celulares pelos cadetes

Além da avaliação sistemática, foi realizado um questionário – presente no apêndice deste trabalho – e foram colhidas 252 respostas. Considerando-se um grau de confiança de 95 por cento, os dados apresentam uma margem de erro de 6 pontos percentuais para mais ou para menos, para representarem o universo total de cadetes.

O questionário foi realizado entre os meses de abril e maio de 2020. A pesquisa foi difundida por meio da ferramenta online *Google Forms* e contou com 252 respostas válidas. Da amostra de cadetes questionada, apenas 2 (1%) afirmaram não utilizar o celular como ferramenta de trabalho.

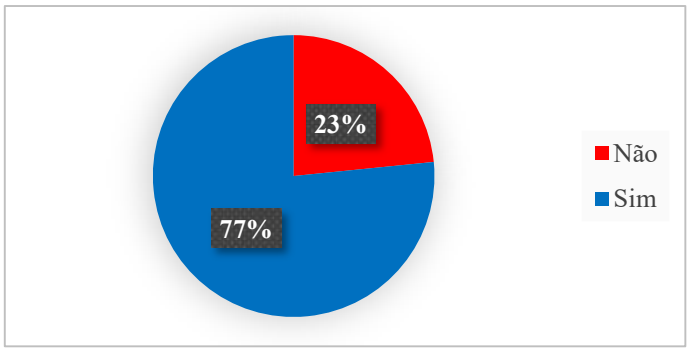
Aos 250 cadetes que responderam que utilizam o celular como ferramenta de trabalho, foi perguntado sobre de que forma estes aparelhos são utilizados profissionalmente. 245 disseram que trocam informações profissionais por meio de grupos de WhatsApp, 244 utilizam o celular para consultar documentos atinentes a profissão militar, 215 utilizam como ferramenta para confecção de trabalhos escolares e meio auxiliar de instrução, 179 utilizam para fotografia e filmagem de atividades na AMAN e 131 utilizam para auxiliar o planejamento de operações no terreno. Os dados em porcentagem foram distribuídos no gráfico 1.

Gráfico 1: Como o celular é usado como ferramenta de trabalho

Fonte: Autor, 2021

Também foi perguntado aos entrevistados se eles acreditavam que a condução de celulares em operações militares seria prática corriqueira. Setenta e sete por cento (77%) dos cadetes (193) responderam que militares conduzem celulares em operações militares e exercícios no terreno.

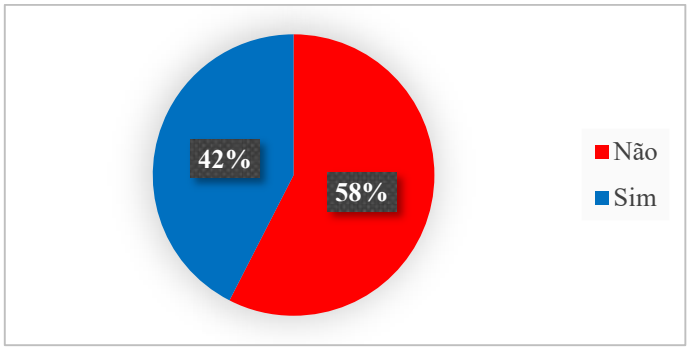
Gráfico 2: Militares conduzem celulares para exercícios no terreno?



Fonte: Autor, 2021

A pesquisa também analisou que porcentagem de cadetes verifica quais as permissões que suas aplicações requerem ao serem baixadas. Cento e quarenta e cinco (145) cadetes (58% do total) responderam que não costumam verificar as permissões que cada um de seus aplicativos requer.

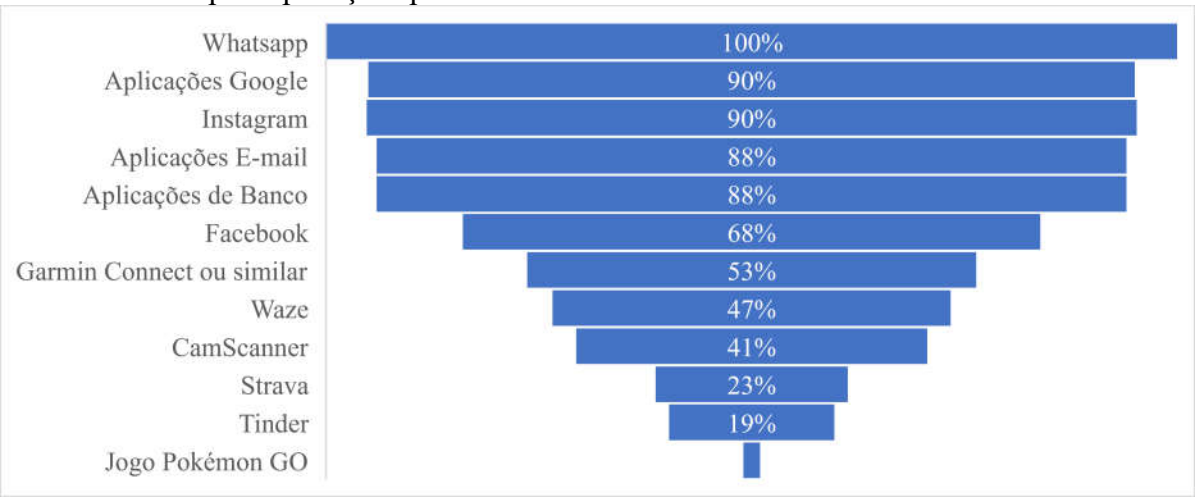
Gráfico 3: Costuma analisar as permissões de seus aplicativos?



Fonte: Autor, 2021

Além da verificação das permissões, perguntou-se quais aplicativos cada cadete possuía em seu dispositivo. Os resultados foram expressos no gráfico 4

Gráfico 4: Principais aplicações presentes nos celulares dos cadetes



Fonte: Autor, 2020

4 DISCUSSÃO DOS RESULTADOS

4.1 AS VULNERABILIDADES DAS PERMISSÕES DOS CELULARES DA AMAN

A primeira conclusão indutiva que se chega, ao observar-se os resultados da pesquisa, é o grande grau de inclusão que o celular possui na rotina profissional dos militares pesquisados. Apenas um por cento dos entrevistados diz não utilizar o celular como ferramenta de trabalho.

Cabe lembrar, que, segundo o manual de Contrainteligência, EB70-MC-10.220, em sua página 3-21, o uso de telefonia móvel para trocar informações sensíveis deve ser evitado.

Surge a preocupação, então, se os futuros oficiais, e futuros difusores das mentalidades de contrainteligência, possuem a consciência de que o celular pode gerar vulnerabilidades e vazar informações e dados sigilosos.

Isso porque, como foi visto na pesquisa, apenas pouco mais de 40% dos cadetes preocuparam-se com as permissões que seus aplicativos requeriam. Cruzando-se esse dado com a análise sistemática das permissões requeridas pelos aplicativos estudados é nítido que as estratégias de segurança da informação de privilégio mínimo não são adotadas.

A seguir, a partir dos resultados expostos pela pesquisa de campo, procurar-se-á demonstrar porque não existe uma mentalidade de contrainteligência no atual Corpo de Cadetes, respondendo ao objetivo do trabalho de identificar se existe uma mentalidade de contrainteligência e de preservação de dados dos celulares dos futuros oficiais da linha de ensino militar bélica.

4.2 UTILIZAÇÃO DE APLICATIVOS PARA LOCALIZAR A TROPA

A pesquisa no âmbito AMAN revelou que existem muitos cadetes que não tomam o devido cuidado com a autorização das permissões em celulares e, além disso, possuem aplicativos que podem expô-los ao inimigo ou a forças adversas em operações.

Pega-se, como exemplo, o Google, aplicativo presente em 9 de cada 10 celulares de cadetes. Este aplicativo, como o Pokémon Go, solicita ao usuário que monitore a sua atividade física. Isso ocorre de maneira latente no aparelho, e não requer que o aplicativo esteja aberto para coletar informações.

Estas permissões, que autorizam o monitoramento de dados de atividade física do usuário, como velocidade de deslocamento e localização GPS, permitem que o aplicativo crie mapas detalhados com as rotas de um militar, em seu sistema.

O Google é apenas um exemplo de como dados podem ser armazenados sem o consentimento ou mesmo conhecimento do usuário. Cabe a ressalva de que estes dados não estão disponíveis para qualquer um. São acessáveis apenas com a senha pessoal do usuário. Contudo, eles existem e, consequentemente, podem ser acessados e explorados em ações de guerra cibernética.

Por sua vez, outros aplicativos, como o Strava (presente em 23 por cento dos celulares analisados), não só armazenam tais dados como os tornaram públicos, sem que seja necessária a autorização de seus usuários para tal. O dado que existia, assim como o do Google, passou não só a ser acessível por pessoas especializadas na coleta de dados cibernéticos, mas como por qualquer pessoa *online.*

Aplicações com essas permissões podem deixar marcados em cartas online rotas de entrada e saída de OMs, evidenciarem horários e itinerários de rondas e auxiliarem a localização de postos de sentinelas, por exemplo.

Faz-se aqui, uma referência ao apresentado neste trabalho durante o referencial teórico. Existem lições aprendidas, em outros exércitos do mundo, em que aplicativos como estes expuseram a localização de tropas em campanha (AUTOR, 2021, p. 19 a 21).

A exposição torna-se evidente quando os cadetes respondem, em sua maioria, (77 por cento) que acreditam que celulares são levados para operações e exercícios no terreno. O número é alto e configura uma mentalidade de conformidade com o uso do celular, por este ser extremamente prático e fácil de ser utilizado.

Existem, doutrinariamente, diversas medidas de proteção eletrônica que visam mascarar a localização de meios de comunicação previstos. Por exemplo, a comunicação via rádios FALCON pode ser criptografada e enviada com saltos de frequência, para que não seja rastreada pelo inimigo. Se os celulares são portados pela tropa, negligencia-se a estratégia de ponto de estrangulamento para a proteção da informação, uma vez que mais um dispositivo capaz de ser rastreado é conduzido pela tropa.

Além disso, não há previsão doutrinaria para o uso do celular em campanha, muito menos previsão para medidas de proteção eletrônica para o seu uso. Assim sendo, a sua simples condução gera dados que podem ser usados pelo inimigo. Seja por meio de aplicativos que armazenam dados pessoais em seus servidores próprios – que por vezes são sediados em países

estrangeiros, contribuindo para a dependência tecnológica das FA- seja por meio de aplicações maliciosas voltadas justamente para roubar dados.

4.3 UTILIZAÇÃO DE APLICATIVOS PARA MONITORAR CONVERSAS

Analisando os dados obtidos, observa-se o quão rotineiro é o uso dos celulares para os cadetes. Noventa e oito por cento utilizam para a comunicação profissional e para consulta de documentos. Estes números só corroboram que a existência de muita informação sensível nesses aparelhos.

A permissão de acesso à câmera do celular pode dar acesso a imagens sobre o que o combatente está vivenciando. Bem como a permissão de acesso ao microfone pode gerar informações em áudio. Observa-se que ambas essas permissões estão presentes em praticamente todas as aplicações.

Se noventa e oito por cento dos cadetes utiliza o celular em ambiente profissional, aplicativos maliciosos que tenham acesso ao microfone e à câmera do celular podem atuar como escutas nas salas de planejamento dos comandantes de pelotão e subunidades.

Outro tipo de permissão presente nos aplicativos é a de acesso aos contatos, telefones e ao armazenamento do telefone. Estas permissões, se exploradas por aplicativos maliciosos, facilitam o trabalho da inteligência inimiga, uma vez que

> O ambiente volátil, incerto, complexo e ambíguo no qual os líderes do século 21 atuam exige a capacidade de discernir, dentre um imenso turbilhão de dados e informações, quais são relevantes, quais verdadeiramente interessam, e quais estão ali para intencionalmente confundir e desorientar. (GOMES FILHO, 2020)

Com aplicações maliciosas que possuam essas permissões, pode-se localizar números de telefones chave, afunilando o número de informações e resgatando dados de celulares que, por pertencerem a comandantes, tem maior potencial de carregarem informações essenciais.

Se os soldados de um pelotão salvam o contato de seus comandantes como “tenente” ou “capitão”, aplicativos com acesso aos contatos do celular podem expor ordens de batalhas e possíveis planejamentos presentes nos celulares dos líderes. Tal problema é claramente visualizado quando trazido ao nível do pelotão. Mais da metade dos cadetes (52%) futuros comandantes de pelotão, responderam que utilizam o celular para o planejamento de operações.

4.4 AS AMEAÇAS DO USO DE CELULAR NO PELOTÃO DE EXPLORADORES

O exposto ao longo do trabalho, pelos casos históricos e análises sistemáticas dos aplicativos, deixa claro que existem deficiências de segurança nos celulares. Assim, respondido o objetivo do trabalho de mapear deficiências na segurança dos celulares, pode-se relacionar essas deficiências como possíveis vulnerabilidades na atuação, em campanha do pelotão de exploradores.

O pelotão de exploradores precisa de comunicações amplas e flexíveis. Assim, este capítulo propõe-se a realizar a relação dos casos históricos apresentados, da pesquisa de campo feita e das missões do pelotão de exploradores, buscando cumprir o objetivo do trabalho de identificar as possíveis consequências da exploração das vulnerabilidades dos celulares conduzidos pelos integrantes de um pelotão de exploradores.

4.4.1 Vulnerabilidades em missões de reconhecimento

Como já foi visto durante o referencial teórico, celulares podem ser alvos da ação psicológica hostil, como a desinformação, como ocorreu durante a anexação da Crimeia pela Rússia. Um ataque de desinformação inimiga nos celulares do pelotão pode gerar graves falhas nas operações de reconhecimento.

Um comandante de pelotão de exploradores, formado pela AMAN, poderia ser suscetível a este tipo de ataque. Como poucos cadetes se preocupam com a condução de celulares em exercícios e operações (23 por cento), existe a possibilidade de que, após formados, os comandantes de pelotão carreguem esse vício para os corpos de tropa e sejam permissivos quanto ao uso do celular no terreno pelos seus subordinados. Dessa maneira, o líder do pelotão pode contribuir para que os celulares de seu pelotão sirvam de receptáculo para produtos de operações psicológicas inimigas.

Desatento a esses possíveis ataques, o pelotão pode receber mensagens falsas de um número identificado como sendo o do seu comandante que, por exemplo, poderiam ordenar o abandono do eixo de reconhecimento. Situação análoga ocorreu na Crimeia, em que mensagens SMS ordenavam a retirada de combate dos soldados ucranianos. Além de aplicativos maliciosos, a permissão de acesso aos SMS está presente em no mínimo 94 % (considerada a margem de erro) dos celulares dos futuros oficiais, por meio do aplicativo *Whatsapp* ou pelo aplicativo da *Garmin Connect*, como apontado pela pesquisa de campo.

Outra situação possível é o uso de notícias falsas para abalar o moral do pelotão. Uma campanha de desinformação inimiga, que faz uso de mensagens falsas utilizando o número de telefone de familiares marcados na agenda de contato como “mãe” ou “pai”, podem fazer com

que o pelotão perca as características essenciais da tropa de cavalaria destacada, como a agressividade e o arrojo no combate.

A falta de atenção com as permissões solicitadas pelas aplicações, constatada pela pesquisa em 58 % dos cadetes, se mantida após o oficialato, pode facilitar o trabalho de tropas inimigas, utilizando-se das aplicações que têm acesso ao telefone ou à lista de contatos. Todos os aplicativos estudados possuíam essas permissões, com exceção do *CamScanner.*

4.4.2 Vulnerabilidades em missões de reconhecimento e de balizamento de zona de reunião

Outras missões típicas do pelotão de exploradores são o reconhecimento e balizamento de zonas de reunião. As consequências da exploração inimiga dos celulares do pelotão nesses tipos de missão podem ser graves.

O pelotão realiza missões em proveito de Forças Tarefas blindadas. Os meios mais nobres do Exército, os carros de combate, concentram-se em zonas de reunião para emissão de ordens, reorganização e recompletamento de munição e combustível.

Como ocorrido na Crimeia, em que russos desencadearam fogos de artilharia sobre posições que apresentavam quantidades anormais de telefonemas e fluxo de dados celulares, um ataque similar pode ocorrer caso o pelotão de exploradores utilize celulares como meio de comunicação.

Dessa maneira, escalona-se, a um nível muito superior ao do pelotão, as perdas geradas pela falta de cuidado com o uso dos celulares, podendo gerar baixas nível subunidade ou unidade.

4.4.3 Vulnerabilidades em missões de escolta de comboios e de controle de estradas

Comboios logísticos precisam da segurança para chegarem aos seus locais de destinos. Nesse tipo de operação, por vezes, o pelotão de exploradores é o responsável por essa segurança. Já em operações de controle de estradas, o pelotão é o responsável pelo controle do fluxo de pessoas e veículos em uma via.

O Manual do pelotão de exploradores (BRASIL, 2002, p. 4-19) assegura que, nesses tipos de operação, é de vital importância que o planejamento seja bem feito e, assim, evitem-se emboscadas que neutralizem o comboio ou que desestruturem o pelotão desdobrado sobre a via.

Como apontado pela pesquisa de campo, contudo, observa-se uma falta de sincronismo entre o que é estipulado pela doutrina nacional e o que é praticado pelos cadetes, no que tange o uso de celulares e o planejamento de operações. Tal assincronia pode acarretar a exploração inimiga das vulnerabilidades dos celulares presentes no pelotão de exploradores.

O planejamento, segundo o manual de Contrainteligencia (BRASIL, 2019) deve ser feito buscando o máximo de sigilo e o mínimo de exposição de dados úteis ao inimigo. Todavia, mais da metade dos entrevistados dizem utilizar o celular para planejarem operações (52 %) e quase a totalidade (98%) dizem utilizar o celular para a consulta de manuais e cartas topográficas.

O planejamento de operações em celulares fica suscetível à exploração cibernética do sistema operacional do celular e à exploração da permissão para acesso de dados que as aplicações requerem. Ressalta aos olhos que todas as aplicações estudadas por este trabalho requeriam a permissão de acesso aos dados do celular.

O vazamento do planejamento desse tipo de operação dá ao inimigo ou oponente vantagem enorme, uma vez que, sabido o itinerário do comboio ou a posição de posto de controle, emboscadas podem ser estabelecidas com segurança e confiabilidade.

4.4.4 Mitigando deficiências no pelotão de exploradores

A ampla gama de missões do pelotão de exploradores pode projetar diferentes tipos de consequências para o pelotão ou FT na qual está inserido. Entretanto, em consonância com o manual de Pelotão de Exploradores (BRASIL, 2002,) o comandante de pelotão deve atuar para mitigar as consequências do uso de celulares.

> O Cmt é responsável pela instalação, operação e manutenção do sistema de comunicações do Pel sob seu comando e pela eficiência operacional da parte que cabe ao Pel no sistema do Esc Sp.(BRASIL 2002 p. 1-14)

Assim, atendendo ao objetivo do trabalho de propor procedimentos e hábitos para reduzir o risco do uso de dados de celulares pelo inimigo, sugere-se que o comandante de pelotão, inicialmente, crie uma mentalidade de contrainteligência em seu pelotão.

Uma medida a ser adotada é a realização de palestras, instruções e aulas durante a formação do futuro oficial na AMAN, a fim de que as deficiências apresentadas por este trabalho sejam evidenciadas aos futuros comandantes de pelotão e, assim, uma maior mentalidade de contrainteligência seja criada.

Além disso, sugere-se que o comandante de pelotão e os comandantes em todos os níveis realizem instruções apontando as vulnerabilidades do celular em campanha. Os casos históricos apresentados neste trabalho podem servir de ilustração para maior compreensão do assunto.

Dadas as instruções, um esforço deve ser realizado a fim de que os exercícios no terreno sejam realizados sem a utilização das funcionalidades do celular, a fim de acostumar as praças a trabalharem sem as facilidades do aparelho.

A prontidão da tropa deve ser constante. Assim, desde a incorporação dos soldados, estes devem ser instruídos a controlarem estritamente os aplicativos instalados, bem como as permissões autorizadas. Tal ação visa impedir a criação de possíveis dados a serem utilizados pelo inimigo.

Contatos de telefone não devem ser salvos com ordens de batalha, postos ou graduações. Assim, evita-se que o inimigo possa facilmente identificar os aparelhos dos comandantes de fração.

Todos esses procedimentos estão em sintonia com a doutrina nacional e visam reforçar as medidas já previstas em manual.

> a) É proibida a difusão de informações sensíveis por aplicativos de mensagem instantânea, mídias sociais e redes de relacionamento.
> b) Evitar o uso de mídias sociais e de aplicativos desconhecidos que possam conter funções como geolocalização e compartilhamento de informações pessoais (BRASIL, 2019, p.3-29)

5 CONSIDERAÇÕES FINAIS

A pesquisa de campo realizada com os futuros oficiais da linha bélica demonstrou que existe pouca preocupação com a segurança dos aparelhos celulares no interior da Academia Militar das Agulhas Negras. Além disso, o alto grau de utilização de celulares pelos cadetes em exercícios no terreno (72%) induz à dúvida se o futuro oficial conseguiria realizar o mesmo planejamento ou trabalhos de coordenação e controle se o uso do celular nos exercícios fosse restringido.

Face a essa realidade, propõe-se um estudo de viabilidade para instruções aos cadetes, ilustrando quais são as vulnerabilidades do uso do celular em campanha e mostrando quais são as formas de mitigar os problemas gerados pelo porte de celular. Além disso, devem ser apresentadas aos cadetes maneiras de substituir as funcionalidades do celular por meios mais seguros.

A conscientização dos futuros comandantes de pelotão é essencial para a difusão desse conhecimento pelos corpos de tropa. Por esse motivo, sugere-se que sejam ministradas instruções para o corpo de cadetes da AMAN, mostrando as falhas nas seguranças de celulares, consequências da exploração das informações pelos aparelhos fornecidas e necessidade de enxergar o celular como uma fonte de dados para o inimigo.

Permissões de localização de GPS e monitoramento de atividade física não devem ser autorizadas em aplicativos de celulares que tenham circulação livre em OM. Outra medida a ser adotada é não salvar os postos e graduações dos militares na agenda de contatos dos celulares da Força. Arquivos oficiais sensíveis ou reservados não devem ser repassados ou armazenados por intermédio de celulares.

As funcionalidades úteis de um celular podem ser substituídas por outros aparelhos. Para a orientação, podem ser utilizados aparelhos GPS, ao invés de aplicativos de celulares com geolocalização, uma vez que aqueles não estão conectados em rede e, desta maneira, são muito menos propensos a serem explorados pela guerra cibernética.

A comunicação entre os integrantes do pelotão deve ser feita em segurança, de maneira criptografada. Existem, no Exército, meios doutrinários para se estabelecer esse tipo de comunicação, utilizando-se os meios de comunicações previstos nos Quadros de Distribuição de Material (QDM), como por exemplo, os rádios FALCON. Assim, o uso desses meios deve ser incentivado e praticado pelos cadetes.

Atitudes como estas devem criar, nos futuros oficiais, responsabilidade e a mentalidade de contrainteligência, que serão difundidas nos corpos de tropa.

Esta pesquisa não exauriu o assunto e diversas outras vulnerabilidades podem surgir com o uso de celular. Como oportunidades de pesquisas futuras, sugere-se o estudo para estabelecimento de procedimentos para o uso do celular em operações de não guerra, ou até mesmo de procedimentos para evitar o desgaste da imagem da Força gerado por fotos ou filmagens de celulares de membros das FA.

O celular é uma ferramenta muito versátil e útil. Assim, bani-lo por completo das FA seria lutar contra a evolução tecnológica e, consequentemente, seria uma medida inviável, tendo em vista que a própria pesquisa de campo demonstrou que somente um por cento dos cadetes não o utiliza como ferramenta de trabalho.

Assim sendo, sugere-se que um estudo para utilização de celulares robustecidos e dotados de softwares livres, auditados e seguros deve ser feito com urgência. Esta é a única maneira, visualizada por este trabalho, para que as úteis ferramentas de um aparelho celular sejam utilizadas pelas tropas brasileiras. Cabe a pesquisa e investimentos na criação de softwares específicos para serem usados pela Força, que armazenem dados de operações em servidores seguros e que não dependam de aplicativos de terceiros bem como na criação de canais de comunicação seguros via celular.

Para o uso seguro do celular, contudo, retorna-se ao conceito de ameaça pelo manual EB70-MC-10.220. Ela define-se pela conjunção de ator, motivação e capacidade de agir. Consequentemente, se um agente inimigo não possui a capacidade de explorar as deficiências apontadas, não há ameaça.

Em operações de guerra, segue-se a doutrina do EB de contrainteligência: o que não é expressamente permitido, deve ser proibido. (BRASIL, 2018). O celular não é meio de comunicação doutrinariamente estabelecido. Seria inconsequente pensar que não há ação inimiga nos celulares na guerra moderna.

Soldados de um pelotão de exploradores que partirem para operações de guerra devem estar cientes que seus celulares podem ser alvo de ação inimiga, seja ela por meio de guerra eletrônica, cibernética ou por ação psicológica. Por isso, além de não ser utilizado como meio de comunicação, o celular não deve ser portado.

A evolução do celular não terminou. À medida que se avança com a tecnologia, aumentam-se as funcionalidades possíveis destes aparelhos. Assim, acreditar que tais equipamentos nunca venham a ser adotados oficialmente pela Força Terrestre é condená-la à obsolescência. É necessário, contudo, que essa evolução seja feita de forma segura.

REFERÊNCIAS

ACADEMIA MILITAR DAS AGULHAS NEGRAS. Cadeira de Cibernética. **Segurança da informação e das Comunicações.** Resende: Acadêmica, 2018

ACADEMIA MILITAR DAS AGULHAS NEGRAS. **Iniciação à pesquisa científica**. 2 ed. Resende, 2019

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBRISO/IEC 27002, **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.** 2 ed. Rio de Janeiro, 2013

BELL, Daniel, **The Coming of Post-Industrial Society: A Venture in Social Forecasting**. Basic Books, 1 ed., Nova Iorque, 2016

BRASIL, Ministério da Defesa, Exército brasileiro, **Caderneta de operações do Pelotão de exploradores,** Edição experimental, Brasília, 2014

BRASIL, Ministério da Defesa, Exército Brasileiro **CI 17 -1/1** Caderno de Instrução Pelotão de exploradores, 1 ed, Brasília, 2002

BRASIL. Ministério da Defesa. Exército Brasileiro.**CI 34-1/1,** Caderno de instrução medidas de proteção eletrônica (MPE), 1 ed., Brasília. 2006

BRASIL. Ministério da Defesa. Exército Brasileiro. **EB70-MC-10.201:** Manual de Campanha a guerra eletrônica na Força Terrestre. 1 ed. Brasília. 2019

BRASIL. Ministério da Defesa. Exército Brasileiro. **EB70-MC-10.220:** Manual de Campanha Contrainteligência. 1 ed. Brasília: 2019

BRASIL. Ministério da Defesa. Exército Brasileiro. **EB70-MC-10.232:** Manual de Campanha Guerra cibernética. 1 ed. Brasília. 2017

BRASIL; Ministério da Defesa, Exército Brasileiro. **C 21-30 –** Manual de campanha abreviaturas, símbolos e convenções cartográficas, 4 ed, Brasília, 2002

BRASIL. Ministério da Defesa. Exército Brasileiro. **C 34-1** Manual de campanha Emprego da guerra eletrônica. 1ed., Brasília, 1999

BROWN, Daniel, **Russian-backed separatists are using terrifying text messages to shock adversaries — and it's changing the face of warfare,** Busnisses Insider, 2018, Disponível em: <https://www.businessinsider.com/russians-use-creepy-text-messages-scare-ukrainians-changing-warfare-2018-8>, Acesso em 27 de maio de 2020

CARDOSO, Faça amor ou faça guerra – Como o Tinder derrotou uma tropa inimiga, **Contraditorium,** 2020, Disponível em :< https://contraditorium.com/2020/01/07/facar-amor-ou-faca-guerra-como-o-tinder-derrotou-uma-tropa-inimiga/>, acesso em 27 de maio de 2020

DURBANO, Vinícius, **Segurança da informação: o que é e 12 dicas práticas para garantir.** Ecoit, segurança digital. Disponível em: <https://ecoit.com.br/seguranca-da-informacao/>. Acesso em 28 Abr. 2020

FITNESS APP STRAVA LIGHTS UP STAFF AT MILITARY BASES, **bbc.com,** 2018, Disponível em: <https://www.bbc.com/news/technology-42853072>, acesso em 27 de Maio de 2020

GEERS, Kenneth**, Cyber war in perspective:russian aggression against Ukraine,** NATO CCD COE Publications, Tallinn 2015.

GILES, Kier, **The next phase of Russian information warfare,** NATO strategic communications centre of excellence, Letônia, 2018

GOMES FILHO, Paulo, **O pensamento crítico e criativo no combate do século 21,** Blog do Paulo Filho, 2020, Disponível em: <http://paulofilho.net.br/blog-do-paulo-filho/o-pensamento-cr%C3%ADtico-e-criativo-no-combate-do-s%C3%A9culo-21>, Acesso e, 30 de Maio de 2020

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO/IEC 27000, **, Information technology – Security techniques – Information security management systems – Overview and vocabulary,** 2018, Disponível em <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>, Acesso em 28 Abr. 2020

JOAN, Bem **Difference between Cellphone and Smartphone.** Differencebetween, Disponível em <http://www.differencebetween.net/object/difference-between-cellphone-and-smartphone/>. Acesso em 24 abr. 2020

KOETSIER, Jhon. **There Are Now 8.9 Million Mobile Apps, And China Is 40% Of Mobile App Spending,** Forbes, 2020, Disponível em : <https://www.forbes.com/sites/johnkoetsier/2020/02/28/there-are-now-89-million-mobile-apps-and-china-is-40-of-mobile-app-spending/#2aa72ff121dd>, Acesso em 27 set 2020

MEIRELLES, Fernando. **Pesquisa Anual do Uso de TI nas Empresas, FGVcia**: Centro e Tecnologia de Informação Aplicada da EAESP, 30ª edição, 2019. Disponível em <://eaesp.fgv.br/sites/eaesp.fgv.br/files/pesti2019fgvciappt_2019.pdf>. Acesso em 27 Abr. 2020

REMEDIO, J.A., SILVA, B. H. S, Privacidade versus **segurança** pública: o acesso ao conteúdo de Celular pela autoridade policial**, Quaestio Iuris,** Rio de Janeiro, vol. 11, nº. 04.

SAIBA quais foram os aplicativos mais baixados no Brasil e no mundo, **exame,** 2020. Disponível em :< https://exame.com/tecnologia/saiba-quais-foram-os-aplicativos-mais-baixados-no-brasil-e-no-mundo/>, Acesso em 4 de abril de 2020

SINGER, P. W. e FRIEDMAN, A **Segurança e guerra cibernéticas: o que todos precisam saber,** 1 ed, Rio de Janeiro, 2017

SOUZA, Lisandro Carmona de. **Os novos vilões da sua privacidade: as permissões dos seus aplicativos – Parte 1: smartphones.** Avast Blog. Disponível em <https://blog.avast.com/pt-

br/os-novos-viloes-da-sua-privacidade-as-permissoes-dos-seus-aplicativos-parte-1-smartphones>. Acesso em 28 abr. 2020.

TEIXEIRA FILHO, Sócrates Arantes. **Segurança da informação descomplicada** 1 ed. Brasília, 2015

TILGHMAN, Andrew. **The Pentagon has banned Pokemon Go from official military phones,** Military Times, 2016, Disponível em: <https://www.militarytimes.com/news/your-military/2016/08/12/the-pentagon-has-banned-pokemon-go-from-official-military-phones>, acesso em 21 de novembro de 2020

VLASOV, D. e SATTER, R. **Ukraine soldiers bombarded by 'pinpoint propaganda' texts,** Associated Press, 2017, Disponível em: <https://apnews.com/article/9a564a5f64e847d1a50938035ea64b8f>, acesso em 18 out de 2020

VOLZ, Dustin, **Russian hackers tracked Ukrainian artillery units using Android implant: report,** Reuters, 2016, Disponível em: <https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU>, acesso em 18 de out de 2020

APÊNDICE

APÊNDICE A – QUESTIONÁRIO

Questionário sobre a utilização dos celulares pelos futuros oficiais do Exército

Este questionário foi elaborado pelo Cadete João Pedro, do terceiro ano do curso de Cavalaria no ano de 2020. Os dados coletados serão utilizados para avaliar a relação dos militares com seus celulares, a fim de estabelecer o quão importantes esses aparelhos são na rotina militar.

Solicita-se que o respondente seja sincero em suas respostas, haja vista que todos os dados serão utilizados de maneira estatística. O anonimato dos respondestes será preservado.

Nome de Guerra:

Número:

Ano:

Arma, quadro ou serviço:

O Sr(a) possui smartfone?

Acredita que o smartfone é essencial em sua rotina?

Quais desses aplicativos você possui? (WhatsApp, Instagram, tinder, Facebook, CamScanner, Google Maps, Waze, Strava, Garmin Connect ou similar, aplicações de bancos, aplicações de e-mail, Pokémon go)

Utiliza seu smartfone como ferramenta de trabalho? Se sim, como? (Grupos de WhatsApp relacionados a trabalho, consulta a manuais e cartas topográficas consulta de documentação de aula, planejamento de operações, fotografia e filmagem)

Costuma analisar as permissões que cada aplicativo requer após seu download?

De sua experiência, o Sr(a) acredita que os militares do EB conduzem aparelhos celulares para as operações?