MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

GAB CMT EX – CIE

ESCOLA DE INTELIGÊNCIA MILITAR DO EXÉRCITO

CURSO DE INTELIGÊNCIA CIBERNÉTICA PARA OFICIAIS

TRABALHO DE CONCLUSÃO DE CURSO (TCC)

Operações interagências: como melhor empregar a inteligência cibernética na obtenção de dados

Brasília

2023

Cap DIRCEU FELIPE CHAVES **STOCKEY** FLORENCE

Operações interagências: como melhor empregar a inteligência cibernética na obtenção de dados

Trabalho de Conclusão de Curso apresentado à Escola de Inteligência Militar do Exército, como requisito para a obtenção do Grau de Pós-graduação *Lato Sensu* de **Especialização em Inteligência Cibernética.**

Orientador: Maj **Dionízio** Santos Rodrigues dos Anjos

Brasília

2023

CATALOGAÇÃO NA FONTE
Biblioteca Cel Forrer Garcia

F633o Florence, Dirceu Felipe Chaves Stockey

Operações interagências: como melhor empregar a inteligência cibernética na obtenção de dados/ Dirceu Felipe Chaves Stockey Florence – 2023.
25 f.

Orientador: Dionísio Santos Rodrigues dos Anjos
Trabalho de Conclusão de Curso (Especialização em Inteligência Cibernética) - Escola de Inteligência Militar do Exército (EsIMEx), Brasília – DF, 2023.

1. Exército Brasileiro 2. Inteligência Cibernética 3. Obtenção de dados
4. Operações Interagências I. Título.

Cap DIRCEU FELIPE CHAVES **STOCKEY** FLORENCE

Operações interagências: como melhor empregar a inteligência cibernética na obtenção de dados

Trabalho de Conclusão de Curso apresentado à Escola de Inteligência Militar do Exército, como requisito para a obtenção do Grau de Pós-graduação *Lato Sensu* de **Especialização em Inteligência Cibernética.**

Aprovado em ___de___de 2023.

COMISSÃO DE AVALIAÇÃO:

_____

DIONÍZIO SANTOS RODRIGUES DOS ANJOS – Maj **-** Presidente
Escola de Inteligência Militar do Exército

_____

RICARDO CÉLIO CHAGAS **BEZERRA FILHO -** Maj - Membro
Escola de Inteligência Militar do Exército

RESUMO

No complexo cenário de operações atual, o Exército Brasileiro não pode mais operar sem o apoio de outras instituições, pois não cabe mais apenas o uso da força para atingir um objetivo militar, mas sim um trabalho coordenado com outras agências, militares ou não, para que os resultados sejam alcançados em maior amplitude. Diante das novas ameaças, o Sistema de Inteligência do Exército (SIEx) passou por uma reorganização, permitindo o trabalho interagências e a maior capacidade de operar no Ambiente Cibernético, desta forma, o objetivo deste trabalho foi avaliar a importância da disciplina de Inteligência Cibernética nas operações militares e estabelecer linhas de ação para melhor organizar uma célula de CYBINT. Durante esta pesquisa foi realizada uma revisão bibliográfica para compreender as capacidades, limitações e suas diferenças para a Inteligência de Fontes Abertas, compreender os aspectos relevantes do trabalho do operador de Inteligência Cibernética e avaliar a dinâmica das relações entre as agências de inteligência nesse tipo de operação. Dessa forma, foi possível compreender que a inteligência cibernética desempenha um papel significativo no ambiente interagências, podendo mesmo esgotar as ações de Inteligência de Fontes Humanas, devido ao seu potencial e ao custo envolvido. Por fim observou-se uma grande dificuldade no fluxo de informações entre as agências, e dessa forma, foram elencadas formas de aproximar os diferentes órgãos para aprimorar o compartilhamento de dados.

Palavras-chave: Exército Brasileiro. Inteligência cibernética. Obtenção de dados. Operações interagências.

ABSTRACT

In the complex scenario of current operations, the Brazilian Army can no longer operate without the support of other institutions, as it is no longer just the use of force to achieve a military objective, but coordinated work with other agencies, military or not, to that results are achieved in greater amplitude. Faced with new threats, the Army Intelligence System (SIEx) underwent a reorganization, allowing interagency work and greater capacity to operate in the Cybernetic Environment. military operations and establishing lines of action to better organize a CYBINT cell. During this research, a bibliographical review was carried out to understand the resources, limitations and their differences for Open Source Intelligence, to understand the relevant aspects of the work of the Cybernetic Intelligence operator and to evaluate the dynamics of the relationships between the intelligence agencies in this type of operation. In this way, it was possible to understand that cybernetic intelligence plays a significant role in the interagency environment, and may even exhaust Intelligence actions from Human Sources, due to its potential and the cost involved. Finally, there was great difficulty in the flow of information between the agencies, and therefore, ways of bringing the different agencies closer together to improve data sharing were listed.

Keywords: Brazilian Army. Cyber intelligence. Data collection. Interagency operations.

SUMÁRIO

1 INTRODUÇÃO

Segundo Bennett e Leimore (2014), as instituições possuem novos desafios devido às características do mundo atual: volátil, incerto, complexo e ambíguo (do inglês, VUCA), isso exige que os Órgãos públicos e privados tenham respostas imediatas diante de crises. Tozzi (2021), por sua vez, afirma que o conceito “VUCA” já não é mais compatível e nos apresenta um novo termo: “BANI”, acrônimo de inglês para frágil, ansioso, não-linear e incompreensível.

Inteligência é o produto da obtenção, busca e análise de informações para a tomada de decisões (SEEDYK, 2019) e, frente ao cenário apresentado, Coutinho (2020) aborda que o trabalho da Inteligência de Estado é vital para a salvaguarda deste e da sociedade e que os avanços tecnológicos trouxeram novas ameaças.

Segundo Filho (2013), esse tipo de ambiente inédito exige o enfrentamento de crises com o apoio de atores governamentais, militares, Organizações Não Governamentais (ONGs), empresas, dentre outros dos mais diversos interesses, definindo-se assim o Ambiente Interagências.

Diante do exposto, questiona-se: o emprego da Inteligência Cibernética é relevante em Operações Interagências para a obtenção de dados? Caso afirmativo, qual forma de maximizar sua eficiência?

Com base na problemática apresentada, este trabalho tem por objetivo investigar a relevância da Inteligência Cibernética em Operações Interagências para a obtenção de dados e identificar as possíveis formas de maximizar sua eficiência.

Para atingir nosso objetivo principal, buscamos inicialmente compreender o ciclo da inteligência para identificar as diferenças e semelhanças entre Inteligência das Fontes Abertas e a Inteligência Cibernética quanto suas características, metodologias de obtenção de dados e função dentro do ciclo de inteligência.

Em seguida, analisaremos as características das operações interagências para compreenderemos como deve ser a relação entre as agências de inteligência envolvidas em uma operação

Por fim, buscamos avaliar a importância da Inteligência Cibernética no contexto das Operações Interagências. Investigamos como essa disciplina contribui para a tomada de decisões estratégicas e táticas no âmbito da cooperação entre diferentes agências de inteligência. Analisamos os benefícios e desafios associados à integração da Inteligência Cibernética nas operações conjuntas, considerando as

demandas do cenário contemporâneo de ameaças e os objetivos das Operações Interagências.

Ao abordar esses aspectos, ampliamos o conhecimento sobre a Inteligência Cibernética e sua aplicação nas Operações Interagências. Nosso objetivo é fornecer insights relevantes que possam contribuir para aprimorar a organização e o aproveitamento dos recursos de Inteligência Cibernética, permitindo uma atuação mais eficaz no enfrentamento dos desafios presentes no ambiente operacional atual.

A técnica de coleta de dados predominante foi a pesquisa bibliográfica em fontes confiáveis, através de bases de dados e revistas científicas. Além disso, foi considerada postagens em blogs de estudiosos ou empresas especializadas em inteligência, defesa ou cibersegurança como fontes complementares de informações, desde que relevantes ao estudo.

A análise dos dados coletados foi realizada por meio de uma pesquisa exploratória em uma abordagem predominantemente qualitativa do conteúdo, que permitiu uma exploração do tema com profundidade, a fim de atingir os objetivos propostos, identificando padrões, categorias e temas relevantes.

Dessa forma, espera-se contribuir para o avanço do conhecimento sobre a aplicação da Inteligência Cibernética em Operações Interagências e para o desenvolvimento de estratégias mais eficientes de coleta de dados nesse contexto.

Diante disso, a pesquisa apresenta como se dá o processo de obtenção de dados de inteligência, inicialmente diferenciando o trabalho realizado pela Inteligência Cibernética com o realizado pela Inteligência das Fontes Abertas, logo em seguida será aprofundado a atuação do operador da fonte cibernética, com suas características, capacidades e limitações, após será abordado como os órgãos de inteligência se relacionam para o trabalho em conjunto, para que na conclusão seja apresentada a resposta do nosso problema e sugestões de aperfeiçoamento para a Doutrina da Inteligência Militar.

2 O PROCESSO DE OBTENÇÃO DE DADOS NA INTELIGÊNCIA MILITAR

O Processo de Integração Terreno, Inimigo, Condições Meteorológicas e Considerações Civis (PITCIC) chamado pela doutrina americana como *Intelligence preparation of the battlefield* é o processo sistemático de análise das variáveis de missão do inimigo, terreno, clima e considerações civis em uma área de interesse para determinar seu efeito nas operações (THE LIGHTINING PRESS, em inglês).

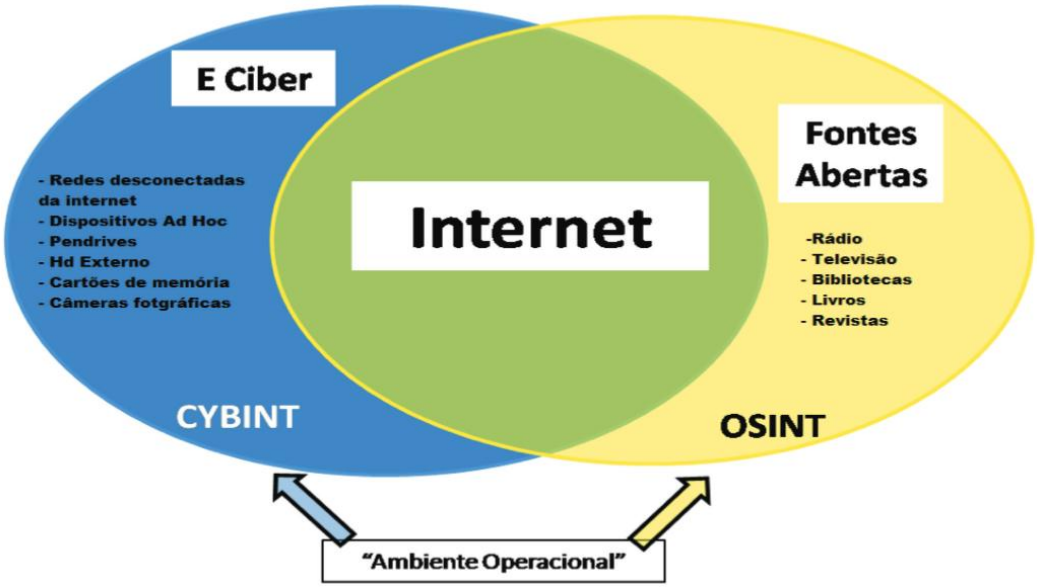
Consideraremos para capítulo e os próximos, algumas definições. Quanto ao Ciclo de Inteligência, Brasil (2015) define o Ciclo de Inteligência como a sequência de orientação, obtenção, produção e difusão. Diferente da doutrina do Exército Brasileiro, Iowa Department of Public Safety estabelece que o ciclo possui cinco fases, sendo neste, estabelecido que a obtenção é focada somente na coleta, enquanto o processamento dos dados coletados é realizado em uma fase adicional.

Embora Sood e Enbody (2014) classifiquem a OSINT como um subtipo da CYBINT, por atuar, predominantemente, no mesmo Ambiente Operacional, também afirma que esses dados devem ser levantados antes de outras disciplinas por se tratarem de levantamentos mais econômicos e sem a exposição dos Agentes de outras disciplinas ao Ambiente Operacional, por não haver a iteração direta com este, porém essa forma de coleta pode não ser muito confiável em certos momentos, exigindo a confirmação através de algumas das técnicas especializadas por outras fontes.

Para Leal (2019), OSINT se vale em coletar dados disponíveis sem restrição de acesso, ou em pesquisa na internet através de uma simples pesquisa no navegador ou por aplicativos e serviços de busca automatizados. Leal (2019) cita, ainda, que algumas técnicas mais avançadas exigem o emprego de um agente mais experiente em Tecnologia da Informação (TI), o que o aproxima do operador de CYBINT, podendo ser delegada a este o emprego de tais ferramentas, por muitas vezes não existir um militar especializado na atividade de OSINT nas Agências de Inteligência (AI) e Órgãos de Inteligência (OI).

Embora o Ambiente Operacional do Operador de CYBINT e de OSINT sejam predominantemente o mesmo, a Rede Mundial de Computadores, em outras fontes Leal (2019) estabelece que algumas fontes de dados são exclusivas da Inteligência Cibernética, enquanto, outras, exclusivas do Operador de Fontes Abertas.

Figura 1 - Diagrama do Ambiente Operacional da CYBINT e da OSINT.



Fonte: Leal (2019).

A Figura 1 ilustra as diferenças no Ambiente Operacional entre a Inteligência de Fontes Abertas da Inteligência Cibernética. Quanto à obtenção de dados por exploração cibernética, abordaremos de forma mais aprofundada no próximo capítulo.

Observamos que pelas características da OSINT, esta disciplina deve ser utilizada antes das demais envolvendo todos elementos disponíveis. É interessante, ainda que, conforme os dados forem obtidos, os elementos especializados nas outras disciplinas iniciem as buscas em outras fontes gradativamente enquanto o operador de CYBINT esgote essa fonte usando técnicas mais avançadas, até que a Inteligência das Fontes Abertas se esgote.

3 TÉCNICAS DE OBTENÇÃO DE DADOS DE FONTES CIBERNÉTICAS

Segundo Wendt (2011), vivemos em um mundo altamente conectado, isso tudo graças ao advento da internet, mas que junto às vantagens, existem muitos problemas como vazamento de dados, espionagem cibernética e interrupção de serviços essenciais caso ocorram ataques em infraestruturas críticas.

Para Bateman, Beecroft e Wilde (2022), os Russos lançaram diversos ataques cibernéticos na guerra contra a Ucrânia destruindo estruturas críticas, enquanto camuflavam sua principal ação: a coleta de informações para uso da Inteligência Militar.

Um ataque cibernético é qualquer esforço intencional para roubar, expor, alterar, desabilitar ou destruir dados, aplicativos ou outros ativos por meio de acesso não autorizado a uma rede, sistema de computador ou dispositivo digital (IBM, 2021). Segundo a empresa Fortinet (2023), os ataques cibernéticos mais comuns são: DoS/DDoS, *Ransomware*, *Man-inThe-Middle* (MITM), *Phishing*, *Password* e SQL *Injection*. Dessas práticas, Bizu, Gopal e Prakash (2019) afirmam que, excluindo as duas primeiras, as demais são técnicas que permitem a realização da Espionagem Cibernética. Segundo MI5 (2016), essa modalidade de espionagem permite o roubo de informações remotamente, de forma econômica, com baixo risco ao agente e em larga escala.

Como parte das atribuições da fração de Inteligência Cibernética, Brasil (2018) estabelece que o Pelotão de Inteligência Cibernética deve monitorar o tráfego de dados de redes, analisar e explorar sistemas de informação disponíveis, recrutar colaboradores no espaço cibernético a fim de obter dados negados, dentre outros.

Para estudar os ataques cibernéticos, dividiremos eles em dois grupos, sendo eles de Engenharia Social e o de exploração de vulnerabilidades.

Em ataques de Engenharia Social uma pessoa de má-fé abusa da ingenuidade ou da confiança de um usuário para persuadi-lo a fornecer informações sensíveis (CLEARSALE, 2023).

Para Fonseca (2017), ataques dessa natureza tendem a ser os mais eficazes nos próximos anos pois, com a modernização das aplicações, a segurança tende ser mais eficientes mas a mente humana não teve mudanças.

Trade Tecnology (2022), afirma que os ataques de *Phishing* e seus derivados são os que apresentam melhores resultados, uma vez que são disseminados em

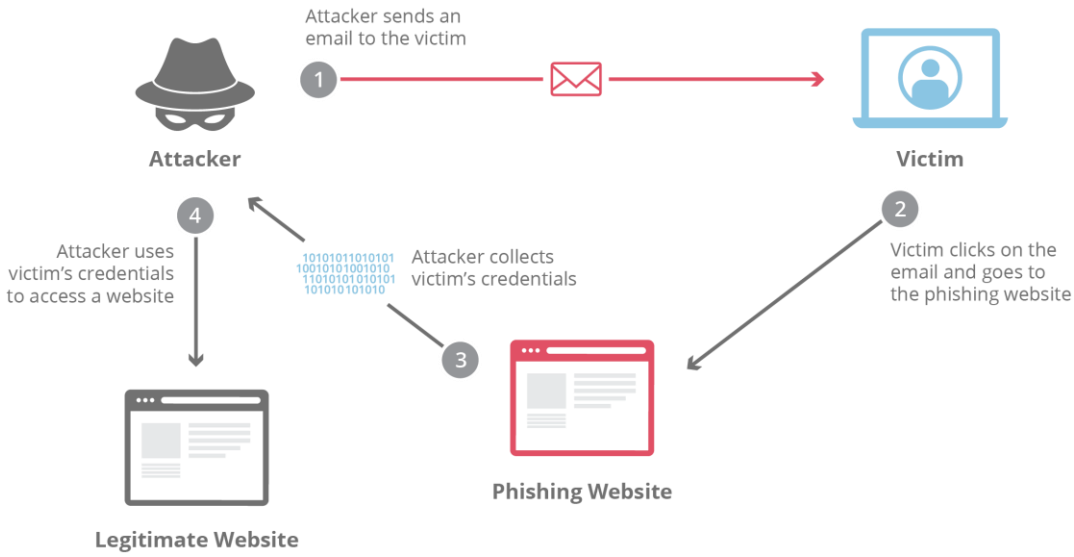
uma grande base de usuários, normalmente dados obtidos publicamente na internet (OSINT).

O Invasor envia uma mensagem tentando persuadir um alvo, caso tenha sucesso, o alvo pode ter informações sensíveis roubadas, permitindo ao atacante obter informações como credenciais, arquivos dentre outros. Observando a Figura 2 podemos tem um esclarecimento de como pode funcionar esse ataque.

Segundo Trade Tecnology (2022), de posse desses dados, o invasor pode agora acessar sistemas autenticados ou usar esses dados para outra atividade de seu interesse.

Fastest VPN (2022) apresenta ataques virtuais derivados do Phishing dos quais, cito alguns: o Vishing, através de ligações telefônicas; o Smishing, que faz o uso de mensagens de SMS; o Baiting, fornece ao usuário uma recompensa clicando em um anúncio e preenchendo algumas informações; e o Spear Phishing, que é usado quando o Hacker já possui uma gama de informações do usuário e precisa de uma específica.

Figura 2 - Ataques de *Phishing*



Fonte: Cloudflare (2023).

Para Itforum (2016), um ataque cibernético dessa categoria pode ocorrer em seis fases, são elas:

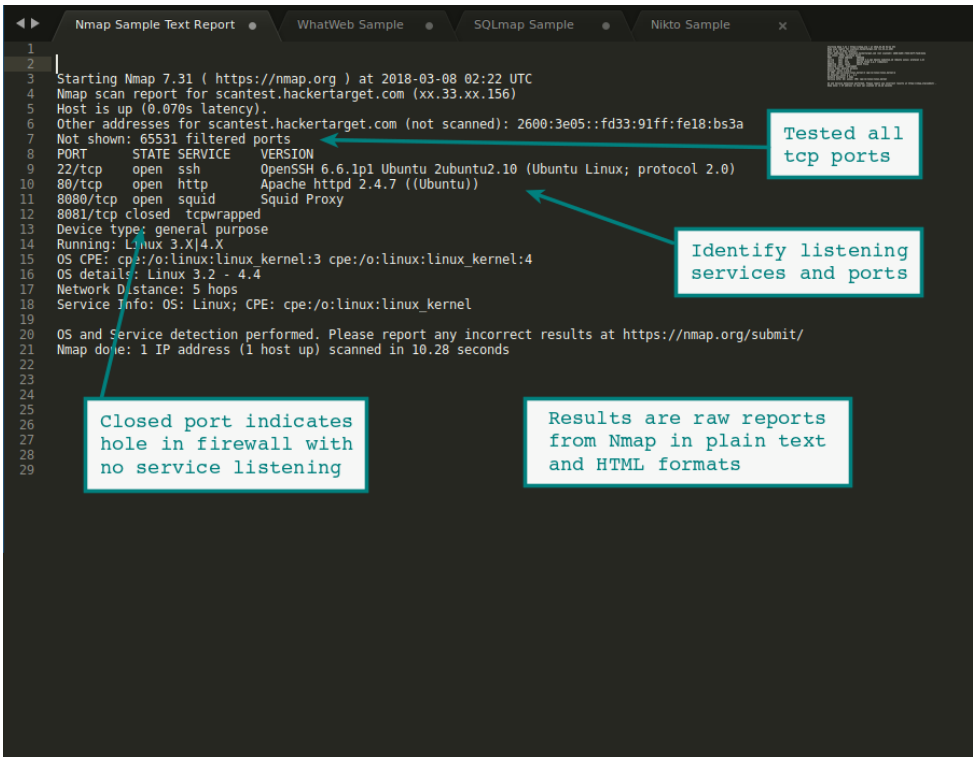
A coleta de informações é a fase que o invasor precisa saber quem invadir. Dessa forma, a etapa consiste na obtenção de dados sobre o alvo, como endereços de IP, recursos humanos e outras julgadas relevantes, podendo nessa etapa recorrer a Fonte de Dados Abertas;

Na Exploração, o Hacker precisa saber o que invadir. Assim, realiza uma varredura (*scan*) para identificar quais versões de *softwares e hardwares* o alvo possui, com a finalidade de procurar por vulnerabilidades que possibilitem a continuidade do ataque. Observe que na Figura 3, com o uso da ferramenta *Network Mapper* (Nmap) foi possível levantar quais as portas, serviços e versões estão abertos, permitindo direcionar o ataque a esses sistemas;

Na Enumeração, é preciso saber como invadir. Então a missão do hacker é buscar maneiras de acessar o ativo, de posse da versão pode ser encontrado programas na internet que automatizem o ataque (exploits);

A Invasão consiste em realizar o ataque propriamente dito, nessa hora, o hacker deve conseguir algum acesso dentro da máquina ou rede do alvo;

Figura 3 – Scan usando a ferramenta NMAP



Fonte: https://hackertarget.com/wp-content/uploads/2018/06/nmap-text-result-sample.png

Para obter o acesso total, na fase da escalada o *hacker* explora falhas, normalmente na configuração, da aplicação para obter um privilégio superior; e na fase da pilhagem, o invasor coleta os dados para os fins desejados.

Segundo Brito (2023), para se tornar um *hacker*, uma pessoa precisa dominar Programação, Criptografia, Redes de Computadores, Sistemas Operacionais, Segurança da Informação, dentre outros. Dias (2022) por sua vez, relata que o Brasil tem um déficit de profissionais de Tecnologia da Informação (TI) em geral, criando uma disputa por esses profissionais nos diversos setores público e privado no Brasil, tornando difícil reter um profissional qualificado dessa área.

Como forma de contornar esse obstáculo e como verificamos, uma das atribuições da fração de Inteligência Cibernética é também a de recrutar colaboradores no Espaço Cibernético.

Essa técnica foi utilizada pela Alemanha, que segundo Sanders (2017), os hackers recrutados tinham como atribuição obter dados de setores-chave e, mais recentemente, segundo Desaunay (2023), a Ucrânia através de seu Ministério da Tecnologia Digital recrutou ao menos duzentos mil *Hackers* movidos por ideologia (*Hacktivistas*) a impor o fim da invasão russa em seu território.

Logo, para avaliarmos a efetividade das ações no espaço cibernético, vamos analisar do possível dano causado por um e-mail falso, utilizando informações pessoais coletadas previamente e enviado a um alvo, ou mais de um, qual a chance de sucesso? E se essa pessoa possui credencial para acessar bases de dados de interesse às operações? Caso essa ação tenha sucesso, pode significar até mesmo no esgotamento das outras fontes de inteligência, passando o foco do trabalho agora em produzir o conhecimento, o que torna a exploração no espaço cibernético extremamente vantajosa.

Observamos até o presente momento sobre as características da Inteligência Cibernética e de seus Operadores. Vejamos agora como se dá o emprego dessa disciplina no Ambiente Interagências à obtenção de dados neste ambiente

4 A OBTENÇÃO DE DADOS EM OPERAÇÕES INTERAGÊNCIAS

O termo interagências deriva, então, da parceria e sinergia de esforços envolvendo órgãos governamentais e não governamentais, podendo ser nacionais e/ou internacionais, estruturados para alcançar objetivos (BRASIL, 2020). A ambigüidade, a velocidade e a interdependência das ameaças transnacionais e não estatais atuais parecem exigir mais do que qualquer conjunto de serviços de inteligência é capaz de fornecer por conta própria (INTELLIGENCE COLLEGE EUROPE, 2022).

Para avaliarmos a relevância nas Operações Conjuntas, precisamos buscar sua origem e evolução em outros países, como os Estados Unidos da América:

> As operações navais do Capitão Thomas MacDonough no Lago Champlain foram um fator vital nas campanhas terrestres da Guerra de 1812. O trabalho em equipe exibido pelo General U. S. Grant e pelo Almirante David D. Porter na Campanha de Vicksburg de 1863 é um bom exemplo de planejamento militar conjunto e execução (JOINT CHIEFS OF STAFF, em inglês).

No território brasileiro, uma ação importante envolvendo outros entes estatais foi a Operação Rio, em 1994 onde houve trocas de experiências e informações entre os militares e os órgãos de segurança do Estado para enfrentar o crime organizado na Capital Fluminense (PEREIRA, 2016).

Segundo Cosendey, essa Operação foi importante para que a força terrestre iniciasse o desenvolvimento de uma doutrina voltada para as Operações de Garantia da Lei e da Ordem e Operações Subsidiárias, sendo a partir desse momento empregada em outras diversas atividades, como a Operação Ágata, a Operação Acolhida e a Pacificação no Rio de Janeiro.

O Exército Brasileiro vem buscando ainda mais a capacidade de atuar dessa forma, a exemplo disso, cito as Diretrizes do Comandante do Exército 2023-2026 que estabelece: buscar, também, aperfeiçoar a interoperabilidade na atuação conjunta e interagências (BRASIL, 2023).

Os ataques de 11 de setembro em Nova York e Washington foram um ponto de virada decisivo na compreensão do fenômeno do terrorismo contemporâneo e foi observada uma grande dificuldade das operações interagências no compartilhamento de informações com outros órgãos. Gardner (2021), afirma que ataques às Torres Gêmeas, no dia 11 de setembro de 2001, nos Estados Unidos da

América poderiam ser evitados se a *Central Intelligence Agency* (CIA) e *Federal of Bureal of Investigation* (FBI) trabalhassem em conjunto.

Essa conjuntura ainda apresenta uma elevada complexidade nos conflitos, denominados assimétricos, estes definidos por Oliveira (2022) conflitos transnacionais com envolvimento de forças irregulares como grupos criminosos, terroristas e narcotraficantes.

Segundo Neto (2017), a principal dificuldade desse tipo de operação é que os integrantes dos órgãos e agências têm medo de compartilhar informações por falta de confiança mútua, e afirma que isso pode ser reduzido com o trabalho conjunto ao longo do tempo.

Outro aspecto a considerar é que Brasil (2015) determina que os dados obtidos serão compartilhados a quem necessita saber somente durante a fase da difusão. Isso torna muito lento o compartilhamento de dados a outras agências, assim levanto três possíveis formas de contornar esse problema.

A primeira é a instalação de uma espécie de “Agência Conjunta”, onde as células de obtenção de dados estejam fisicamente próximas ou em contato constante por áudio ou vídeo, ampliando assim a integração entre os órgãos, como consequência, a eficiência dos trabalhos. Como aspectos negativos destaco que cada órgão possui sua doutrina específica, e isso exigiria um tempo necessário de adaptação de trabalho conjunto.

A segunda linha levantada é a inserção de um elemento de ligação de cada agência, esse elemento tem como função impedir que haja duplicidade no trabalho das agências, como ponto negativo, foi levantado uma alta necessidade de profissionais para cumprir esse requisito por ser um elemento adicional de cada órgão para cada célula de Inteligência.

A terceira linha levantada é na alimentação de um banco de dados conjunto entre as agências, dessa forma, todos os interessados teriam acesso aos dados presentes. Para que esse método seja eficaz, é necessário que esses dados sejam disponibilizados, tão breve quanto obtidos, permitindo maior velocidade no fluxo de informações entre agências, porém exige uma flexibilização no ciclo de inteligência.

O quadro 1 apresenta um comparativo das linhas de ação levantadas considerando os fatores: Compartimentação, Velocidade, redundância, adaptação doutrinária e adaptação de trabalho conjunto.

Quadro 1 – Comparativo das Linhas de Ação

Fator	L. Aç. 1	L. Aç. 2	L. Aç. 3
Permite compartimentação de informações	1	2	5
Permite velocidade no fluxo de informação	5	3	4
Diminui a redundância na obtenção	5	3	2
Não exige adaptação doutrinária	1	3	2
Não exige adestramento conjunto	1	3	3

Fonte: O autor.

Diante do exposto, pudemos observar a relevância do trabalho conjunto das agências na obtenção de dados de inteligência, apesar das dificuldades, os órgãos envolvidos devem envidar esforços para aproximar seus integrantes. Outro aspecto a considerar é na velocidade do fluxo de informações, sendo interessante que o compartilhamento ocorra ainda na fase da obtenção.

5 CONCLUSÃO

Essa pesquisa primeiramente buscou separar as atribuições do Operador de OSINT do Operador de CYBINT, embora alguns estudiosos citados os considerem sinônimos ou atribuem a obtenção de dados por Fontes Abertas ao operador de Inteligência Cibernética por entender que ambos os dados são extraídos do mesmo ambiente, observamos que essa concepção não é interessante, pelos motivos elencados abaixo.

Os Operadores de Fontes Cibernéticas são, elementos escassos ou inexistentes, por serem disputados nos setores público e privado das instituições e, muitas vezes, os únicos com capacidade técnica a atuar nesse ambiente.

Na obtenção da maioria dos dados por Fontes Abertas, não é exigido elevado conhecimento em Tecnologia da Informação, dessa forma, deve-se buscar utilizar o Profissional de Inteligência especializado nessa área, ou em sua ausência, em qualquer outro operador que esteja ocioso em suas atividades.

Outra característica destacada é que a CYBINT, caso tenha sucesso e comprometa um alvo altamente compensador, é capaz de obter todos os dados necessários para a produção do conhecimento ao decisor. Mesmo que não possa comprometer o alvo principal, é possível, com a mistura de técnicas de Engenharia Social com Exploração de Vulnerabilidades, comprometer alvos secundários, para assim, escalar privilégios e obter informações necessárias para o cumprimento da missão.

No que tange às Operações Conjuntas, pudemos observar que a atuação conjunta dos diversos Órgãos trazem efeitos positivos às operações como um todo, na atividade de inteligência, isso não é diferente. Esforços conjuntos evitam redundância de trabalho e fornece ao decisor maior detalhamento de informações quanto às oportunidades e ameaças.

Cabe salientar que o Comando deverá decidir previamente qual a linha de ação mais adequada e essa decisão dependerá de qual o nível de integração com outras agências, da necessidade de compartimentação e da necessidade de velocidade no compartilhamento de informações.

Dessa forma, pudemos avaliar que a obtenção de dados de Inteligência da Fonte Cibernética é imprescindível e que é fundamental a presença destes operadores na atividade de OSINT. Em operações interagências, devido a baixa

capacidade na obtenção de dados dessa disciplina e sua complexidade, se faz ainda mais necessário os esforços conjuntos.

REFERÊNCIAS

BATEMAN, Jon; BEECROFT, Nick; WILDE, Gavin. **What the Russian Invasion Reveals About the Future of Cyber Warfare. Carnegie Endowment**. 2022. Disponível em: https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667. Acesso em: 1 abr. 2023

BENNETT, N., & LEIMONE, G. J. What VUCA really means for you. **Harvard Business Review**, jan./feb., 2014. Disponível em: https://hbr.org/2014/01/what-vuca-really-means-for-you. Acesso em: 7 abr. 2023.

BRASIL. Ministério da Defesa. Exército Brasileiro. **Diretriz do Comandante do Exército 2023-2026**. Brasília, 2023.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **Batalhão de Inteligência Militar**. Manual EB70-MC-10.302. Brasília, DF, 2018.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **Inteligência**. Manual EB20-MC-10.207. Brasília, DF, 2015.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **Inteligência Militar Terrestre**. Manual EB20-MF-10.107. Brasília, DF, 2015.

BRITO, Sunamita. **Como ser um Hacker?** 2023. Disponível em: https://www.bitmag.com.br/como-ser-um-hacker-o-que-precisa-estudar-para-se-tornar-um-hacker-nos-explicamos-tudo/. Acesso em: 9 abr. 2023.

ENGENHARIA Social: o que é, tipos de ataque, técnicas e como se proteger. 2022. Disponível em: https://blogbr.clear.sale/engenharia-social-o-que-e-e-como-se-proteger. Acesso em: 07 abr. 2023.

CLOUDFLARE. **O que é um ataque de phishing?** Disponível em: https://www.cloudflare.com/pt-br/learning/access-management/phishing-attack/. Acesso em: 8 abr. 2023.

COSENDEY, Felipe R. As operações de cooperação e coordenação com as agências. **Military Review**, maio, 2021.

COUTINHO, Lilian. LGPD e inteligência: os limites no tratamento de dados pessoais coletados em fontes abertas. **Revista Nacional de Inteligência**, n. 15, dez. 2020.

DESAUNAY, Dominique. **Governo Ucraniano quer integrar hackers voluntários em seu exército**. RFI, 5 abr. 23. Disponível em: https://www.rfi.fr/br/europa/20230405-governo-ucraniano-quer-integrar-hackers-volunt%C3%A1rios-em-seu-ex%C3%A9rcito. Acesso em 22 abr. 23.

DERENCINOVIC, Davor; GETOS, Anna M. **Cooperation of law enforcement and intelligence agencies in prevention and suppression of terrorism. Revue internationale de droit pénal**. Disponível em: https://www.cairn.info/revue-

internationale-de-droit-penal-2007-1-page-79.htm&wt.src=pdf. Acesso em: 1º ar. 2023.

DIAS, Márcia C. **Déficit de profissionais de TI deve chegar a quase 800 mil em 2025, apenas no Brasil**. Gazeta do Povo. 18 mar. 22. Disponível em: https://www.gazetadopovo.com.br/gazz-conecta/brasil-vai-precisar-de-quase-800-mil-profissionais-de-ti-ate-2025/. Acesso em: 23 abr. 23.

FASTEST VPN. **Tipos de Ataque de Engenharia Social**. Disponível em: https://fastestvpn.com/pt/blog/ataques-de-engenharia-social/. Acesso em: 17 abr. 2023.

FILHO, Jonas O. S. **As Operações Militares no Ambiente Interagências**. DefesaNet, 2013. Disponível em: https://www.defesanet.com.br/doutrina/noticia/11634/as-operacoes-militares-no-ambiente-interagencias/. Acesso em: 7 abr. 2023.

FONSECA, Marcelo. Engenharia Social: **Concientizando o elo mais fraco da Segurança da Informação**. Orientador: Camel Adré de Godoy Farah. TCC (Pós-graduação) – Especialização de Inteligência de Segurança Pública, Universidade do Sul de Santa Catarina. Brasília, 2017.

FORTINET. **What is a Cyber Attack?** 2023. Disponível em: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks. Acesso em: 7 abr. 2023.

GARDNER, Frank. **Afeganistão:** 5 lições aprendidas com a 'guerra ao terror' desde o 11 de Setembro. BBC News, 11 set. 2021. Disponível em: https://noticias.uol.com.br/ultimas-noticias/bbc/2021/09/11/afeganistao-as-5-licoes-aprendidas-com-a-guerra-ao-terror-desde-o-11-de-setembro.htm. Acesso em: 24 abr. 23.

IBM. **What is a cyberattack?** Disponível em: https://www.ibm.com/topics/cyber-attack. 7 set. 2021 Acesso em: 27 maio 2023.

INTELLIGENCE COLLEGE EUROPE. **Intelligence Cooperation in the 21st Century**. 2022. Disponível em: https://www.intelligence-college-europe.org/intelligence-cooperation-in-the-21st-century/. Acesso em: 1º abr. 2023.

IOWA DEPARTMENT OF PUBLIC SAFETY **The Intelligence Production Cycle**. Disponível em: https://dps.iowa.gov/divisions/intelligence/intel-cycle. Acesso em: 26 maio 2023.

ITFORUM, **Todo ciberataque tem seis fases**. Disponível em: https://itforum.com.br/noticias/todo-ciberataque-tem-seis-fases/. Acesso em: 10 abr. 2023.

JOINT CHIEFS OF STAFF. **Origin of Joint Concepts**. Disponível em: https://www.jcs.mil/About/Origin-of-Joint-Concepts/. Acesso em: 23 abr. 23.

LEAL, Luís H. CYBINT X OSINT: Semelhanças, Diferenças e Responsabilidades. A **Lucerna**, 2019. Disponível em: http://www.ebrevistas.eb.mil.br/lucerna/article/view/11300/9040. Acesso em: 13 abr. 2023.

MI5. **Introduction to Cyber**. Disponível em: https://www.mi5.gov.uk/cyber. 2016 Acesso em: 16 abr. 2023.

NETO, José C. A; BARP, Wilson J; CARDOSO, Luis F. C. **Modelo Brasileiro do Ambiente Interagências para Operações na Fronteira**. Disponível em: https://rbed.abedef.org/rbed/article/download/74656/42064#:~:text=A%20atividade%20interag%C3%AAncias%20no%20Brasil,raramente%20tratado%20em%20debates%20acad%C3%AAmicos. Acesso em: 29 abr. 23.

OLIVEIRA, Jeanderson S. **A integração da inteligência militar e da inteligência policial em operações interagências**. Orientador: Fábio Cerqueira Viana Pio. Trabalho de Conclusão de Curso (Especialização em Análise de Inteligência) - Escola de Inteligência Militar do Exército. Brasília, 2022.

PEREIRA, Fábio S. **O ambiente interagências nas Operações de Pacificação do Complexo da Maré**. Orientador: Octavio Amorim Neto. Dissertação de Mestrado – Mestrado em Escola Brasileira de Administração Pública, Escola Brasileira de Administração Pública e de Empresas. Rio de Janeiro, 2016.

SANDERS, Lewis. **Serviço de Inteligência da Alemanha Recruta Hackers**. Made for Minds, 22 mar. 2017. Disponível em: https://www.dw.com/pt-br/servi%C3%A7o-de-intelig%C3%Aancia-da-alemanha-recruta-hackers/a-38066817. Acesso em: 22 abr. 23.

SEEDYK, Christopher. Characterizing Cyber Intelligence as an All-Source Intelligence Product. **Defense System**, 2 nov. 2019. Disponível em: https://dsiac.org/articles/characterizing-cyber-intelligence-as-an-all-source-intelligence-product/. Acesso em: 1º abr. 2023.

SOOD, K. Aditya; ENBODY, Richard, **Inteligence Gathering**. Targeted Cyber Attacks, 2014. Disponível em: https://www.sciencedirect.com/topics/computer-science/intelligence-gathering. Acesso em: 12 abr. 23.

THE LIGHTINING PRESS, **Intelligence Preparation of the Battlefield (IPB)**. Disponível em: https://www.thelightningpress.com/intelligence-preparation-of-the-battlefield/. Acesso em: 26 maio 2023.

TOZZI, Elisa. **Criador do termo BANI explica como sobreviver na era do caos**. VocêRH, 27 jul. 2021. Disponível em: https://vocerh.abril.com.br/futurodotrabalho/criador-do-termo-bani-explica-como-sobreviver-na-era-do-caos/. Acesso em: 7 abr. 2023.

TRADE TECHNOLOGY, **Os 3 principais golpes de engenharia social**. Disponível em: https://tradetechnology.com.br/blog/3-principais-golpes-de-engenharia-social/ Acesso em: 27 maio 2023.

WENDT, Emerson. Ciberguerra, Inteligência Cibernética e Segurança Virtual: alguns aspectos. **Revista Nacional de Inteligência**, n. 6, abr. 2011.