DISSERTAÇÃO DE MESTRADO PROFISSIONAL

FRAMEWORK DE INTELIGÊNCIA CIBERNÉTICA PARA INTERAÇÃO HUMANA UTILIZANDO AS MELHORES PRÁTICAS DE FONTES ABERTAS

ALCIDES FRANCINALDO SOUZA MACÊDO

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

FRAMEWORK DE INTELIGÊNCIA CIBERNÉTICA PARA INTERAÇÃO HUMANA UTILIZANDO AS MELHORES PRÁTICAS DE FONTES ABERTAS

ALCIDES FRANCINALDO SOUZA MACÊDO

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

PPEE.MP.054

Banca Examinadora

Prof. Flávio Elias Gomes de Deus, Ph.D, FT/UnB _____
Orientador

Prof. Laerte Peotta, Ph.D, FT/UnB _____
Coorientador

Prof. Banca 1, Ph.D, FT/UnB _____
Examinador interno

Prof. Banca 2, Ph.D, FT/UnB _____
Examinador interno

FICHA CATALOGRÁFICA

MACÊDO, A. S.
FRAMEWORK DE INTELIGÊNCIA CIBERNÉTICA PARA INTERAÇÃO HUMANA UTILIZANDO AS MELHORES PRÁTICAS DE FONTES ABERTAS [Distrito Federal] 2023.
PPEE.MP.054, xvi, 43 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. *Human Intelligence*	2. *Open Source Intelligence*
3. Engenharia Social	4. Coleta de Informações
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

MACÊDO, A. S. (2023). *FRAMEWORK DE INTELIGÊNCIA CIBERNÉTICA PARA INTERAÇÃO HUMANA UTILIZANDO AS MELHORES PRÁTICAS DE FONTES ABERTAS*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 43 p.

CESSÃO DE DIREITOS

AUTOR: ALCIDES FRANCINALDO SOUZA MACÊDO
TÍTULO: FRAMEWORK DE INTELIGÊNCIA CIBERNÉTICA PARA INTERAÇÃO HUMANA UTILIZANDO AS MELHORES PRÁTICAS DE FONTES ABERTAS.
GRAU: Mestre em Engenharia Elétrica ANO: 2023

ALCIDES FRANCINALDO SOUZA MACÊDO
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho aos mestres que direta ou indiretamente foram responsáveis pelo meu crescimento acadêmico.

AGRADECIMENTOS

Agradeço a Deus pelo dom da vida e pela oportunidade de fazer o bem e, à minha família, pela compreensão permanente e o apoio incondicional.

RESUMO

Os conceitos tradicionais e doutrinários da cibersegurança envolvem, de forma simplificada, as camadas física, lógica e social. Esta pesquisa objetiva abordar um terceiro aspecto para utilização de coleta de informações sobre usuários no mundo virtual visando obter colaboração para fornecimento de informações de maior qualidade para incrementar medidas de segurança cibernética, inclusive, aplicando métodos utilizados pela chamada engenharia social para reunir as melhores práticas de coleta de informações baseadas num *framework* envolvendo técnicas de inteligência de fontes humanas (HUMINT) e inteligência de fontes abertas (OSINT) para aumentar a capacidade das estruturas organizacionais de cibersegurança, privadas ou públicas, na identificação e prevenção de ameaças a partir da colaboração de usuários previamente identificados. Na consecução deste objetivo, esta pesquisa buscou investigar a aplicabilidade de técnicas de gerenciamento de fontes humanas e fontes abertas através da proposição de um *framework* de boas práticas para ações de coleta em fontes abertas, a partir dos seguintes objetivos: 1) revisar a literatura recente sobre os ataques baseados em engenharia social; 2) revisar os conceitos empregados em HUMINT; 3) revisar os conceitos empregados em OSINT; 4) propor um *framework* de boas práticas para orientar os profissionais de segurança cibernética a interagirem com eventuais perpetradores de ataques; 5) validar o *framework* a partir de questionários com profissionais em cibersegurança. A partir da metodologia de um estudo de caso, foram selecionadas 21 boas práticas, agrupadas nas categorias analíticas procedimental e psicológica, que foram depuradas por 15 especialistas, agentes policiais, que atuam na coleta de informações em fontes abertas.

ABSTRACT

The traditional and doctrinal concepts of cybersecurity, in a simplified form, the physical, logical and social federations. This research aims to address a third aspect for the use of collecting information about users in the virtual world in order to obtain collaboration to provide higher quality information to increase cybersecurity measures, including applying methods used by the so-called social engineering to gather the best practices of collection of information captured in a framework involving human source intelligence (HUMINT) and open source intelligence (OSINT) techniques to increase the capacity of organizational cybersecurity structures, private or public, in identifying and preventing threats based on user collaboration previously identified. In achieving this objective, this research sought to investigate the applicability of management techniques for human sources and open sources by proposing a framework of good practices for collection actions in open sources, based on the following objectives: 1) review the recent literature about attacks based on social engineering; 2) review the concepts used in HUMINT; 3) review the concepts used in OSINT; 4) propose a framework of best practices to guide cybersecurity professionals in interacting with adverse attack aggressors; 5) validate the framework based on questionnaires with cybersecurity professionals. Based on the methodology of a case study, 21 good practices were selected, grouped in procedural and psychological analytical categories, which were debugged by 15 specialists, waiting agents, who work in the collection of information from open sources.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AVFTEQS	Aqui vai ficar toda e qualquer sigla

Fim da Lista de Siglas

1 INTRODUÇÃO

Os conceitos tradicionais e doutrinários da cibersegurança envolvem, de forma simplificada, as camadas física, lógica e social, prevalecendo o consenso de que o sistema estará seguro se essas três camadas estiverem com níveis de conformidade apropriados. Diante das dificuldades para conceituar "segurança" para interfaces humanas e sociais,a indústria e a pesquisa acadêmica têm sido compelidas a tratar a cibersegurança com foco nas camadas físicas e lógicas [1].

De acordo com as abordagens mais pesquisadas, ao nível das camadas físicas e lógicas, a efetiva segurança depende da implementação de estratégia cibernética baseada no entendimento do *mindset hacker* com testes de penetração por *red team* e na defesa ampla e profunda com ações de *blue team* [2]. Sob ótica das camadas física e lógica, há diversos *frameworks* para defesa cibernética proativa com apenas alguns abordando a camada social, de forma tangencial, através do tratamento centrado na "cultura de segurança" do usuário.

Contudo, a partir da metade dos anos 2000, o campo de pesquisa sobre criminalidade *online* expandiu-se de discussões teóricas e práticas sobre a natureza do cibersegurança nas camadas físicas e lógicas que suportam o ambiente virtual para abordagens relacionadas aos espaços sociais, onde também ocorrem danos tangíveis ao patrimônio e o bem-estar físico e emocional das pessoas. Com a ampliação das pesquisas para a camada social, o escopo da investigação acadêmica também foi expandido para pesquisas de larga escala populacional, incluindo amostras populacionais de jovens e novos métodos criminosos e não-criminosos que têm sido utilizados para o entendimento da natureza do cibercrime [3, 4, 5, 6, 7].

No âmbito da camada social, as ameaças se conformam nas interações humanas baseadas no entrelaçamento entre informação e tecnologia que deslocam o ponto central das discussões para a sociedade informacional com as interdependências das relações humanas baseadas no uso das redes sociais que resultam no volume crescente da oferta de informações produzidas pelos próprios usuários.

Ao afetar todos os campos da atividade humana, a massiva oferta de informações também configura desafios para a segurança cibernética, particularmente para a atividade de coleta de informação de qualidade. Diante da possibilidade de geração de informação pelo próprio usuário através de redes sociais, a interação entre informação e tecnologia resulta em novas possibilidades de coleta e processamento de informações na *web* como subsídio para a implementação de políticas de segurança da informação, desde ambientes corporativos do setor privado até a vertente de *law enforcement* ou de Estado para segurança nacional. [8]

A coleta de informações como recorte da atividade de segurança pública abrange fundamentalmente a coleta e o processamento de informações para subsidiar o processo gerencial na administração dos órgãos de segurança pública ou na condução de ações de repressão à criminalidade, principalmente, no espaço cibernético onde se oferece uma série de serviços e no seu ambiente transitam informações sigilosas estão sujeitas a ameaças provenientes de crimes cibernéticos, primeiro nível de ameaça, espionagem industrial

eletrônica, ameaças de segundo nível e, a guerra cibernética, no terceiro nível [7].

Além da coleta sistemática para subsídios de ações de *law enforcement*, o levantamento bibliográfico indicou a existência de farta literatura relacionando a coleta de informações em redes sociais com ações de marketing empresarial, principalmente, na vertente conhecida por *profiling* para segmentação de companhas comerciais também conhecido por marketing de influência [9] com o objetivo de influenciar pessoas e influenciar seus comportamentos.

Esta pesquisa objetiva abordar um terceiro aspecto para utilização de coleta de informações sobre usuários no mundo virtual visando obter colaboração para fornecimento de informações de maior qualidade para incrementar medidas de segurança cibernética, inclusive, aplicando métodos utilizados pela chamada engenharia social. Neste sentido, a engenharia social é definida como ramo da ciência social aplicada relacionada com o gerenciamento de seres humanos de acordo com seu lugar e função na sociedade, além de organizar os métodos que são para obter informações pessoais ou confidencias que podem ser utilizadas para fins ilícitos [10].

No contexto definido pelo uso pervasivo da tecnologia, intensas interações humanas e grande volume de informações, esta pesquisa pretende reunir as melhores práticas de coleta de informações baseadas num *framework* envolvendo técnicas de inteligência de fontes humanas (*HUMINT*) e inteligência de fontes abertas (*OSINT*) para aumentar a capacidade das estruturas organizacionais de cibersegurança, privadas ou públicas, na identificação e prevenção de ameaças a partir da colaboração de usuários previamente identificados.

Nesse sentido, se pretende abordar possibilidades que possam aumentar a capacidade de entender e detectar ataques de engenharia social de modo a ampliação da mentalidade tecnológica prevalecente para considerar também o fator humano em associação com o uso da tecnologia [11] e, sobretudo, utilizar a metodologia de ataque de modo reverso para aumentar a consciência situacional do profissional de segurança cibernética com a proposição, do lado das defesas proativas, a substituição de engenharia social por técnicas de HUMINT.

1.1 DELIMITAÇÃO DO PROBLEMA

A coleta a partir de duas fontes combinadas, sugere uma abordagem *multi-source* para integrar informações variadas como o fito de se obter informações mais complexas, confiáveis, consistentes e precisas. Contudo, no âmbito dos estudos de inteligência e da segurança cibernética, ainda que de forma inadvertida, desenvolveu-se a técnica conhecida por "engenharia social"que desde os seus primórdios combinava técnicas de *HUMINT* e *OSINT*.

Desta forma, a partir da intersecção de técnicas de coleta de informações entre *HUMINT* e *OSINT* quais as melhores práticas para proposição de um *framework* para interação com usuários em redes sociais? Considerando que as habilidades do "engenheiro social"têm íntima relação com as técnicas utilizadas no

gerenciamento de fontes humanas e o "meio"para lançar ou preparar o ataque consiste em técnicas de fontes abertas.

1.2 OBJETIVOS

Esta pesquisa pretende ampliar o debate subjacente sobre o comportamento do usuário malicioso através da proposição de um *framework* que forneça diretrizes para interação com este tipo de usuário, de modo que os times de segurança possam avaliar a eventual aproximação e abordagem para proposição de colaboração para busca de informações como forma de facilitar o manuseio do volume de informações criadas nas redes sociais que permeia todos os campos da atividade humana.

1.2.1 Objetivo Geral

O objetivo dessa pesquisa é desenvolver um *framework* a partir de conceitos que possam auxiliar os profissionais de segurança cibernética a selecionar colaboradores potenciais com critérios objetivos que possibilitem medir a confiabilidade da informação obtida.

1.2.2 Objetivos Específicos

Os objetivos específicos a serem atingidos, são os seguintes:

- Revisar a literatura recente sobre os ataques baseados em engenharia social.
- Revisar os conceitos empregados em HUMINT.
- Revisar os conceitos empregados em OSINT.
- Propor um framework de boas práticas para orientar os profissionais de segurança cibernética a interagirem com eventuais perpetradores de ataques.
- Validar o *framework* a partir de entrevistas com profissionais em cibersegurança

A partir dos objetivos expostos, foram aplicados questionários para comunidade de profissionais da área de segurança cibernética para validar o *framework*, conforme resultados no Capítulo 4 com o intuito de verificar a viabilidade de aplicar de forma conjugada as técnicas de OSINT e HUMINT na coleta de informações durante interação com usuários de redes sociais.

1.3 JUSTIFICATIVAS

A engenharia social representa importante meio para obtenção de informações protegidas e consiste no ataque em si ou na preparação para ataques de maiores proporções. Nesse sentido, esta pesquisa pode

explorar o contexto onde esses ataques são realizados para aumentar o conhecimento sobre a própria metodologia utilizado pelos atacantes com pode prover elementos para formação e treinamento de profissionais de segurança cibernética que, eventualmente, necessitem recrutar colaboradores no contexto do cometimento desses ataques.

Ressaltando que o potencial da coleta de dados na enorme quantidade de material disponibilizado na web através de fóruns e quadros de mensagens, sites de crítica e opinião, marcadores sociais, compartilhamento de mídia, blogs, microblogs e redes sociais, bem como as limitações relativas à sua implementação, apresenta-se a seguinte indagação de pesquisa: Como a abordagem baseada em técnicas de HUMINT (*Human Intelligence*) conjugadas com técnicas de OSINT (*Open Source Intelligence*) podem ser aplicadas em ambiente virtual para intensificar a segurança cibernética.

Apesar destes resultados, a obtenção de informações a partir do uso e do gerenciamento de informantes é uma área pouco pesquisada [12, 13], mesmo a habilidade de obter informações através da interação com seres humanos compor a subcultura da atividade policial [14].

1.4 ORGANIZAÇÃO DESTE TRABALHO

Neste primeiro Capítulo foi realizado uma breve contextualização e foram determinados objetivos a serem alcançados. O restante deste trabalho é estruturado da seguinte forma:

No Segundo Capítulo é apresentada a revisão bibliográfica das pesquisas mais recentes sobre a aplicação das técnicas de HUMINT em ambiente virtual. Além disso, algumas pesquisas relacionadas que auxiliaram na resolução do problema proposto.

Em seguida, no Capítulo 3 é apresentada metodologia exploratória para o problema de interseção entre HUMINT e OSINT, além da definição do problema, abordando-se conhecimentos relacionados à estratégia de solução: proposição de *framework* de boas práticas para interação com potenciais perpetradores de ataques de Engenharia Social.

O Capítulo 4 define as bases para o estabelecimento do novo *framework* em suas partes constitutivas. Apresentam-se detalhes sobre cada uma das boas práticas e, por fim, a forma como os dados foram modelados.

No Capítulo 5 são apresentados e discutidos os resultados obtidos.

2 REFERENCIAL TEÓRICO

No dia 25 de abril de 1947, quando se desenrolavam as discussões para o estabelecimento do sistema de defesa nacional do Estados Unidos no pós-guerra, o diplomata Allen Dulles, futuro Diretor da CIA de fevereiro de 53 a novembro de 61, declarou, em depoimento para o Comitê do Serviço Militar do Senado Norte-americano, que 80 por cento das informações demandadas pela inteligência americana poderiam ser obtidas de forma “aberta, normal e transparente” [15].

Para Dulles, o glamour e o mistério sobrevalorizavam a obtenção de informações através da estrutura burocrática dos serviços de inteligência e de seus agentes secretos, enquanto a maior parte da coleta e do processamento de inteligência era realizado através de "métodos normais, abertos e transparentes", como contatos diplomáticos, relações pessoais, notícias de rádio e jornais impressos [15]. O depoimento de Allen Dulles valoriza a coleta de informações sem depender de dispendiosas estruturas operacionais por estarem disponíveis em repositórios abertos que se tornaram disponíveis desde o advento da imprensa.

De fato, desde o início do século XVI a imprensa de tipos móveis de Gutemberg provocou a expansão das publicações e foi criticada por Erasmo de Roterdã, que propalava a dificuldade de se encontrar um “lugar na Terra” isento dos livros, editados aos milhares a cada ano sem que alguém fosse capaz de saber quais valeriam a pena ler, segundo a historiadora [16]. Esse foi o primeiro cenário de sobrecarga de informações que influenciou a transformação da sociedade na alta Idade Média. Circunstâncias semelhantes às retratadas por [16] estiveram presentes após a Segunda Guerra Mundial. Dessa feita, em vez de críticas desairosas, Allen Dulles referiu-se à sobrecarga de informações como a principal fonte de insumos para a coleta de informações [15].

Naqueles idos, os avanços científicos e técnicas decorrentes da Segunda Guerra Mundial estavam sendo reconhecidos e publicizados através da Ciência da Informação, que buscava implementar soluções teóricas e aplicadas a fim de tornar mais acessível a crescente oferta de informações [17]. Nesse sentido, surge a proposição de Vannevar Bush para disponibilizar ao público o crescente acervo de conhecimento [18] através de uma solução tecnológica que promovesse fluxos informacionais entre usuários e repositórios de informações.

A profusão de fontes de informação e a agitação acadêmica que se seguiu à Segunda Gerra configurou o contexto tecnológico que resultou em diversos avanços, a exemplo da conferência *Dartmouth Summer Research Project Artificial Intelligence* no âmbito do Departamento de Matemática do Universidade de Dartmouth por iniciativa do Professor John McCarthy que organizou um grupo de estudo para esclarecer e desenvolver ideias sobre inteligência artificial lançando as bases para o surgimento de um novo campo de estudo relacionando automação e cibernética [19]. É possível relacionar este contexto com a implementação do *Advanced Research Projects Agency* (ARPA) fundado pelo Departamento de Defesa dos Estados para promover o compartilhamento de dados entre instituto de pesquisas através uma rede de computadores [20].

Com o a disseminação do uso da Internet para além das pesquisas de interesse militar e de defesa, se inicia um processo de aprimoramento técnico que vai resultar no surgimento da chamada Web 2.0, também conhecida por web participativa. Ao cunhar o termo Web 2.0 no ano de 1999, Darcy Dinucci antecipou o caráter pervasivo da Internet através do seu alcance a diversos tipo dispositivos, além das páginas www em telas de computadores até TVs, telefones celulares, painéis de automóveis, *gadgets* portáteis para jogos e outros [8] atuando todos como transportadores de informações e provedores de interatividade entre pessoas e instituições.

A intensidade e a diversificação no uso da tecnologia de internet resultou no aumento da capacidade de interação e na produção de informação, compelindo o surgimento de uma nova disciplina de coleta de informações a SOCMINT (*Social Media Intelligence*) que se refere a metodologias para coletar informações sobre interações sociais no âmbito da OSINT (*Open Source Intelligence*)[21].

Nesse sentido, a coleta de informações através de OSINT pode atuar em paralelo com outras disciplinas de coleta, no caso dessa pesquisa, com a disciplina de HUMINT, que consistem em ações especializadas que são agrupadas em "fluxos informacionais estruturados" na dimensão *single-sources collection* que são os meios operacionais para obtenção de informações. Mais tarde essas informações serão submetidas à etapa denominada *all-sources analysis*, que relaciona o processo analítico utilizado no processamento de informações [22].

Dessa forma, as informações fluem das disciplinas de coleta, *single-sources*, para a fase analítica, *all-source analysis*, onde ocorre a validação da informação através da fusão com o produto de outras disciplinas de coleta, por isso a fase de análise também pode ser definida como um processo de fusão de informações oriundas de diferentes fontes gerando um produto de inteligência *multi-source*. Nesta pesquisa, se pretende defender, através da proposição de um *framework*, uma abordagem *dual-source* capaz de combinar metodologias da disciplina de HUMINT com OSINT, respectivamente a mais antiga e restrita com a mais recente e popular.

O trabalho de coleta de informações para alimentar a atividade de inteligência, via de regra, começa pela coleta de informações que podem ser obtidas de modo mais fácil e seguro e avançam para métodos mais difíceis e arriscados, na dimensão *single-sources collection*. Assim, as ações se iniciam na coleta de informações disponíveis em fontes abertas e mídias sociais (OSINT e SOCMINT, respectivamente, *Open-Source Intelligence* e *Social Midia Intelligence*) e vão evoluindo de para metodologias mais complexas e dispendiosas, passando por HUMINT (*Human Intelligence*) até as disciplinas técnicas que envolve sensores de imagens e sinais.

A etapa seguinte ocorre na dimensão *all-sources analysis*, em que as informações coletadas são reunidas e interpretadas através de processos analíticos que diferenciam o produto da atividade inteligência da informação coletada por sua capacidade explicativa e/ou preditiva. Contudo os métodos estanques estruturados como *single-sources* ou *all-sources* necessitam ser redimensionados para comportar as mudanças das interações entre informação e tecnologia, de modo a desenvolver soluções teóricas e aplicadas que aumentem a acessibilidade da crescente oferta de informações resultante da diversidade dessas interações

que podem estar relacionadas com atividade maliciosa.

2.1 CICLO DE INTELIGÊNCIA

Marco Cepik argumenta que a atividade de inteligência é organizada em conjuntos delimitados de "fluxos informacionais estruturados" em "duas dimensões". A primeira relaciona os meios operacionais utilizados para coletar informações de um adversário, enquanto a segunda é caracterizada pelo processo analítico que diferencia o produto da atividade inteligência da informação coletada por sua "capacidade explicativa e/ou preditiva" [23].

Segundo Michel Herman, as "duas dimensões" dos "fluxos informacionais estruturados" estão acomodadas em uma fase intermediária constituída pelo estágio de coleta, que abrange fontes e meios utilizados para a obtenção de informações denominado *single-sources collection*, e pelo estágio de análise das informações obtidas pelas fontes singulares, denominado *all-sources analysis* [22].

Segundo Marco Cepik, os estágios de coleta (*single-sources collection*) e análise (*all-sources analysis*) são as etapas fundamentais do "fluxo informacional estruturado" denominado Ciclo de Inteligência, que, em sua forma ampliada, possui até dez etapas principais que caracterizam a atividade de Inteligência, na seguinte ordem [23]. A figura 2.1 ilustra estes estágios.

Figura 2.1: Estágios de Coleta, segundo CEPIK

Fonte:O próprio autor

No ramo policial, a atividade de Inteligência policial vem se consolidando como um instrumento fundamental para apoiar ações de combate à criminalidade em geral e, principalmente, aos crimes de alta complexidade, nos quais é necessário identificar, entender e revelar os aspectos ocultos da atuação criminosa que seriam de difícil detecção pelos meios tradicionais de investigação policial. Contudo, a busca de informações pura e simples precisa ser somada a outras práticas que transformem dados dispersos em informações úteis para a atividade policial. O processo que agrupa essas práticas é conhecido como Ciclo de Inteligência.

Através das etapas do Ciclo de Inteligência, as investigações policiais são instruídas a partir de um processo que se inicia com a demanda de informações específicas e evolui para ações de planejamento, coleta, análise e difusão para os demandantes ou instâncias superiores.

O Ciclo de Inteligência pode ser definido como uma cadeia de etapas em que se decompõe o processo da atividade de Inteligência. A maioria dos organismos de Inteligência, no Brasil e no exterior, utiliza o modelo de Ciclo de Inteligência adotado pelo Programa de Inteligência do FBI e apresentado por David Carter em *Law Enforcement Intelligence: a guide for state, local, and tribal law enforcement agencies*, no qual são estabelecidos seis momentos de um processo que pode ser retroalimentado à medida que evolui a investigação, os quais são apresentados abaixo [24]:

> I - REQUIREMENTS: Requirements are identified information needs – what we must know to safeguard the nation. ... Requirements are developed based on critical information required to protect the United States from National Security and criminal threats.
>
> II - PLANNING AND DIRECTION: Planning and direction is the management of the entire effort from identifying the need for information to delivering the intelligence product to the consumer. It involves the implementation of plans to satisfy requirements levied on the FBI as well as identifying specific collection requirements based on FBI needs. Planning and direction are also responsive to the end of the cycle because current and finished intelligence, which supports decision making, generates new requirements.
>
> III - COLLECTION: Collection is the gathering of raw information based on the requirements. Activities such as interviews, technical and physical surveillances, human source operations, searches, and liaison relationships results in the collection of intelligence.
>
> IV - PROCESSING AND EXPLOITATION: Processing and exploitation involves converting the vast amount of information collected to a form usable by analysts. This is done through a variety of methods including decryption, language translation, and data reduction. Processing includes the entering of raw data into databases where it can be exploited for use in the analysis process.
>
> V - ANALYSIS AND PRODUCTION: Analysis and production is the converting of raw information into intelligence. It includes integrating, evaluating, and analyzing available data, and preparing intelligence products. The information's reliability, validity, and relevance is evaluated and weighed. The information is logically integrated, put in context, and used to produce intelligence. This includes both "raw" and "finished" intelligence. Raw intelligence is often referred to as "the dots". ... "Finished" intelligence reports "connect the dots" by putting information in context and drawing conclusions about its implications.

> VI - DISSEMINATION: Dissemination is the distribution of raw or finished intelligence to the consumers whose needs initiated the intelligence requirements. FBI intelligence customers make decisions – operational, strategic, and policy – based on the information. These decisions may lead to the levying of more requirements, thus continuing the FBI intelligence cycle.

Versão resumida e de tradução livre:

> I - Requerimento: momento inicial em que o decisor estratégico ou autoridade competente demanda suas necessidades informacionais, que são traduzidas em requerimentos.
>
> II - Planejamento: etapa em que a equipe estabelece metas de coleta e análise bem como os formatos de disponibilização do produto para o cliente e o tempo necessário para tal.
>
> III - Coleta: ações para atender as demandas requeridas através da reunião das informações necessárias através de um ou de vários mecanismos de coleta.
>
> IV - Processamento: envolve o agrupamento, a organização das informações coletadas.
>
> V - Análise: extração de padrões, significados, inferências e constatações que têm como base o conjunto de informações coletadas para atender os requerimentos informacionais.
>
> VI - Disseminação: consiste na disponibilização do produto informacional para a autoridade requerente ou para o decisor estratégico.

David Carter [24] afirma que *"pieces of information gathered through the collection process are not Intelligence. Rather, Intelligence is the knowledge derived from the logical integration and assessment of that information and is sufficiently robust to enable law enforcement to draw conclusions related to particular crime"*.

Ao mesmo tempo em que Carter [24] ressalta a importância de coligir informações em um processo organizado, também observa que a junção de informações deve ser submetida a um padrão analítico capaz de produzir um sentido amplo para informações esparsas. Assim, um volume agregado de informações é estratificado para possibilitar a identificação de padrões de ocorrências, características organizacionais e de processos e indivíduos que, de forma isolada, passariam despercebidos.

Para o escopo desta pesquisa, o conceito de vigilância para coleta de informações está difuso no âmbito das disciplinas de coleta (*single-sources collection*) e é considerada o alicerce da atividade de inteligência [25]. As disciplinas de coleta definem os métodos de obtenção de acordo com a natureza dos dados a serem explorados e com a habilidade de consegui-los de diversas maneiras, ao custo orçamentário que consome até quatro quintos do total das despesas governamentais para a área da inteligência, sendo a maior parte utilizada para financiar plataformas tecnológicas, especialmente satélites [26].

Nesse âmbito, os meios de coleta e as fontes típicas de informações definem disciplinas especializadas (*single-sources collection*) que são reconhecidas pelos acrônimos derivados da doutrina norte-americana: HUMINT (*human intelligence*), SIGINT (*signals intelligence*), IMINT (*imagery intelligence*), MASINT (*mesurement and signature intelligence*) e OSINT (*open sources intelligence*) [22].

Tem-se, portanto, os distintos segmentos de obtenção de dados agrupados no estágio *single-sources collection*, que compreendem desde as fontes mais antigas e mais baratas até as modernas e dispendiosas estruturas de captação de imagens e sinais [22]:

a) HUMINT (*human intelligence*): informações obtidas a partir de fontes humanas, entendendo-se por isso: entrevistas, ligações com outras agências, obtenção clandestina de informações e rede de contatos. O acrônimo HUMINT foi incorporado ao jargão internacional para evitar o termo espionagem, inadequado sob o ponto de vista legal e político [23];

b) IMINT (*imagery intelligence*): método de coleta que utiliza a captura e a interpretação de imagens fotográficas e multiespectrais;

c) MASINT (*measurement and signature intelligence*): processamento de informações obtidas através da mensuração técnica e científica de sinais térmicos, sísmicos e magnéticos, dentre outros, de forma a localizar a origem geográfica de tal sinal bem como a identificar o equipamento que lhe deu origem;

d) OSINT (*open sources intelligence*): é a utilização de fontes abertas ao público, como jornais, periódicos, bancos de dados, documentários, entrevistas, teses e pesquisas acadêmicas, grupos de discussão na Internet, sites especializados, etc., sendo que tais fontes públicas podem ser impressas ou eletrônicas [27].

Com o advento da Internet, a vigilância tradicional, dependente das capacidades humanas para analisar e capturar dados sem a intermediação da tecnologia, perdeu importância na atividade de inteligência em decorrência do fim da Guerra Fria e dos avanços da tecnologia, que fizeram disseminar nas estruturas burocráticas e operacionais a crença de que as disciplinas agrupadas no campo de TECHINT poderiam responder pela maior parte da coleta de informações, subestimando a coleta de informações a partir de fontes humanas – disciplina de HUMINT [28].

Conforme já mencionado, nos países centrais, a etapa de coleta consome até quatro quintos dos orçamentos governamentais para a área de inteligência, com a maior parte desse percentual destinada ao financiamento das disciplinas agrupadas no âmbito da TECHINT [26]. Como exemplo, pode-se citar as várias opções de monitoramento através de programas ultrassecretos conduzidos pelos Estados Unidos e pelo Reino Unido para monitorar bilhões de mensagens de e-mail e seus metadados, conforme revelações dos Projetos TEMPORA e PRISM feitas por Edward Snowden [29, 30, 31].

Portanto, o ganho de importância das plataformas de monitoramento, agrupadas no campo de disciplinas TECHINT, começa logo após a Segunda Guerra, com a publicidade decorrente do sucesso de Bletchley Park , que animou os defensores da Inteligência de Sinais (SIGINT) a aprimorar a interceptação, a decodificação, a tradução e a análise de mensagens por uma terceira pessoa além do emissor e do destinatário pretendido [23].

Dessa forma, os avanços que começaram nos laboratórios de Bletchley Park e alcançaram as sofisticadas redes de vigilância estruturada em equipamentos satelitais, passando pelo ambicioso sistema ECHELON até os Projetos TEMPORA e PRISM, resultaram na proposição do termo *Dataveillance*, que consiste

no “uso sistemático de sistema de dados para investigação ou monitoramento de ações ou comunicações de uma ou mais pessoas” [32]. O termo *Dataveillance* surgiu em contraposição à abordagem de vigilância tradicional, que depende das capacidades humanas não mediadas por tecnologia para analisar e capturar dados.

As possibilidades do monitoramento sistemático de dados decorrente do crescimento das mídias sociais representam uma proposta promissora para melhorar a efetividade das ações de segurança pública através da configuração de uma nova disciplina de coleta Social Intelligence (SOCINT) ou Social Midia Intelligence (SOCMINT).

Para Laura Donohue [33], a SOCINT é definida como a coleta de dados digitais das relações sociais que ocorrem na Internet, apesar de a comunidade de inteligência estadunidense considerar a coleta de informações em mídias sociais como um apêndice da disciplina de *Open Source Intelligence* (OSINT) e *Signals Intelligence* (SIGINT), que abrange coleta a partir da comunicação direta, *Communications Intelligence* (COMINT), e da interceptação de sinais eletrônicos relacionados ou não com a comunicação entre pessoas, ELINT (*Electronic Intelligence*).

Nesse sentido, a coleta de dados é a atividade de recuperar objetos informacionais disponíveis na web que, na atividade de inteligência, são “pegadas digitais” que evidenciam padrões individuais, grupais ou comportamento social [34] através da ampliação de conceitos e ferramentas matemáticas para análise de redes sociais [35].

Heather Williams e Illana Blum [36] concluem, no relatório editado pela *Rand Corporation Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, que os órgãos de inteligência ainda não estão preparados para a evolução da Web 2.0 que possui páginas dinâmicas e conteúdo gerado pelos usuários para a Web 3.0, incluindo processamento direto e indireto de dados, aprendizado de máquina e automatização de processamento. As autoras defendem a análise de inteligência baseada em OSINT para a “segmentação” da investigação e para melhorar o processo de recrutamento de colaboradores, e citam o cruzamento de dados psicométricos e a análise de big data na campanha do presidente norte-americano Donald Trump.

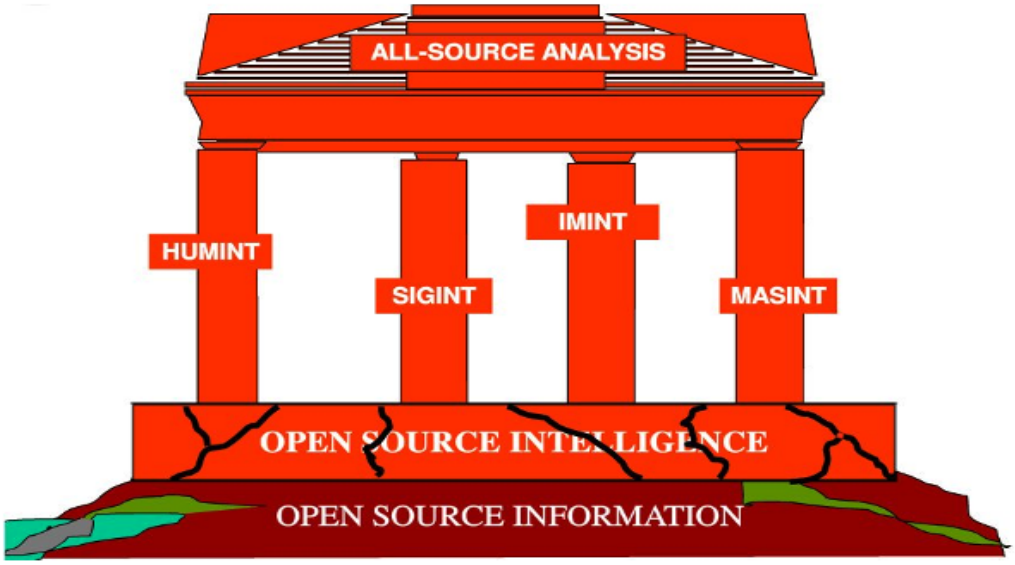
2.2 OPEN SOURCE INTELLIGENCE (OSINT)

A disciplina de OSINT é um subgrupo de conceito de Inteligência que produz conhecimento a partir de informações disponíveis de todos que desejarem ter acesso, mas tem o mesmo objetivo, localizar e afastar ameaças e encontrar e promover oportunidades, através da superação desafios relacionados com grau de incerteza, validação de informações obtidas por outros meios, prospecção de interpretações alternativas e outros [37]. A consecução dos objetivos depende, segundo Benes, da aferição precisa da relevância dos dados coletados diante da quantidade de dados disponíveis com o advento das redes sociais.

Como citado anteriormente, a importância da coleta de informações a partir de "métodos normais,

abertos e transparentes"[15] é refletida na Figura 2.2, onde estão representadas as disciplinas de coleta (HUMINT, SIGINT, IMINT, MASINT) que são os pilares de suporte a análise de informações e estão fundadas sobre a coleta em fonte aberta (OSINT) que, por sua vez, baseia-se em toda e qualquer informação aberta. Contudo, essa abordagem decorrente do pós Segunda Guerra necessita ser ampliada muitas vezes, considerando que naquela época a oferta de OSINT advinha tão somente de material impresso (jornais, livros, documentos acadêmicos, etc.) ou audiovisual divulgado por rádios e televisão. Diante da miríade de fontes abertas de informações e sua importância para subsidiar atividades de investigação criminal ou produção de informações estratégicas, esta pesquisa busca evidências sobre a aplicabilidade da abordagem colaborativa na coleta de informações para otimizar ações de coleta e processamento de informações de forma distribuída entre profissionais de segurança cibernética.

Figura 2.2: *All sources intelligence*



Fonte:(STEELE, 2001)[38]

Nesse cenário virtual caracterizado por oferta abundante de dados, Stottlemyre [39] sugere que a principal mudança na atividade de coleta de informações decorre da imbricação entre OSINT e HUMINT resultante das interações humanas em redes sociais.

Em busca de um conceito para *crowdsourcing intelligence*, Stottlemyre [39] seguiu reunindo os temas comuns presentes, em primeiro lugar, na definição proposta por Brabham [40], que estabeleceu *crowdsourcing* como um modelo *online* de produção para resolução distribuída de problemas que nivela a inteligência coletiva de comunidades a fim de atender específicos objetivos organizacionais específicos.

Desse modo, Stottlemyre [39] argumenta que a definição de Brabham implica três condições necessárias para a implementação de um sistema de *crowdsourcing*. Primeiro, na existência de uma organização que demande a resolução de um problema. Em segundo, que a organização demandante solicite a participação abrangente de muitas pessoas, preferencialmente reunidas em uma plataforma *online* para interagirem em busca da solução do problema proposto. O tamanho e a forma da comunidade demandada dependem

das especificidades do problema a ser abordado. Em terceiro lugar, apesar de a definição de Brabham não mencionar a necessidade de voluntariado, esse autor recomenda que os membros da comunidade optem por participar de forma voluntária para garantir que as informações aduzidas ao sistema de forma espontânea.

Além da abordagem de Daren Brabham, Stottlemyre [39] adiciona elementos da definição de Inteligência, cuja missão é coletar a maior quantidade possível de informações sobre um alvo através de *single-sources collection* para posterior análise e produção de informações estratégicas a fim de dar suporte à decisão, ou como informação coletada, processada e condensada para atender as necessidades informacionais de decisores estratégicos, ou, ainda, informação relevante para a formulação e implementação de políticas de governo relacionadas com segurança nacional e ao enfrentamento de ameaças atuais ou potenciais. Dessa forma, o autor acrescenta a existência de intenção prévia de coletar informações para utilização no processo decisório.

Das cinco disciplinas especializadas de coleta (OSINT, HUMINT, SIGINT, MASINT e GEOINT), Stottlemyre [39] ressalta que OSINT e HUMINT são as disciplinas que tratam da coleta de informações sob a interferência direta de seres humanos, portanto, são as únicas que podem ser agrupadas em ambiente de *crowdsourcing*, que depende inteiramente da atividade humana.

Para relacionar a definição de OSINT com o conceito unificado de *crowdsourcing intelligence*, Stottlemyre (2015) defende a necessidade de examinar a definição de OSINT contida na legislação norte-americana e na doutrina da comunidade de inteligência estadunidense. De acordo com o *National Defense Authorization Act for Fiscal Year* 2006, OSINT é a informação que é produzida a partir de informações disponíveis publicamente que são coletadas, processadas e difundidas na periodicidade necessária para atender uma demanda específica [39].

A *Intelligence Community Directive* 301 anota que "*open source collection*" significa "obter posse de" informação que foi coletada e disseminada por outros, restando aos agentes o uso em "*second-hand*" da informação coletada em fontes abertas. Assim, em vez de coleta de informações em fontes abertas, a *Intelligence Community Directive* 301 recomenda a denominação de aquisição de informações em fontes abertas [39].

Em atenção à ubiquidade inerente à disciplina de OSINT, Lowenthal e Clark [41] destacam a necessidade de diferenciar a informação obtida por *collection activities* da informação oriunda de *acquisition activities* para se determinar o valor da resposta destinada a uma demanda informacional.

No âmbito das definições acima, de forma genérica, a coleta de inteligência deve acumular informações para subsidiar o processo decisório; de forma específica, a coleta de OSINT deve objetivar a aquisição de informação de "*second-hand*" e por sua vez, a coleta de HUMINT deve envolver a obtenção de informações de seres humanos. Portanto, a inteligência obtida a partir de abordagens de *crowdsourcing* deve ser considerada uma disciplina de coleta separada de OSINT e HUMINT por envolver demandas informacionais que se tornam públicas para os membros do sistema de *crowdsourcing* [39]. A resolução de problemas de forma distribuída em uma "*crowd*" pressupõe a existência de uma "inteligência coletiva",

em que a capacidade cognitiva do grupo pode ser considerada independente e maior que a capacidade de membros individuais (SALMINEN, 2013).

De acordo com o modelo proposto por Salminen [42], o processo de construção da inteligência coletiva começa pela combinação das restrições do meio-ambiente com as capacidades humanas de interação (inteligência, confiança, motivação e outros fatores psicológicos e culturais), que cria as regras de interação entre agentes cognitivos submetidos a necessidades informacionais. As necessidades informacionais, por sua vez, estimulam o relacionamento interagentes que resulta em melhor integração de informação que será agregada em um sistema de memória coletiva que executa ações de integração e acúmulo de acordo com mais ou menos regras de interação.

Salminen [42] afirma que as alterações na memória coletiva retroalimentam os agentes com informações que podem modificar o meio ambiente informacional através do fluxo de saída de informações do sistema, perfazendo um complexo sistema adaptativo formado pelos agentes, pelas regras de interação, pela memória coletiva e pelas restrições do meio ambiente.

2.3 HUMAN INTELLIGENCE (HUMINT) EM AMBIENTE VIRTUAL

Conforme mencionado anteriormente, a Internet provocou mudanças significativas na organização da sociedade, influenciando todos os ramos da ação humana, incluindo a atividade de inteligência e a coleta de informações, ambas compreendidas como recorte do meio social. Segundo Robert Clark [43], a coleta de informações a partir do ambiente cibernético pode ser a mais importante fonte de dados para a atividade de inteligência nos dias de hoje.

Ao denominar a coleta em ambiente cibernético de *cyber collection* (CYBINT), Clark [43] argumenta que as disciplinas tradicionais de coleta não abrangem as especificidades da CYBINT, embora apresentem alguns aspectos de OSINT com coleta intensiva na *web*, ou mesmo de SIGINT, com interceptação de comunicações na Internet.

Contudo, não é possível caracterizar, fora da disciplina de CYBINT os programas maliciosos que infectam computadores para capturar arquivos ou danificar sistemas informáticos, ativar câmeras de vídeo e operação a partir de fontes humanas para coleta em computadores que nunca se conectam à Internet [43], a exemplo da operação envolvendo o vírus *stuxnet* que danificou o sistema de controle das centrífugas do programa iraniano de enriquecimento de urânio.

Dessa forma, demonstra-se que a interação entre as disciplinas de coleta abrange situações que exigem abordagens conjugadas de duas ou mais especialidades de coleta. Segundo Siman-Tov e Tal [44], o crescimento da importância das interações virtuais resultou em questionamentos sobre a relevância da coleta a partir de HUMINT na Internet, uma vez que o ciberespaço é uma cena importante para a atuação da segurança pública.

O desenvolvimento tecnológico, segundo Gioe [45], impactou profundamente nas operações de coleta a partir de fontes humanas devido à sobrecarga de informações que podem ser obtidas *online*, além da possibilidade de alterações no trabalho de coleta desenvolvido pela fonte humana. Em um primeiro momento, o impacto do desenvolvimento tecnológico diminuiu a importância da coleta tradicional, fontes humanas e vigilância física, que dependem das capacidades humanas para analisar e capturar dados sem a intermediação da tecnologia [28].

Após o advento da tecnologia e o crescimento da crença popular de que a coleta tradicional não seria eficaz para subsidiar ações contra a nova configuração de atividades terroristas baseadas nos recursos de comunicação da Internet, as disciplinas agrupadas no âmbito de techint assumiram o protagonismo na coleta de informações e no incremento das capacidades preditivas dos órgãos de inteligência norte-americanos [45].

Segundo Cummings [46], a *Central Intelligence Agency* desencorajou a coleta a partir de fontes humanas após os atentados de 11 de setembro e incrementou o uso de coletores eletrônicos, eclipsando a disciplina de HUMINT na luta contra o terrorismo. Nesse cenário, cliques no mouse e dicionários *online* têm mais glamour e efetividade do que as "capas sobretudo e adagas brilhantes" de outrora, fazendo crescer a percepção do anacronismo da coleta a partir de fontes humanas [47].

De fato, não é possível contestar a importância da coleta baseada em OSINT, seja pela massiva oferta de informações de diferentes tipos e formatos, seja para a conveniência política de utilização de uma fonte de coleta segura e sem riscos de exposição perante os adversários inseridos em ambientes restritos. Contudo, como já abordado acima, o advento da comunicação via Internet disseminou o uso da chamada Web 2.0 através das redes sociais, resultando no surgimento de uma subárea no domínio OSINT, a Inteligência de Mídia Social (Social *Media Intelligence* – SOCMINT) especializada na coleta de informações a partir de redes sociais, com potencial para minimizar a importância da disciplina de HUMINT [21].

Para Gioe [45], a inovação tecnológica que incrementa a importância da coleta a partir de OSINT e SOCMINT não vai diminuir a importância da disciplina de HUMINT, mas vai dar-lhe uma nova dimensão através de novas capacidades e novos desafios:

1. a oferta massiva de dados facilitará a avaliação da efetividade de operações de coleta baseadas em fontes humanas;
2. a disseminação do uso de funções de biometria pode auxiliar na identificação de pessoas;
3. a disseminação do uso de redes sociais pode aumentar a vulnerabilidade de operações de coleta no âmbito de SOCMINT.

O mesmo autor argumenta que as soluções não são fáceis e não envolvem somente a comunidade de inteligência para prospectar as soluções de mais inovação e criatividade que as mesmas tecnologias permitem.

Além do escopo da atividade de inteligência, Zeng et al. [48] argumentam que o avanço das tecnologias da Web que, no primeiro momento, promoveram a acessibilidade a recursos de computação através de dispositivos móveis com acesso a conteúdo de mídias sociais, começaram a estender suas influências para além da computação pessoal, estimulando a colaboração e reforçando a interatividade; conformou-se, então, o paradigma *social computing*.

O conceito de *social computing* começou a ser construído por Ellis, Gibbs e Rein [49], com a proposição de ferramentas computacionais como suporte para resolução de problemas através de grupos de colaboração, também chamados de aplicações de *groupware* ou *Computer Supported Cooperative Work* (CSCW). Atualmente, a grande expansão do escopo da *social computing* estimulou a aplicação de tecnologias de computação para análises de comportamento social e estudos na área de criação de agentes sociais artificiais a fim de facilitar estudos sociais e a dinâmica social humana através da utilização de tecnologia da informação [48].

O *framework*, resultado dessa pesquisa, propõe ampliar a atividade de coleta para além da captura de informações em ambiente virtual típicas de OSINT e SOCMINT. Contudo, a fusão de HUMINT, OSINT e SOCMINT¸em ambiente virtual depende de ações inseridas em contextos de grupos restritos de indivíduos com dinâmicas de compartilhamento limitado diferente dos conteúdos que alcançam públicos mais amplos e diversos [50].

Muitos desses indivíduos interagem na rede "camuflados" por contas piratas e/ou *fake* que têm como objetivo provocar danos à imagem de outros participantes, através da "trolagem" ou da perturbação do ambiente digital com postagens ofensivas e instigando confrontos entre os participantes, de preferência em participantes nas quais elas possam repercutir, além de obtenção e/ou supressão de informações dos participantes para o cometimento de crimes cibernéticos e no "mundo físico", como aponta Glenny [7].

No âmbito de suas pesquisas sobre terrorismo, Briggs e Strugnell [51] sustentam que o uso da Internet por grupos extremistas possibilitou a quebra de barreiras existentes no mundo físico para determinados grupos de pessoas, particularmente na participação de mulheres em movimentos jihadistas, pois o encontro físico de mulheres com homens pode ser tido no mundo árabe como inaceitável fora do círculo familiar, dificultando o envolvimento e a participação feminina em grupos extremistas.

As mesmas autoras também afirmam que o anonimato e a liberdade de ação podem tornar aceitáveis a expressão de certos pensamentos em público, com a vantagem de alcançar muitos usuários interessados no tema [51]. Para Glenny "a internet é uma teoria da grande bolha – resolvemos um problema que a afeta, mas outro, aparentemente intratável, vem à tona em outra parte". Dessa forma, a internet gera uma quantidade gigantesca de dados e informações que tem pouco ou nenhum valor, outro montante com pouca ou nenhuma interpretação e uma pequena parcela é perigosa por sua falsidade [7].

Com o advento da Internet, a vigilância tradicional, dependente das capacidades humanas para analisar e capturar dados sem a intermediação da tecnologia, perdeu importância na atividade de inteligência em decorrência do fim da Guerra Fria e dos avanços da tecnologia, que fizeram disseminar nas estruturas

burocráticas e operacionais a crença de que as disciplinas de coleta agrupadas no campo de TECHINT (*technical intelligence*) poderiam responder pela maior parte da coleta de informações, subestimando a coleta de informações a partir de fontes humanas – disciplina de HUMINT [28].

De fato, não é possível contestar a importância da coleta baseada em OSINT, seja pela massiva oferta de informações de diferentes tipos e formatos, seja para a conveniência política de utilização de uma fonte de coleta segura e sem riscos de exposição perante os adversários inseridos em ambientes restritos. Contudo, como já abordado acima, o advento da comunicação via Internet disseminou o uso da chamada Web 2.0 através das redes sociais, resultando no surgimento de uma subárea no domínio OSINT, a Inteligência de Mídia Social (*Social Media Intelligence* – SOCMINT) especializada na coleta de informações a partir de redes sociais, com potencial para minimizar a importância da disciplina de HUMINT [21].

Para Gioe [45], a inovação tecnológica que incrementa a importância da coleta a partir de OSINT e SOCMINT (*Social Media Intelligence*) não vai diminuir a importância da disciplina de HUMINT, mas vai dar-lhe uma nova dimensão através de novas capacidades e novos desafios: (1) a oferta massiva de dados facilitará a avaliação da efetividade de operações de coleta baseadas em fontes humanas; (2) a disseminação do uso de funções de biometria pode auxiliar na identificação de pessoas; (3) a disseminação do uso de redes sociais pode aumentar a vulnerabilidade de operações de coleta no âmbito de SOCMINT. O mesmo autor argumenta que as soluções não são fáceis e não envolvem somente a comunidade de inteligência para prospectar as soluções de mais inovação e criatividade que as mesmas tecnologias permitem.

Nesse cenário virtual caracterizado por oferta abundante de dados, Stottlemyre [39] sugere que a principal mudança na atividade de coleta de informações decorre da imbricação entre OSINT e HUMINT através da denominada *crowdsourcing intelligence*, uma nova disciplina especializada de coleta a partir das interações humanas em redes sociais.

Entretanto, segundo [28, 41], a coleta de informações em ambiente virtual dependeria, além das habilidades de OSINT e SOCMINT, do processo de aquisição da fonte humana que é estruturado em quatro fases interdependentes que se iniciam com:

1. a identificação da potencial fonte;
2. o desenvolvimento da colaboração;
3. o recrutamento; e
4. o desligamento.

Essas fases configuram um processo que se inicia com ações para confirmar se a eventual fonte humana tem acesso às informações demandadas, ações que estão relacionadas com o conhecimento de dados biográficos e profissionais, bem como motivações e características comportamentais para o desenvolvimento de estratégias para estabelecer vínculos e confiança mútua, de modo a convencer a fonte humana a fornecer informações repercutindo no mundo real as relações virtuais.

As referências encontradas indicam a prevalência do interesse de pesquisa no desenvolvimento de ferramentas para explorar o potencial da oferta de dados em ambientes de Internet. A existência de mais estudos nessa área respaldaria a elaboração de estratégias capazes de integrar duas ou mais disciplinas de coleta a fim de incrementar a produção de subsídios para ações de segurança cibernética.

Desde a fase preliminar, observou-se que a coleta de dados para a produção de subsídios informacionais destinados à ações de segurança cibernética ocorre através da pesquisa direta em buscadores on-line, sites de mídias sociais e bancos de dados de acesso restrito. Com grande impacto no resultado das ações de enfrentamento à criminalidade, a qualidade da informação depende das habilidades dos profissionais de segurança cibernética na coleta de informações, com pouca integração durante a fase de *all-sources collection*.

Ao selecionar como objeto de pesquisa uma unidade com a proposta de analisá-la em profundidade [52], a escolha da metodologia de estudo para desenvolver uma proposta de *framework* baseado em *human intelligence* (HUMINT) e *open source intelligence* (OSINT) para coleta de informações em ambiente virtual tem caráter exploratório, descritivo e qualitativo em relação ao grupo alvo sobre o grupo-alvo composto pelos profissionais em de segurança cibernética que executam a coleta de informações em ambientes de Internet.

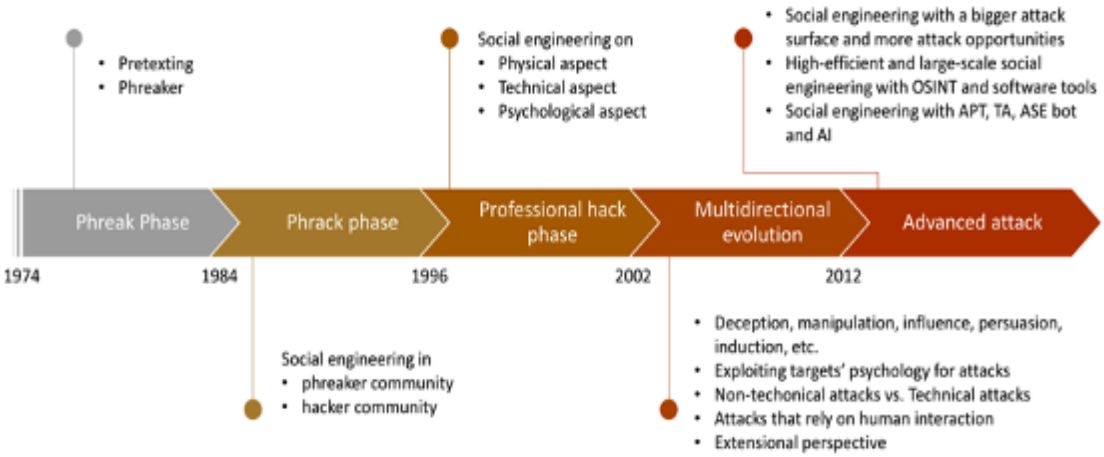
2.4 ENGENHARIA SOCIAL

No domínio da segurança da informação, usuários são frequentemente classificados como o "elo mais fraco"das políticas de segurança cibernética [53], de modo que infraestruturas são atacadas a partir de ações descuidadas de usuários que revelam senhas, abrem anexos de mensagens maliciosas ou visitam sites inidôneos. O termo mais utilizado para definir o processo de abordagem e comprometimento do usuário é engenharia social. A engenharia social, segundo Hasle et al [54], pode ser considerado o "*hacking* de seres humanos ao persuadir ou enganar usuários para obter informações ou assistência voluntária para acessar infraestruturas físicas ou sistemas tecnológicos que podem ser mais ou menos resistentes

Embora os ataques de engenharia social representem 13 por cento do comprometimentos da empresas pesquisadas no Relatório Anual da ISACA's *State of Cibersecurity* do ano de 2022, os ataques baseadas em manipulação psicológica de usuários para obtenção informações ou indução de comportamento começaram a ser noticiados no ano de 1974 sob o nome de *pretexting*, quando um grupo de *hackers* chamados de "*phreaks* de telefone"descobriu como hackear o maior sistema telefônico do mundo, a rede da *American Telephone & Telegraph* (AT&T) fundada por Graham Bell, através de abordagens de operadores de comutação centrais da companhia telefônica que eram persuadidos a colaborar com o hackers [55].

A figura 2.3 mostra a evolução do conceito de engenharia social desde o ano de 1974 quando o conceito de manipulação de pessoas era relacionado a *pretexting* até ataques avançados que a partir de 2012 passam a utilizar o conceito proposto por [48]:

Figura 2.3: *The conceptual evolution of social engineering in cybersecurity*



Fonte:(WANG ET AL, 2020)[48]

1. *FASE PHREAK*: utilização do *pretexting* como abordagem de persuasão de operadores comutação da AT&T através da utilização de falsa identidade.
2. *FASE PHRACK*: além da persuasão por *pretexting* induzir atitudes, os *hackers* começam a buscar acesso a sistema de computadores através do engano.
3. *FASE DE PROFISSIONALIZAÇÃO*: aumento dos casos de abordagens mais complexas e diversas através de aproximações físicas e desenvolvimento de meios técnicos baseados em mensagens para remessas de *phishing* e *trojans*, além do aprimoramento da influência social para manipulação.
4. *FASE DA EVOLUÇÃO DO CONCEITO MULTIDIRECIONAL*: disseminação generalizada de ataques de engenharia social com atração do conhecimento do grande público com surgimento de várias descrições conceituais baseadas em abordagens interdisciplinares como ciência da computação e redes, tecnologia da informação, psicologia e neurolinguística, bem como melhoramentos nos ataques através do aprimoramento conceitual.
5. *FASE DE ATAQUES AVANÇADOS*: a partir de 2012 com o desenvolvimento de ecossistemas baseados em tecnologia da informação com ampla utilização de redes sociais, internet das coisas, conexão de internet em plantas industriais, dispositivos móveis e vestíveis, ocorre o enfraquecimento da zona de segurança e a conformação de uma superfície de ataque muito mais ampla.

A vulnerabilidade de usuários a abordagens baseadas em engenharia social não é um problema recente. Contudo, o comportamento dos usuários no contexto das redes sociais tem afetado a capacidade de detectar tentativas de manipulação resultando em novas características e novos elementos que justificam pesquisas mais aprofundadas sobre aspectos comportamentais, cognitivos e socioemocionais que se relacionam com a capacidade a capacidade dos usuários de repelir abordagens que apelem para aspectos emocionais [56].

Segundo Albladi, a susceptibilidade para abordagens de engenharia social pode ser medida, proporcional ou inversamente proporcional, sob a perspectiva dos hábitos do usuário, da sua percepção das interações

e da perspectiva socioemocional [56].

2.4.1 Perspectiva dos hábitos

O envolvimento com os serviços de comunicação das redes sociais, pelo percentual de amigos exclusivos das redes sociais indicam proporcionalmente a predisposição do usuário para abordagens de engenharia social. Por outro lado, a susceptibilidade a abordagens de engenharia social é inversamente proporcional à experiência em redes sociais.

1. Nível de envolvimento reflete que o usuário pode ser menos cuidadoso com as orientações para selecionar as associações requeridas ou recebidas de outros usuários, resultando em maior susceptibilidade a manipulação proveniente de usuários maliciosos. O nível de envolvimento também é indicado pelo tempo que usuário dedica à interação na rede social.

2. Número de conexões está relacionado com a satisfação que usuários manifestam ao conectar-se em uma rede social e ampliar sua rede de contatos. com uma grande quantidade aumenta a possibilidade de do comprometimento de informações restritas através da divulgação para um contato confiável que também será lido por um usuário malicioso.

3. A experiência em redes sociais, em contrapartida, diminui a susceptibilidade a abordagens de engenharia social. Incluído ao contexto da rede social, a experiência no mundo virtual é preditor de comportamento cuidadoso.

2.4.2 Perspectiva da autopercepção

A forma como o usuário percebe sua atuação nas redes sociais com relação ao risco, a sua competência e seu conhecimento de cibercrime influencia sua susceptibilidade a abordagens de engenharia social.

1. A percepção do risco relacionada ao gerenciamento das interações em redes sociais tem direta influência no cuidado ao utilizar serviços online e diminui a vulnerabilidade do usuário às ameaças.

2. A competência do usuário é definida como conhecimento sobre a tecnologia e sua capacidade de usá-la para evitar situações de risco.

3. A experiência em redes sociais, em contrapartida, diminui a susceptibilidade a abordagens de engenharia social. Incluído ao contexto da rede social, a experiência no mundo virtual é preditor de comportamento cuidadoso.

2.4.3 Perspectiva Socioemocional

Nesta perspectiva, os fatores intrínsecos e subjetivos influenciam na adoção de comportamentos de riscos em ambientes de redes sociais, principalmente, confiança e motivação, focos desta parte da pesquisa.

1. A predisposição para confiar nos relacionamentos construídos em redes sociais é um preditor de que de que o usuário A percepção do risco relacionada ao gerenciamento das interações em redes sociais tem direta influência no cuidado ao utilizar serviços online e diminui a vulnerabilidade do usuário às ameaças.

2. A motivação que impulsiona pessoas para exposição a riscos em redes sociais através de elevados níveis de interação está relacionada com a o atendimento de necessidades pessoais vinculadas a aceitação e recompensa

Workman [57] ressalta que os aspectos emocionais são explorados para construir um relacionamento amigável com o usuário sob ataque para estimular o desenvolvimento de confiança, considerando que seres humanos processam estímulos de maneira diferente e o resultado desses processos podem resultar em mudanças de atitudes e, consequentemente, de comportamentos diante de restrições normativas ou regulamentares.

O "*hackeamento* de humanos", segundo Barrett [58], consiste na avaliação de um indivíduo ou grupo de indivíduos a partir da coleta do maior possível de informações sobre que possibilite conhecer os selecionados, principalmente, das fragilidades que puderam ser utilizadas para reforçar a conexão entre o atacante e o usuário, de modo a garantir o estabelecimento de chamado *rapport*.

O estabelecimento do *rapport* pode depender da utilização de uma abordagem *pretexting*, onde o atacante se apresenta com outra identidade que possa representar autoridade hierárquica em algum sentido, de modo a convencer o usuário a fornecer dados sensíveis [59]. Após estabelecer o contato inicial, o atacante busca ampliar a conexão com o usuário através de demonstração de familiaridade para explorar a tendência dos seres humanos de desenvolver simpatia para com os que lhes parecem semelhantes.

A preparação e o lançamento de abordagens baseadas em engenharia social dependem do desenvolvimento conjunto de técnicas baseadas em teorias psicológicas conjugadas com aspectos tecnológicos da segurança da informação. Sob o aspecto da abordagem psicológica, Tetri e Vourinen [60] ressaltam que a simples transposição de conceitos da psicologia para o campo da segurança cibernética pode criar problemas, a exemplo da persuasão utilizada por vendedores induzir eventuais compradores que se diferencia da indução para violação de políticas de segurança da informação.

Os ataques de engenharia social têm pessoas como objetivo preferencial muito mais que estruturas de tecnologia de informação, por isso a maioria dos ataques se baseia na personificação de falsa identidade que pode variar desde o contato direto e até complexas montagens de "histórias de cobertura"[61] que utilizam os seguintes vetores de ataque:

1. E-mail: e-mails de *phishing/spear-phishing* usados para manipular um alvo para que visite um site malicioso ou abra um arquivo malicioso.

2. Telefone: *phishing* de voz ou "*vishing*", usado para extrair informações diretamente ou persuadir um alvo a interagir com um site malicioso ou arquivo entregue anteriormente.

3. Físico: obter acesso físico ao site de uma organização ou sistemas, através do uso de um pretexto enganoso, ou entrega de mídia física (por exemplo, queda de um pendrive).

Edwards et al (2017) ressalta que a principal fonte de informações para preparação desses ataques são coletas realizadas em fontes abertas que são separadas em dois tipos principais:

1. Bootstrap: são dados utilizados para iniciar o ataque, a partir do direcionamento para um indivíduo ou grupo de indivíduos, indicados como mais suscetíveis e segregados dos menos vulneráveis, a exemplo de pessoal dos times de Tecnologia da informação e segurança.

2. Intensificador: são dados que podem ser utilizados para aumentar a eficácia do ataque, a exemplo de menção de um contato pessoal da pessoa sob ataque ou fato ou atividade de interesse do alvo.

As premissas básicas do estudo estão relacionadas com o processo de aquisição de informação através de fonte humana em ambiente virtual, conforme referências a literatura consultada, envolve o colaborador como fornecedor de informações e o controlador na posição do profissional de segurança cibernética encarregado de estabelecer o gerenciamento das relações interpessoais relacionadas com:

1. Personalidade do controlador: a literatura consultada relaciona a existência de perfis de personalidade caracterizados por confiança, extroversão, estabilidade emocional e bom avaliador de pessoas [62, 63, 64, 65], assim como habilidade para confrontar informantes [66].

2. Rapport: habilidade de estabelecer relações interpessoais com base na empatia e no respeito, capacidade de escutar e entender [67, 68, 69, 13].

3. Motivação do informante: a precisa identificação dos elementos que impulsionam o informante é apontado por vários autores como fundamental para a relação de colaboração [70]. Estudos conduzidos nos EUA e no Reino Unido identificaram uma série de motivações, incluindo leniência no sistema de justiça criminal, recompensa financeira, vingança ou remoção de concorrentes criminosos, e até mesmo motivações morais ou interpessoais [12].

4. Estabelecendo a cooperação: este aspecto ressalta que um informante não é um entrevistado com acesso a informação, é um participante ativo na coleta e processamento de informações e deve ter a centralidade da atenção [67, 12, 62, 71, 72, 73].

5. Obtenção de informações: baseada em técnicas de elicitação de informações, inclui métodos de entrevista direcionados para o fornecimento de informações e como pode ser melhorado [74, 13, 75, 76].

6. Detecção de informações falsas: envolve ação deliberada para detectar e coibir a transmissão de informação falsa [77].

7. Engenharia social: entre hackers e profissionais de segurança cibernética a prática de acessar e controlar informações sigilosas é denominada de “engenharia social” [78, 79] envolvem um amplo espectro de artifícios para comprometer sistemas de segurança da informação [80]. Sob a ótica dos

perpetradores de crimes online, a engenharia social é aplicada de modo casual e fluído por pessoas com "atributos" relacionados com o contexto social, as fragilidades da natureza humana, as complexidades das redes sociais, o papel das convenções sociais e as limitações do processamento e raciocínio humano. Esses atributos são organizados em quatro categorias correspondentes a diferentes estágios de ação de engenharia social [81, 82, 5].

O estudo recente de Kevin Steinmetz et al (83) demonstra que muitos "engenheiros sociais" aplicam seus golpes após um planejamento rigoroso que considera todas as circunstâncias que podem influenciar na susceptibilidade da potencial vítima, na apresentação e nas chances de sucesso. Assim, o planejamento envolve as seguintes etapas:

1. Pesquisa: consiste na reunião do maior número possível de informação que possa ajudar o "engenheiro social" a montar o golpe com base em pretextos, identidade falsa ou montagem de um cenário.

2. Avaliação: apreciação das habilidades decorrentes e experiencias anteriores ou formação técnica relacionada com a vítima.

3. *Timing*: consiste em avaliar o tempo de duração do golpe para construir "pretextos" fortes o bastante para suportar a duração do golpe.

4. Proximidade: o estabelecimento de proximidade com a vítima consiste na "construção de relacionamento" para dar a impressão de se tratar um participante integrado na network da vítima ou de uma pessoa amável. Para a consecução desse objetivo, podem ser utilizadas as seguintes técnicas:

   (a) *Rapport*: estratégia de aproximação que evita abordagem incisiva, agressiva ou intimidativa, com preferência para apresentações sutis e amáveis.

   (b) Integração ao networking: consiste em adotar medidas para simular a participação no meio social da vítima.

5. Ativação: é o estágio posterior ao estabelecimento de proximidade, quando o perpetrador efetiva manobras para obter a atitude esperada, relacionada ao fornecimento de informações críticas ou de atitudes favoráveis ao "engenheiro social". As principais técnicas são pedidos de ajuda ou oferta de incentivos.

6. Ocultação: consiste em medidas adotados pelo perpetrador para evitar o surgimento de suspeitas caso a o estágio da ativação resulte em insucesso, desse modo, evita-se a detecção e mantem-se a integridade do ardil para reutilização posterior.

As técnicas de engenharia social resumidas acima, são passíveis de utilização de por profissionais de segurança pública, em algumas situações pode ser, inclusive, preferenciais. Contudo, em havendo importância do gerenciamento de fontes humanas para a ações de segurança cibernética, há que se discutir e implementar técnicas para gerenciar essas fontes de forma efetiva e profissional.

As operações de coleta de informações derivadas de fontes humanas têm seu centro de gravidade nos "agentes controladores" que são responsáveis pela coleta de informações e pelas próprias fontes humanas. (23). Na perspectiva das fontes humanas, de forma geral, pode-se utilizar a pirâmide de sensitividade proposta por Herman para designar a quantidade de fontes e o valor informacional na área de HUMINT (22).

As características mencionadas têm que ser aplicáveis e independentes da plataforma envolvida, de modo que as estratégias de coleta sejam centradas nas caraterísticas principais utilizadas por engenheiros sociais em um ataque de ciclo completo, a exemplo das definições adotadas pelo CESG(2015) que abrangem 3 fases distintas.

2.4.4 Fase 1 - Preparação

1. A escolha do alvo depende da quantidade de informações sobre a pessoa e seu ambiente, inclusive, sobre a seleção de um ou mais atributos de vulnerabilidade. Entende-se que a segmentação de alvos por escolha de vulnerabilidades implica na seleção explícita de um indivíduo ou grupo de usuários. Por outro lado, a segmentação ampla consiste na seleção do maior número possível de indivíduos.

2. A estratégia de abordagem define qual vetor de aproximação será utilizado e quais informações serão necessárias para manter esse canal conectado ao alvo. Via de regra, essas abordagens são direcionadas par ao alvo através de contatos por redes sociais, os quais podem ser automatizados ou manuais

2.4.5 Fase 2 - Exploração

1. A obtenção e a manutenção da colaboração do alvo dependem da capacidade de manter o alvo conectado com o engenheiro social, seja através de elementos visuais ou comportamentais. Os elementos visuais estão relacionados com o aspecto da abordagem que pode ser definida tanto pela aparência quanto pelos elementos gráficos relacionados aos engenheiros sociais.

2. Os elementos comportamentais relacionam com a obtenção de colaboração a partir da indução do usuário a acreditar no aspecto legítimo das ações do engenheiro social e da interface utilizada.

2.4.6 Fase 3 - Execução

1. O alcance dos objetivos estabelecidos implica na paralisação de outras investidas para evitar a detecção potencial da busca por colaboração. Nesse sentido, a persistência da abordagem é definida pelo CESG (2015) como *One-off*. Por outro lado, abordagens contínuas podem ser executadas para ampliar o espectro da busca por usuários susceptíveis, embora represente o risco de detecção.

2. A segmentação da execução em etapas está relacionada com o grau de persistência do usuário alvo. A abordagem *single-step* requer que o usuário inicie a colaboração de forma imediata após a primeira abordagem. A presença de resistência do usuário implica na adoção de uma abordagem *multistep* para reforçar os elementos de indução do usuário à colaboração.

3 METODOLOGIA

A revisão de literatura e da pesquisa em bases de dados bibliográficas demonstra que a maioria dos estudos está direcionado para o entendimento dos ataques de engenharia social baseados em informações coletadas com a utilização de ferramentas de OSINT, com prevalência do interesse de pesquisa na atuação dos "engenheiros sociais". A existência de mais estudos nessa área respaldaria a elaboração de estratégias capazes de integrar as disciplinas de HUMINT e OSINT a fim de incrementar a produção de subsídios para proteção cibernética e atuação estatal na repressão de delitos que se desenvolvem em ambiente virtual.

Desde a fase preliminar, observou-se que a coleta de dados para a produção de subsídios informacionais ocorre através da pesquisa direta em buscadores *online*, sites de mídias sociais e bancos de dados de acesso restrito, com pouca ou nenhuma utilização das informações para gestão de fontes humanas. Com grande impacto no resultado das ações de prevenção de ataques, a qualidade da informação depende mais das habilidades dos profissionais de segurança cibernética que efetuam a coleta de informações do que da integração de mais de uma disciplina de coleta, no caso, da integração de fontes humanas com a fontes abertas.

Para a compreensão das dinâmicas informacionais que ocorrem na coleta de informações, o estudo de caso é o mais indicado para o desenvolvimento do entendimento e compreensão dos fenômenos organizacionais pouco conhecidos e para o desenvolvimento de novas abordagens sem a exigência de representatividade ou mensuração de frequências estatísticas, além de proporcionar a generalização analítica dos fenômenos pesquisados [84].

Trata-se, portanto, de uma lide empírica para investigar um fenômeno contemporâneo inserido no seu contexto real sem limites definidos entre o fenômeno e o contexto [84] onde persiste a necessidade de se adotar uma estratégia de pesquisa que tenha por objeto a análise detalhada de um fenômeno [52]), que relacionam a metodologia de estudo de caso com a necessidade de “iluminar uma decisão ou um conjunto de decisões” através do estudo da motivação do processo de coleta de informações e aproximação, em ambiente virtual, de usuários para compreender como se pode implementar e com quais resultados possíveis [85].

A pesquisa de um fenômeno em seu ambiente natural através da observação e da aplicação de um questionário estruturado constitui o estudo de caso como metodologia qualitativa [86] com foco no caráter subjetivo do objeto estudado para compreender as dinâmicas de comportamento do grupo-alvo, de modo a fornecer descrições, testar teorias ou gerar teorias e modelos [87, 88], através de uma estratégia de pesquisa concentrada na investigação de um tópico empírico seguindo um conjunto de procedimentos pré-especificados em etapas para pesquisas direcionadas para casos:

1. críticos que dependam de testes para hipóteses ou teorias previamente desenvolvida;
2. extremos ou únicos que necessitem de estudos aprofundados para determinar se as proposições de

uma teoria são corretas ou se há explanações alternativas mais relevantes e, finalmente; e

3. reveladores que ainda não tenham sido submetidos a investigação científica para produção de conhecimentos relacionados aos componentes de um fenômeno [89].

Nesse sentido, considerando a ausência de um paradigma unificado para avaliar a aplicação de técnicas de engenharia social, uma ampla classe de tópicos é intrinsecamente importante para estabelecer o eventual nexo causal entre cada tópico estudo [90].

3.1 ESTUDO DE CASO

Ao selecionar como objeto de pesquisa uma unidade com a proposta de analisá-la em profundidade [52], a escolha da metodologia de estudo para desenvolver a pesquisa A intersecção entre OSINT e HUMINT tem caráter exploratório, descritivo e qualitativo em relação ao grupo alvo sobre o grupo-alvo composto pelos policiais que executam a coleta de informações em ambientes de Internet.

As premissas básicas do estudo de caso são:

1. Elaboração de estudo no campo da segurança cibernética relacionado à utilização de abordagem de gestão de fontes humanas combinada com ferramentas de fontes abertas por profissionais de segurança cibernética; e
2. Melhoria da produção de informação para suporte à proteção de ativos de infraestrutura de tecnologia da informação.

Após a realização de pesquisa bibliográfica, explorou-se a atividade de coleta por meio de entrevistas semiestruturadas para obtenção de contribuições ao entendimento das dinâmicas informacionais que envolvem os procedimentos de OSINT.

Consoante o caráter exploratório da pesquisa, optou-se por fazer um questionário estruturado para explorar os tópicos básicos com possibilidade de o respondente fazer comentários de forma bastante aberta, de modo a aprofundar o tema de acordo com a perspectiva do respondente. Foram apresentadas 21 perguntas vinculadas às boas práticas selecionadas e que abordavam os seguintes tópicos:

1. Definição de OSINT;
2. Definição de HUMINT;
3. Oportunidades decorrentes do uso de OSINT;
4. Oportunidades decorrentes do uso de HUMINT;
5. Dificuldades decorrentes do uso de OSINT;
6. Dificuldades decorrentes do uso de HUMINT;

7. Oportunidades decorrentes da combinação de OSINT e HUMINT; e

8. Dificuldades decorrentes da combinação de OSINT e HUMINT.

Os questionários *online* foram distribuídos através do *Microsoft Forms* entre abril e maio de 2023 e foram respondidos por 15 policiais que atuam na coleta de dados em ambientes virtuais para atender demandas na produção de conhecimentos de inteligência.

Para a análise de dados, os itens mencionados na literatura foram tratados como categorias analíticas, onde estão agrupadas as boas práticas identificadas nas obras consultadas e em trechos dos dados coletados, que não estão presentes na literatura consultada, mas que foram indicadas com impactantes na coleta de dados na Internet. No espaço para comentários, forma colhidas as sugestão e opiniões pessoais dos respondentes, as quais foram utilizadas para reformular o texto das boas práticas selecionadas.

A tabela 3.1, a seguir, contém a lista de boas práticas identificadas, agrupadas em torno das categorias analíticas Institucional e Procedimental e que representam a versão inicial do *framework* de boas práticas.

Tabela 3.1: *Framework* para interação em redes sociais (versão inicial)

Boas práticas	**Autor**
Implementação de manuais de vigilância em ambiente virtual.	Estudo de Caso
Implementação de manuais de coleta de dados em ambiente virtual.	Estudo de Caso
Orientar sobre a coleta de informações estratégicas para suporte ao processo decisório.	Estudo de Caso
Promover especialização nas disciplinas de coleta.	Cepik (2003), Carter (2004), Lowenthal (2009), Herman (1996)
Estabelecer o grau de relevância dos dados coletados.	Libor Benes (2012)
Estimular a adoção de ferramentas automatizadas para coleta de dados.	Janta, Hamdan e Othman (2009)
Difundir as possibilidades de coleta em ambiente cibernético.	Clark (2013)
Promover a interação entre as disciplinas de coleta.	Siman-Tov; Tal (2015)
Avaliar a eficiência da tecnologia frente as disciplinas de coleta não tecnológicas	Mercado (2004), Omand, Bartlett e Miller (2012)
Avaliar a eficiência das disciplinas de coleta não tecnológica frente diante do advento da tecnologia.	Gioe (2017), Zeng et al. (2007)
Avaliar medidas de interação entre OSINT e HUMINT.	Stottlemyre (2015), Gioe (2017)
Obter colaboração através do estímulo emocional.	Haste, 2005; Dhillon, 2007
Demonstrar simpatia para influenciar pessoas.	Workman, 2007
Desenvolver capacidade de estabelecer *rapport*.	Barret, 2003
Desenvolver capacidade de representar outra identidade.	Robinson (2021), Dubin (2002)
Desenvolver capacidade de mentir.	Hancok (1998)
Desenvolver capacidade de construir familiaridade.	DOLAN, 2004 (2009)
Desenvolver capacidade de oferecer contrapartidas.	Schifreen (2006)
Desenvolver capacidade de observação discreta.	Thornburgh (2004)
Desenvolver habilidade de promover validação social.	Schiller et al (2007)
Desenvolver habilidade para estabelecer autoridade.	Thomas (2003)
Utilização de de Jargão.	Lafrance (2004),

4 VALIDAÇÃO DO *FRAMEWORK*

As boas práticas selecionadas no referencial teórico e encetadas no estudo de caso, assim como o contexto fático verificado, permitiram a confirmação das boas práticas que seguem apresentadas na forma final de cada prática dentro das categorias previamente identificadas. Os questionários para validação do *framework* foram submetidos aos especialistas no final de abril/2023 e início de maio/2023. Foram convidados 40 especialistas, dos quais 15 responderam os questionários de forma completa. O questionário foi concebido com afirmações a serem respondidas através uma escala *Likert* com seis alternativas com equivalência entre 1 e 6, com 1 correspondendo a "discordo totalmente" e 6 "concordo completamente".

Ao fim e ao cabo, a avaliação dos especialistas confirmou as boas práticas. Contudo, algumas apresentaram alto grau de discordância. A partir das respostas dos participantes, apresenta-se a forma final de cada boa prática, ressaltando que não é muito claro o limiar de cada uma das boas práticas, inclusive, algumas podem perpassar o contexto de outra ou podem ser classificadas na categoria Psicológico ou Procedimental. Portanto, as boas práticas foram agrupadas, classificadas e sistematizadas em duas categorias: psicológico e procedimental, ambas com 20 boas práticas.

4.1 PROCEDIMENTAL

Essa categoria é constituída de nove boas práticas que se referem aos arranjos organizacionais para acomodar as estruturas de coleta de dados.

4.1.1 Implementação de manuais de coleta de dados em ambiente virtual

A primeira boa prática apresentada afirmava que a implementação de manuais de coleta em ambiente virtual é um nivelador de conhecimentos e habilidades para os profissionais de segurança cibernética que atuam na coleta de dados em fontes abertas, de nodo a normatizar e estimular a ampliação da coleta." Os quinze respondentes concordaram completamente com a implementação de manuais de vigilância em ambiente virtual. Nos comentários, todos fizeram referência à necessidade de uniformização e atualização de procedimentos através da edição de manuais e protocolos para atuação policial em ambiente virtual. Diante disso, essa boa prática manteve a redação: **"Implementar manuais de coleta em ambiente virtual"**.

4.1.2 Implementação de manuais de vigilância em ambiente virtual

A segunda boa prática dessa categoria postulava que implementação de manuais de vigilância em ambiente virtual padroniza as ações de dos profissionais de segurança cibernética no sentido de relacionar quais técnicas poderiam levar aos melhores resultados. Os quinze respondentes concordaram completamente com a implementação de manuais de coleta de dados em ambiente virtual. Nos comentários, todos fizeram

referência à necessidade de uniformização e atualização de procedimentos através da edição de manuais e protocolos para coleta de informações em ambiente virtual. Diante disso, essa boa prática manteve a redação: “Implementar manuais de coleta de vigilância ambiente virtual”.

4.1.3 Orientar sobre a coleta de informações estratégicas para suporte ao processo decisório

A terceira boa prática da categoria Psicológico propunha a expedição de orientações sobre a coleta de informações estratégicas para suporte ao processo decisório, pois embora este estudo de caso tenha direcionamento meramente operacional, é possível que informações sobre identificação de pessoas acabem tangenciando os interesses dos gestores da organização. Os quinze especialistas concordaram parcialmente com a afirmação. Nos comentários, 12 especialistas afirmaram que a eventual colaboração deve permanecer circunscrita a aspectos gerais das situações sob escrutínio operacionais da segurança cibernética.

Três respondentes comentaram que a colaboração deve se restringir aos ambientes operacionais, além diferenciar “indivíduos externos” entre membros de outros órgãos de segurança pública e cidadãos do povo não vinculados a organizações policiais. Dessa forma, essa boa prática foi decomposta em: “Promover especialização nas disciplinas de coleta” para garantir que a informação produzida a partir do cidadão comum se diferencie da produção decorrente de agentes policiais vinculado a outros órgãos de segurança que estaria relacionada com outra boa prática: “Avaliar a implementação de grupos de colaboração composto por indivíduos vinculado a outras organizações policiais”.

4.1.4 Estabelecer o grau de relevância dos dados coletados

Por sua vez a quarta boa prática propõe que o estabelecimento do grau de relevância dos dados coletados referencia e orienta todos os membros da equipe de segurança cibernética sobre avaliação da informação de modo objetivo. A totalidade dos especialistas concordou parcialmente com a implantação de medidas de produtividade. Nos comentários, dez respondentes afirmaram que o termo “métrica de produtividade” se relaciona com medidas impossíveis de implementação, eis que para determinados casos o nome de uma pessoa pode ser uma informação crucial, em outros a placa de um carro, o horário de um evento, uma imagem fotográfica, etc. Em cada situação operacional, cada um desses subsídios pode ter uma dificuldade diferente para obtenção que não pode ser avaliada de acordo com uma regra geral. Assim, alterou-se essa boa prática para: “Avaliar a implementação de critérios de utilidade da informação”. A mudança é para contemplar a utilidade da informação que deve anteceder o controle quantitativo do nível de produtividade.

4.1.5 Estimular a adoção de ferramentas automatizadas para coleta de dados

A sexta boa prática da categoria Psicológica propunha adotar políticas de estímulo à adoção de ferramentas automatizadas para coleta de dados”. Os quinze respondentes concordaram completamente com o mapeamento contínuo de dificuldades inerentes a implementação de um sistema de *crowdsourcing*. Nos

comentários, todos mencionaram o estabelecimento de confiança dos participantes quanto ao efetivo uso da informação para resolução de crimes, assim como na segurança da informação processada através de uma plataforma de *crowdsourcing*. Com este *feedback*, manteve-se a redação: “Estimular a adoção de ferramentas automatizadas para coleta de dados”.

4.1.6 Promover a interação entre as disciplinas de coleta

A sexta boa prática dessa categoria afirma a necessidade de se promover a interação entre as disciplinas de coleta, principalmente, entre HUMINT e OSINT, eis o *locus* por excelência o meio das redes sociais, onde a produtividade tem demonstrado a necessidade utilização de técnicas de recrutamento e gestão de fontes humanas. Para esta boa prática, os respondentes concordaram completamente, inclusive com o oferecimento de comentários sobre a utilização de ferramentas de rede sociais como o Microsft Teams para manutenção de grupos especializados na troca de informações passíveis de utilização em investigações policiais. Com a concentração de respostas manteve-se a redação: “Promover a interação entre as disciplinas de coleta”.

4.1.7 Promover pesquisas com a finalidade melhorar a vigilância de dados na Internet

A sétima boa prática pressupunha que a promoção de pesquisas com a finalidade melhorar a vigilância de dados na Internet, de modo a inserir no cotidiano da segurança cibernética a prospecção acadêmica de novos meios e técnicas para garantir a permanente atualização das ações de busca de dados e informações. Contudo, houve grande dispersão nas respostas enviadas, com 9 respondentes recomendando a segmentação dessa boa prática em “Avaliar a eficiência das disciplinas de coleta não tecnológicas” e "Avaliar a eficiência das disciplinas de tecnológicas". Os outros 6 participantes defenderam que a promoção de pesquisas somente na área de técnicas de HUMINT, eis que a tecnologia é um aspecto organizacional permanente. Diante concordância dos respondentes com a promoção de pesquisas relacionadas ao incremento da capacidade de vigilância tecnológica segregou-se a boa prática em “Avaliar a eficiência das disciplinas de coleta não tecnológicas” e "Avaliar a eficiência das disciplinas de tecnológicas".

4.1.8 Avaliar a eficiência das disciplinas de coleta não tecnológica frente diante do advento da tecnologia

A oitava boa prática afirmava que avaliações de eficiências direcionadas os resultados das disciplinas de coleta não tecnológica frente diante do advento da tecnologia”. Neste item, seguindo a tendência da oitava boa prática, os especialistas também demonstraram elevada dispersão: quatro concordaram, cinco concordaram parcialmente e seis discordaram parcialmente. Nos comentários, os especialistas abordaram algumas questões como a possibilidade de outros usuários da plataforma perceberem o uso investigativo ou por pessoas interessadas em fornecer informações erradas para desorientar a atuação dos profissionais de segurança cibernética ou comprometer a segurança física da pessoa que participa da plataforma. Com base neste *feedback*, alterou-se a redação da boa prática para: “Avaliar a utilização de recursos tecnológicos compatíveis com a busca em fontes abertas”.

4.1.9 Avaliar medidas de interação entre OSINT e HUMINT

A nona e última boa prática da categoria Psicológica estabelecia que medidas de interação entre OSINT e HUMINT necessitam de avaliação prévia para verificar a aplicabilidade e eficiência. Neste item, os especialistas foram unânimes na implementação de ampla avaliação de metodologias para conjugar práticas de OSINT com HUMINT. Diante disso, essa boa prática manteve a redação: "Avaliar medidas de interação entre OSINT e HUMINT".

Com relação às alterações produzidas a partir do *feedback* dos especialistas respondentes, a dimensão psicológica do *framework* de boas práticas inicialmente estava composta de oito práticas, das quais sete sofreram alterações, das quais uma foi decomposto em duas boas práticas e apenas uma permaneceu como na versão inicial. As práticas versam sobre os arranjos institucionais para acomodar um sistema de colaboração para produção de informações subsidiárias à gestão de investigações policiais.

4.2 PSICOLÓGICO

A segunda categoria contempla 11 boas práticas relacionadas aos aspectos psicológicos da coleta, processamento e difusão dos dados obtidos em ambientes virtuais.

4.2.1 Obter colaboração através dos estímulos emocionais

A primeira boa prática apresentada na categoria Procedimental afirmava que a obtenção de colaboração depende da exploração de emocional. Os quinze respondentes concordaram completamente com a utilização de conhecimento de psicologia comportamental para convencer usuários a iniciar atividade de colaboração o profissional de segurança cibernética. Nos comentários, todos fizeram referência à necessidade de uniformização e atualização de procedimentos através da edição de manuais e protocolos para atuação em ambiente virtual. Diante disso, essa boa prática manteve a redação: "Obter colaboração através dos estímulos emocionais".

4.2.2 Demonstrar simpatia para influenciar pessoas

Por sua vez, a segunda boa prática dessa categoria propunha que o desenvolvimento da habilidade de causar simpatia durante a interação e redes sociais como uma necessidade para influenciar pessoas". Os quinze respondentes concordaram completamente com a implementação de manuais de coleta de dados em ambiente virtual. Nos comentários, todos fizeram referência à promoção de sessões com psicólogos especializados para aprimorar a técnica de desenvolver simpatia. Diante disso, essa boa prática manteve a redação: "Demonstrar simpatia para influenciar pessoas".

4.2.3 Desenvolver capacidade de estabelecer *rapport*

A terceira boa prática afirmava o *rapport* bem desenvolvido é primordial para estabelecer a interação e a futura confiança. Os quinze respondentes concordaram completamente sobre a importância para iniciar e manter a interação com eventuais colaboradores. Diante disso, essa boa prática manteve a redação: “Orientar sobre a coleta de elementos probatórios (fontes de prova e meios de prova)”.

4.2.4 Desenvolver capacidade de representar outra identidade

A quarta boa prática defende que a capacidade assumir e representar outra identidade é primordial para estabelecer qualquer abordagem inicial. Os quinze respondentes concordaram completamente sobre o desenvolvimento da habilidade de representar outra identidade. Diante disso, essa boa prática manteve a redação: “Desenvolver capacidade de representar outra identidade”.

4.2.5 Desenvolver capacidade de mentir

A quinta boa prática propunha o desenvolvimento da capacidade de mentir é primordial para atuação encoberta em redes sociais. Os quinze respondentes concordaram completamente sobre a necessidade de desenvolver a capacidade de mentir. Diante disso, essa boa prática manteve a redação: “Desenvolver capacidade de mentir”.

4.2.6 Desenvolver capacidade de construir familiaridade

A sexta boa prática afirmava que a capacidade de construir "familiaridade” deve ser desenvolvida para garantir o sucesso da abordagem inicial. Os quinze respondentes concordaram completamente sobre a necessidade de "parecer familiar". Diante disso, essa boa prática manteve a redação: “Desenvolver capacidade de construir familiaridade”.

4.2.7 Desenvolver capacidade de oferecer contrapartidas

A sétima boa prática pressupunha que o "oferecimento de contrapartidas"é um pré-requisito para manter a colaboração em níveis satisfatórios. Nos comentários, os especialistas anotam que nenhuma relação de estabelece através de mão única, sendo necessária fazer concessões de para o usuário manter-se na colaboração. Diante disso, essa boa prática manteve a redação: “Desenvolver capacidade de oferecer contrapartidas”.

4.2.8 Desenvolver capacidade de observação discreta

A oitava boa prática relacionava a capacidade de observar de forma discreta favorece a coleta de informações. Os quinze respondentes concordaram totalmente e anotaram que muitas informações não objeto da interação entre o profissional de segurança cibernética, mas em postagens do colaborador com outros

usuários ou imagens disponibilizadas. Diante disso, essa boa prática manteve a redação: “Desenvolver capacidade de observação discreta”.

4.2.9 Desenvolver habilidade de promover validação social

A nona boa prática pressupõe o processo de validação social como aspecto fundamental para manutenção da interação em nível de colaboração. Os quinze especialistas concordaram totalmente com necessidade de construir uma interação baseada na validação das ações dos colaboradores. Diante disso, essa boa prática manteve a redação: “Desenvolver habilidade de promover validação social”.

4.2.10 Desenvolver habilidade para estabelecer autoridade

A décima primeira boa prática afirmava que a percepção de autoridade configura uma interação baseada em referências de hierarquia. Os quinze especialistas concordaram completamente sobre o desenvolvimento do senso de autoridade e anotaram é complementar ao referenciamento hierárquico. Diante disso, essa boa prática manteve a redação: “Desenvolver habilidade para estabelecer autoridade”.

4.2.11 Utilização de Jargão

A décima segunda boa prática referia a utilização do jargão da área de atuação do colaborador como ferramenta construir e manter a confiança entre o profissional de segurança cibernética e o usuário colaborador. Os quinze especialistas concordaram completamente sobre a necessidade de desenvolver discurso condizente com a área do colaborar para manter o *rapport*. Diante disso, essa boa prática manteve a redação: “Utilização de de Jargão”.

4.3 VERSÃO FINAL DO *FRAMEWORK*

Após a verificação com os especialistas, o *framework* ficou com duas dimensões e 21 boas práticas, são elas: institucional (9) e procedimental (12). As práticas podem ser observadas na Tabela 4.1.

Tabela 4.1: *Framework* para interação em redes sociais

Boas práticas	**Autor**
Implementação de manuais de vigilância em ambiente virtual.	Estudo de Caso
Implementação de manuais de coleta de dados em ambiente virtual.	Estudo de Caso
Orientar sobre a coleta de informações estratégicas para suporte ao processo decisório.	Estudo de Caso
Promover especialização nas disciplinas de coleta.	Cepik (2003), Carter (2004), Lowenthal (2009), Herman (1996)
Estabelecer o grau de relevância dos dados coletados.	Libor Benes (2012)
Estimular a adoção de ferramentas automatizadas para coleta de dados.	Janta, Hamdan e Othman (2009)
Difundir as possibilidades de coleta em ambiente cibernético.	Clark (2013)
Promover a interação entre as disciplinas de coleta.	Siman-Tov; Tal (2015)
Avaliar a eficiência da tecnologia frente as disciplinas de coleta não tecnológicas	Mercado (2004), Omand, Bartlett e Miller (2012)
Avaliar a eficiência das disciplinas de coleta não tecnolóogica frente diante do advento da tecnologia.	Gioe (2017), Zeng et al. (2007)
Avaliar medidas de interação entre OSINT e HUMINT.	Stottlemyre (2015), Gioe (2017)
Obter colaboaração através do estímulo emocional.	Haste, 2005; Dhillon, 2007
Demonstrar simpatia para influenciar pessoas.	Workman, 2007
Desenvolver capacidade de estabelecer *rapport*.	Barret, 2003
Desenvolver capacidade de representar outra identidade.	Robinson (2021), Dubin (2002)
Desenvolver capacidade de mentir.	Hancok (1998)
Desenvolver capacidade de construir familiaridade.	DOLAN, 2004 (2009)
Desenvolver capacidade de oferecer contrapartidas.	Schifreen (2006)
Desenvolver capacidade de observação discreta.	Thornburgh (2004)
Desenvolver habilidade de promover validação social.	Schiller et al (2007)
Desenvolver habilidade para estabelecer autoridade.	Thomas (2003)
Utilização de de Jargão.	Lafrance (2004),

O quadro anterior demonstra a relação de boas práticas articuladas entre si e agrupadas nas dimensões Instrumental e Procedimental, de modo que possam balizar o planejamento e a tomada de decisões relacionadas às ações de busca de informações em ambiente *online*.

5 CONCLUSÃO

O cenário da segurança cibernética tem sido configurado, como área de intenso uso de tecnologia, por ações relacionadas a soluções industriais e de pesquisa concentradas nas camadas físicas e lógicas. Desta forma, o consenso que o sistema estará seguro se essas três camadas estiverem com níveis de conformidade apropriados fica fragilizado, eis que as dificuldades para conceituar "segurança" das interfaces humanas e sociais.

Nesse sentido, essa dissertação foi elaborada com foco nas necessidades dos profissionais de segurança cibernética de melhorar seu processo de *all-sources intelligence* , buscando-se explorar a menos dispendiosa disciplina de coleta, fontes abertas (*open-source intelligence*), com a mais antiga, fontes humanas (*human intetelligence*) unidas através das possibilidades tecnológicas da "engenharia social".

Com relação ao alcance do objetivo geral da dissertação: **proposição de um *framework* que permita classificar este tipo de usuário de acordo com perfis predefinidos**, após a análise da literatura disponível e dos dados obtidos sobre a atuação dos agentes policiais encarregados de coletar informações, é possível afirmar que existem boas práticas que podem melhorar a coleta de informações através da combinação de OSINT e HUMINT, mas, considerando que não há soluções técnicas prontas para uso, o *framework* proposto representa um modelo balizador para a atividade de coleta de informações na internet.

Para cumprir o objetivo geral proposto, foram estabelecidas e percorridas três etapas básicas:

A primeira consistiu em estabelecer categorias de análise e estudar como ocorre o tratamento de dados na atividade de inteligência policial, através da descrição da atividade de inteligência policial inserida no contexto da *web* com realce às peculiaridades da coleta de informações em fontes abertas, que resultou na identificação de boas práticas, na coleta de informações em fontes abertas, com enfoque na abordagem de engenharia social.

A segunda fase compreendeu a análise da coleta de informações em OSINT associada à coleta através de fontes humanas, a partir de um estudo de caso com agentes policiais que atuam na área de tratamento de informações coletadas através de fonte abertas e fontes humanas.

A partir da análise dos resultados do estudo de caso, surge a terceira etapa, que se destinou a avaliar a aplicabilidade das boas práticas selecionadas. De fato, o estudo de caso objetivou identificar quais iniciativas e ações podem se constituir em boas práticas para o tratamento de dados na atividade de inteligência policial.

Ao se investigar as oportunidades proporcionadas pelas boas práticas que contribuem para melhoramentos na coleta de dados, o estudo de caso demonstrou que os arranjos institucionais têm impactado mais o desempenho na atividade de coleta, inclusive através da solução de dificuldades nas ações interagências

e na falta de unidades organizacionais especializadas em coleta.

Conforme demonstrado na subseção 4.3, que contém a versão final do *framework* de Boas Práticas, o resultado principal desta pesquisa se reflete na seleção de 21 (vinte e uma) ações agrupadas nas categorias Institucional e Procedimental.

Na categoria Institucional, apareceram como ameaças, a interação com outros órgãos de segurança pública e o envolvimento de pessoas externas da organização. Por sua vez, na dimensão Procedimental está concentrada a maior parte das oportunidades para ampliação da coleta, a partir de ferramentas de engenharia social.

Como demonstrado, as dificuldades são muitas e abrangem um amplo espectro que vai de gestões materiais como implementação de estruturas físicas e lógicas até mudanças na cultura de funcionamento de unidades de inteligência.

Assim, o estudo de caso possibilitou a compreensão da urgência para institucionalização dos aparatos organizacionais de coleta de informação em ambiente virtual, cabendo a nós, pesquisadores, policiais e gestores, a tarefa de pensar, repensar, refletir e dialogar o "como fazer" a atividade de coleta de informação em ambiente virtual.

5.1 TRABALHOS FUTUROS

Os resultados obtidos demonstram o uso disseminado de abordagens *multi-sources* para coleta de informações, inclusive, com combinação de metodologias de gerenciamento de fontes humanas e fontes abertas. A prevalência dessas metodologias, combinadas ou não, impele os profissionais de segurança cibernética na busca de melhoramentos das ações de coleta, de modo a incrementar precisão e a efetividade das informações com a adoção de métodos automatizados para coletar informações e selecionar potenciais colaboradores. Assim, a proposição do *framework* não se esgota em si e exige nas pesquisas relacionadas com metodologias que possam melhorar o perfilamento e a identificação de pessoas como aplicações para coleta de biometria comportamental ou até propor novas ontologias para segurança cibernética.

REFERÊNCIAS BIBLIOGRÁFICAS

1 KUEHL, D. The information revolution and the transformation of warfare. In: *The History of Information Security*. [S.l.]: Elsevier, 2007. p. 821–832.

2 DIOGENES, Y.; OZKAYA, E. *Cybersecurity??? Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics*. [S.l.]: Packt Publishing Ltd, 2018.

3 HOLT, T. J.; BOSSLER, A. M. Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge, 2015.

4 PIPLAI, A.; MITTAL, S.; JOSHI, A.; FININ, T.; HOLT, J.; ZAK, R. Creating cybersecurity knowledge graphs from malware after action reports. *IEEE Access*, IEEE, v. 8, p. 211691–211703, 2020.

5 LEUKFELDT, E. R. Cybercrime and social ties: Phishing in amsterdam. *Trends in organized crime*, Springer, v. 17, p. 231–249, 2014.

6 BACK, S.; SOOR, S.; LAPRADE, J. Juvenile hackers: An empirical test of self-control theory and social bonding theory. *International Journal of Cybersecurity Intelligence & Cybercrime*, v. 1, n. 1, p. 40–55, 2018.

7 GLENNY, M. *Darkmarket: Cyberthieves, cybercops and you*. [S.l.]: Random House, 2011.

8 DINUCCI, D. Design & new media: Fragmented future-web development faces a process of mitosis, mutation, and natural selection. *PRINT-NEW YORK-*, BRUIL & VAN DE STAAIJ, v. 53, p. 32–35, 1999.

9 NARASSIGUIN, A.; SARGENT, S. Data science for influencer marketing: feature processing and quantitative analysis. *arXiv preprint arXiv:1906.05911*, 2019.

10 DICTIONARY, M.-W. Merriam-webster. *On-line at http://www. mw. com/home. htm*, v. 8, n. 2, 2002.

11 PECH, Y. Vers une intelligence cyber? penser le renseignement augmenté dans la noosphère. *Prospective et stratégie*, Cairn/Softwin, n. 1, p. 73–102, 2019.

12 BILLINGSLEY, R. *Covert Human Intelligence Sources: The'unlovely'Face of Police Work*. [S.l.]: Waterside Press, 2009.

13 NUNAN, J.; STANIER, I.; MILNE, R.; SHAWYER, A.; WALSH, D. Eliciting human intelligence: police source handlers' perceptions and experiences of rapport during covert human intelligence sources (chis) interactions. *Psychiatry, psychology and law*, Taylor & Francis, v. 27, n. 4, p. 511–537, 2020.

14 PURPURA, P. *Terrorism and homeland security: An introduction with applications*. [S.l.]: Elsevier, 2011.

15 GROSE, P. *Gentleman Spy: The Life of Allen Dulles*. [S.l.]: Univ of Massachusetts Press, 1996.

16 BLAIR, A. M. *Too much to know: Managing scholarly information before the modern age*. [S.l.]: Yale University Press, 2010.

17 SARACEVIC, T. Relevance reconsidered. In: *Proceedings of the second conference on conceptions of library and information science (CoLIS 2)*. [S.l.: s.n.], 1996. p. 201–218.

18 BUSH, V.; THINK, A. W. M. The atlantic monthly. *As we may think*, v. 176, n. 1, p. 101–108, 1945.

19 NILSSON, N. J.; HILPISCH, Y.; YAO, M.; ZHOU, A.; JIA, M.; BAESEN, B.; VLASSELAER, V. V.; VERBEKE, W. The quest for ai: A history of ideas and achievements. *Erişim adresi: http://ai. standford. edu/˜ nilsson/(Özgün eser 2009 tarihlidir)*, 2010.

20 HAUBEN, R. The birth and development of the arpanet. *Michael Hauben and Ronda Hauben, Netizens: On the History and Impact of Usenet and the Internet. John Wiley and Sons*, 1997.

21 OMAND, D.; BARTLETT, J. C. miller (2012),'introducing social media intelligence (socmint)'. *Intelligence & National Security*, v. 27, n. 6.

22 HERMAN, M. *Intelligence power in peace and war*. [S.l.]: Cambridge University Press, 1996.

23 CEPIK, M. *Espionagem e democracia*. [S.l.]: FGV Editora, 2003.

24 CARTER, D. L. *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies*. [S.l.]: US Department of Justice, Office of Community Oriented Policing Services . . . , 2004. v. 16.

25 GONCALVES, J. B. *Atividade de inteligência e legislação correlata*. [S.l.]: Impetus, 2009.

26 LOWENTHAL, M. M. *Intelligence: From secrets to policy*. [S.l.]: CQ press, 2022.

27 CLARK, R. M. *Intelligence analysis: a target-centric approach*. [S.l.]: CQ press, 2019.

28 UCAK, H. *Law enforcement intelligence recruiting confidential informants within "religion-abusing terrorist networks"*. [S.l.]: Virginia Commonwealth University, 2012.

29 HARDING, L. *The Snowden files: The inside story of the world's most wanted man*. [S.l.]: Guardian Faber Publishing, 2014.

30 BALL, J. Nsa's prism surveillance program: how it works and what it can do. *The Guardian*, v. 8, 2013.

31 BUMP, P. The uk tempora program captures vast amounts of data–and shares with nsa. *The Atlantic Wire. Retrieved*, v. 23, 2013.

32 CLARKE, R. Dataveillance by governments: The technique of computer matching. *Information Technology & People*, MCB UP Ltd, v. 7, n. 2, p. 46–85, 1994.

33 DONOHUE, L. K. The dawn of social intelligence (socint). *Drake L. Rev.*, HeinOnline, v. 63, p. 1061, 2015.

34 ZHANG, D.; GUO, B.; LI, B.; YU, Z. Extracting social and community intelligence from digital footprints: an emerging research area. In: SPRINGER. *Ubiquitous Intelligence and Computing: 7th International Conference, UIC 2010, Xi'an, China, October 26-29, 2010. Proceedings 7*. [S.l.], 2010. p. 4–18.

35 WASSERMAN, S.; FAUST, K. Social network analysis: Methods and applications. Cambridge university press, 1994.

36 WILLIAMS, H. J.; BLUM, I. *Defining second generation open source intelligence (OSINT) for the defense enterprise*. [S.l.], 2018.

37 BENES, L. Osint, new technologies, education: Expanding opportunities and threats. a new paradigm. *Journal of Strategic Security*, JSTOR, v. 6, n. 3, p. 22–37, 2013.

38 STEELE, R. D. Open source intelligence. In: *Handbook of intelligence studies*. [S.l.]: Routledge, 2007. p. 147–165.

39 STOTTLEMYRE, S. A. Humint, osint, or something new? defining crowdsourced intelligence. *International Journal of Intelligence and CounterIntelligence*, Taylor & Francis, v. 28, n. 3, p. 578–589, 2015.

40 BRABHAM, D.; CROWDSOURCING, M. *Press Essential Knowledge*. [S.l.]: Cambridge, 2013.

41 LOWENTHAL, M. M.; CLARK, R. M. *The five disciplines of intelligence collection*. [S.l.]: Sage, 2015.

42 SALMINEN, J. et al. The role of collective intelligence in crowdsourcing innovation. Lappeenranta University of Technology, 2015.

43 CLARK, R. M. Perspectives on intelligence collection. *Journal of US Intelligence Collection*, v. 20, p. 47–52, 2013.

44 TAL, A.; SIMAN-TOV, D. Humint in the cybernetic era: gaming in two worlds. *Military and Strategic Affairs*, v. 7, n. 3, p. 96, 2015.

45 GIOE, D. V. 'the more things change': Humint in the cyber age. *The Palgrave handbook of security, risk and intelligence*, Springer, p. 213–227, 2017.

46 CUMMINGS, C. *What's the Point of Spies?* 2015. Disponível em: <http://www.telegraph.co.uk/culture/books/bookreviews/11648193/Whats-the-point-of-spies.html>. Acesso em 12 dez 2018.

47 MERCADO, S. A venerable source in a new era: Sailing the sea of osint in the information age. *Studies in Intelligence*, v. 48, n. 3, p. 45–55, 2004.

48 WANG, F.-Y.; CARLEY, K. M.; ZENG, D.; MAO, W. Social computing: From social informatics to social intelligence. *IEEE Intelligent systems*, IEEE, v. 22, n. 2, p. 79–83, 2007.

49 ELLIS, C. A.; GIBBS, S. J.; REIN, G. Groupware: some issues and experiences. *Communications of the ACM*, ACM New York, NY, USA, v. 34, n. 1, p. 39–58, 1991.

50 WU, P. Impossible to regulate: Social media, terrorists, and the role for the un. *Chi. J. Int'l L.*, HeinOnline, v. 16, p. 281, 2015.

51 BRIGGS, R.; STRUGNELL, A. Radicalisation: The role of the internet. *Policy Planners' Network Working Paper, London: Institute for Strategic Dialogue*, 2011.

52 GODOY, A. S. A pesquisa qualitativa e sua utilização em administração de empresas. *Revista de administração de empresas*, SciELO Brasil, v. 35, p. 65–71, 1995.

53 MULLIGAN, D. K.; SCHNEIDER, F. B. Doctrine for cybersecurity. *Daedalus*, MIT Press One Rogers Street, Cambridge, MA 02142-1209, USA journals-info . . . , v. 140, n. 4, p. 70–92, 2011.

54 HASLE, H.; KRISTIANSEN, Y.; KINTEL, K.; SNEKKENES, E. Measuring resistance to social engineering. In: SPRINGER. *Information Security Practice and Experience: First International Conference, ISPEC 2005, Singapore, April 11-14, 2005. Proceedings 1*. [S.l.], 2005. p. 132–143.

55 LAPSLEY, P. Phreaking out ma bell. *IEEE Spectrum*, IEEE, v. 50, n. 2, p. 30–35, 2013.

56 ALBLADI, S. M.; WEIR, G. R. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, SpringerOpen, v. 3, n. 1, p. 1–19, 2020.

57 WORKMAN, M. Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, Taylor & Francis, v. 16, n. 6, p. 315–331, 2007.

58 BARRETT, N. Penetration testing and social engineering: Hacking the weakest link. *Information Security Technical Report*, Elsevier, v. 8, n. 4, p. 56–64, 2003.

59 ALEXANDER, M.; WANNER, R. Methods for understanding and reducing social engineering attacks. *SANS Inst*, v. 1, p. 1–32, 2016.

60 TETRI, P.; VUORINEN, J. Dissecting social engineering. *Behaviour & Information Technology*, Taylor & Francis, v. 32, n. 10, p. 1014–1023, 2013.

61 EDWARDS, M.; LARSON, R.; GREEN, B.; RASHID, A.; BARON, A. Panning for gold: Automatically analysing online social engineering attack surfaces. *computers & security*, Elsevier, v. 69, p. 18–34, 2017.

62 KLEINMAN, S. M. Kubark counterintelligence interrogation review: Observations of an interrogator. *Interrogation: Science and Art*, v. 209, p. 95–140, 2006.

63 REDLICH, A. D.; WILFORD, M. M.; BUSHWAY, S. Understanding guilty pleas through the lens of social science. *Psychology, Public Policy, and Law*, American Psychological Association, v. 23, n. 4, p. 458, 2017.

64 RUSSANO, M. B.; NARCHET, F. M.; KLEINMAN, S. M. Analysts, interpreters, and intelligence interrogations: Perceptions and insights. *Applied cognitive psychology*, Wiley Online Library, v. 28, n. 6, p. 829–846, 2014.

65 RUSSANO, M. B.; NARCHET, F. M.; KLEINMAN, S. M.; MEISSNER, C. A. Structured interviews of experienced humint interrogators. *Applied cognitive psychology*, Wiley Online Library, v. 28, n. 6, p. 847–859, 2014.

66 BIRKETT, J.; PIKE, G. *Exploring rapport and communication methods between Covert Human Intelligence Sources (CHIS) and CHIS Handlers throughout a CHIS lifecycle*. [S.l.]: National Crime Agency London, 2017.

67 ALISON, L.; ALISON, E.; NOONE, G.; ELNTIB, S.; WARING, S.; CHRISTIANSEN, P. The efficacy of rapport-based techniques for minimizing counter-interrogation tactics amongst a field sample of terrorists. *Psychology, public policy, and law*, American Psychological Association, v. 20, n. 4, p. 421, 2014.

68 ALISON, L.; ALISON, E. Revenge versus rapport: Interrogation, terrorism, and torture. *American psychologist*, American Psychological Association, v. 72, n. 3, p. 266, 2017.

69 HUMANN, M.; TEJEIRO, R.; RATCLIFF, J.; CHRISTIANSEN, P. et al. Observing rapport-based interpersonal techniques (orbit) to generate useful information from child sexual abuse suspects. *Investigative interviewing: Research & Practice*, v. 12, n. 1, p. 22–39, 2022.

70 DABNEY, D. A.; TEWKSBURY, R. *Speaking truth to power: Confidential informants and police investigations*. [S.l.]: Univ of California Press, 2016.

71 SCHIRMAN, N.; YOUSEF, M. H. *The green prince*. [S.l.]: Rapid Eye Movies HE GmbH, 2015.

72 STORM, M.; CRUICKSHANK, P.; LISTER, T. *Agent storm: my life inside al-Qaeda*. [S.l.]: Penguin UK, 2014.

73 YOUSEF, M. H.; BRACKIN, R. Son of hamas: A gripping account of terror. *Betrayal, Political Intrigue, and Unthinkable Choices (Carol Stream: Tyndale House, 2010)*, p. 253–255, 2010.

74 BRANDON, S. E. Towards a science of interrogation. *Applied Cognitive Psychology*, Wiley Online Library, v. 28, n. 6, p. 945–946, 2014.

75 NUNAN, J.; STANIER, I.; MILNE, R.; SHAWYER, A.; WALSH, D.; MAY, B. The impact of rapport on intelligence yield: police source handler telephone interactions with covert human intelligence sources. *Psychiatry, Psychology and Law*, Routledge, v. 29, n. 1, p. 1–19, 2022.

76 VRIJ, A.; GRANHAG, P. A. Eliciting information and detecting lies in intelligence interviewing: An overview of recent research. *Applied Cognitive Psychology*, Wiley Online Library, v. 28, n. 6, p. 936–944, 2014.

77 VRIJ, A. *Detecting lies and deceit: Pitfalls and opportunities*. [S.l.]: John Wiley & Sons, 2008.

78 HADNAGY, C. *Social engineering: The art of human hacking*. [S.l.]: John Wiley & Sons, 2010.

79 MITNICK, K. D.; SIMON, W. L. *The art of deception: Controlling the human element of security*. [S.l.]: John Wiley & Sons, 2003.

80 ICCC, F. *2019 Internet Crime Report*. 2019. Disponível em: <https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf>.

81 CORNISH, D. B. The procedural analysis of offending and its relevance for situational prevention. *Crime prevention studies*, v. 3, n. 1, p. 151–196, 1994.

82 CORNISH, D. B.; CLARKE, R. V. Analyzing organized crimes. *Rational choice and criminal behavior: Recent research and future challenges*, Routledge New York, NY, v. 32, p. 41–63, 2002.

83 STEINMETZ, K. F.; PIMENTEL, A.; GOE, W. R. Performing social engineering: A qualitative study of information security deceptions. *Computers in Human Behavior*, Elsevier, v. 124, p. 106930, 2021.

84 ROBERT, Y. et al. Estudo de caso: planejamento e métodos. *Porto Alegre: Bookman*, 2001.

85 SCHRAMM, W. Notes on case studies of instructional media projects. ERIC, 1971.

86 CRESWELL, J. W.; CLARK, V. L. P. *Pesquisa de Métodos Mistos-: Série Métodos de Pesquisa*. [S.l.]: Penso Editora, 2015.

87 BONOMA, T. V. Case research in marketing: opportunities, problems, and a process. *Journal of marketing research*, SAGE Publications Sage CA: Los Angeles, CA, v. 22, n. 2, p. 199–208, 1985.

88 EISENHARDT, K. M. Building theories from case study research. *Academy of management review*, Academy of Management Briarcliff Manor, NY 10510, v. 14, n. 4, p. 532–550, 1989.

89 SILVA, G. O. da; OLIVEIRA, G. S. de; SILVA, M. M. da. Estudo de caso único: uma estratégia de pesquisa. *Revista Prisma*, v. 2, n. 1, p. 78–90, 2021.

90 GERRING, J. *Pesquisa de estudo de caso: princípios e práticas*. [S.l.]: Editora Vozes, 2019.