DISSERTAÇÃO DE MESTRADO PROFISSIONAL

PROPOSTA DE UM MÉTODO PARA INTELIGÊNCIA DE FONTES ABERTAS: VALORES E PRINCÍPIOS PARA UMA ATIVIDADE ÉTICA E PROFISSIONAL

Roberto Tanabe

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSTA DE UM MÉTODO PARA INTELIGÊNCIA DE FONTES ABERTAS: VALORES E PRINCÍPIOS PARA UMA ATIVIDADE ÉTICA E PROFISSIONAL

PROPOSAL OF A METHOD FOR OPEN-SOURCE INTELLIGENCE: VALUES AND PRINCIPLES FOR AN ETHICAL AND PROFESSIONAL ACTIVITY

Roberto Tanabe

Orientador: Prof. Dr. Robson de Oliveira Albuquerque, FT/UnB

Coorientador: Prof. Dr. Demétrio Antônio da Silva Filho, FT/UnB

PUBLICAÇÃO: PPEE.MP.028

BRASÍLIA-DF

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

PROPOSTA DE UM MÉTODO PARA INTELIGÊNCIA DE FONTES ABERTAS: VALORES E PRINCÍPIOS PARA UMA ATIVIDADE ÉTICA E PROFISSIONAL

Roberto Tanabe

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

Banca Examinadora

Prof. Robson de Oliveira Albuquerque, Ph.D, FT/UnB _____
Orientador

Prof. Rafael Rabelo Nunes, Ph.D, FT/UnB _____
Examinador Interno

Prof. Leandro Alves Neves, Ph.D, Unesp _____
Examinador externo

FICHA CATALOGRÁFICA

TANABE, ROBERTO
PROPOSTA DE UM MÉTODO PARA INTELIGÊNCIA DE FONTES ABERTAS: VALORES E PRINCÍPIOS PARA UMA ATIVIDADE ÉTICA E PROFISSIONAL [Distrito Federal] 2022.
xvi, 77 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. OSINT	2. INTELIGÊNCIA
3. FONTES ABERTAS	4. MÉTODO
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

TANABE, R. (2022). *PROPOSTA DE UM MÉTODO PARA INTELIGÊNCIA DE FONTES ABERTAS: VALORES E PRINCÍPIOS PARA UMA ATIVIDADE ÉTICA E PROFISSIONAL* . Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 77 p.

Roberto Tanabe
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Aos meus pais, Hiromiti e Ivanilza, que me deram a vida, me criaram com amor e dedicaram-se, com sacrifícios, para educar os seus filhos e netos.

AGRADECIMENTOS

À Agência Brasileira de Inteligência (ABIN), por meio da Escola de Inteligência (Esint), que em parceria com a Universidade de Brasília (UnB) proporcionou esta oportunidade de cursar o Mestrado Profissional na linha de pesquisa em Segurança e Inteligência Cibernética, com área de interesse em Inteligência em fontes de dados abertas (OSINT).

Aos meus chefes na Superintendência Estadual Amazonas (SEAM) pela compreensão com o tempo necessário ao desenvolvimento deste trabalho.

Também aos meus colegas de SEAM que souberam entender as minhas ausências e "carregaram o piano" do trabalho diário, muitas vezes, sem a minha participação.

Aos meus filhos Vinícius (15), Helena (11) e Luiza (7), e à minha esposa Daisy, que se esforçaram para entender que mesmo presente eu estava virtualmente ausente.

Em especial ao meu professor orientador Robson de Oliveira Albuquerque, ao qual fui apresentado como um colega de trabalho, que conheci de verdade nos momentos de dificuldade e que passou a ser um amigo nessa caminhada do Mestrado Profissional.

Muito obrigado a todos.

RESUMO

A Inteligência de fontes abertas (OSINT) tem sido definida na literatura de várias maneiras diferentes. Não há consenso sobre o assunto dada a variedade de tipos de informações, usos, métodos e técnicas envolvidas. Para a comunidade de Inteligência, ela é reconhecida, principalmente, como uma disciplina de coleta com foco em fontes abertas. Para os praticantes de OSINT, há uma forte associação do termo com ferramentas. A comunidade científica, no que lhe concerne, tenta aproximar o conceito de OSINT das técnicas e métodos especializados, não apenas no panorama da coleta, mas também na análise. Considerando estes aspectos, o objetivo desta dissertação é propor um método que aproxime OSINT de uma atividade profissional suportada por valores, princípios e técnicas especializadas. O conceito de OSINT, neste sentido, está mais orientado para um fluxo de trabalho que descreve como os requisitos definidos por um usuário são atendidos para assessorar um processo de tomada de decisão. Dessa forma, OSINT como um método é orientada por um conjunto de princípios que orienta um padrão de comportamento baseado na ética e em uma metodologia que pretende atingir um desempenho profissional. Este comportamento é sustentado por valores que são padrões morais em benefício da sociedade. Com estes pressupostos em mente, este trabalho posiciona o OSINT no ciclo de Inteligência e apresenta os princípios que a apoiam como disciplina, amplia o escopo do que a literatura de referência apresenta como ferramentas de OSINT, e fornece argumentação para que a função de coleta tenha a mesma atenção dada à análise. Os resultados demonstram que: os princípios encontrados na literatura de referência não são suficientes e precisam de outros norteadores como a prevenção de *burnout*, a flexibilidade e a prontidão; ao contrário do que se costuma associar, as disciplinas de coleta também são de processamento e análise, e OSINT não deve ser a primeira fonte de coleta, mas sim o arquivo interno de cada organização; o problema da sustentabilidade das ferramentas pode ser minimizado com critérios objetivos de segurança, confiabilidade e legalidade; é preciso reconhecer a importância de coletores de Inteligência assim como é feito com os analistas; e que o método proposto organiza a execução de OSINT dentro de um ciclo de Inteligência que considera múltiplas fontes.

ABSTRACT

Open Source Intelligence (OSINT) has been defined in the literature in several different ways. There is no consensus on the subject, given the variety of information types, uses, methods, and techniques involved. To the Intelligence community, it is primarily recognized as a collection discipline with a focus on open-sources. For OSINT practitioners, there is a strong association of the term with tools. The scientific community, in turn, tries to bring the OSINT concept closer to specialized techniques and methods, not only in the collection landscape, but also in analysis. Considering these aspects, the aim of this dissertation is to bring the practice of OSINT closer to specific methods supported by specialized values, principles and techniques. The concept of OSINT, in this sense is more oriented towards a workflow that describes how user-defined requirements are met to assist a decision-making process. Thus, OSINT as a method is guided by a set of principles that drives a pattern of behavior based on ethics and a methodology that aims to achieve professional performance. This behavior is underpinned by values that are moral standards for the benefit of society. With these assumptions in mind, this work places OSINT in the intelligence cycle and presents the principles that support it as a discipline, expands the scope of what the reference literature presents as OSINT tools, and provides argumentation for giving the collection function the same attention given to analysis. The results show that: the principles found in the reference literature are not sufficient and need other guideposts such as burnout prevention, flexibility and readiness; contrary to what is usually associated, collection disciplines are also processing and analysis disciplines, and OSINT should not be the first collection source, but rather the internal archive of each organization; the problem of tool sustainability can be minimized with objective criteria of security, reliability and legality; the importance of Intelligence collectors must be recognized just as it is done with analysts; and that the proposed method organizes OSINT execution within an Intelligence cycle that considers multiple sources.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Acadêmicos, investigadores, profissionais e amadores praticam a Inteligência de Fontes Abertas (*Open-Source Intelligence* - OSINT) como um modo de pesquisa que recorre a vários serviços on-line para coletar a partir de fontes abertas e produzir informações úteis, dessa forma, projetando OSINT como um panóptico da população [20].

As informações de fontes abertas estão disponíveis publicamente e o seu acesso não depende de custos elevados ou tecnologias avançadas. A publicação de informações na *web* e, especialmente, em plataformas de mídias sociais facilitou o seu acesso e aumentou a quantidade de dados disponíveis. Esta ampla disponibilidade elevou o número de investigações *on-line* e promoveu o rápido desenvolvimento de ferramentas para facilitar a obtenção de tais informações. A coleta de informações a partir de fontes abertas é fundamental para a produção de conhecimento que apoie a tomada de decisões.

Tal é essa abundância de informações que a Inteligência de fontes abertas não é mais vista apenas como uma das disciplinas de Inteligência ao lado da *Human Intelligence* (HUMINT) ou da *Imagery Intelligence* (IMINT), mas ascende como uma mentalidade [21] que molda um comportamento com valores e princípios para os profissionais da área e vai ao nível de várias técnicas e ferramentas que popularizam o seu uso para muito além das agências de governos.

Considerando esses pressupostos, deve-se observar que não parece apropriado definir OSINT com base em um conjunto de ferramentas ou uma lista de *sites* e serviços *on-line*. As ferramentas são aceleradoras ou facilitadoras de uma técnica, mas podem ser removidas, inutilizadas ou desatualizadas e tendem a uma abordagem automatizada que obscurece a compreensão do funcionamento das técnicas em favor de um ganho imediato.

OSINT costumava ser entendida como algo restrito a agências de Inteligência de Estado ou serviços secretos de nações. Entretanto, a facilidade de acesso às informações de fontes abertas em meio digital permitiu que qualquer pessoa com acesso à internet se tornasse um potencial praticante de OSINT. E, em função disso, sempre que viável, as características de OSINT estudadas neste trabalho terão a maior abrangência possível, não limitada às agências estatais ou à prática realizada em poucos países. Entretanto, por esta dissertação ser desenvolvida dentro de um Mestrado profissional em parceria com a Escola de Inteligência (Esint) da Agência Brasileira de Inteligência (ABIN), aprofundamentos e exemplos considerarão a realidade do Brasil.

A definição complexa dos limites conceituais de OSINT e as inúmeras possibilidades de explorar as suas técnicas, ferramentas e aplicações, em rápidas e constantes alterações, juntamente com uma ampla e diversificada arena de praticantes, caracterizam uma natureza sempre em mudança deste campo de atuação e fomenta a proliferação de alguns entendimentos equivocados, em especial: o foco em ferramentas ao invés de valores, princípios e métodos; a subestimação da etapa da coleta; e a supervalorização da coleta difícil.

Ferramentas capacitam a execução de uma técnica que é uma forma específica de executar uma tarefa. Um método é uma abordagem sistemática de técnicas e ferramentas em um campo de estudo ou disciplina

[22]. Segundo o dicionário Merriam-Webster, disciplina é um campo de estudo e também um conjunto de princípios que regem um código de conduta ou uma atividade. Na Inteligência, disciplinas também são áreas de coleta definidas que utilizam categorias específicas de recursos técnicos ou humanos [3]. Os princípios são padrões consistentes e mensuráveis para apoiar a profissionalização de uma disciplina e podem ser aplicados de forma constante, enquanto técnicas e ferramentas mudam [7]. Os valores, conforme descritos pelos Fundamentos Doutrinário da Doutrina Nacional da Atividade de Inteligência [2], são padrões morais de comportamento que definem uma ética para a Atividade de Inteligência. As ferramentas utilizadas em OSINT mudam rápida e constantemente como resultado de atualizações das plataformas digitais, as suas estruturas de dados e as suas diversas formas e disponibilidade de acesso.

Reduzir a prática de OSINT à aplicação de ferramentas caracteriza uma abordagem imediatista que, normalmente, leva a realizações de curto prazo. Este aspecto acaba dificultando a prática sustentável de OSINT, implicando em intervalos de treinamento mais curtos e aumentando a dependência dos seus praticantes pelos desenvolvedores destas ferramentas e dos seus custos correspondentes, corroborando com um ciclo insustentável de ferramentas que quebram continuamente.

Uma metodologia pode ser definida como a soma dos métodos, técnicas e procedimentos, que inclusive podem ser automatizados com o suporte de ferramentas específicas utilizadas em uma disciplina [22]. Se um tomador de decisão precisa de conhecimento para que a sua escolha tenha o impacto desejado, ele deve recorrer à Inteligência, que por sua natureza, utiliza métodos bem definidos para gerar conhecimento. Nesse sentido, das incertezas que cercam o mundo real, surgem dados brutos, abundantes em fontes abertas que, no que lhe concerne, precisam seguir um ciclo de Inteligência para se transformar em informações ou novos conhecimentos úteis ao decisor.

A função de análise é indispensável para a produção de Inteligência e implica extrair significado do que foi coletado. Portanto, sem coleta não há análise e, assim como há analistas especializados, há coletores especializados nas suas diversas técnicas e tipos de informações. Geralmente, a etapa da coleta de fontes abertas não depende de tecnologia de ponta e está intensamente ligada ao uso corriqueiro da internet e dos seus principais serviços, como mecanismos de busca, e-mail e plataformas de mídias sociais. A partir disso, surge uma ilusão de que todos têm a disciplina e as habilidades necessárias para coletar fontes abertas em ambientes digitais. Como a coleta é uma etapa indispensável da produção de Inteligência, ela também requer habilidades adquiridas através de treinamentos especializados que distinguem os amadores dos profissionais. O domínio de uma técnica requer anos de aprendizagem e prática [23].

O valor do produto Inteligência não é determinado pela dificuldade na sua produção, mas pelo grau de satisfação do usuário que precisa dele [5]. Como a informação de fonte aberta é a de mais fácil acesso, menor custo e risco, alguns analistas e tomadores de decisões tendem a minimizar o valor de tais informações. O *custo* aqui é usado em um sentido amplo, abrangendo tanto o elemento financeiro como também a praticidade e conveniência. As operações de vigilância física, por exemplo, são dispendiosas para executar e manter e, dependendo do caso, resultados similares podem ser alcançados com OSINT.

Os serviços de Inteligência estimam que cerca de 80% de suas informações vêm de OSINT [24]. Esta porcentagem é difícil de verificar e varia de uma agência para outra, mas é um lembrete de que o desafio é desenvolver protocolos eficazes para inferir informações e verificá-las rápida e eficientemente [25]. Considerando a comunidade de Inteligência dos EUA, também é notável que 80% das informações

que a comunidade de Inteligência precisa estão disponíveis publicamente, mas 95% do orçamento é gasto nos outros 20% de informações que não são de OSINT [26]. Para o governo britânico, o financiamento para pesquisa de fonte aberta pode ser de apenas 1% em relação a outras fontes, e a Inteligência resultante disso está entre 35 e 90% [27].

Dessa forma, OSINT demanda um trabalho focado, estruturado e rigoroso para o qual uma metodologia que descreva as suas etapas possa ser usada como uma abordagem compreensível para todo o processo [9].

1.1 MOTIVAÇÃO E JUSTIFICATIVA

Sem método, um membro da comunidade de Inteligência corre o risco de divagar, atrasar ou perder relevância na corrida com outros membros pela qualidade do produto que a Inteligência deve gerar. A evolução no panorama de todas as mídias, a digitalização das informações e a conectividade mundial não são apreciadas em todo o seu potencial, principalmente ao se considerar critérios de oportunidades de coleta, fazendo do investimento em OSINT uma das recomendações para vencer essa disputa [28].

Sendo OSINT implementável em quase todas as atividades humanas relacionadas à informação [9] e tendo a necessidade de se obter mais dados e informações para a construção de conhecimentos, identifica-se em OSINT vantagens considerando a quantidade de informações disponíveis em fontes abertas, a elevada capacidade computacional disponível para tratar de grandes conjuntos de dados e o avanços das áreas de *big data* e de aprendizagem de máquina para identificar correlações complexas que são normalmente imprevisíveis para humanos [22].

O tema da metodologia de OSINT, tendo como premissa estudos avançados para essa finalidade, é consoante com o artigo 4º da lei 9883 de dezembro de 1999 que diz competir à ABIN "promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência" [29].

Esse alinhamento também é encontrado na Política Nacional de Inteligência (PNI) que lista a "pesquisa e desenvolvimento tecnológico para as áreas de Inteligência e Contrainteligência" como seu VIII instrumento [30]. Também é encontrado como os desafios 2.1 e 2.2, respetivamente, "maior utilização de tecnologias de ponta, especialmente no campo cibernético" e "intensificação do uso de tecnologias de tratamento e análise de grandes volumes de dados (*Big Data e Analytics*)" dos eixos estruturantes definidos pela Estratégia Nacional de Inteligência (ENINT) [31].

1.2 OBJETIVO GERAL

Esta dissertação propõe o desenvolvimento de um método para OSINT que mapeie os processos e os descreva, mediante uma ordem de execução lógica, coerente e fundamentada em valores e princípios éticos, metodológicos e profissionais, que consiga abranger do planejamento à avaliação dos resultados e evidencie a função da coleta com a mesma importância dada à análise.

1.2.1 Objetivos Específicos

Segundo o objetivo geral estabelecido, os seguintes objetivos específicos são tratados:

- Identificar valores e princípios como base para uma abordagem eficiente e sustentável da prática de OSINT;
- Propor um método para OSINT que localize as suas técnicas dentro do processo de produção de Inteligência;
- Defender a profissionalização da função de coleta como uma atividade precursora, distinta e tão importante quanto a de análise; e
- Valorizar OSINT como a disciplina primária da coleta de Inteligência e a que primeiro deve ser ensinada.

1.3 PRINCIPAIS CONTRIBUIÇÕES

Apresenta-se uma revisão bibliográfica da literatura de referência sobre OSINT e a atualização do estado da arte com foco em princípios e métodos e não no uso de ferramentas. Esses princípios para OSINT foram categorizados com origem na literatura especializada e na experiência do autor na prática e na docência da disciplina.

As disciplinas de Inteligência costumam ser relacionadas a etapa da coleta, mas são claras as técnicas que também a colocam nas etapas processamento e análise. Além disso, OSINT não deve ser a primeira fonte de coleta, mas sim o arquivo interno de cada organização.

O estudo das doutrinas nacionais de Inteligência dos EUA e do Brasil permitiu uma interpretação e inferência dos métodos para OSINT das agência de Inteligência desses países. A esses métodos foi adicionada a descrição dos métodos, técnicas e ferramentas para OSINT de outros autores e organizações não estatais.

Isso reforçou a justificativa para o redirecionamento do foco de OSINT das ferramentas para os seus princípios e métodos, objetivando uma prática profissional. Esse ajuste também se dá pela expansão do entendimento do que são ferramentas para OSINT e pela aplicação de critérios objetivos para minimizar o problema da sua inerente insustentabilidade.

Um encadeamento lógico da ordem de execução de OSINT dentro do ciclo de Inteligência considerando outros tipos de fontes é explicado e exemplificado com o relacionamento dos princípios com as partes que compõem o método proposto e o detalhamento em um caso de uso.

A própria lógica da existência das disciplinas de Inteligência é a especialização da sua prática. Se existe uma análise específica para cada tipo de fonte também existe uma forma específica de coletar. Assim, promove-se o reconhecimento da importância de coletores de Inteligência assim como é feito com os analistas.

Um artigo intitulado *OSINT Methods in the Intelligence Cycle* (Métodos para OSINT no ciclo de Inteligência) foi submetido e aceito para o CSEI 2022 *IV CONGRESS OF COMPUTER SCIENCE, ELECTRONICS AND INDUSTRIAL* sendo apresentado no dia 7 de novembro de 2022. Até a data da conclusão desta dissertação, o artigo não foi oficialmente publicado. A cópia do trabalho encontra-se no Apêndice desta dissertação.

1.4 ORGANIZAÇÃO DO TRABALHO

O restante desta dissertação está organizado da seguinte forma: no Capítulo 2 apresentado estão o estado da arte e os principais trabalhos relacionados em OSINT, bem como alguns conceitos necessários para uma melhor compreensão. No Capítulo 3, discute-se sobre o foco em ferramentas, sobre as disciplinas de Inteligência e a sua associação principal à coleta, a localização de OSINT no ciclo de Inteligência, a necessidade de outros princípios para OSINT e a formação de profissionais dedicados, além da apresentação do método proposto. No Capítulo 4, justifica-se o porquê de OSINT não ser a primeira fonte de coleta, mostra-se uma reunião das técnicas e princípios de OSINT tratados neste trabalho, explica-se o uso de métodos como pré requisitos para ferramentas de OSINT, expande-se o entendimento sobre o que são ferramentas de OSINT, apresenta-se a relação entre os valores e as ferramentas, justifica-se a adoção de coletores de Inteligência com a mesma importância dada aos analistas e operacionais, sendo apresentado um caso de uso. Por fim, no Capítulo 5, conclui-se com as principais observações deste documento e a indicação de trabalhos futuros.

2 TRABALHOS RELACIONADOS E ESTADO DA ARTE

Atualmente, OSINT pode ser abordada sob múltiplos pontos de vista. Nos tópicos a seguir, alguns deles são apresentados segundo a literatura de referência.

2.1 CONCEITOS

Para uma melhor compreensão desta dissertação, os principais termos foram revisados e refinados para auxiliar no entendimento mais amplo dos assuntos ligados direta e indiretamente sobre OSINT e as suas relações com a área de Inteligência.

2.1.1 Inteligência

A Inteligência é entendida de forma amplamente diversificada e não há consenso sobre o seu significado [32]. O conceito de inteligência é problemático em alguns idiomas, como o português, porque também se refere à capacidade intelectual de compreender pelo raciocínio [25], enquanto no inglês identifica uma série de práticas utilizadas para obter e usar informações para qualquer finalidade [33]. De modo geral, também representa uma atividade, com o objetivo de produzir conhecimento oportuno, para assessorar um tomador de decisão. O conhecimento produzido por esta atividade também é chamado de Inteligência, assim como a organização que a executa [34]. Este produto de Inteligência é gerado a partir da coleta e análise de informações de várias fontes.

2.1.2 Dado, Informação e Conhecimento

Para os fins deste trabalho, os seguintes termos ficam assim definidos.

- Dado: é a forma primária de informação sem qualquer sentido embutido em si. São fatos, tabelas, gráficos, imagens, etc. que não foram correlacionados, integrados, avaliados ou interpretados [35].
- Informação: definido como uma série de dados organizados de um modo significativo, analisados e processados [36]. Trata-se de um fenômeno, fato ou evento conhecido, algo que está estritamente ligado ao passado e não ao futuro [37].
- Conhecimento: representação de coisa, ou evento real, ou hipotético, de interesse para a Atividade, produzida pelo profissional de Inteligência [2]. A Inteligência como produto é uma expressão do conhecimento.

2.1.3 Ciclo de Inteligência

O *modus operandi* para a produção de Inteligência costuma ser representado por uma sequência de etapas cíclicas, chamado ciclo de Inteligência [2]. Cada organização segue um ciclo próprio cuja quantidade de etapas varia em função do nível de detalhamento que se dá a cada uma delas.

2.1.4 Fonte Aberta

Se a fonte é aberta, então ela está disponível ao público. Ou seja, é acessível a qualquer pessoa por meios legais, incluindo solicitação, observação e compra [5]. Entretanto, a disponibilidade de uma fonte aberta varia entre informações totalmente acessíveis e informações que são apenas parcialmente acessíveis, nas quais, mesmo que o acesso seja público, a origem das informações viria de ações de legalidade duvidosa, tais como vazamentos ou intrusões de redes de computadores que nem sempre são facilmente caracterizadas [38]. O acesso também depende da capacidade do profissional de OSINT em localizar, interpretar e, às vezes, inferir a partir das informações disponíveis [25]. Portanto, mesmo que esteja disponível, pode requerer treinamento especializado.

2.1.5 Informações de Fontes Abertas

Informações de Fontes Abertas (*Open-Source Information* - OSINF) são as informações que qualquer membro do domínio público pode observar, comprar ou solicitar sem requerer status legal especial [7].

2.1.6 Disciplina de Inteligência

Da perspectiva da comunidade de Inteligência, há várias categorias nas quais dividimos os tipo de informações que são coletadas, processadas e analisadas. Chamamos estas categorias de disciplinas de Inteligência (INT) [39]. Uma INT é tipificada pelo emprego de fontes, métodos e técnicas específicas para trabalhar cada tipo de informação.

2.1.7 Fonte Única, Múltipla ou Todas as Fontes

O uso das INTs pode estar direcionado a uma única fonte (*Single-Source*), a múltiplas fontes (*Multi-Source*) [40] e a todas as fontes (*All-Sources*). Essa divisão permite a especialização tanto dos meios de coleta como os de processamento e os de análise [39].

2.1.8 Operação de Inteligência

É definida como as ação especializada e encoberta (secreta) para obter informações que não estão disponíveis publicamente [2]. Entretanto, mesmo que não estejam disponíveis publicamente, isto não significa que as operações de Inteligência não se baseiem em dados e informações coletadas publicamente.

2.2 VALORES E PRINCÍPIOS DA ATIVIDADE DE INTELIGÊNCIA

Segundo Cepik [41], uma profissão se define por sua especificidade cognitiva, valorativa e social, e assim se difere de uma mera ocupação na estrutura produtiva. Para avaliar se a Atividade de Inteligência se caracteriza como uma profissão, teríamos que verificar os seguintes critérios, entre outros: se tal atividade tem requisitos cognitivos específicos, métodos, conteúdos; e se ela gera um código de ética próprio, semelhante a profissões como de medicina, direito e jornalismo. A profissionalização também implica a aquisição constante de novas habilidades para acompanhar o avanço tecnológico [42].

Entendendo a coleta de fontes abertas como uma profissão, há uma consequente necessidade de instrução e treinamento. Para mitigar os riscos de capacitações efêmeras baseadas em ferramentas sem durabilidade conhecida é necessário identificar práticas éticas, metodológicas e profissionais [7]. Como o campo de OSINT está em constante evolução, essa abordagem permitiria um registro mais claro e sustentável do conhecimento necessário para seu desenvolvimento [25].

Na Doutrina Brasileira, valores são definidos como padrões de comportamento morais no interesse da Sociedade e do Estado. Princípios são concepções fundamentais que norteiam a Atividade de Inteligência [2]. Mas, em muitos casos, valores e princípios são usados como sinônimos.

2.2.1 Valores do Código de Ética e Conduta da ABIN

Além da observância dos deveres e atribuições previstas no ordenamento legal e no que regula as atividades dos servidores públicos federais, também cabe aos agentes públicos da ABIN um código de conduta.

O Art. 7º do Código de Ética e Conduta da ABIN [14] apresenta valores éticos que devem nortear a conduta profissional dos agentes públicos da ABIN (Tabela 2.1).

Tabela 2.1: Valores do Código de Ética e Conduta da ABIN [14].

Valores	Descriçao
Lealdade	Fidelidade ao Estado Democrático de Direito e aos seus fundamentos.
Imparcialidade	Isenção, no exercício da atividade de Inteligência, de juízos de valor decorrentes de interesses ou convicções pessoais de caráter filosófico, ideológico, religioso, político, societário ou corporativo.
Profissionalismo	Dedicação, compromisso e empenho nas atividades desenvolvidas e no cumprimento da missão institucional, somados à busca contínua de aperfeiçoamento pessoal e profissional.
Cooperação	Soma de esforços compartilhados.
Segurança	Empenho constante no emprego de medidas que assegurem o tratamento adequado de assuntos sigilosos e a integridade física dos agentes públicos e minimizem riscos no desenvolvimento das ações de Inteligência.
Excelência do Produto	Esforço para que o produto da ABIN seja ímpar e oportuno.

2.2.2 Princípios da Atividade de Inteligência da Doutrina Nacional

Na Tabela 2.2 estão as normas básicas e gerais de conduta encontradas no Fundamentos Doutrinários da Doutrina Nacional da Atividade de Inteligência [2].

Tabela 2.2: Princípios da Atividade de Inteligência da Doutrina Nacional [2]

Princípios	Descrição
Amplitude	Obter os mais completos resultados nos trabalhos desenvolvidos.
Controle	Supervisão adequada das ações.
Imparcialidade	Abordar o assunto com isenção de forma a não distorcer os resultados dos trabalhos.
Interação	Estabelecer e adensar relações de cooperação que possibilitem otimizar esforços.
Objetividade	Planejar e executar ações para atingir objetivos previamente definidos.
Oportunidade	Apresentar resultados em prazo apropriado para sua utilização.
Segurança	Adoção de medidas de salvaguarda adequadas.
Simplicidade	Planejar e executar ações de modo a evitar complexidade, custos e riscos desnecessários.

2.3 PRINCÍPIOS PARA OSINT

Os valores e princípios da Atividade de Inteligência na totalidade são também os de suas INTs que trazem ainda outros princípios para orientar cada uma delas.

Com o objetivo de evitar distorções decorrentes de fatores subjetivos, ordenar os diversos recursos para a sua execução e estabelecer uma ontologia que convencione a linguagem de uma profissão, considera-se a adoção de princípios para guiar a prática de OSINT.

OSINT, ao lado de HUMINT, são as INTs mais democráticas porque não dependem de tecnologia avançada e soluções de alto custo financeiro, tais como satélites e radares [5]. Por esses motivos, são as INTs mais utilizadas por organizações não estatais ou de menor poderio financeiro.

São exemplos dessas organizações o *Bellingcat*, um grupo internacional de pesquisadores, investigadores e jornalistas usando fontes abertas para relatar uma variedade de questões, desde crimes contra a humanidade, até o rastreamento do uso de armas químicas e conflitos ao redor do mundo [43].

Outro exemplo é o *Trace Labs* [17], uma organização sem fins lucrativos cuja missão é acelerar a reunificação familiar de pessoas desaparecidas, treinando os seus membros na prática de OSINT.

Temos também o Centro de Direitos Humanos da Escola de Direito da Universidade da Califórnia, Berkeley, que realiza pesquisas sobre crimes de guerra e outras violações graves do direito humanitário internacional e dos direitos humanos usando métodos baseados em evidências e tecnologias inovadoras para realizar investigações de fontes abertas. Eles desenvolveram, em parceria com o Escritório de Direitos Humanos das Nações Unidas, um protocolo internacional, o Protocolo de Berkeley para Investigações de Fontes Abertas Digitais (*Berkeley Protocol on Digital Open Source Investigations* [7]), que articula padrões e diretrizes profissionais que visam melhorar o seu uso efetivo em investigações criminais e de

direitos humanos internacionais [44].

Estas organizações são como comunidades de prática OSINT, às vezes estruturadas em trabalho colaborativo e, às vezes, em competições entre pesquisadores, conhecidas como *Capture the Flags* (CTFs) [16], onde quem responder corretamente o maior número de perguntas usando OSINT, vence.

A Tabela 2.3 reúne os princípios praticados pelo *Bellingcat* [15], o *Trace Labs* [17] e o Protocolo Berkeley [7], além dos apresentados por Belghith *et al.* [16].

Tabela 2.3: Princípios de OSINT segundo Bellingcat [15], Belghith, Y. *et al.* [16], Protocolo Berkeley [7] e Trace Labs [17].

Princípios	**Bellingcat [15]**	**Belghith, Y. *et al.* [16]**	**Protocolo Berkeley [7]**	**Trace Labs [17]**
Accountability	-	-	✓	-
Acurácia	✓	-	✓	-
Colaboração/Cooperação	✓	-	-	✓
Competência	-	-	✓	-
Comunidade	-	-	-	✓
Consciência de Segurança	-	-	✓	-
Curiosidade	-	-	✓	-
Dignidade/Integridade	✓	-	✓	-
Diversidade/Inclusão	-	-	✓	-
Humildade	-	-	✓	-
Independência	-	-	✓	-
Inovação/Inventividade	✓	-	-	✓
Legalidade	-	✓	✓	-
Minimização de Dados	-	-	✓	-
Não rastreabilidade	-	✓	✓	-
Objetividade	-	-	✓	-
Preservação	-	-	✓	-
Reconhecimento Passivo	-	✓	-	-
Tenacidade	✓	✓	-	-
Transparência	✓	✓	✓	-

Os princípios da Tabela 2.3 são descritos a seguir:

- *Accountability*: os profissionais de OSINT devem conseguir dizer como fizeram o seu trabalho através de um registro claro das suas ações e de supervisão. Isto inclui: a documentação das ferramentas utilizadas, a configuração dos equipamentos, os perfis adotados e a evolução passo-a-passo da coleta [7].

- *Acurácia*: a seleção, interpretação ou apresentação tendenciosa dos dados pode ser mitigada pelo teste de múltiplas hipóteses e a revisão por outros coletores do material obtido [7]. Deve-se utili-

zar somente material confiável de modo a garantir a qualidade da coleta por meio da precisão das informações.

- *Colaboração/Cooperação*: mesmo que um trabalho de OSINT possa ser realizado por uma única pessoa, é claro que devido à enorme quantidade de informações e à complexidade dos fatos e situações que um usuário da Atividade de Inteligência deve estar interessado, OSINT é melhor executada como um trabalho em equipe, o que também possibilita dividir a tarefa entre uma força de trabalho especializada visando o alcance dos objetivos [45] e fomentar a diversidade e a inclusão.

- *Competência*: uma capacitação especializada deve proporcionar aos profissionais de OSINT o treinamento adequado para adquirir habilidades técnicas, agir de forma ética e seguir um método de coleta. Como OSINT é a primeira INT no ciclo de Inteligência, o treinamento nela deve acontecer logo no início da formação do profissional. A experiência em sala de aula mostra que é nesse momento que os futuros profissionais são reconectados com o princípio da humildade para reconhecer que eles não sabem usar profissionalmente o que pensavam saberem fazer.

- *Comunidade*: o livre compartilhamento de OSINF e a transparência metodológica são as bases das comunidades que se organizam em torno de OSINT para colaboração entre os seus membros, mas também para competições ou coletas envolvendo muitas pessoas [16], típico de CROSINT (Inteligência *Crowdsourced*). Estas comunidades também têm um papel relevante no treinamento daqueles interessados em aprender ou melhorar as técnicas de coleta e em divulgar novidades sobre esse campo.

- *Consciência de Segurança*: todos os profissionais que realizam coletas *on-line* devem ter consciência básica de segurança operacional para garantir que minimizem os seus rastros digitais e estejam cientes dos riscos potenciais. As organizações que conduzem OSINT devem assegurar que os seus profissionais recebam treinamento de segurança da informação para compreender os riscos que podem enfrentar e ter uma compreensão dos três pilares fundamentais da segurança da informação: a) confidencialidade (permitindo apenas o acesso dos usuários autorizados); b) integridade (assegurando que os dados não sejam adulterados); e c) disponibilidade (assegurando que os sistemas e dados estejam disponíveis para os usuários autorizados quando eles precisarem deles) [46]. Avaliações de ameaças e riscos devem ser conduzidas antes de iniciar atividades de coleta *on-line* e devem ser revisadas periodicamente. A segurança é responsabilidade de todos, não apenas das unidades de tecnologia da informação ou dos gestores de segurança orgânica, ou corporativa.

- *Curiosidade*: Litman e Spielberger [47] afirmam que a curiosidade pode ser amplamente definida como um desejo de adquirir novas informações e experiências sensoriais que motivam o comportamento exploratório. É o princípio que com a tenacidade impulsiona uma coleta.

- *Dignidade/Integridade*: os direitos humanos devem servir como padrões para uma prática ética de OSINT [15]. Caso não seja necessário, deve-se evitar a exposição de toda a extensão do sofrimento, violência ou outra situação que comprometa a segurança física, psicológica ou digital das pessoas envolvidas [7].

- *Diversidade/Inclusão*: para uma compreensão holística de fatos e situações, uma variedade de experiências e perspectivas deve ser incorporada à Inteligência para mitigar vieses e preconceitos por

meio de uma equipe diversificada, também em gênero [7]. Tomando como exemplo as plataformas de mídias sociais, a sua operação costuma ser feita em escala global, incorporando conteúdos de várias culturas, idiomas, faixas etárias e outras diversidades que devem ser compreendidas pela equipe de coleta.

- *Humildade*: os praticantes de OSINT devem ser humildes para permanecerem conectados com o que não sabem e com suas limitações, para estarem prontos para examinar o que pensam saber e para reconhecer possíveis erros diminuindo possíveis danos [7]. O uso corriqueiro da *web* e de mídias sociais pode gerar um falso senso de proficiência sobre esta atividade, mas assim como alguém que dirige todos os dias de casa para o trabalho não é um motorista profissional, o mesmo se aplica a um usuário que usa um mecanismo de busca generalista como o Google para encontrar informações quando comparado a um coletor profissional de OSINT que usa a mesma ferramenta para criar o seu próprio mecanismo de busca programável [48].

- *Independência*: conflitos de interesse podem gerar influência inadequada que compromete os praticantes de OSINT e a própria coleta. Portanto, o princípio da transparência deve ser empregado para mitigar esta influência e ajudar a verificar a independência de uma coleta. É também um requisito para a avaliação de ferramentas.

- *Inovação/Inventividade*: quando um novo serviço *on-line* ou banco de dados aparece, as maneiras de explorá-los não são conhecidas nem claras, exigindo um esforço para aprender novas maneiras de obter informações dessas fontes. Novas tecnologias são a própria expressão das inovações digitais que nos oferecem mais informações, maneiras de interagir e com as quais OSINT trabalha continuamente.

- *Legalidade*: os profissionais de OSINT devem cumprir a lei e, para isso, devem ter um entendimento básico da legislação aplicável ao seu trabalho, em particular, a proteção de dados e o direito à privacidade, que são tratados não apenas pela legislação internacional de direitos humanos, mas também pela legislação nacional de vários países. O cumprimento da lei é fundamental para os profissionais de Inteligência de Estado.

- *Minimização de dados*: deve-se coletar apenas o necessário para atender aos requisitos do tomador de decisão, de modo a evitar contratempos através da análise de material desnecessário, os seus custos de armazenamento e violações de privacidade [49]. Esta abordagem valoriza o planejamento da coleta no que diz respeito a delimitação do assunto quanto ao período relevante, uma definição clara do que precisa ser obtido e a conformidade com o prazo para a difusão do resultado. Por este princípio, a coleta manual teria prioridade sobre a coleta em larga escala, geralmente automatizada, já que favoreceria a discrição [7].

- *Não rastreabilidade*: organizações que praticam OSINT devem ter a sua infraestrutura, incluindo *hardware* e *software*, montada para proporcionar a não rastreabilidade de forma a não se poder atribuir suas ações aos seus profissionais [7], a menos que o contrário seja desejável. Isto requer a manutenção de uma separação entre os dispositivos e perfis pessoais dos profissionais e os dispositivos e perfis utilizados durante o trabalho de coleta.

- *Objetividade*: os preconceitos pessoais, culturais e estruturais têm o potencial de afetar o trabalho dos profissionais de OSINT que devem assegurar uma abordagem objetiva, desenvolvendo e implementando múltiplas hipóteses de trabalho. A forma como a informação na internet é estruturada e apresentada aos usuários pode significar que mesmo quando os termos de busca são os mesmos, os mecanismos de busca apresentem resultados muito diferentes. Os algoritmos empregados por essas ferramentas de busca podem comprometer a objetividade dos resultados [50]. Estes resultados também podem ser influenciados por vários fatores técnicos, incluindo o dispositivo utilizado e o histórico de busca anterior do usuário. Os profissionais de OSINT devem contrabalançar tais resultados aplicando variações dos fatores técnicos para garantir que os resultados da busca sejam os mais diversos possíveis, por exemplo, usando diferentes mecanismos de busca, navegadores, idiomas, e também configurações locais de acesso. Finalmente, os profissionais devem se esforçar continuamente para estar atentos e corrigir seus próprios preconceitos, que podem ser subconscientes [7].

- *Preservação*: se a coleta é necessária, também é a preservação do material coletado. Dessa forma, a acessibilidade ao material coletado deve ser mantida, tanto para fins de *accountability* quanto para uso em trabalhos futuros. Complementarmente, outra abordagem refere-se à preservação de informações que podem ter a sua disponibilidade pública alterada a qualquer momento, ou mesmo apagadas. O profissional de OSINT deve saber como preservar as informações coletadas de modo a obtê-las em seu formato nativo ou o mais próximo dele possível [7]. Ao coletar uma postagem em uma mídia social, por exemplo, é necessário preservar como ela foi percebida no momento da coleta por meio de uma foto da tela, o seu código *HyperText Markup Language* (HTML) e, eventualmente, a própria experiência de navegar naquela página através de um vídeo ou uma cópia *on-line* em um ambiente sob o controle do coletor.

- *Reconhecimento Passivo*: OSINT realiza um reconhecimento passivo como uma tentativa para obter informações sobre computadores, redes, pessoas e organizações, sem se envolver ativamente com os esses sistemas ou pessoas. É a delimitação objetiva entre uma ação de OSINT e uma ação de engenharia social [51].

- *Tenacidade*: a informação desejada pode estar no próximo clique em uma longa sequência de resultados. A persistência é crucial em uma área de busca que parece inesgotável e gigantesca como a internet. A resiliência deve ser combinada com um planejamento claro que estabeleça os requisitos de forma objetiva no prazo para que a Inteligência seja oportuna. Sem requisitos claros, a tenacidade tende a causar um efeito conhecido na comunidade OSINT como "buraco de coelho", quando um coletor sai em busca de algo sem ter certeza do que é, portanto, não consegue saber quando o objetivo foi alcançado.

- *Transparência*: como princípio ético, a transparência tem a ver com a forma como os profissionais se comportam e se fazem perceber pelo mundo exterior e entre eles mesmos para que os envolvidos conheçam seus métodos e possam se comunicar efetivamente. Há também uma transparência necessária para garantir o princípio profissional de *accountability*. Por razões de segurança, o anonimato de coletores ou a não atribuição de suas ações podem ser importante e justificar o uso de identidades virtuais falsas. Entretanto, esta prática pode prejudicar a credibilidade da coleta, dos coletores ou da organização e até mesmo contaminar as informações coletadas quando, por exemplo, se obtém

conexões de mídias sociais sob pretextos falsos.

2.4 DISCIPLINAS DE INTELIGÊNCIA

Uma Disciplina de Inteligência é um recorte de especialização da Atividade com a caracterização pelo emprego de fontes de determinado tipo, métodos e técnicas específicas. Cinco INTs são listadas como clássicas [17], são elas:

- *Inteligência de Fontes Abertas (OSINT)*: é vista com várias definições na literatura de referência e isso tem gerado debates que duram mais de 50 anos na Comunidade de Inteligência [6]. Um dos mais comuns, o da Inteligência americana, define OSINT como "Inteligência produzida a partir de informações publicamente disponíveis que são coletadas, exploradas e divulgadas em tempo hábil para um público apropriado com o propósito de atender a uma exigência específica de Inteligência" [3]. Para Jardines, é a "informação que está publicamente disponível a qualquer pessoa através de meios legais, incluindo solicitação, observação ou compra, que é posteriormente adquirida, examinada e analisada de modo a cumprir uma exigência de Inteligência" [5]. Já Pastor-Galindo *et al.* dizem que ela "consiste na coleta, processamento e correlação de informações públicas de fontes de dados abertas" [9].

- *Inteligência Humana (HUMINT)*: é a coleta de informações fornecidas diretamente por uma fonte humana. É o único tipo de coleta em que o coletor interage diretamente com a fonte da informação, controla os tópicos de discussão e dirige as ações da fonte [52]. É a principal disciplina das ações operacionais (secretas) de coleta.

- *Inteligência de Imagens (IMINT) ou Inteligência Geoespacial (GEOINT)*: estão ligadas à exploração e análise de imagens e informações geoespaciais para descrever, avaliar e representar visualmente características físicas e atividades georreferenciadas [3].

- *Inteligência de Sinais (SIGINT)*: é a forma de Inteligência derivada da coleta e processamento de várias formas de dados e informações transmitidas eletronicamente. Estas formas são a comunicação de material de linguagem humana e dados derivados de dispositivos de transmissão eletrônica, principalmente radares [53] e antenas.

- *Inteligência de Medições e Assinaturas (MASINT)*: é a Inteligência produzida através da análise quantitativa e qualitativa dos atributos físicos dos alvos e eventos para caracterizar e identificar esses alvos e eventos [54]. Inclui vários tipos de sensores, como sismógrafos, medidores de radiação, mas também os rastros digitais deixados quando se acessa algo na internet.

Além das INTs clássicas ou tradicionais, há muitas outras que são subdivisões especializadas das cinco anteriores ou que procuram abordar novas formas de coleta de informações. Dentre elas temos:

- *Inteligência de Mídias Sociais (SOCMINT)*: as plataformas de mídias sociais, por exemplo, são parte do que é explorado pela SOCMINT. Inteligência derivada de conteúdo postado em plataformas de

mídia social como Facebook, Instagram, Twitter, LinkedIn, YouTube e TikTok [55]. Embora os dados disponíveis em sites de mídia social possam estar abertos ou fechados ao público, eles são geralmente considerados como parte do domínio OSINT porque são plataformas públicas *on-line*.

- *Inteligência Crowdsourced (CROSINT)*: combina HUMINT e OSINT abordando muitas pessoas amplamente, publicamente - não dissimuladamente - para fornecer informações sensíveis, mas não classificadas [56]. A coleta coletiva e não disfarçada em OSINT é um exemplo de CROSINT.

A união de todas as INTs permitiria uma análise de todas as fontes (*All-Sources*) inclusive de fontes secretas por meio de meios de coleta igualmente secretos, torna este tipo de análise diferente do que se poderá esperar encontrar em qualquer universidade, por exemplo [41]. A Figura 2.1 representa esta visão.

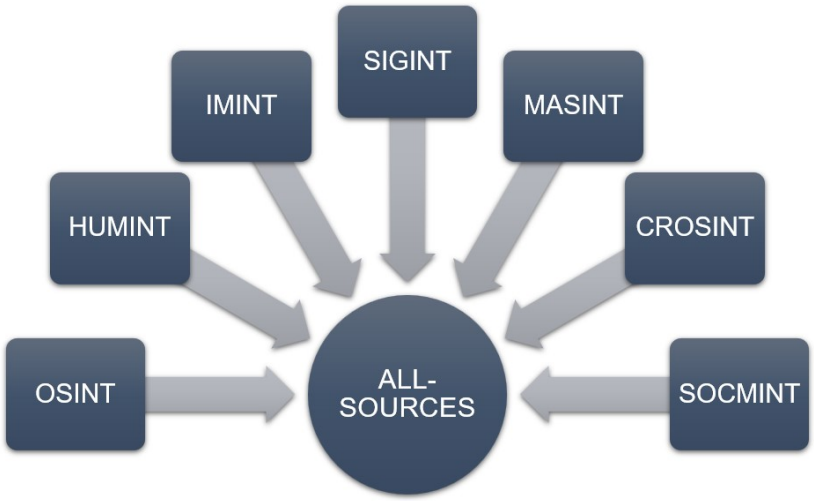

Figura 2.1: Todas as INTs permitiriam uma análise de todas (*All-Sources*). Fonte [o autor]

Há informações publicamente disponíveis em todas as INTs portanto, há uma parte de fontes abertas em todas as disciplinas. A Figura 2.2 ilustra como OSINT permeia as outras INTs.

Há vantagens significativas do uso de múltiplas fontes (Multi-INT). A corroboração de várias fontes é obtida comparando a Inteligência derivada de uma fonte com aquela derivada de pelo menos outra fonte, para que características comuns ou contradições possam ser identificadas, e assim, aumentando a certeza e reduzindo riscos. A Inteligência de múltiplas fontes terá frequentemente um grau de confiança maior do que a Inteligência de única fonte devido a sua resistência ao engano. O cruzamento de vários tipos de coleta pode permitir a observação simultânea com o consequente aumento da densidade de informações sobre um alvo [57].

Nos EUA é comum a existência de agências especializadas em determinada INT, denominadas “agências de fonte única”, que coletam e fazem o processamento inicial do seu material, difundindo as suas conclusões. Essa separação teria o propósito de manter a originalidade da fonte, deixando-a livre das influências de outras [58].

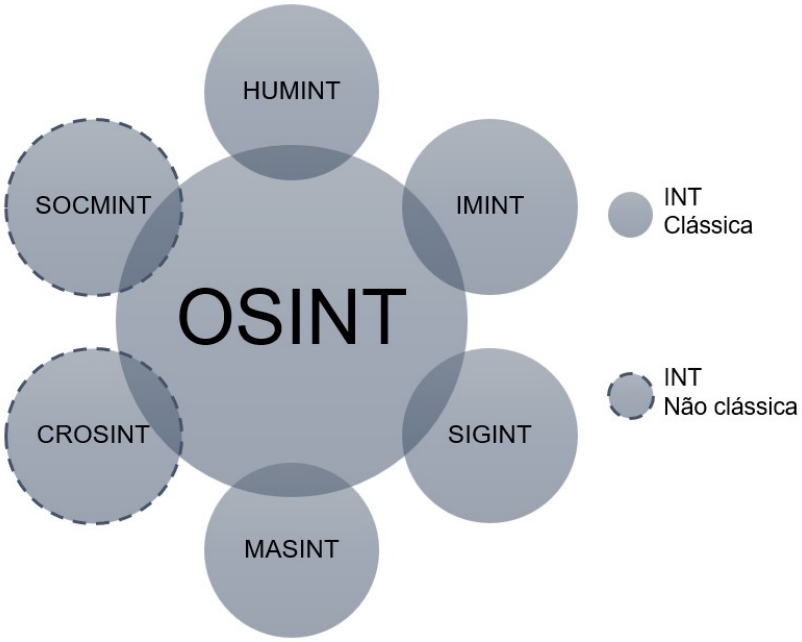

Figura 2.2: Há uma parte OSINT em todas as INTs. Fonte [o autor]

2.5 CICLOS DE INTELIGÊNCIA E MÉTODOS PARA OSINT

Ciclos de Inteligência representam o nível mais geral e abrangente do *modus operandi* para o desenvolvimento do produto Inteligência. Sendo as agências de governos organizações que se valem do segredo para o sucesso das suas atividades, a publicação detalhada das metodologias para a produção da Inteligência nem sempre está disponível. Dessa forma, os ciclos de Inteligência de cada organização acabam sendo um dos poucos materiais disponíveis sobre como se dá esse desenvolvimento, tornando alguns ciclos, na prática, a própria expressão de um método.

Diversas organizações de Inteligência possuem ciclos e nomenclatura próprios. Em geral, o ciclo é formado por ações que: a) definem os requisitos de informação de um decisor (Direção); b) estabelecem um plano para atender a estes requisitos (Planejamento); c) coletam as informações necessárias para desenvolver um produto final (Coleta); d) processam as informações coletadas em um formato utilizável (Processamento); e) analisam as informações para obter significado (Análise); f) consolidam o produto de Inteligência (Produção); g) transmitem a Inteligência ao usuário que a demandou (Difusão); e h) avaliam constantemente todas estas ações (Avaliação).

As etapas ou fases não são imutáveis e se permeiam continuamente umas às outras. Isto é facilmente visível na fase de Planejamento. Todas as fases precisam de um planejamento e há um planejamento geral que organiza todo o desenvolvimento da Inteligência a partir da definição dos requisitos do usuário. De forma análoga, o mesmo acontece com a fase da Avaliação. A Figura 2.3 representa um ciclo de Inteligência generalista.

A seguir, são apresentados alguns ciclos encontrados na literatura especializada.

Figura 2.3: As etapas do Ciclo de Inteligência genérico. Fonte [o autor]

2.5.1 O ciclo básico

A versão do ciclo da Inteligência adotada pela Organização do Tratado do Atlântico Norte (OTAN) na Figura 2.4 é composto por 4 etapas: Direção, Coleta, Processamento e Disseminação, sendo intitulado ciclo da Inteligência "tradicional" ou "básico" [1]. Essa definição se alinha com o modelo das funções essenciais da Inteligência proposto na revisão da Doutrina de Inteligência do Reino Unido [40]. Em síntese, a Atividade de Inteligência teria que saber o que o seu usuário precisa, coletar e analisar informações para transformá-las em Inteligência, e então, entregar esse produto para o usuário.

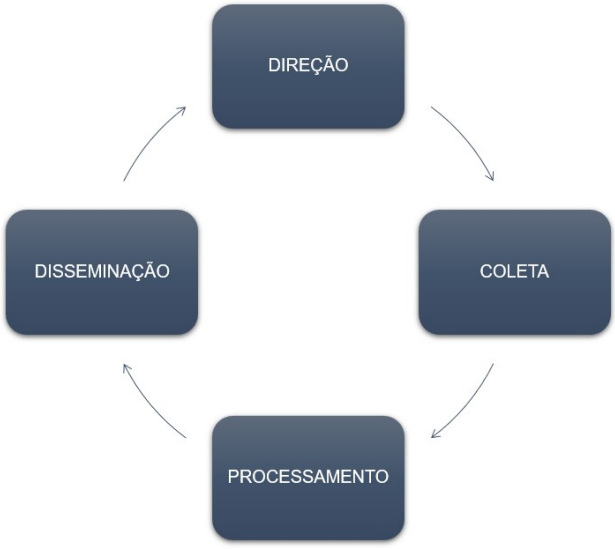

Figura 2.4: Ciclo de Inteligência (adaptado de P. Davies *et al.*[1])

2.5.2 O ciclo da Doutrina Brasileira

O ciclo de Inteligência da Doutrina Nacional da Atividade no Brasil [2] da Figura 2.5, é formado por 5 etapas: Política, Planejamento, Reunião, Processamento e Difusão. As etapas da Política e do Planejamento se desdobram do que estava na etapa da Direção do ciclo básico [1]. A palavra "Reunião" reforça a ideia de obtenção por meio de intercâmbio entre unidades do próprio órgão e outras instituições.

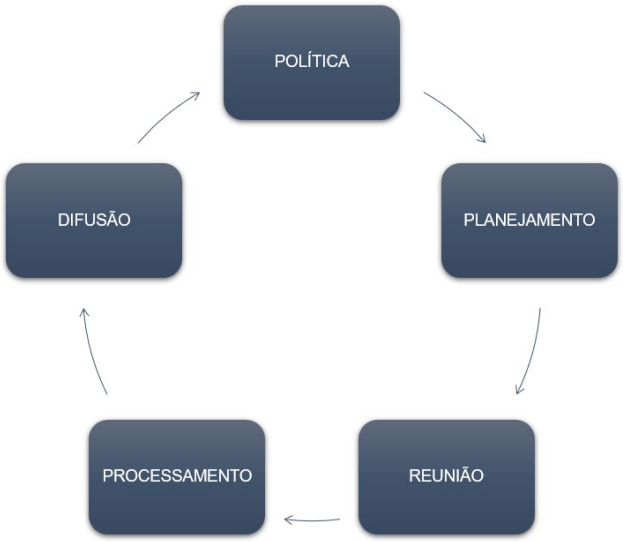

Figura 2.5: Ciclo de Inteligência (adaptado da Doutrina Naciona da Atividade de Inteligência [2])

2.5.3 O ciclo da Doutrina dos EUA

A comunidade de Inteligência dos EUA é encabeçada pelo *Office of the Director of National Intelligence* (ODNI) [3] que apresenta um ciclo de Inteligência (Figura 2.6) com seis etapas:

- Planejamento e Direção: estabelecer os requisitos de Inteligência do usuário e planejar as atividades de Inteligência de acordo;
- Coleta: reunir os dados brutos necessários para produzir o produto acabado;
- Processamento e Exploração: converter os dados brutos em um formato compreensível que seja utilizável para a produção do produto acabado;
- Análise e Produção: integrar, avaliar, analisar e preparar as informações processadas para inclusão no produto final;
- Disseminação: entregar o produto acabado ao consumidor que o solicitou e a outros conforme o caso; e
- Avaliação: adquirir continuamente *feedback* durante o Ciclo de Inteligência e avaliar esse *feedback* para refinar cada passo individual e o ciclo como um todo.

Aqui, a função da Análise fica explícita no ciclo e a Avaliação se destaca da Disseminação.

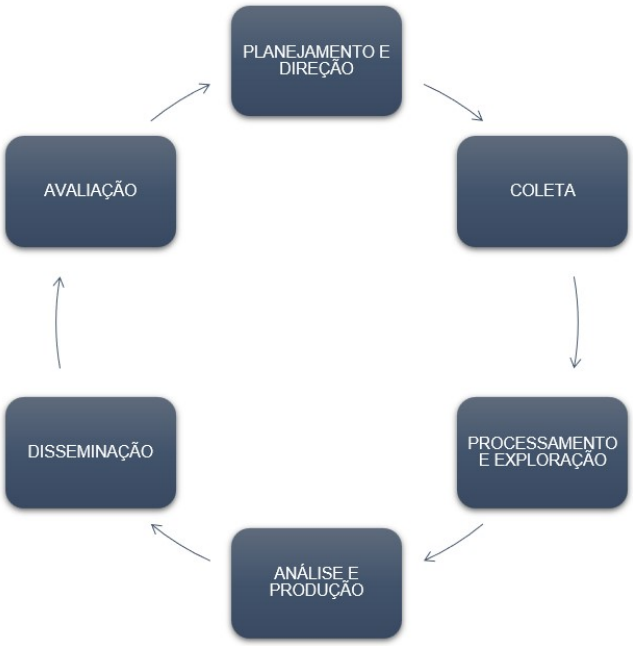

Figura 2.6: Ciclo de Inteligência (adaptado da Doutrina dos EUA [3])

2.5.4 O ciclo de Evans

Evans [4], se vale de experiências do ambiente operacional e da Inteligência militar, para apresentar um modelo com 8 etapas: Planejamento, Direção, Coleta, Processamento, Análise, Produção, Disseminação e Revisão. Esse modelo, mais detalhado, permite o tratamento mais especializado da informação em cada uma das suas etapas e acrescenta uma fase contínua de Avaliação e interação com o usuário (Figura 2.7).

2.5.5 O Método na Doutrina Brasileira

Considerando o caderno de Fundamentos Doutrinários da Doutrina Nacional da Atividade de Inteligência [2], não há menção aos termos "OSINT" ou "Inteligência de Fontes Abertas". É sabido haver uma Metodologia de Produção do Conhecimento (MPC) que trata sobre o ciclo de Inteligência na ABIN [59]. No entanto, este documento não é de domínio público.

Dos Fundamentos Doutrinários [2], temos a apresentação de um ciclo de Inteligência com as seguintes fases:

- Política: elaboração dos documentos e demandas que orientam a atuação da Inteligência;
- Planejamento: preparação para a elaboração de determinado conhecimento;
- Reunião: obtenção de conhecimentos e dados que contribuem para a produção do conhecimento;
- Processamento: submissão dos dados e conhecimentos obtidos a métodos analíticos; e
- Difusão: transmissão do conhecimento produzido ao usuário.

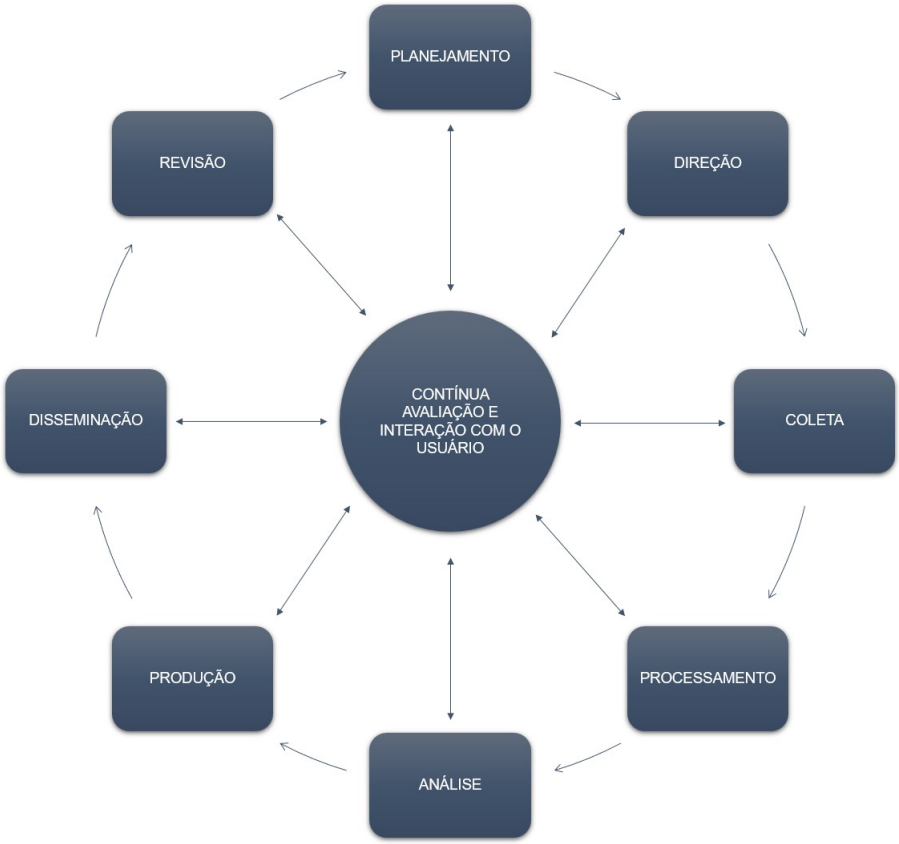

Figura 2.7: Ciclo de Inteligência (adaptado de Evans [4])

2.5.6 O Método na Doutrina Americana

Dentro da comunidade de Inteligência dos EUA, a exploração de OSINT é gerenciada através de cada etapa do processo conhecido como TCPED - *Tasking*, *Collection*, *Processing*, *Exploitation* e *Dissemination* (Tarefa, Coleta, Processamento, Exploração e Disseminação) [5], como visto na Figura 2.8.

- Tarefa: envio de um pedido de informações (*Request For Information* - RFI) a um coletor;
- Coleta: determinação do que adquirir e depois adquirindo-o;
- Processamento: obtenção das informações em um formato útil, como a transcrição e tradução de uma transmissão de rádio em língua estrangeira para texto em inglês;
- Exploração: validação e análise das informações adquiridas e organização do produto final; e
- Disseminação: envio das informações ao solicitante e compartilhamento com qualquer outro consumidor que possa precisar delas.

2.5.7 Métodos para OSINT descritos por outros autores

Enquanto alguns autores enquadram OSINT em um ciclo de Inteligência que aceite todas as INTs, outros autores organizaram um ciclo específico para OSINT. Esses ciclos valorizam as fontes abertas de todas

Figura 2.8: Processo TCPED [5]. Fonte [o autor]

as INTs e detalham o caminho desde a identificação do que é necessário saber até a entrega do produto ou relatório adequado. Quando vista como um ciclo próprio, OSINT deixa de ser uma disciplina exclusiva de coleta, passando a possui etapas específicas de planejamento, processamento, análise, produção e difusão, conforme descrito nos próximos itens.

2.5.7.1 O ciclo OSINT de Williams e Blum

Williams e Blum [6], apresentam um ciclo OSINT com 4 etapas: Coleta, Processamento, Exploração e Produção (Figura 2.9). De forma geral, essas etapas tratam de adquirir informações, validar essas informações, identificar o valor das informações e fornecê-las aos clientes.

- Coleta: a primeira etapa inclui a identificação de informações potencialmente úteis e a retenção desse material. A aquisição é a coleta física ou eletrônica dessas informações. A retenção é a manutenção contínua da OSINF adquirida.
- Processamento: envolve a validação das informações e a sua utilização. O processamento pode assumir muitas formas, incluindo a tradução de materiais de sua língua original para o inglês e a transformação de materiais de vídeo ou fotografias em um formato utilizável. OSINT tem uma abundância de informações disponíveis em um formato menos estruturado, tornando o processamento muito mais complicado. A agregação pode envolver redução ou integração na tradução de um corpo de dados em um formato utilizável.
- Exploração: procura determinar se a informação é o que parece ser (Autenticação) e qual é o seu valor para a Inteligência (Contextualização). A exploração também é referida como análise.
- Produção: nela as informações são fornecidas ao usuário de uma forma utilizável. Este usuário será, na maioria das vezes, um analista de Inteligência de todas as fontes que está em posição de incorporá-las em uma produção Multi-INT. Entretanto, um produto de fonte aberta também pode ser altamente

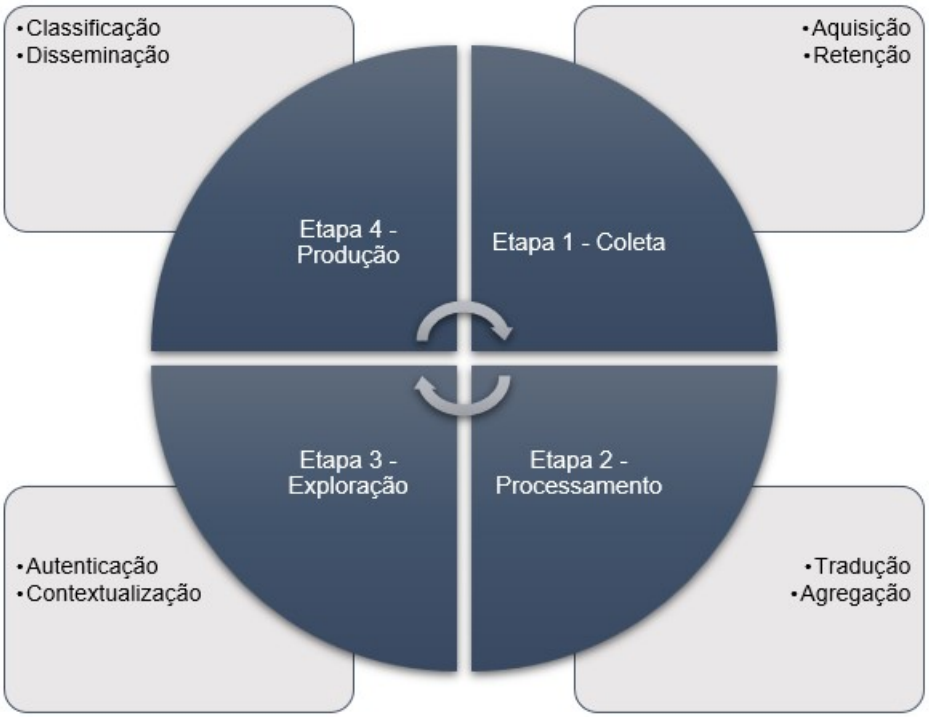

Figura 2.9: Ciclo OSINT (adaptado de Williams e Blum [6])

prioritário ou suficientemente completo para ser fornecido diretamente a um tomador de decisão. Classificação é a atribuição de um nível de sigilo. A análise de fonte aberta é mais frequentemente disseminada na forma de um relatório escrito. Entretanto, os produtos também podem tomar a forma de *briefings* verbais ou visualizações gráficas.

2.5.7.2 O ciclo para Investigações de Fontes Abertas do Protocolo Berkeley

Para o Protocolo Berkely [7], OSINT refere-se a uma subcategoria de informações de fontes abertas que são coletadas e utilizadas para o propósito específico de auxiliar na formulação de políticas e tomada de decisões, na maioria das vezes em um contexto militar ou político. A investigação de fonte aberta, por sua vez, refere-se ao uso de informações de fonte aberta para funções de coleta de informações e provas.

O ciclo do Protocolo Berkeley (Figura 2.10) possui 6 etapas assim definidas.

- Consulta *On-line*: com dois processos para descobrir informações *on-line*: (a) pesquisa, ou seja, descobrir informações e fontes de informação; e (b) monitoramento, ou seja, descobrir novas informações através da revisão consistente e persistente de um conjunto de fontes constantes;
- Avaliação Preliminar: antes de ser coletado, um material deve passar por uma verificação prévia para evitar a coleta excessiva e para cumprir os princípios de minimização de dados e investigação focada, bem como, para garantir que a coleta do material não viole o direito à privacidade dos indivíduos;
- Coleta: aqui é o ato de obter a posse de uma cópia das informações digitais através de uma captura de tela, conversão para PDF (*Portable Document Format*), *download* forense ou outra forma de captura.

Figura 2.10: o ciclo para Investigações de Fontes Abertas (adaptado do Protocolo Berkeley [7])

Os métodos de coleta podem variar dependendo se o conteúdo digital tem potencial valor probatório em processos judiciais, se será usado ou confiado para fins de tomada de decisão ou se contribuirá apenas para o desenvolvimento interno do trabalho;

- Preservação: para que o material digital permaneça acessível e utilizável com a finalidade de garantir a responsabilidade legal, ele precisa ser preservado. O objetivo é gerenciar e manter o material digital de forma que garanta a sua disponibilidade, autenticidade e uso potencial pelos instrumentos de prestação de contas, incluindo a sua admissibilidade em processos judiciais;
- Verificação: refere-se ao processo de estabelecer a precisão ou validade das informações, que foram coletadas *on-line*. A verificação é dividida em três considerações: a fonte, o item ou arquivo digital e o conteúdo, que devem ser analisados coletivamente e comparados para garantir a consistência; e
- Análise Investigativa: é a prática de revisão e interpretação de informações factuais para desenvolver conclusões substantivas relevantes para a tomada de decisões ou para a construção de casos investigativos.

2.5.7.3 O ciclo OSINT do Bellingcat

O ciclo apresentado pelo Bellingcat mostra que o trabalho tende a começar com uma abundância de informações pouco relevantes, que ao longo de suas 7 etapas, entregaria ao usuário de Inteligência uma pequena quantidade de informações muito relevantes [8]. O ciclo começa na Identificação com a localização das fontes de informação e a determinação de seu escopo, amplitude e profundidade. Então, a Coleta e a Preservação ocorreriam simultaneamente para obter a informação e protegê-la contra adulteração e destruição. Em seguida, na Verificação, são utilizadas ferramentas de análise geoespacial, pesquisa reversa de imagens e análise visual de dados. Na Análise, o Que, Quando, Quem, Como e Onde do caso são respon-

didos. Em seguida, na Revisão e Confirmação, ocorre a referência cruzada do conteúdo e a classificação de incidentes. Por fim, as informações são apresentadas ao usuário e armazenadas em um banco de dados. É o único ciclo encontrado que menciona a inserção da informação produzida em um banco de dados. Na Figura 2.11 está ilustrado o ciclo OSINT do Bellingcat.

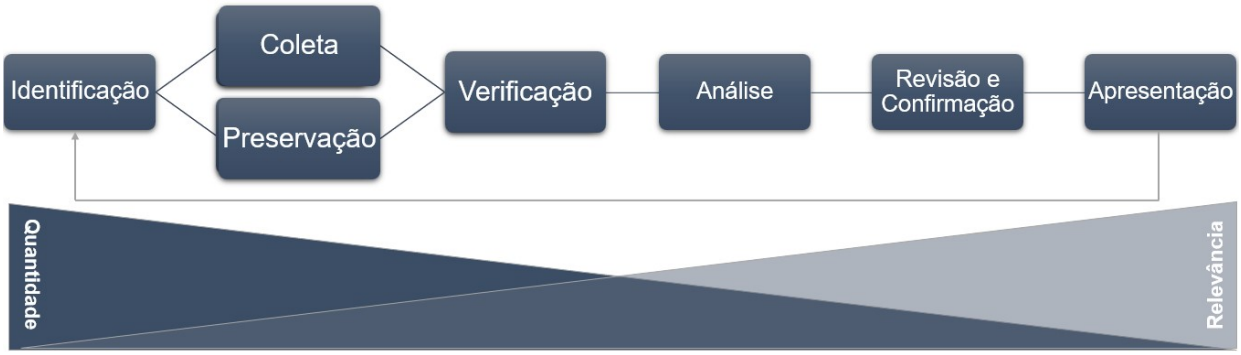

Figura 2.11: Ciclo de Inteligência (adaptado do Bellingcat [8])

2.5.7.4 A abordagem de Pastor-Galindo *et al.* para OSINT

Pastor-Galindo *et al.* [9] propõem um fluxo de trabalho que expande a quantidade de dados sobre um alvo a partir de um dado atômico, um dado que funciona como ponto de partida para a pesquisa, por exemplo, um nome de usuário, um e-mail, uma localização ou um nome real. A execução de técnicas específicas para cada dado gera uma saída que pode ser aproveitada como entrada de outro processo (transferência de dados) que explora outra técnica para gerar mais dados, os que são então agrupados em três conjuntos de informações: pessoais, organizacionais e rede de computadores. Técnicas de aprendizado de máquina e inteligência artificial são aplicadas a esses resultados para extrair conhecimento implícito para detectar padrões, perfis de comportamento, prever valores e correlacionar eventos. A Figura 2.12 ilustra a sua abordagem.

- Coleta: considerando que ao menos uma peça atômica de dados sobre o alvo está disponível, a partir desse ponto inicial, o coletor aplica as técnicas de OSINT mais adequadas para derivar mais dados. Neste sentido, os resultados obtidos com uma técnica específica são uma transferência de dados a ser utilizada por outro tipo de técnica.
- Análise: as iterações contínuas através das diferentes técnicas de OSINT devem ser analisadas e compreendidas para gerar informações úteis. Os resultados são considerados como informação de saída e são categorizados em três grupos principais:
  - Informações pessoais: reúnem os detalhes de identidade da pessoa que são obtidos principalmente a partir do nome real, endereço de e-mail, nome de usuário, redes sociais e mecanismos de busca;
  - Informação organizacional: é formada por aspectos de um grupo, organização ou empresa composta de indivíduos. São essencialmente coletadas por meio de redes sociais, mecanismos de busca, localização, nome de domínio e técnicas de endereços IP (*Internet Protocol*); e

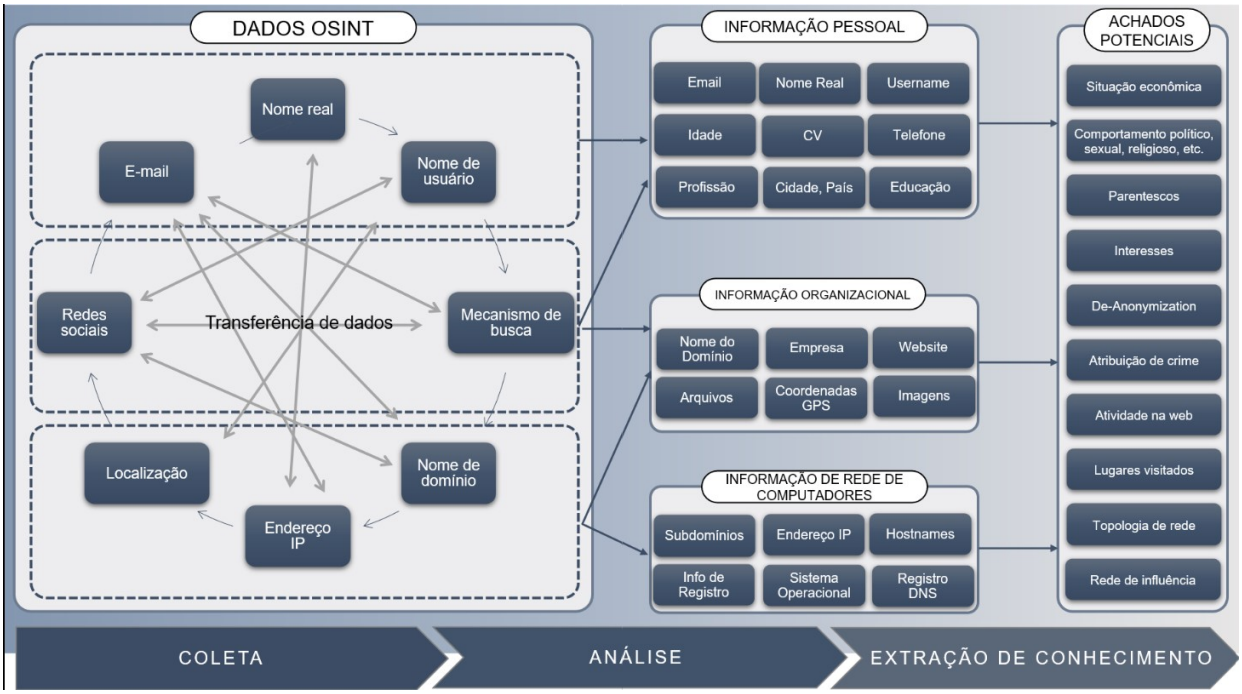

Figura 2.12: Método para OSINT (adaptado de Pastor-Galindo *et al.* [9])

  - Informações de rede: abrangem dados técnicos de sistemas e topologias de comunicação, o que geralmente é conseguido através de técnicas de localização, nome de domínio e endereço IP.

- Extração de Conhecimento: conduz ao que proporcionará um reconhecimento atraente do alvo [60]. Para este fim, considere-se a extração de conhecimento como o tratamento dos resultados da análise (informação de saída) usando técnicas de mineração de dados e inteligência artificial. Estas técnicas permitem inferir questões complexas e de alto valor sobre o alvo que não são explicitadas publicadas na internet [61].

2.6 TÉCNICAS DE OSINT

As técnicas de OSINT compreendem uma abordagem que perdurará ao longo do tempo em comparação com ferramentas ou serviços *web* como visto por Pastor-Galindo *et al.* [9], que também apresentam uma lista de técnicas com foco na coleta de informações. O Protocolo de Berkeley [7] segmenta as técnicas por tipos de análise. Williams e Blum [6], por sua vez, trazem da SOCMINT as técnicas de redes sociais aplicadas às plataformas de mídias sociais. Outros autores representam as técnicas por meio de fluxos de trabalho ou diagramas que funcionam como um guia para os praticantes de OSINT.

2.6.1 Pastor-Galindo *et al.*

Pastor-Galindo *et al.* (9) consideram que a saída de uma técnica de coleta para um tipo de informação pode ser utilizada como a entrada para uma técnica de outro tipo, conduzindo à completude do conjunto

de informações necessárias. Cada tipo de informação possui um conjunto de técnicas correspondentes conforme a Tabela 2.4.

Tabela 2.4: Técnicas de OSINT segundo Pastor-Galindo *et al.* (9)

Técnica	Desrição
Mecanismo de Busca	Os motores ou mecanismos de busca são serviços na *web* que recebem uma consulta textual tentando fornecer informações que correspondam à entrada, retornando informações valiosas ao usuário.
Redes Sociais	Muitas informações pessoais ou informações sobre organizações podem ser encontradas em plataformas de mídias sociais como Facebook, Instagram, Twitter, YouTube, LinkedIn e TikTok.
E-mail	Um endereço de e-mail é único e funciona com uma entrada para vários serviços na web.
Nome de Usuário	Nomes de usuário usados para serviços *on-line* também são uma boa maneira de coletar informações sobre uma pessoa. O mesmo nome de usuário pode ser usado em diferentes serviços da *web* ao mesmo tempo e, em cada um deles, revelar mais informações.
Nome Real	Procurar o nome real de um alvo também pode produzir bons resultados. Além das redes sociais, os serviços especializados em dados pessoais podem revelar endereços residenciais, números de telefone, contas de e-mail, nomes de usuário e muito mais.
Localização	Pesquisar os locais relacionados a um alvo pode dar indicações sobre o comportamento de uma pessoa, conhecer a localização geográfica de atuação de uma empresa ou o local de um evento. Fotos, endereços e coordenadas GPS são dados que podem ser obtidos.
Protocolo de Internet (IP)	Os endereços IP são importantes para a análise forense digital, coletando o máximo de informações possíveis de um evento em uma rede de computadores.
Nome de domínio	Estão relacionados ao nome das páginas na *web*. Eles podem revelar informações sobre o alvo, como a pessoa que registrou o nome do domínio, e-mail e a data.

2.6.2 Protocolo Berkeley

O Protocolo de Berkeley [7] apresenta as seguintes técnicas de análise conforme a Tabela 2.5.

Tabela 2.5: Técnicas de OSINT do Protocolo Berkeley [7]

Técnica	Descrição
Análise Técnica	Metadados: são os dados sobre outros dados. São relevantes para descrever um item e as circunstâncias de sua geração, disseminação ou alteração.
	Código-fonte: a linguagem de programação por trás de qualquer página da *web*, *software* ou arquivo é onde reside o código-fonte. Essa codificação pode conter meta conteúdo ou conteúdo oculto.

Continuação da Tabela 2.5

Técnica	Descrição
Análise de Conteúdo	Geolocalização: é a identificação da localização de um objeto ou atividade.
	Cronolocalização: semelhante à geolocalização com a identificação de datas e horários de um evento.
Análise Investigativa	Comparação de imagem/vídeo: é o processo de comparação de características de objetos, pessoas e/ou lugares com outros itens quando pelo menos um deles é uma imagem.
	Interpretação de imagem/vídeo: análise de armas, ferimentos, sangue, veículos e bens militares, tatuagens, ou análise de marcas de pneus de um carro, ou a altura de um indivíduo fazem parte da interpretação de imagem/vídeo.
	Análise espacial: pode incluir conteúdo visual e análise de metadados para itens que fornecem coordenadas geográficas ou nomes de locais. Envolve examinar diferentes objetos e características da paisagem e compará-los com imagens de satélite ou outras, dados geográficos, mapas e contextos.
	Mapeamento de atores: é uma técnica para identificar atores-chave e os seus relacionamentos e canais de influência.
	Análise de redes sociais: é o mapeamento e medição de relacionamentos entre pessoas, grupos, organizações, computadores, URLs (*Uniform Resource Locator*), e outras entidades de informação ou conhecimento conectadas em plataformas de mídias sociais.
	Mapeamento de incidentes: técnica usada para estabelecer as relações temporais e geográficas entre diferentes incidentes.

2.6.3 Williams e Blum

Williams e Blum [6] veem o seguinte sobre análise de conteúdo de mídia social conforme a Tabela 2.6.

Tabela 2.6: Técnicas OSINT de Williams e Blum [6]

Técnica		Descrição
Análise Léxica		Pode agregar grandes corpos de texto e, no seu nível mais básico, mostrar os termos mais pesquisados em um mecanismo de busca ou mostrar quais palavras-chave apareceram com mais frequência. Em um nível superior, pode inferir informações sobre as pessoas envolvidas nas mídias sociais, incluindo características demográficas.
Tipos de Análise Léxica:	Análise de Sentimentos:	A principal função da análise de sentimentos é avaliar uma opinião expressa *on-line* e categorizá-la como expressão de uma posição positiva, negativa ou neutra.
	Processamento da Linguagem Natural (PLN):	Os avanços tecnológicos em PLN reduziram significativamente o tempo necessário para traduzir e entender um texto. A velocidade é uma vantagem óbvia quando os analistas de Inteligência estão determinando quanta ameaça uma postagem individual em um site representa no futuro imediato.

Tabela 2.6. Continuação da página anterior

Técnica	Descrição	
	Aprendizagem de Máquina:	É o processo de ensinar um *software* a tomar decisões após o processo de tomada de decisão desejado ter sido modelado. Requer especialistas em aprendizado de máquina e linguística para projetar corretamente os parâmetros.
Análise de Redes Sociais	Muito antes das plataformas de mídias sociais baseadas na *web* de hoje, a Análise de Redes Sociais tentou explicar as relações entre indivíduos como uma série de trocas que podem ser mapeadas para explicar o passado e prever interações futuras. A intenção da Análise de Redes Sociais não é explicar os indivíduos, mas compreender a rede de atores conectados. Na era da internet, criou uma oferta exponencial de novos pontos de dados no estudo das interações de rede.	
Geoespacial	Expandiu-se significativamente com a criação de plataformas de mídias sociais que podem vincular automaticamente uma postagem a um local específico. Geralmente, funciona em combinação com outros métodos para produzir uma imagem mais detalhada da dinâmica social relevante para os coletores de Inteligência.	

2.6.4 Técnicas descritas como fluxos de trabalho

Alguns autores preferem descrever as técnicas por meio de diagramas que desenham fluxos de trabalho mostrando o caminho a ser percorrido para se trabalhar com cada tipo de informação.

Por exemplo, os diagramas de Bazzell [10] mostram procedimentos e ferramentas que podem revelar qual e-mail ou rede social está relacionada a um nome real (Figura 2.13). Bazzell também apresenta diagramas para nomes de usuário, locais, e-mails, telefones e nomes de domínio.

Esses fluxos de trabalho por tipo de dados diminuem a abstração do que deve ser feito na etapa de coleta do ciclo de Inteligência ao especificar uma forma de trabalho que considera o ecossistema de cada pesquisa e as suas características de acesso, regionalismos, preferências e capacidade técnica do praticante de OSINT. Esta abordagem pode ser vista no trabalho de Kwon *et al.* [11] que adaptou vários dos diagramas de Bazzell para a realidade da Coreia do Sul (Figura 2.14).

Outro autor entre os praticantes de OSINT é conhecido como Sinwindie [12] e também utiliza o modelo apresentado por Bazzell para criar os seus próprios diagramas. Por exemplo, Sinwindie desenvolveu o diagrama apresentado na Figura 2.15 e muitos outros como e-mail, IP, imagem, *username*, *website* e várias mídias sociais, entre elas, Tumblr, Snapchat e Reddit.

A união de vários diagramas permitiria ir de um tipo de informação a outro, numa transformação contínua da saída obtida por uma técnica em entrada para a próxima técnica. Isso pode ser ilustrado na Figura 2.16 pelo uso do analisador gráfico de Hoffman [13]. Sua lista inclui: foto de perfil do avatar, nome de domínio, imagem, e-mail, URL, IP, conta de mídia social, serviço oculto TOR, registros governamentais, nome/sobrenome, nome da empresa, telefone, áudio, vídeo, GPS, *hashtags*, endereço físico, *string*, endereço de criptomoeda, veículo, rede sem fio MAC (BSSID) e nome da rede sem fio (SSID).

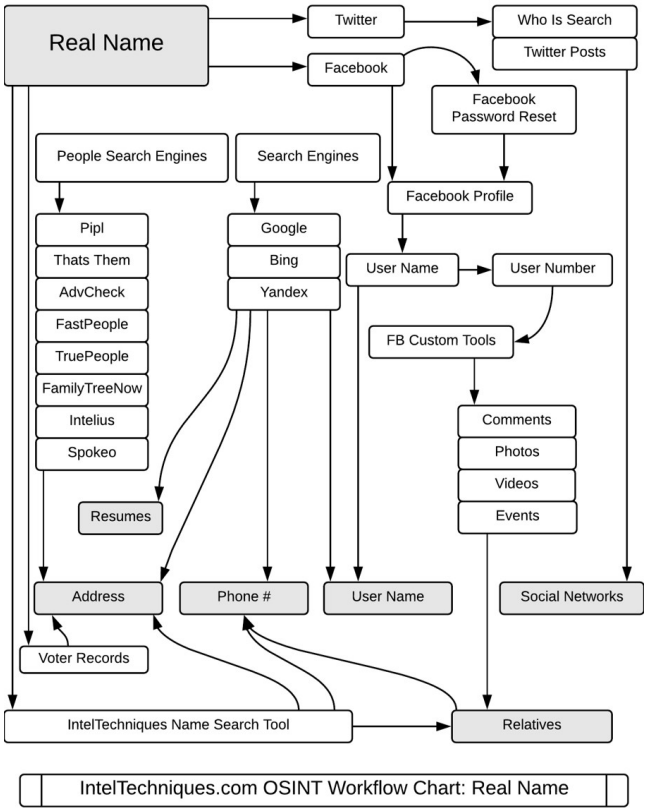

Figura 2.13: Fluxo de trabalho para um nome real de Bazzell [10].

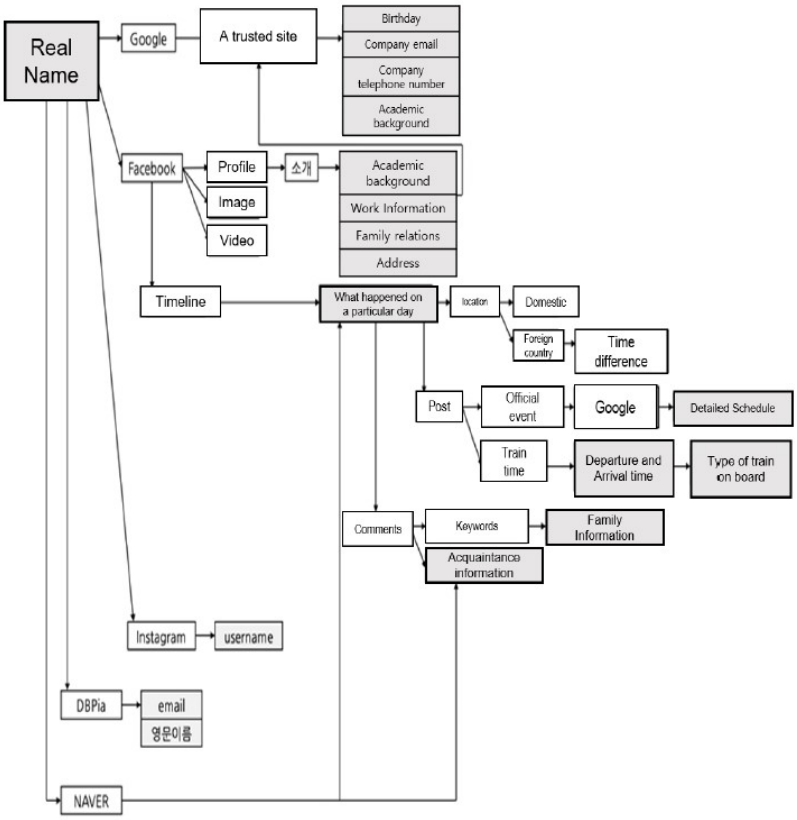

Figura 2.14: Fluxos de trabalho para um nome real de Kwon *et al.* [11].

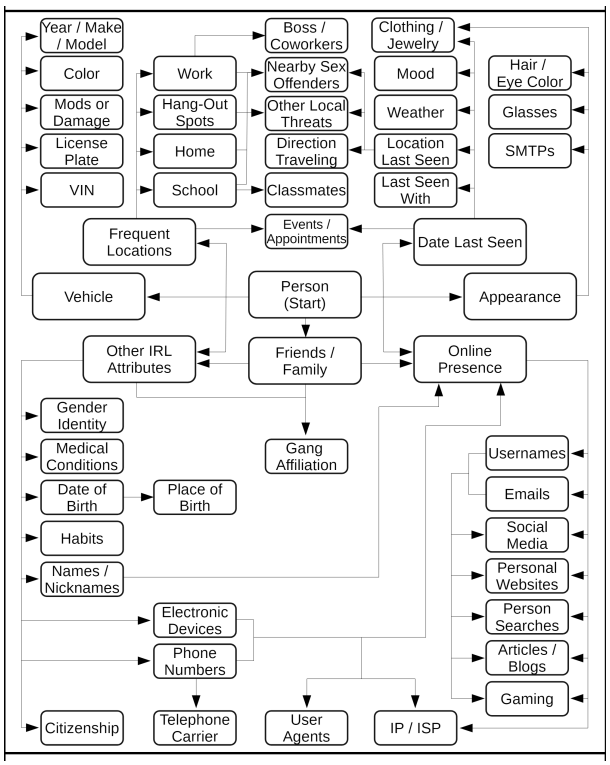

Figura 2.15: Diagrama de Sinwindie para o tipo pessoa [12].

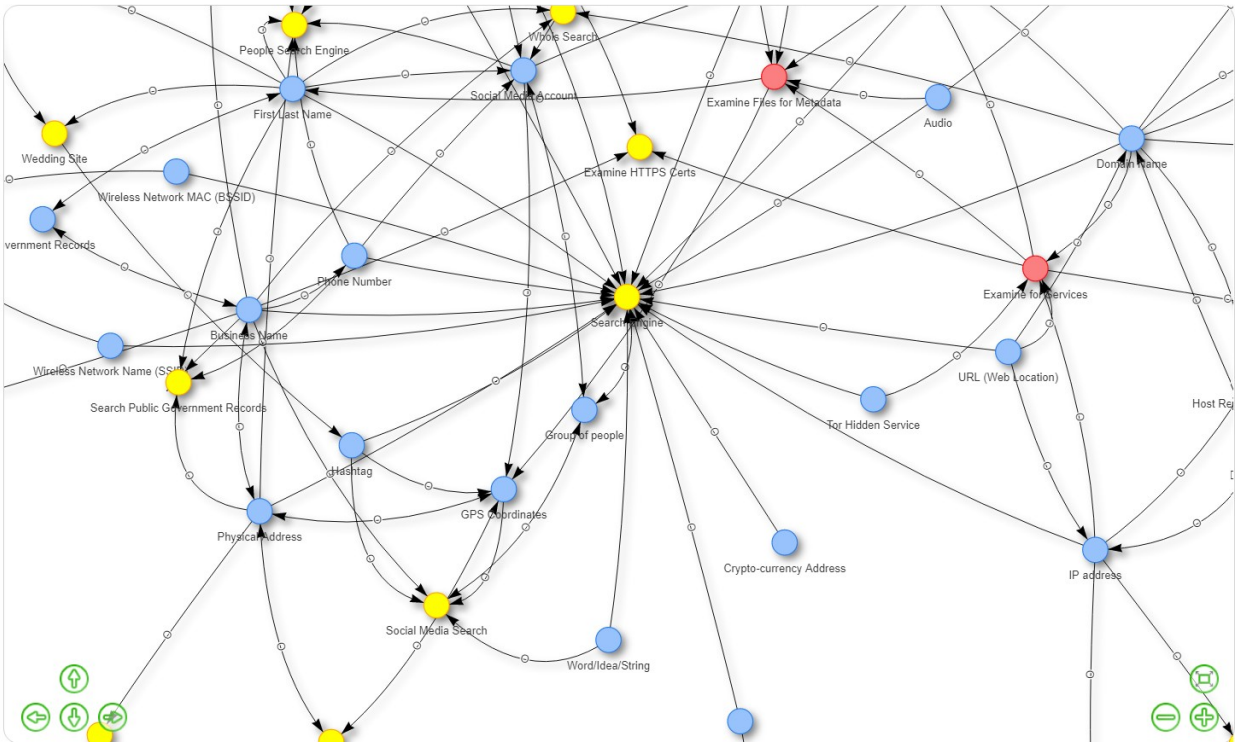

Figura 2.16: Analisador gráfico para OSINT de Hoffman [13].

2.7 FERRAMENTAS PARA OSINT

Para fins de OSINT, as ferramentas costumam estar associadas à ideia de *software*, solução que tende a ser apresentada como simplificadora de uma ação mais complexa e seria realizada "com apenas alguns cliques". Além disso, a automatização do uso concatenado de diversos serviços que exploram um tipo de informação, seguindo um fluxo de trabalho como em um algoritmo, também pode implicar no uso de ferramentas.

As ferramentas utilizadas variam de simples *plug-ins* de navegador a serviços *on-line*, bancos de dados de referência e aplicações instaladas. Cada praticante de OSINT tenderá a uma lista própria de ferramentas favoritas [19].

Segundo Pastor-Galindo *et al.* [9], em 2019, as ferramentas mais relevantes estão apresentas na Tabela 2.7, com as principais características.

Tabela 2.7: Ferramentas de OSINT em evidência segundo Pastor-Galindo *et al.* [9]

Ferramenta	Entrada	Saída	Plataforma	Interface
FOCA	Arquivos	Metadados	Windows	Stand-alone
Maltego	Informação pessoal, de organizações, de redes e arquivos	Informação de identificação	Linux, Windows, MAC	Stand-alone
Metagoofil	Nome do domínio e arquivo	Informação de rede e arquivo	Linux, Windows	Linha de comando
Recon-NG	Informação pessoal ou domínio	Identificação de pessoal, de rede e arquivo	Linux	Linha de comando
Shodan	Palavra-chave, IP, Hostname	Informação de rede	On-line	Web
Spiderfoot	E-mail, nome real, telefone domínio, IP Host name	Informação de rede	Linux, Windows, MAC	Web
The Harvester	Organização, Domínio, DNS	Informação de identificação e de rede	Linux, Windows, MAC	Linha de comando
Whois	IP, Domínio	Informação do registro do domínio	Linux, Windows, MAC	Linha de comando

Em um *survey* publicado pelo Bellingcat em 2022, mais de 500 praticantes de OSINT responderam quais eras as suas ferramentas favoritas [18]. As 10 mais citadas estão na Tabela 2.8.

Tabela 2.8: Ferramentas de OSINT mais citadas em *survey* pelo Bellingcat [18]

Ferramenta	Descrição
Google (mecanismo de busca)	Usada mesmo pelos praticantes mais experientes.
Google Earth Pro	Valorizada pelo acesso livre às imagens de satélite históricas e atuais.

Table 2.8 continued from previous page

Ferramenta	Descrição
Maltego	Usado para encontrar conexões ocultas entre pessoas ou organizações e a reunir informações relacionadas a um caso de pesquisa.
Google Maps	Para a busca por endereços.
Mecanismos de Busca (nenhum específico ou muitos mencionados)	Mais citados: Bing, Yandex e DuckDuckGo.
Wayback Machine - Internet Archive	Para a busca de versões antigas de sites.
Tineye	Para a busca reversa de imagens.
Python (*scripts*)	Diversos programas com interface em linha de comando.
Sentinel Hub	API (*Application Programming Interface*) para explorar imagens satelitais.
Shodan	Mecanismo de busca para dispositivos conectados à internet.

Williams e Blum [6] não tratam de nenhuma ferramenta específica. O mesmo se dá no Protocolo Berkeley [7] que reconhece a importância do treinamento no uso de ferramentas e *software* específicos como parte essencial para melhorar a qualidade das investigações digitais de fontes abertas, mas não se concentra em nenhuma ferramenta específica, e sim nos princípios e metodologias que podem ser aplicados de forma consistente, mesmo quando a própria tecnologia muda.

2.7.1 Critérios para a avaliação de ferramentas quanto à segurança, confiabilidade e legalidade

Revell *et al.* [19] apresentam uma estrutura de avaliação de ferramentas para OSINT conforme a Tabela 2.9. O intuito é mitigar os problemas comuns de sustentabilidade no uso dessas ferramentas e estabelecer critérios objetivos para a sua adoção quanto à segurança, confiabilidade e a legalidade.

Tabela 2.9: Critérios para a verificação de ferramentas de Q. Revell *et al.* [19].

Critério	Descrição e Discussão
Segurança	Compartilhar informações é uma parte necessária de uma investigação on-line, mas o ideal seria limitar-se apenas às informações que o usuário percebe como necessárias. Os controles de segurança ajudam a garantir que os dados do usuário e da organização não sejam inadvertidamente compartilhados com terceiros.
Privacidade	Muitas vezes, serviços anunciados como gratuitos dependem da publicidade para suas receitas, e os anunciantes estão interessados em coletar informações sobre um indivíduo para melhor direcionar os anúncios. Isto levou a uma infraestrutura para identificar o indivíduo que acessa um serviço e tem o potencial de vincular perfis profissionais ou particulares com o objeto de uma investigação.

Continuação da Tabela 2.9

Critério	Descrição e Discussão
Proteção contra *Malware*	Considera que proteções mais eficazes utilizarão as características de segurança nativas da própria ferramenta. Ou seja, a ferramenta tem que considerar isso como parte das suas atribuições e não terceirizar para a infraestrutura.
Pacote de Softwares Desnecessários	Alguns desenvolvedores e distribuidores de arquivos acrescentam à aplicação desejada um *software* indesejado como parte do processo de instalação. Isso pode gerar desde um incômodo que deixa o computador mais lento ou ainda um risco de segurança para um computador.
Serviços Baseados em Nuvem	Como o serviço reúne mais informações, ele tem uma imagem não apenas de uma investigação individual, mas potencialmente informações através de investigações ou organizações.
Confiabilidade	O praticante precisa da ferramenta para funcionar de forma confiável e consistente, agora e no futuro. O suporte ao usuário deve estar disponível se necessário, e a ferramenta deve idealmente oferecer uma trilha de auditoria das ações do usuário.
Qualidade do Código	A qualidade de qualquer *software* é provavelmente mais confiável se muitos indivíduos tiverem contribuído para seu desenvolvimento, é um produto bem estabelecido e existe um regime rigoroso e confiável para verificar a existência de erros.
Padrões e Formatos Abertos	O uso de padrões e formatos abertos permite que a organização mantenha o controle das suas informações. Isto tem uma série de benefícios: permitindo maior interoperabilidade e compartilhamento de informações, as informações podem continuar a ser usadas à medida que novos *software*s são desenvolvidos e não há dependência de fornecedores únicos.
Legalidade	Ao avaliar a ferramenta para sua adequação, o profissional também deve ter consciência dos termos de licenciamento do *software* ou serviço.
Licença	Os termos da licença dependerão do uso dado a ferramenta. O uso "pessoal" pode ser gratuito, e qualquer outro uso incorreria em um custo.
Autoridades	Existem serviços e fontes de dados cuja finalidade é fornecer dados pessoais, ou tornar os dados "pirateados" publicamente disponíveis. Alguns países possuem autoridades para a proteção de dados que fiscalizam ou normatizam esses serviços.

2.8 PROFISSIONAIS DE OSINT

Para Cepik [41], a Inteligência é constituída por quatro funções: coleta, análise, contrainteligência e ações clandestinas. Em muitos países, a função da coleta é atribuída aos oficiais de Inteligência, enquanto a da análise é responsabilidade dos analistas de Inteligência.

Vários serviços de Inteligência ou órgãos de governos reconhecem cargos, emprego ou profissões rela-

cionados especificamente à função da Coleta, ou ao trabalho com OSINT, em seus quadros de funcionários. A Tabela 2.10 apresenta algumas dessas profissões.

Tabela 2.10: Trabalhos relacionados à coleta ou a OSINT em serviços de Inteligência ou organizações de governos

Cargo ou Emprego	**País**	**Organização**	**Descrição**
Collection Manager [62]	EUA	Homeland Security	Aplicar um profundo conhecimento de todas as fontes, sistemas de gerenciamento de requisitos de coleta e capacidades de bancos de dados de pesquisa.
Open Source Targeter [63]	EUA	CIA	Conduzir pesquisas e análises na internet sobre alvos relevantes, ao mesmo tempo em que alavancam ferramentas, conjuntos de dados e metodologias avançadas para operações secretas e fornecer pistas operacionais.
Open Source Collection Specialist [64]	EUA	CIA	Gerenciar a coleta sistemática de informações disponíveis publicamente em uma determinada região para atender às necessidades dos clientes.
Open Source Exploitation Officer [65]	EUA	CIA	Descobrir, coletar e avaliar informações disponíveis publicamente, desenvolver planos para usar ferramentas e metodologias eficazes para pesquisar e coletar informações.
Open Source Analysts [66]	Austrália	Office of National Intelligence (ONI)	Coletar, interpretar e divulgar sistematicamente informações disponíveis ao público relativas a assuntos de importância política, estratégica ou econômica para a Austrália para apoiar as prioridades de inteligência do governo, o trabalho da Comunidade de Inteligência Nacional e agências parceiras aliadas.
Open Source Current Intelligence Analyst [67]	Austrália	Current Intelligence and Publishing Branch	Coletar material de fontes abertas, incluindo mídia social, mídia tradicional e outro material *on-line*, para tratar de prioridades de Inteligência.
Investigador de OSINT [68]	Holanda	Administração Fiscal e Aduaneira	Combinar informações de informantes com OSINT. Pesquisa todas as camadas da web para obter informações valiosas.
Investigador de OSINT para Trabalho e Renda [69]	Holanda	Inspeção do Trabalho	Conduzir investigações de fontes abertas. Monitoramento em tempo real e coleta sistemática de informações. Fornece produtos especializados de Inteligência para programas de investigação.

Continuação da Tabela 2.10

Cargo ou Emprego	País	Organização	Descrição
Investigator, Open-Source Intelligence [70]	Canadá	College of Immigration and Citizenship Consultants	Investigar as reclamações de má conduta profissional. Coletar e analisar a fontes abertas para fornecer conhecimentos especializados sobre este método de investigação à equipe.
Engenheiro analista de dados ofensivos cibernéticos [71]	França	DGSE	Realizar buscas de informações em OSINT (entre outras).

2.9 SÍNTESE DO CAPÍTULO

Neste capítulo foram apresentados diversos conceitos importantes para uma melhor compreensão desta dissertação. Em seguida, foram listados valores e princípios que regem a Atividade de Inteligência e os princípios utilizados por diversas organizações e autores ligados à OSINT. Esses valores e princípios disciplinam um comportamento, uma forma de agir, de se organizar.

As Disciplinas de Inteligência foram explicadas como especializações da Atividade de Inteligência que consideram o tipo de fonte de informação e o meio onde elas se encontram. Elas especializam a prática e demandam uma descrição de etapas sucessivas para se obter um resultado, uma sequência lógica de etapas, um método.

O ciclo de Inteligência é uma representação do método que descreve como as organizações de Inteligência desenvolvem o seu produto. Algumas versões do ciclo foram apresentadas, inclusive aquelas tratadas por organizações e autores que se dedicam especificamente à OSINT.

Cada etapa desses ciclos são compostas por muitas tarefas com diversas técnicas para a sua execução. Essas técnicas foram categorizadas e listadas de acordo com cada autor ou organização. Algumas ferramentas em evidência também foram descritas.

O capítulo termina com um apanhado de diversos cargos de trabalho que se dedicam à OSINT ou à etapa da coleta em diversas organizações e os seus respectivos países.

Esses valores, princípios, disciplinas, métodos, técnicas e ferramentas formam uma ontologia ao redor de OSINT e especificam uma prática profissional.

3 DISCUSSÃO DO PROBLEMA E PROPOSTA DE SOLUÇÃO

Explicados e exemplificados valores, princípios, disciplinas, métodos, técnicas, ferramentas e profissões de OSINT, se discute aqui os entendimentos equivocados sobre OSINT, problemas na execução do ciclo sendo apresentadas algumas propostas de soluções.

3.1 OBSERVAÇÕES SOBRE O FOCO EM FERRAMENTAS

Valores devem estar entre o mais alto nível de norteadores do comportamento de uma profissão. Princípios também guiam esse comportamento de modo mensurável, orientando uma prática específica. Disciplinas permitem uma especialização baseada na segmentação de tipos de informações, nos meios de acesso e tecnologias disponíveis. A técnica orienta o como fazer, enquanto uma ferramenta capacita a técnica. Métodos encadeiam de uma forma lógica a execução das técnicas e o uso de ferramentas. Valores e princípios devem ser duradouros à medida que disciplinas e métodos mudam e técnicas ferramentas se tornam obsoletas. A Figura 3.1 ilustra essa perspectiva.

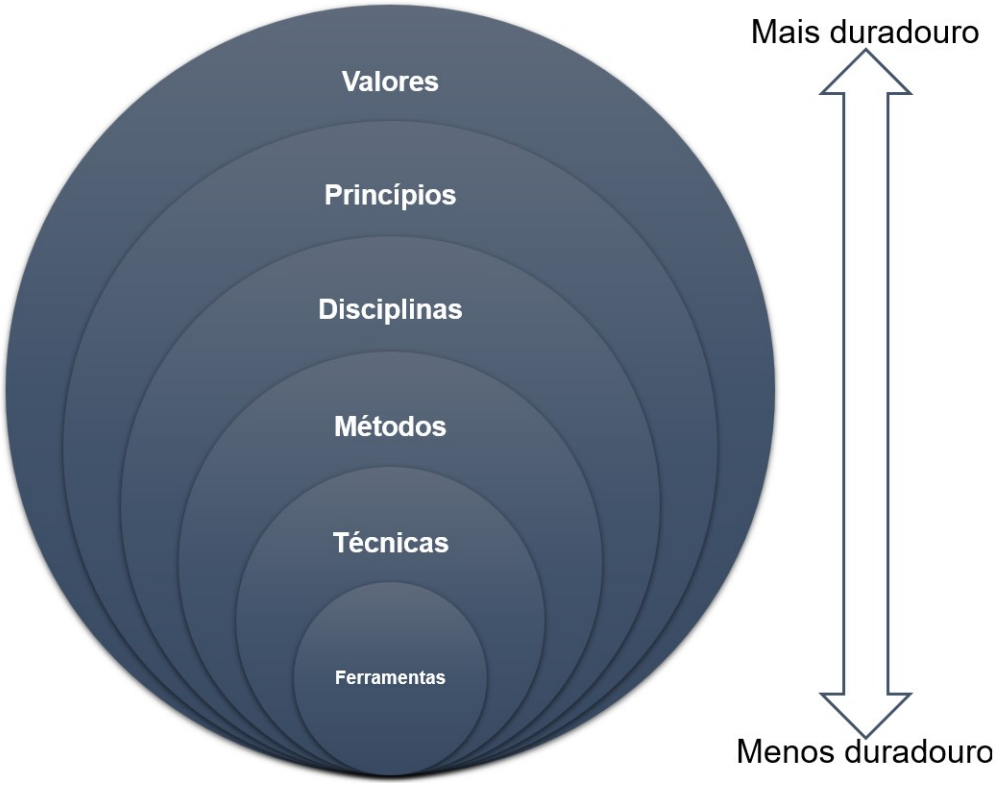

Figura 3.1: A resistência ao tempo dos valores às ferramentas. Fonte [o autor]

Várias ferramentas estão disponíveis para diferentes propósitos de OSINT. A abordagem imediatista

tende a favorecer um resultado efêmero sobre o entendimento da execução de uma técnica [7] e trata a tecnologia como um fim em si e não como um meio para o produto de Inteligência [72].

3.1.1 Ferramentas COTS

No caso da comunidade de Inteligência dos EUA, Williams e Blum [6] alertam os profissionais de Inteligência sobre o uso de ferramentas COTS (*Commercial Off-The-Shelf* ou ferramentas comerciais de prateleira) devido à incompatibilidade de propósitos de ferramentas projetadas para fins comerciais, geralmente para entender o comportamento do consumidor para melhor posicionamento de um produto no mercado, que raramente coincidem com os da Inteligência de Estado. Também chamam a atenção para a incapacidade das agências estatais de avaliar adequadamente ferramentas, fornecedores e tecnologias que mudam em um ritmo mais rápido do que sua capacidade de avaliação, especialmente considerando a prevalência de *startups* nesse mercado em oposição a fornecedores estáveis.

A utilização de ferramentas COTS especializadas para atender às necessidades dos órgãos de Inteligência em OSINT também precisa superar desafios que estão fora do domínio tecnológico e que pertencem à natureza sigilosa desses órgãos, como a integração com sistemas com informações sigilosas, a ausência de controle sobre a funcionalidade e o desempenho dessas ferramentas, o *design* sem obrigação de interoperar com outras ferramentas COTS ou as dos próprios órgãos e a grande variação no comportamento dos fornecedores dessas ferramentas diante de mudanças de mercado, fusões ou aquisições de empresas ou desenvolvimentos tecnológicos imprevisíveis [73].

3.2 DISCIPLINA DE COLETA, PROCESSAMENTO E ANÁLISE DE INTELIGÊNCIA

O termo "Disciplina de Inteligência" está muito mais associado à função da coleta do que de análise [74]. No entanto, é inegável que se há uma especialização para a coleta de determinado tipo de fonte, também há para o seu manuseio em caso de conversões de formatos, adequações e, é claro, para a sua análise.

Se as INTs forem consideradas apenas como disciplinas de coleta de Inteligência, a especialização aplicada deixaria de fora todas as técnicas de processamento e análise. Assim, apenas a análise de todas as fontes (*All-Sources*) teria valor.

Para a etapa da Coleta, tem-se técnicas como as que buscam mais informações sobre e-mails, localizações e IPs. No Processamento, por exemplo, a edição de fotos ou vídeos para se obter uma melhor qualidade da imagem que será submetida a uma busca reversa ou a uma técnica de cronolocalização também é típica da disciplina OSINT. Na etapa da Análise, são várias as técnicas para Redes Sociais, Geolocalização ou Processamento da Linguagem Natural. A separação clara entre um conjunto de técnicas de coleta e outro para análise indica que as INTs podem ter os seus escopos compreendidos para as etapas de Coleta, Processamento e Análise.

Também típica de OSINT, a imensa quantidade de informações encontradas em fontes abertas é fre-

quentemente citada como justificativa para uma inevitável checagem da credibilidade das fontes [7]. Isso é corroborado por Jardines [5] que nos lembra que as informações coletadas de fontes abertas foram publicadas por outros, com seus próprios preconceitos e interesses. Dessa forma, OSINT é feita essencialmente a partir de informações coletadas de segunda mão, exigindo uma análise que verifique a credibilidade das fontes, algo que já teria sido feito se comparado pela perspectiva das demais INTs. Por isso, assim como qualquer ação de coleta pressupõe uma etapa de planejamento, uma análise que verifique a credibilidade das fontes é intrínseca ao processo de coleta de OSINT.

3.3 OSINT NO CICLO MULTI-INT

Há muitos processos para a coleta de informações de fontes abertas. Neste sentido, é necessária uma sequência de passos ou métodos que direcione a prática da coleta para obter resultados eficientes [15]. O ciclo de Inteligência representado na Figura 3.2 ilustra estas etapas, considerando uma única fonte, ou seja, qualquer INT unicamente. Considerando uma organização que tem acesso, como é mais provável, apenas a fontes abertas, esse ciclo se torna o próprio ciclo de Inteligência dessa organização.

Figura 3.2: Ciclo de Inteligência de única fonte. Fonte [o autor]

Em [3], [2] e [75], OSINT é descrita como parte da etapa de coleta do ciclo de Inteligência. Os resultados de cada INT precisam ser adicionados com os resultados obtidos das outras INTs e ordenados para serem executados em uma ordem que priorize as de menor complexidade, custo e risco, quase sempre, o caso de OSINT [5]. Entretanto, para que esses resultados sejam obtidos, as fases de Processamento e Análise específicas de cada INT também precisam acontecer. Observa-se também que a saída da etapa da Análise de cada INT também precisa ser consolidada em um produto, difundida e avaliada, mas essas etapas não parecem necessitar de processos que sejam diferentes para uma determinada INT. Assim, um ciclo de Inteligência de múltiplas fontes ficaria como o da Figura 3.3.

Uma visualização mais detalhada de um ciclo de Inteligência Multi-INT com OSINT e HUMINT está

Figura 3.3: Ciclo de Inteligência Multi-INT. Fonte [o autor]

na Figura 3.4, onde na etapa de Coleta do ciclo Multi-INT, ocorre uma chamada aos ciclos de única fonte OSINT e HUMINT que entregam os seus resultados de volta ao ciclo Multi-INT na etapa do Processamento. Essa mesma lógica se aplicaria para qualquer número de INTs. Destaca-se que a etapa da Direção não está no ciclo de cada INT porque a sua execução e efeitos devem valer para todo o ciclo de Inteligência, sendo que as particularidades de cada INT devem ser tratadas na etapa do Planejamento de cada ciclo de única fonte.

3.3.1 OSINT sob a perspectiva de primeira fonte

Todos os ciclos estudados até aqui procedem com a coleta de informações considerando as disciplinas de Inteligência. Nestes casos, deixam-se de lado os dados, informações e conhecimentos já possuídos ou previamente produzidos pela organização de Inteligência.

Considerando, por exemplo, a missão da ABIN de "antecipar fatos e situações que possam impactar a segurança da sociedade e do Estado brasileiros(...)" [45], se a missão for cumprida, ao menos parte das informações desejadas já estarão disponíveis para a organização de Inteligência. Não fica claro nos ciclos de Inteligência americano e brasileiro um passo que enriqueça a base de informações internas, que é descrito apenas no ciclo do Bellingcat.

Se a nova informação produzida não for incorporada ao conhecimento da organização de Inteligência, corre-se o risco constante de coletar novamente algo que já foi coletado em outro trabalho.

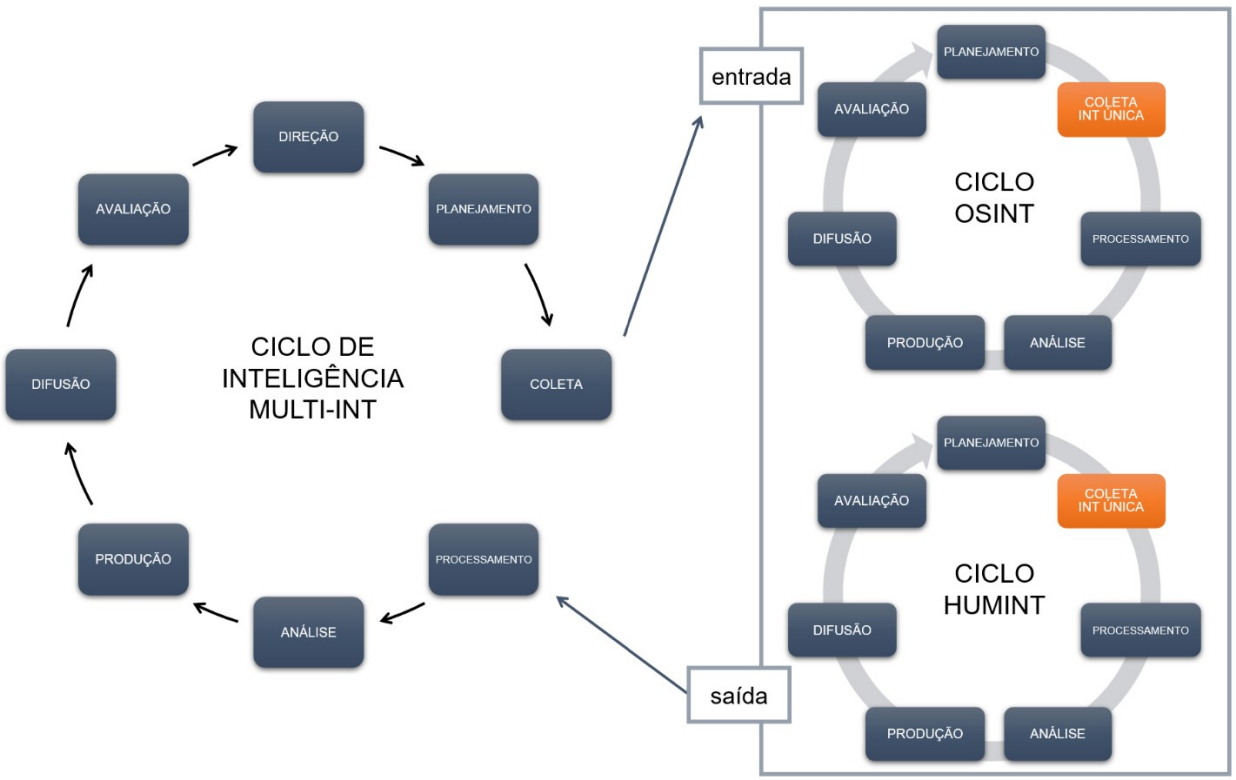

Figura 3.4: Ciclo de Inteligência Multi-INT com OSINT e HUMINT. Fonte [o autor]

3.4 VALORES E PRINCÍPIOS

Considerando a Doutrina da Atividade de Inteligência brasileira, os Valores estão listados apenas no Código de Ética e não nos Fundamentos Doutrinários [2], mas eles são apresentados como equivalentes aos Princípios em uma lista de "princípios e valores éticos" [14]. Alguns elementos estão presentes ao mesmo tempo da lista de Valores e na de Princípios, como é o caso da "imparcialidade", da "segurança" e da "cooperação", que aparece nos Princípios como "interação", possuindo o mesmo sentido de esforços compartilhados para a consecução de objetivos. Além disso, a "excelência do produto" parece carecer da conotação moral atribuída aos Valores.

Os Princípios apresentados na Tabela 2.2 são, então, considerados fundamentais para a Atividade de Inteligência brasileira. Outros podem se juntar a esses quando a Atividade se especializa tratando de uma Disciplina específica, como é o caso dos Princípios para OSINT apresentados na Tabela 2.3. Neste caso, também encontramos sobreposição de Princípios Fundamentais e os Princípios de OSINT, como é o caso da Objetividade e do Princípio fundamental Controle, quem em OSINT costuma ser apresentado como *Accountability*.

O Profissionalismo, embora não esteja listado como um princípio em si, é uma categoria de princípio, portanto tem o mesmo caráter norteador para as ações que todos os outros. A ABIN tem o profissionalismo como um valor institucional, mas há uma compreensão diferente do princípio para OSINT. Na ABIN, trata-se de "dedicação, compromisso e engajamento nas atividades desenvolvidas e no cumprimento da missão institucional, somados à busca contínua de aprimoramento pessoal e profissional" [14]. Enquanto

para OSINT significa uma forma metódica de fazer, distante do amadorismo, com bases éticas.

3.4.1 A necessidade de outros Princípios

Crises de saúde pública como a da pandemia da COVID-19 demonstraram a necessidade da prevenção do esgotamento físico e mental dos profissionais expostos constantemente a conteúdos violentos, ofensivos, tristes ou nojentos que podem desencadear sintomas de estresse [76] podendo levar ao esgotamento ou burnout. Assim, recomenda-se que estes profissionais também tenham apoio psicológico e sejam treinados para reconhecer estes sintomas e mitigar a exposição a tal conteúdo. Também a ansiedade de informação, entendida como a distância entre o que compreendemos e o que achamos que deveríamos compreender [77], tende a gerar esse esgotamento.

O desenvolvimento de novas tecnologias e atualizações constantes em OSINT exigem um princípio de Flexibilidade dos profissionais e do métodos para que eles possam ser adotados adequadamente. Está intrinsecamente relacionado ao princípio da Competência, pois o treinamento constante permite a adaptabilidade às novas tecnologias que certamente virão.

O treinamento das equipes de OSINT deve ser constante e passar por rotinas de reciclagem para se manter atualizado com a exploração de novos tipos e formatos de informação, bem como dos equipamentos e sistemas de segurança, conduzindo a necessidade de um princípio de Prontidão.

A interseção dos Valores da ABIN, dos Princípios da Atividade de Inteligência brasileira e os Princípios para OSINT é mostrada na Figura 3.5.

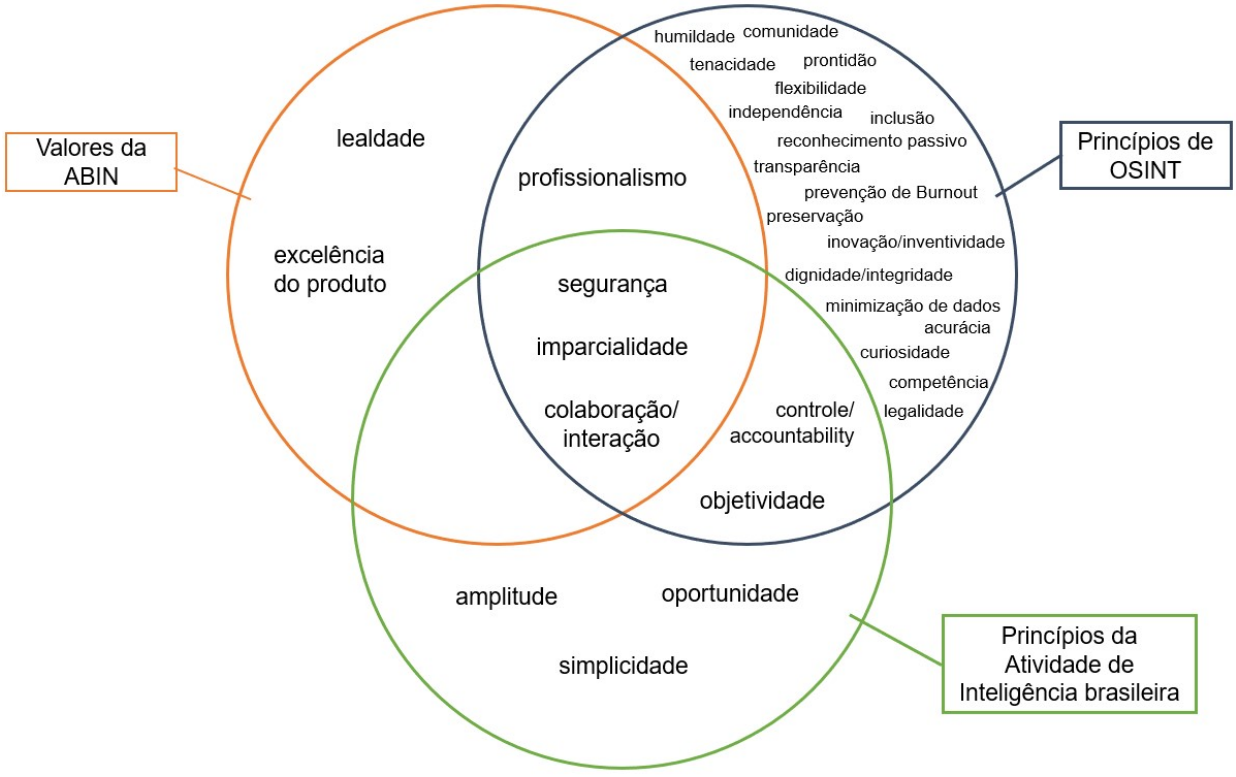

Figura 3.5: Interseção dos Valores da ABIN, dos Princípios da Atividade de Inteligência brasileira e os Princípios para OSINT. Fonte [o autor]

3.5 O MÉTODO PROPOSTO

Os caminhos percorridos pela informação dentro da disciplina OSINT são múltiplos e dependem do tipo de informação disponível. A cada tipo de informação correspondem vários tipos de técnicas. A junção de todos esses múltiplos caminhos e o encadeamento lógico de cada processo desenham um método para OSINT.

Fonte aberta precisa de verificação, e esta é uma função de análise. Às vezes, para que essa verificação aconteça, é necessário converter as informações, traduzindo-as ou transformando-as em um formato que possa ser utilizado. Observamos aqui a interpenetração das etapas de Coleta, Processamento e Análise do ciclo de Inteligência. Embora tradicionalmente as INTs sejam conhecidos como disciplinas de Coleta, na prática as etapas de Processamento e Análise também estão presentes.

A Figura 3.6 desenha a união do ciclo de Inteligência com uma abordagem Multi-INT e, em detalhes, as técnicas de Coleta, Processamento e Análise para OSINT em um método encadeado com as outras INTs com um começo e um fim bem definido. Um ciclo de múltiplas fontes organiza todo o desenvolvimento do produto e invoca os ciclos de única fonte de cada INT disponível e necessária. Uma explicação de cada etapa é apresentada a seguir.

3.5.1 Direção Multi-INT

Nessa etapa são definidos os requisitos e realizados todos os esclarecimentos necessários antes de serem transmitidos a unidades de coleta e análise específicas. Apesar de ser considerado um processo cíclico, a definição dos requisitos do usuário (assuntos de interesse, necessidades, etc.) normalmente é o início para o desenvolvimento da Inteligência. Ela funciona como um pré-requisito para as demais etapas, pois sem uma definição clara dos objetivos do trabalho, torna-se exaustivo e ocasional alcançar resultados que atendam aos assessoramento do usuário tomador de decisão. A partir daí, as etapas de Planejamento e Avaliação ocorrem paralelamente a todas as outras etapas.

3.5.2 Planejamento Multi-INT

A partir da definição das necessidades informacionais do usuário, ocorre a delimitação essencial do que já se sabe, do que falta saber e do tempo disponível para a consecução do trabalho.

Também é no Planejamento que são determinadas as fontes de informação necessárias, ou seja, quais INTs serão trabalhadas.

3.5.3 Coleta/Processamento/Análise Multi-INT

Ao iniciarmos esta grande etapa de Coleta, Processamento e Análise, usamos todas as INTs disponíveis, começando, quase sempre, por OSINT.

Ocorre então a sucessiva execução dos ciclos de única fonte para cada INT disponível e necessária e as respectivas etapas de Planejamento, Coleta, Processamento, Análise, Produção, Difusão e Avaliação.

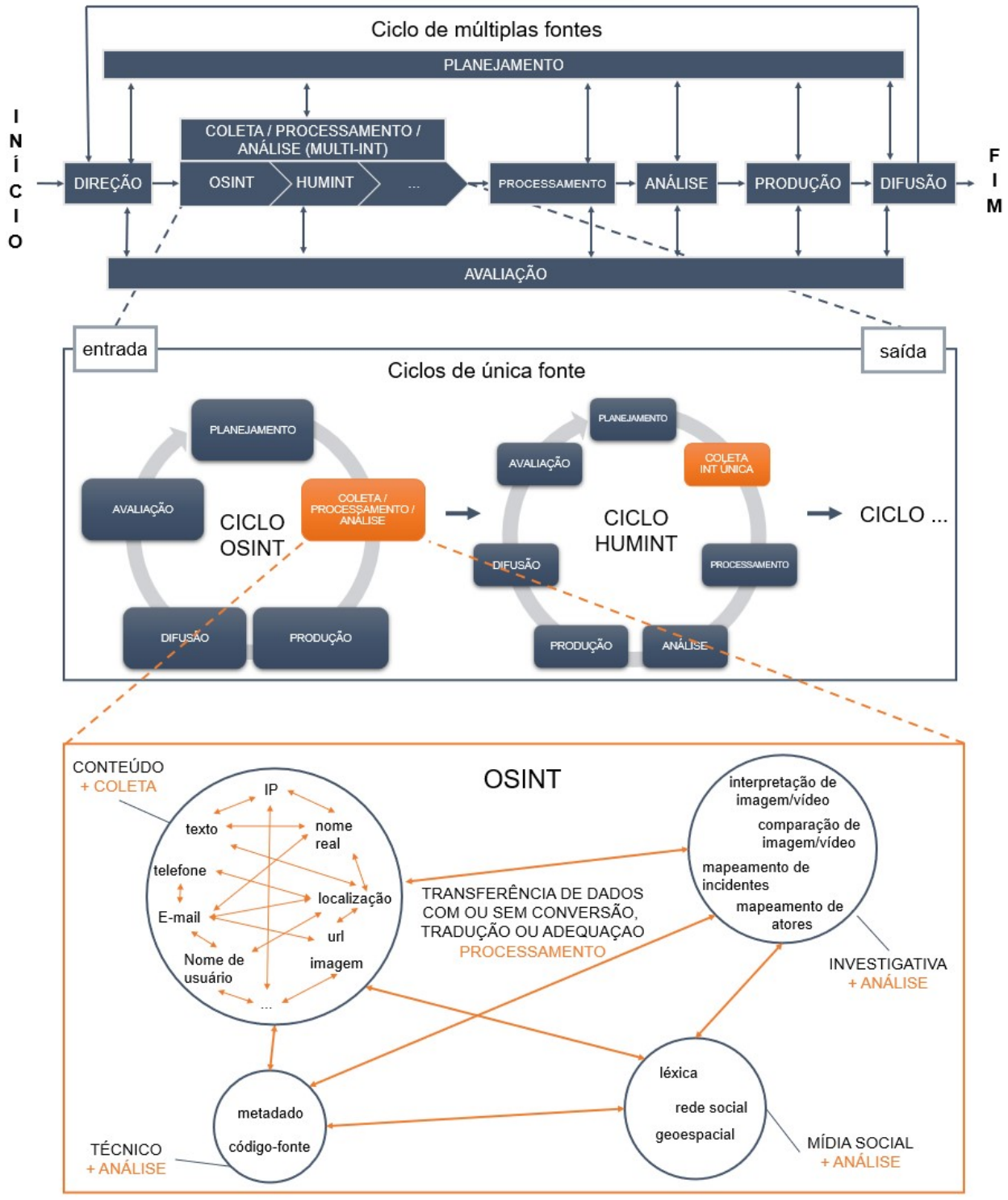

Figura 3.6: Método para OSINT. Fonte [o autor]

Aqui, apenas o ciclo OSINT será detalhado.

3.5.4 Planejamento de OSINT

Dependendo da informação inicial obtida da Direção e delimitada no Planejamento Multi-INT, o Planejamento de OSINT começa mostrando as características da especialização da disciplina quando aplica, por exemplo, princípios como a Prevenção de *Burnout*, preparando os profissionais para reconhecer e mitigar riscos de traumas, e o princípio do Reconhecimento Passivo para traçar os planos de mitigação de rastros digitais. Como a preparação do ambiente digital onde o trabalho ocorrerá considerando a configuração de máquinas, ferramentas, perfis e redes de acesso às fontes abertas.

3.5.5 Coleta/Processamento/Análise de OSINT

Todas as categorias de técnicas possuem particularidades que as aproximam mais de uma etapa do que de outra. No entanto, como já foi explicado, fonte aberta demanda verificação. Sempre que uma técnica de coleta for aplicada, intrinsecamente ocorrerá uma técnica de análise. Para que o resultado da saída de uma técnica seja usado como a entrada de outra, ocorrerá, no mínimo, uma transferência de dados entre elas, e quase sempre, algum Processamento para que o resultado seja utilizável na técnica seguinte.

Neste trabalho, consideramos que os motores de busca não são um tipo de informação que pode servir de ponto de partida para uma pesquisa, como colocado por Pastor-Galindo *et al.* [9], mas que podem ser técnicas ou ferramentas de recuperação de texto, sendo o tipo de texto o mais frequente e mais usado como um ponto de partida em pesquisas OSINT. Dessa forma, o tipo texto é transformado em outros tipos de informação que seguem para análise técnica, investigativa e de mídia social.

3.5.6 Produção de OSINT

O resultado é formalizado em um produto com todas as informações relevantes encontradas nesta INT.

3.5.7 Difusão de OSINT

O produto é distribuído tanto para a sequência da etapa do Processamento do ciclo Multi-INT quanto para subsidiar os ciclos das outras INTs. Um cuidado próprio de OSINT na Difusão é limpeza dos rastros digitais da pesquisa.

3.5.8 Avaliação de OSINT

Todas as etapas do ciclo OSINT são verificadas com a busca de avaliações da qualidade do trabalho para a melhoria das tarefas. Por exemplo, aqui se faria a avaliação do funcionamento de ferramentas. O resultado seria utilizado em uma próxima execução do ciclo, dando a noção de um processo contínuo.

3.5.9 Processamento, Análise, Produção e Difusão Multi-INT

O ciclo continua considerando os resultados obtidos de todas as disciplinas especializadas. O processamento deve providenciar que todos os resultados sejam utilizáveis para que a análise de todas as fontes aconteça. Assim, na Produção, o produto final seguirá o princípio da amplitude e deverá ser difundido para o usuário final.

3.5.10 Avaliação Multi-INT

Vista como uma etapa paralela a todo o ciclo, além de se preocupar com a qualidade da resposta percebida pelo usuário final quanto aos seus requisitos, ela também deve aferir as demais etapas na busca contínua da melhoria dos processos e mitigação de riscos.

3.6 A NECESSIDADE DE ESPECIALIZAÇÃO EM OSINT DOS PROFISSIONAIS DE INTELIGÊNCIA

No Brasil, a Lei Nº 11.776, de 17 de setembro de 2008, instituiu o Plano de Carreiras e Cargos da ABIN e criou as carreiras de Oficial de Inteligência, Oficial Técnico de Inteligência, Agente de Inteligência e Agente Técnico de Inteligência. As duas últimas com função de gestão técnico-administrativas, suporte e apoio logístico. Ao Agente de Inteligência coube o suporte especializado às atividades decorrentes das atribuições do Oficial de Inteligência [78]. Antes do Plano de Carreiras, o Oficial de Inteligência era conhecido como Analista de Informações.

São atribuições do cargo de Oficial de Inteligência, entre outras, planejar, executar, coordenar, supervisionar e controlar:

- a produção de conhecimentos de inteligência;
- as ações de salvaguarda de assuntos sensíveis;
- as operações de inteligência;

Dessa forma, infere-se que cabe ao Oficial de Inteligência a execução de todo o ciclo de Inteligência e que uma parte está dedicada mais para a produção de conhecimentos, outros para a salvaguarda de assuntos sensíveis e outros às operações.

Como OSINT é, geralmente, a primeira disciplina da coleta, se ela não for executada corretamente, as outras INTs estarão prejudicadas e, por conseguinte, a Análise.

A abordagem utilizada pela Inteligência dos EUA é mais condizente com esse grau de especialização, segmentando coletores e analistas, e ainda estabelecendo funções de gestão de coleta com foco nas etapas de Direção, Planejamento e Avaliação (ver Tabela 2.10).

Ainda que se tenha profissionais altamente capacitados em análise de Inteligência, se não houver o que analisar, todo o desenvolvimento do produto Inteligência estará comprometido.

3.7 SÍNTESE DO CAPÍTULO

Foi discutido o foco dado às ferramentas quando se trata de OSINT e o conflito disso com os valores, princípios e métodos. Valores e princípios devem ter longa duração enquanto as ferramentas quebram e demandam constante atualização. Em especial, foi apresentado o caso das ferramentas COTS.

Disciplinas de Inteligência costumam ser associadas à etapa da coleta do ciclo de Inteligência e essa abordagem vai de encontro às técnicas de processamento e análise típicas para cada tipo de fonte de informação.

O ciclo de Inteligência é executado de formas diferentes quando temos uma única fonte de quando duas ou mais são consideradas. Em qualquer cenário, parece ser inapropriado iniciar uma coleta sem procurar primeiro dentro da própria organização de Inteligência.

Novos desafios implicam em novos princípios para OSINT e isso é esperado em uma área que se atualiza constante e rapidamente.

Foi apresentado o método proposto nesta dissertação e as suas etapas foram detalhadas.

Por fim, discutiu-se a necessidade de profissionais especializados em coleta condizente com o nível de especialização demandado.

4 RESULTADOS

A pesquisa sobre os problemas apresentados e a solução proposta levaram a resultados que buscam avançar as discussões sobre OSINT como uma área de estudo.

4.1 O ARQUIVO É A PRIMEIRA FONTE

OSINT é geralmente considerada "a fonte de primeiro recurso" [79], no entanto, isso não parece fazer sentido para um ciclo de Inteligência. A fonte de primeiro recurso deve ser o próprio arquivo de informações da organização de Inteligência. A Figura 4.1 apresenta uma condicional que só realiza as disciplinas de coleta se a informação desejada não estiver no arquivo e atribui à Difusão um processo que insira ou atualize as informações no arquivo da própria Inteligência.

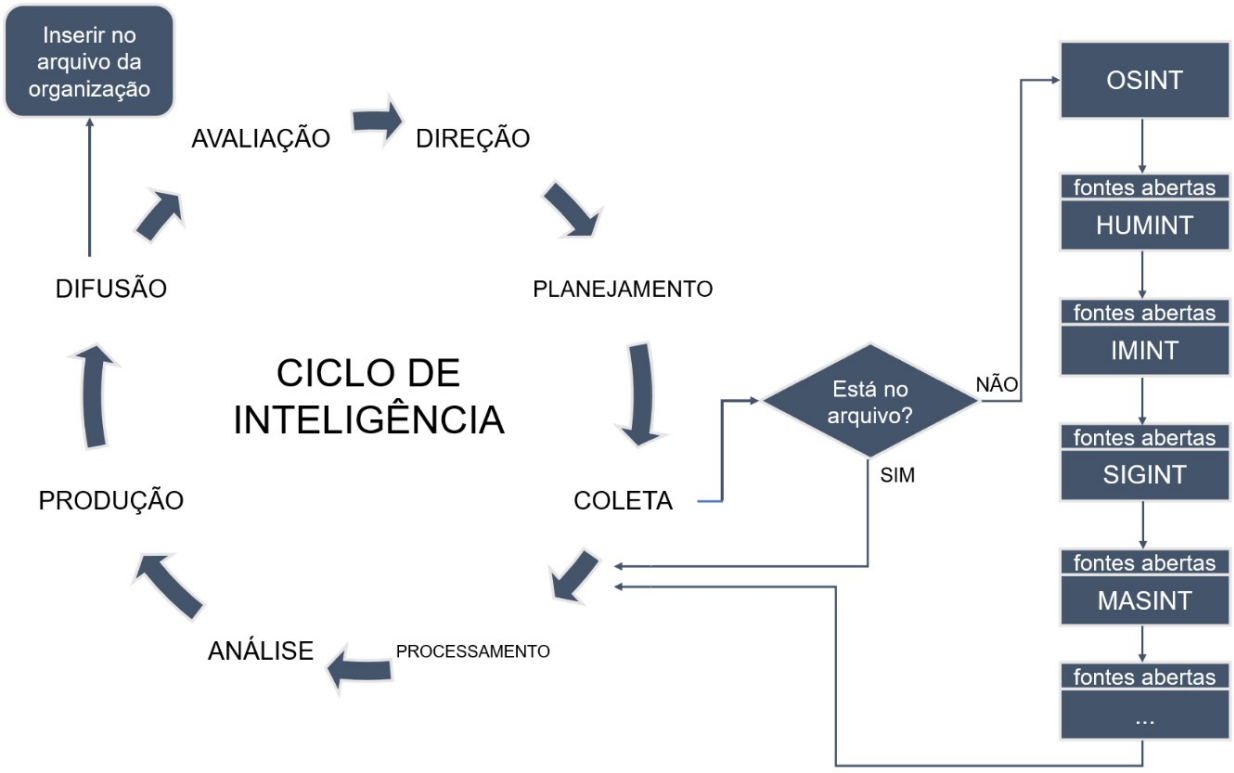

Figura 4.1: Ciclo de Inteligência com uma base de informações interna como primeira fonte de coleta e uma etapa de alimentação da base de informações. Fonte [o autor]

4.2 REUNIÃO DAS TÉCNICAS DE OSINT

Na Tabela 4.1 foram reunidas todas as técnicas apresentadas neste trabalho, com as suas respectivas categorias para organizar os diversos pontos de partida e, por consequência, os diversos pontos de chegada.

Tabela 4.1: Reunião e categorização das técnicas para OSINT

Técnicas de OSINT		
Categoria	**Técnica**	
Análise de Conteúdo	Tipos de Dados ou Informação	Mecanismo de Busca
		E-mail
		Nome de Usuário
		Nome Real
		Localização
		Nome de Domínio
		URL
		IP
		Imagem
		Vídeo
		Telefone
		Serviço TOR
		Áudio
		Veículo
		Criptomoeda
		SSID/BSSID
		Empresa
	Geolocalização	
	Cronolocalização	
Análise Técnica	Metadados	
	Código-Fonte	
Análise Investigativa	Comparação de Imagem/Vídeo	
	Interpretação de Imagem/Vídeo	
	Mapeamento de Atores	
	Mapeamento de Incidentes	
Análise de Mídia Social	Análise Léxica	Análise de Sentimento
		Processamento da Linguagem Natural
		Aprendizagem de Máquina
	Análise de Rede Social	
	Geoespacial	Geotagging

4.3 REUNIÃO DOS PRINCÍPIOS DE OSINT APRESENTADOS NESTA DISSERTAÇÃO COM OS DOS TRABALHOS RELACIONADOS

Prevenção de *Burnout*, Flexibilidade e Prontidão são são considerados princípios por esta dissertação. O primeiro é um princípio porque a exposição de um profissional a conteúdos perigosos pode acontecer a qualquer momento e comprometer a sua saúde e segurança. O segundo é uma característica moderna de

OSINT que apoia a adoção dos princípios listados como base para um trabalho sustentável e implica no terceiro para estar constantemente preparado para as mudanças que estão por vir.

Para atender ao princípio da Legalidade, se faz necessária a inclusão de princípios vindo das leis de proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia [8].

Princípios éticos e metodológicos profissionalizam uma atividade e perduram enquanto tecnologias e ferramentas mudam. Em OSINT, promovem a qualidade, reforçando a credibilidade, a confiabilidade e a potencial utilidade da informação produzida, minimizando possíveis danos aos vários interessados [7]. A Tabela 4.2 reúne todos os princípios tratados nesta dissertação.

Tabela 4.2: Princípios para OSINT.

Princípios	Bellingcat (15)	Trace Labs (17)	Berkely Protocol (7)	Belghith, Y. *et al.* (16)	GDPR (49)	Este trabalho
Princípios Éticos						
Dignidade/Integridade	✓	-	✓	-	-	✓
Diversidade/Inclusão	-	-	✓	-	-	✓
Humildade	-	-	✓	-	-	✓
Imparcialidade	-	-	-	-	-	✓
Independência	-	-	✓	-	-	✓
Tenacidade	✓	-	-	✓	-	✓
Transparência	✓	-	✓	✓	✓	✓
Princípios Metodológicos						
Acurácia	✓	-	✓	-	✓	✓
Colaboração	✓	✓	-	-	-	✓
Comunidade	-	✓	-	-	-	✓
Curiosidade	✓	-	-	-	-	✓
Inovação/Inventividade	✓	✓	-	-	-	✓
Minimização de Dados	-	-	✓	-	✓	✓
Não Rastreabilidade	-	-	✓	✓	-	✓
Preservação	-	-	✓	-	-	✓
Prevenção de *Burnout*	-	-	-	-	-	✓
Reconhecimento Passivo	-	-	-	✓	-	✓
Princípios Profissionais						
Accountability	-	-	✓	-	✓	✓
Competência	-	-	✓	-	-	✓
Consciência de Segurança	-	-	✓	-	-	✓
Flexibilidade	-	-	-	-	-	✓
Legalidade	-	-	✓	✓	✓	✓
Objetividade	-	-	✓	-	-	✓
Prontidão	-	-	-	-	-	✓

4.4 MÉTODOS COMO PRÉ-REQUISITOS PARA FERRAMENTAS DE OSINT

O foco nas ferramentas quando se trata de OSINT implica em uma questão de sustentabilidade. Os critérios apresentados por Revell *et al.* [19] colaboram de forma objetiva para a escolha de ferramentas e como avaliá-las em seu uso.

Além disso, uma ferramenta sem método carece de propósito já que o seu usuário não terá a orientação, também objetiva, da sua utilidade, gerando um provável efeito de "buraco de coelho". Antes da definição, compra ou treinamento de uma ferramenta, o método no qual ela será utilizada deve estar estabelecido.

4.5 EXPANSÃO DO ENTENDIMENTO DAS FERRAMENTAS DE OSINT

Algumas ferramentas são aplicativos ou serviços *on-line*, acessados por meio de um site e funcionam como um mecanismo de busca especializado em um tipo de informação, como nome de usuário, endereço IP ou e-mail. Os mecanismos de busca generalistas, como Google, Yandex ou Bing, geralmente são o ponto de partida para consultas *on-line* para obter mais informações. No entanto, para acessar o endereço desses buscadores precisamos de um navegador, que no que lhe concerne é instalado em um sistema operacional dentro de uma máquina (talvez virtual) que se conecta à internet por meio de um Provedor de Serviços de Internet (*Internet Service Provider* - ISP). No controle de tudo isso está uma pessoa e o seu perfil de acesso virtual. Todos esses itens podem ser entendidos como ferramentas e deixam rastros digitais (*fingerprinting* digital [76]) que podem tanto identificar o usuário que acessa um conteúdo *on-line* quanto segmentar esse mesmo conteúdo. Na prática, um mesmo serviço pode apresentar conteúdos diferentes dependendo do perfil de acesso. Portanto, não é apenas uma questão de confidencialidade de acesso, mas também de disponibilidade.

Para os propósitos deste estudo e especialmente para atender aos princípios de não rastreabilidade e consciência de segurança, o escopo das ferramentas foi estendido aos seguintes elementos:

- *endereço IP*: a cada acesso à internet é atribuído um endereço IP que pode revelar quem é o ISP, a localização do acesso, a organização que fornece o acesso ou a sua infraestrutura de rede. Para proteger essas informações é necessário disfarçar o IP, com a ajuda de um IP intermediário, que é utilizado pela origem da conexão para realizar os acessos no destino. Desta forma, o destino conhece apenas o IP intermediário. Entre as várias ferramentas que implementam esse disfarce estão a Rede Privada Virtual (*Virtual Private Network* - VPN), proxies ou a rede The Onion Router (TOR) [80].
- *Dispositivo, sistema operacional e navegador*: um IP é atribuído a uma interface de rede vinculada a um dispositivo. Essa ferramenta é a máquina (hardware) com a qual acessamos a internet e que possui um sistema operacional (*software*) como Linux, Windows, iOS ou Android. Esse conjunto de hardware e software também pode ser disfarçado por meio de máquinas virtuais que permitem, por exemplo, um notebook simular outros equipamentos, inclusive celulares. No topo dessa cadeia de acesso estão os navegadores, com as suas diversas configurações e extensões que conferem a esses aplicativos outras funcionalidades, incluindo a possibilidade de alterar o *User-Agent*, o qual é uma identificação que os navegadores passam para os sites e que esses sites usam para fornecer conteúdo e formatação adequados. A união das variáveis de configuração de hardware, sistemas operacionais, navegadores e os seus *User-Agents* formam os rastros digitais conhecidos como *fingerprinting* e são um exemplo da parte OSINT que existe no MASINT.
- *Sock Puppets*: seria inútil disfarçar todos os itens apresentados anteriormente se os dados nos perfis de acesso como e-mail, nomes de usuário e imagens apontassem para as identidades reais dos pro-

fissionais de OSINT. A não atribuição dos acessos da coleta às identidades reais dos profissionais de OSINT é a base do princípio de segurança nesta disciplina sendo feita com o uso de perfis falsos, conhecidos como *sock puppets* [77], ou seja, uma conta de usuário controlada por um indivíduo que pretende ocultar a sua verdadeira identidade ou obter acesso a um conteúdo específico desse tipo de conta de usuário. Um conjunto de *sock puppets* é como uma caixa de ferramentas, em que cada um tem um uso específico.

- *Comunicação e compartilhamento de informações*: invocando o princípio da colaboração, são necessárias ferramentas que permitam *feedbacks* rápidos sobre as descobertas, como WhatsApp, Slack, Signal ou Discord e para a troca de ideias, como discos virtuais ou planilhas para compartilhamento de informações.

4.6 DAS FERRAMENTAS AOS VALORES ÉTICOS

Valores e princípios compõem a formação mais duradoura de um profissional de OSINT. As ferramentas são a parte mais efêmera.

Partindo-se de ferramentas como o Google, Bing ou Yandex, descobrimos que cada uma possui particularidades sobre o seu modo de operação, com comandos específicos para delimitação, filtragem e ordenação dos resultados. A busca por uma mesma palavra nessas três ferramentas retorna resultados diferentes e em uma ordem diferente. Como cada uma trabalha com um algoritmo de indexação próprio, uma página encontrada em uma delas pode não aparecer nas outras duas.

Todas essas ferramentas recorrem à técnica que trata dos mecanismos de busca e as suas formas de indexar informações e organizar resultados. Ao se entender a maneira como ocorrem as indexações é possível explorar melhor os operadores booleanos, acessar conteúdos exclusivos para os motores de indexação ou mesmo utilizar a navegação pelos índices para não deixar rastros da investigação dos servidores de páginas dos alvos.

A ordem do uso de cada mecanismo de busca pode variar conforme o idioma do termo buscado, ou se a informação é do tipo imagem, de qual região geográfica é a imagem ou se o que buscamos não está acessível para os IPs de onde nos encontramos. Essa ordenação e o encadeamento desses processos até que se encontre a informação desejada, desenham um método.

Cada organização de Inteligência possui um *modus operandi* para o desenvolvimento do seu produto. Todas recorrerão a algum tipo de informação como ponto de partida desse desenvolvimento e cada tipo de informação definirá uma disciplina com um código de conduta e vários princípios.

Esses princípios são norteadores de ações, preferencialmente quantificáveis, mensuráveis, que devem diminuir a subjetividade a ajudar os profissionais a tomar decisões no cumprimento da sua missão organizacional.

Valores e princípios são muitas vezes usados como sinônimos, sendo que aos valores costuma-se atribuir uma ética moral, um balizador de alto nível de um padrão de comportamento. Destaca-se aqui o valor do profissionalismo porque é à ética profissional que associamos um fazer metodológico. Se a prática de

OSINT é um fazer profissional, então tem de haver uma forma correta de fazer, um método.

4.6.1 Valores e princípios ao longo do método

A seguir, alguns exemplos práticos da aplicação dos valores e princípios em OSINT.

Já na fase do Planejamento, são necessárias medidas de proteção para a segurança dos profissionais de Inteligência. O princípio da Prevenção de *Burnout* e as medidas para a redução de rastros digitais indesejáveis do Reconhecimento Passivo devem ser observados. A Não Rastreabilidade é um dos objetivos se *sock puppets* forem utilizados. Se o trabalho for muito complexo e exigir uma equipe, a Diversidade e a Inclusão trarão benefícios que permitirão uma compreensão mais completa de um caso.

Na fase da Coleta, antes de proceder com a obtenção de uma informação, deve-se observar se o princípio da Dignidade/Integridade não será afetado. E a Minimização de Dados precisa ser considerada antes de seguir para a Preservação de uma informação.

Na Análise, o princípio da Acurácia é condicionante para uma correta avaliação da credibilidade das fontes, sem a qual as informações analisadas carecem de valor.

Na Avaliação, a efemeridade das ferramentas não deve ser deixada de lado e os seus resultados precisam ser verificados com Independência.

Para além do dever profissional de cumprir uma tarefa, a Curiosidade impulsionará o trabalho, colocando a Tenacidade à prova e sendo balizada pela Objetividade. Em todo o desenvolvimento da Inteligência há de se manter uma Humildade para continuar conectado com o que não se sabe e se autoquestionar sobre o que se pensa saber.

4.7 CASO DE USO: EXECUÇÃO DO MÉTODO PROPOSTO

Suponha-se que um decisor demande assessoramento de uma instituição de Inteligência e que esta instituição disponha apenas de fontes abertas para o seu trabalho. De modo a fornecer alguns exemplos de contexto do uso do OSINT na perspectiva da Inteligência, a Figura 4.2 compara os ciclos de inteligência dos EUA, do Brasil e do método proposto nesta dissertação. A palavra Reunião (*Gathering* em inglês) usada na doutrina brasileira reforça a ideia de juntar tudo o que foi coletado e depois passar à fase em que a análise ocorre, ali chamada de Processamento.

Considerando o método proposto nesta dissertação, seguiríamos os seguintes passos.

1. Início: a Inteligência é demandada e o ciclo começa pela etapa da Direção;
2. a Inteligência precisa definir quais são as necessidades informacionais do seu usuário tomador de decisão na etapa da Direção. O ciclo dos EUA coloca essa tarefa com o Planejamento e o Brasil chama essa parte de Política. Seguindo o método proposto, a Direção estabelece junto ao decisor o que deverá ser buscado. A separação entre Direção e Planejamento, parece apropriada, pois difere o que será desenvolvido do como será desenvolvido.

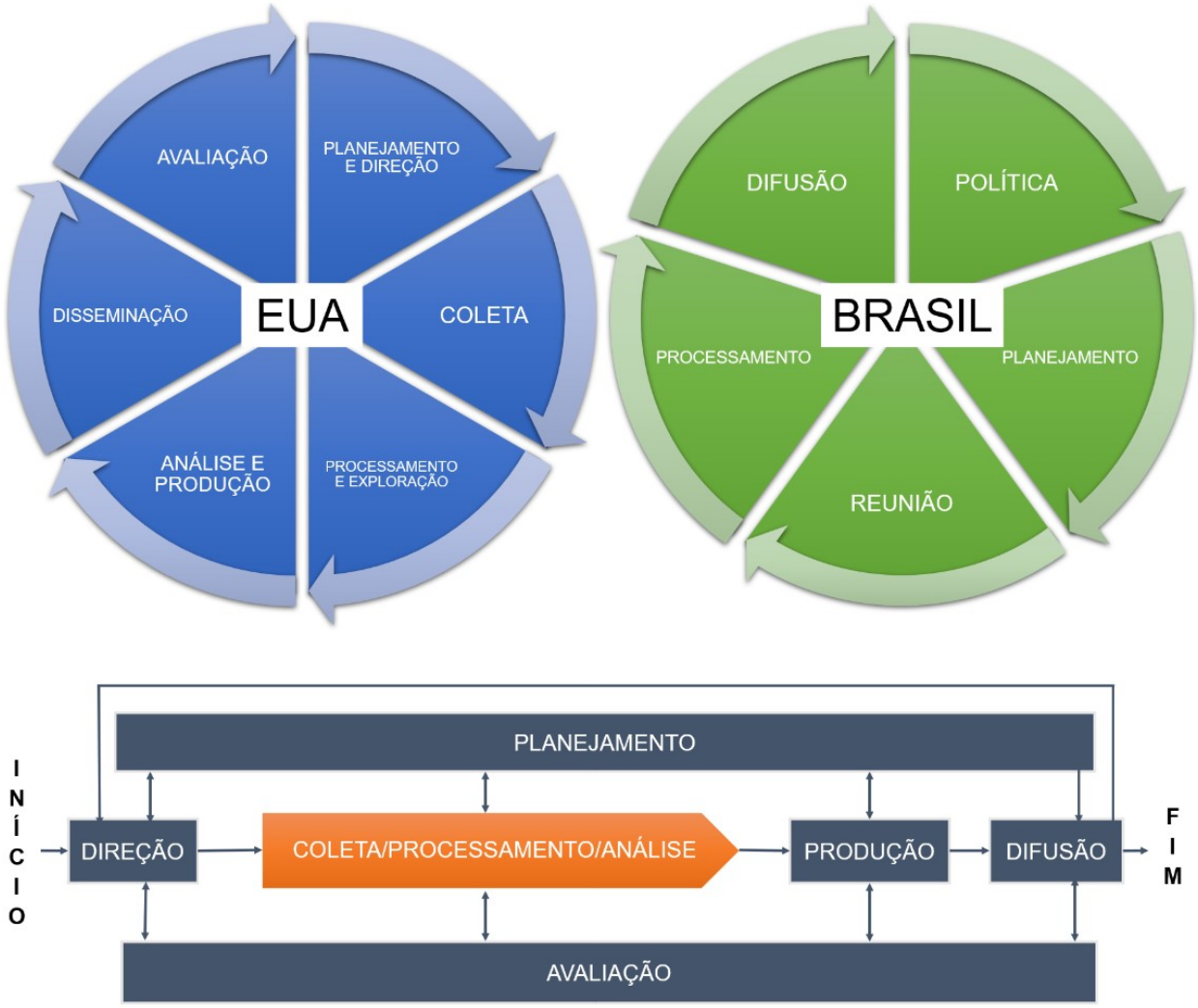

Figura 4.2: Ciclos de Inteligência rodando executando OSINT. EUA, Brasil e o proposto neste trabalho. Fonte [o autor]

3. O Planejamento no método proposto tem as mesmas funções dos demais ciclos, mas corre visualmente em paralelo a todas as etapas do ciclo. A mensagem é que cada etapa precisa de um planejamento e o ciclo todo também;

4. Dos requisitos do usuário e do Planejamento serão extraídas informações que servirão como ponto de partida para as etapas de Coleta, Processamento e Análise, que de tanto se sobreporem, na prática e no método proposto, formam uma grande etapa de Coleta/Processamento/Análise. Fonte aberta demanda verificação e toda análise demanda a coleta do que será analisado.

5. Antes de proceder com a coleta fora da organização, é crucial consultar o arquivo interno para saber se o que se precisa já está na base de conhecimentos da instituição;

6. Por exemplo, se partirmos da fotografia de um alvo, podemos tanto usar a técnica que busca a mesma imagem em outras bases de dados para se obter mais informação quanto a análise da interpretação da imagem para saber mais sobre os elementos visuais que a compõe;

7. A partir da mesma imagem poderíamos analisar os seus metadados e descobrir uma coordenada geográfica que indicaria o local onde ela foi registrada;

8. Como as coordenadas estavam um um formato diferente do aceito pelos mecanismos de busca disponíveis, foi necessário um processamento para converter as coordenadas em um formato utilizável;

9. A pesquisa por fotos publicadas nas proximidades daquela coordenada resulta em uma série de perfis em mídias sociais;

10. A análise de redes sociais desses perfis indica qual deles possui o maior número de conexões. Na descrição da conta há o endereço de um site;

11. O site está hospedado em um endereço IP com muitos outros sites;

12. O mapeamento das datas de registros desses sites indica que a maioria foi criada em um mesmo dia e que um deles foi registrado no dia anterior;

13. Esse site tem um e-mail registrado como o de contato do seu desenvolvedor;

14. Esse e-mail está associado a diversos perfis em mídias sociais que possuem um seguidor em comum. O mesmo com o maior número de conexões da análise de redes sociais;

15. O perfil desse seguidor publica fotos, muito parecidas com a que serviu como ponto de partida, indicando que fazem parte do mesmo contexto;

16. Todas as novas informações descobertas são organizadas para a formalização de um documento na fase da Produção;

17. Com o produto pronto, parte-se para a entrega ao usuário final. Nessa Difusão também ocorre a inserção das novas informações no arquivo da instituição;

18. Assim como a Direção estava mais próxima do usuário decisor, a Avaliação deve aferir se o usuário está satisfeito com as respostas obtidas, ou seja, se os seus requisitos foram atendidos;

19. Análoga ao Planejamento, a Avaliação também ocorre paralelamente desde a definição dos requisitos;

20. Fim: a execução do desenvolvimento da Inteligência é encerrada, mas como se trata de algo cíclico, novas demandas serão solicitadas e novos requisitos serão respondidos.

4.8 ANALISTAS, OPERACIONAIS E COLETORES DE INTELIGÊNCIA

Na comunidade de Inteligência dos EUA, especialmente na Agência Central de Inteligência (CIA), há profissionais especializados em análise, como o *Cyber Threat Analyst*, e profissionais especializados em coleta, como o *Open-Source Collection Specialist* [64] e o *Open-Source Exploitation Officer* [65]. Há também o *Open-Source Targeter*, que aproxima o OSINT de ações encobertas, conduzindo pesquisas e análises na Internet sobre alvos relevantes, enquanto alavanca ferramentas, conjuntos de dados e metodologias para operações adicionais encobertas e fornece pistas operacionais [63]. Na prática, transforma dados em operações de HUMINT. Estes profissionais de coleta empregam fontes abertas como precursores e capacitadores para todas as coletas encobertas e todas as outras INTs. Operações de Inteligência e coletas de alto custo, são recursos escassos. Portanto, as fontes abertas devem ser utilizadas para preservar estes recursos [81].

Como os ciclos podem ser tantos quanto forem as INTs e que, considerando OSINT, são muitas as técnicas e ferramentas de coleta e análise, espera-se um nível intenso e duradouro de dedicação do profissional dessa disciplina.

Existe demanda para coletores de Inteligência, especialmente, nas abundantes fontes abertas digitais.

4.9 SÍNTESE DO CAPÍTULO

O arquivo de uma instituição é a primeira fonte de consulta. Se não estiver lá, faz sentido procurar fora, começando pelas fontes abertas.

As técnicas apresentadas nesta dissertação foram reunidas e categorizadas em uma única tabela. O mesmo foi feito com os princípios para OSINT.

Ferramentas são essenciais e compõem um conjunto maior de elementos do que se costuma perceber. Mas ferramentas precisam funcionar em um método previamente estabelecido, e não o contrário.

Valores e princípios não devem ser noções gerais e rarefeitas para guiar um comportamento. Eles devem ser sólidos e de fácil percepção ao longo de todo o desenvolvimento de um produto de OSINT.

Por fim, foi apresentado um caso de uso que demonstra a execução do método proposto nesta dissertação.

5 CONCLUSÕES E TRABALHOS FUTUROS

Quando as informações necessárias para responder às exigências de um usuário não estão na base de informações de uma organização de Inteligência, elas podem ser buscadas por meio de OSINT. A gestão inadequada ou simplesmente inexistente desta base de informações tornam, na prática, as fontes abertas o primeiro destino das consultas. Se a coleta com OSINT não for feita corretamente, surge a possibilidade de uma ação encoberta para obter informações que estavam disponíveis para o público. De fato, ao impor a não atribuição, espera-se que ações encobertas equivalentes sejam implementadas para proteger a prática de OSINT. Neste sentido, a justificativa para conduzir uma operação de Inteligência envolve necessariamente uma execução prévia de OSINT.

Os métodos para OSINT são geralmente apresentados como versões do ciclo genérico de Inteligência. Além disso, é claro que há um tempo apropriado para fazer OSINT e que esta parte deve ser concluída antes de passar para outras fontes de coleta.

OSINT não deve ser resumida a uma lista de *sites*, aplicativos ou bases de dados. É claro que elas ajudam os profissionais a coletar informações, mas se a técnica que a ferramenta facilita não for totalmente compreendida, o resultado também não será. E isso também pode comprometer os princípios da independência e da imparcialidade. Este equívoco atinge principalmente os novatos, que são atraídos para o campo OSINT por seu aspecto tecnológico [16] ou por gestores sem familiaridade com a área. Como exemplo neste trabalho, são citadas algumas ferramentas que podem auxiliar determinadas técnicas, mas deve-se lembrar que uma ferramenta pode ser removida, inutilizada ou ficar desatualizada.

É compreensível o desejo por uma lista definitiva de ferramentas. São várias as listagens de serviços *on-line*, bancos de dados e *softwares* disponíveis na *web* como o OSINT *Framework* de Justin Nordine [82] e o OSINT Brazuca, com contexto no Brasil [83] . Entretanto, gerar e manter uma lista de ferramentas é uma tarefa sem fim à medida que os sites desaparecessem, e novas aplicações surgem [19].

A enorme quantidade de informações de fontes abertas na internet, as mudanças rápidas e contínuas nas suas tecnologias e uma abordagem imediatista por parte dos seus praticantes levaram o foco de OSINT ao uso de ferramentas em vez de métodos com valores e princípios. Os valores e princípios são o mais importante e devem vir em primeiro lugar. O foco nas ferramentas é enganoso e afasta o coletor OSINT da prática sustentável e profissional.

OSINT tem uma comunidade maior de profissionais do que outras INTs devido ao fácil acesso à internet, baixo custo, menor risco e instruções sobre técnicas e ferramentas tão difundidas quanto as próprias fontes abertas. Não é necessário estar em uma agência de Inteligência para fazer OSINT, mas se estiver, é imperativo que esta prática seja profissional.

Analistas analisam e operacionais executam ações secretas, inclusive para reunir informações. Mas por óbvio, para haver análise é necessário obter o que se pretende analisar e uma ação secreta para reunir informações não deve ser a primeira opção de ação, partindo-se da lógica de que o mais simples, de menor risco e de menor custo deve ser feito primeiro. Assim sendo, como já adotado pela americana Agência Central de Inteligência (CIA) com os seus profissionais especializados em OSINT ([64], [65] e

[63]), defende-se aqui que a Doutrina da Atividade de Inteligência brasileira reconheça a habilitação desse coletor especialista em fontes abertas no seu rol de profissionais.

Esta dissertação mostra uma maneira adequada de fazer OSINT. A coleta é uma das etapas do ciclo de Inteligência e tem os seus princípios, métodos, técnicas e ferramentas que requerem treinamento especializado e anos de dedicação. O valor do papel do coletor, especialmente em OSINT, ainda não é reconhecido, mas os grandes atores deste campo estão em movimento. Na área da cibersegurança, é uma carreira que está emergindo como uma das mais promissoras [84].

A medida da qualidade da Inteligência não está na dificuldade de obtê-la, mas no quão bem ela atende às necessidades do usuário. A informação de fonte aberta está presente em todas as INTs e é a mais facilmente obtida. Portanto, OSINT é a disciplina de coleta do ciclo de Inteligência que deve ser realizada, e ensinada, em primeiro lugar com foco em método, profissionalismo e ética.

5.1 TRABALHOS FUTUROS

Como trabalhos futuros, esta dissertação destaca:

- O mapeamento de outras técnicas e ferramentas para a coleta e análise de outros tipos de informações específicos;
- O desenvolvimento de um conteúdo programático para a capacitação de profissionais de Inteligência especializados em OSINT;
- O aprofundamento dos estudos sobre a Prevenção de *Burnout* para o trabalho com grandes quantidades de dados em ambientes com elevada ansiedade da informação;

REFERÊNCIAS BIBLIOGRÁFICAS

1 DAVIES PHILIP HJ; GUSTAFSON, K.; RIGDEN, I. The intelligence cycle is dead, long live the intelligence cycle: Rethinking intelligence fundamentals for a new intelligence doctrine. In: *Understanding the intelligence cycle*. Routledge, 2013. p. 70–89. Acessado em: 14/10/2022. Disponível em: <https://www.taylorfrancis.com/chapters/edit/10.4324/9780203558478-11/intelligence-cycle-dead-long-live-intelligence-cycle-rethinking-intelligence-fundamentals-new-\intelligence-doctrine-philip-davies-kristian-gustafson>.

2 ABIN. *Doutrina Nacional da Atividade de Inteligência - Fundamentos Doutrinários*. Gabinete de Segurança Institucional, 2016. "Portaria n.o 244-ABIN/GSI/PR", Coletânea de Legislação. Acessado em: 21/06/2022. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/Legislao3V5.pdf>.

3 ODNI Office of the Director of National Intelligence. U.S. National Intelligence: An Overview. *U.S. National Intelligence: An Overview*, 2013. Acessado em: 10/07/2022. Disponível em: <www.dni.gov/files/documents/USNI\%202013\%20Overview_web.pdf>.

4 EVANS, G. Rethinking military intelligence failure – putting the wheels back on the intelligence cycle. *Defence Studies*, Routledge, v. 9, n. 1, p. 22–46, 2009. Disponível em: <https://doi.org/10.1080/14702430701811987>.

5 JARDINES, E. A. Open source intelligence. In: *The 5 Disciplines of Intelligence Collection*. [S.l.]: Mark M. Lowenthal, Robert M. Clark, Ed. Los Angeles, CA, USA: C Press , ISBN: 9781452217635, 2015. p. 5–43.

6 WILLIAMS, H.; BLUM, I. Defining second generation open source intelligence (osint) for the defense enterprise. *RAND Corporation*, May 2018. Acessado em: 29/05/2022, doi: 10.7249/RR1964. Disponível em: <www.rand.org/pubs/research_reports/RR1964.html>.

7 Office of the United Nations High Commissioner for Human Rights (OHCHR) and the Human Rights Center at the University of California and Berkeley School of Lawl. *Berkeley Protocol on Digital Open Source Investigations*. 2020. Acessado em: 17/07/2022. Disponível em: <www.ohchr.org/Documents/Publications/OHCHR_BerkeleyProtocol.pdf>.

8 BELLINGCAT. *Workflow*. 2018. Acessado em: 20/05/2022. Disponível em: <https://yemen.bellingcat.com/methodology/workflow>.

9 PASTOR-GALINDO, J.; NESPOLI, P.; MÁRMOL, F. G.; PÉREZ, G. M. The not yet exploited goldmine of osint: Opportunities, open challenges and future trends. *IEEE Access*, v. 8, p. 10282–10304, 2020. Doi: 10.1109/ACCESS.2020.2965257. Disponível em: <https://ieeexplore.ieee.org/document/8954668>.

10 BAZZELL, M. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*. [S.l.: s.n.], 2022. ISBN-13: 979-8794816983.

11 KWON, H.; JIN, S.; SIM, M.; KWON, H.; LEE, I.; LEE, S.; KIM, M. "expanded workflow development for osint(open source intelligence)-based profiling with timeline." journal of digital convergence 19. *Journal of Digital Convergence*, v. 3, p. 187–94, March 2021. Doi: 10.14400/JDC.2021.19.3.187. Disponível em: <https://koreascience.kr/article/JAKO202111752550291.page>.

12 SINWINDIE. *GitHub - sinwindie/OSINT: Collections of tools and methods created to aid in OSINT collection*. 2022. Acessado em: 05/07/2022. Disponível em: <https://github.com/sinwindie/OSINT>.

13 HOFFMAN, M. *Introducing OSINT YOGA*. 2018. Acessado em: 05/07/2022. Disponível em: <https://webbreacher.com/2018/06/24/introducing-osint-yoga/>.

14 ABIN. *Código de Ética e Conduta dos Agentes Públicos da Agência Brasileira de Inteligência*. Gabinete de Segurança Institucional, 2022. "Portaria Nº 66/GAB-DIVAP/GAB/DG/ABIN/GSI/PR, de 17 de fevereiro de 2022.", Coletânea de Legislação. Acessado em: 21/09/2022. Disponível em: <https://www.gov.br/abin/pt-br/assuntos/noticias/abin-aprova-novo-codigo-de-etica-e-conduta/CodigodeEticaeCondutaABIN.pdf/@@download/file/CdigodeticaeCondutaABIN.pdf>.

15 BELLINGCAT. *Editorial Standards and Practices*. 2020. Acessado em: 22/05/022. Disponível em: <https://www.bellingcat.com/app/uploads/2020/09/\Editorial-Standards-Practices.pdf>.

16 BELGHITH, Y. The social structures of osint: Examining collaboration and competition in open source intelligence investigations. *Master Thesis, Virginia Tech*, v. 2021, Jun 2022. Acessado em: 26/05/2022. Disponível em: <http://hdl.handle.net/10919/103944>.

17 Trace Labs. *What We Do*. 2022. Acessado em: 22/05/2022. Disponível em: <https://www.tracelabs.org/about/what-we-do>.

18 WILD, J. *These are the Tools Open Source Researchers Say They Need*. Bellingcat, 2022. Acessado em: 18/10/2022. Disponível em: <https://www.bellingcat.com/resources/2022/08/12/these-are-the-tools-open-source-researchers-say-they-need/>.

19 REVELL, Q.; SMITH, T.; STACEY, R. Tools for osint-based investigations. In: ____. *Open Source Intelligence Investigation: From Strategy to Implementation*. Cham: Springer International Publishing, 2016. p. 153–165. ISBN 978-3-319-47671-1. Disponível em: <https://doi.org/10.1007/978-3-319-47671-1_10>.

20 ECONOMIST, T. *The promise of open-source intelligence*. 2021. Acessado em: 29/05/2022. Disponível em: <https://www.economist.com/leaders/2021/08/07/the-promise-of-open-source-intelligence>.

21 CORREIA, C. C. Opportunity: Competitive intelligence and information management. In: *The Emerald Handbook of Modern Information Management*. Emerald Publishing Limited, 2017. p. 811–844. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/978-1-78714-525-220171034/full/html>.

22 FURUHAUG, R. A. Open source intelligence methodology. *Master thesis, School of Computer Science and Informatics, University College Dublin, Ireland*, 2019. Acessado em: 15/06/2022.

23 HARARI, Y. N. *Sapiens - A sociedade afluente original*. New York, NY: Harper ebook, position 891, ISBN: 8525432180, 2015.

24 GIBSON, D. S. Exploring the role and value of open source intelligence. *Open Source Intelligence in the Twenty-First Century, Palgrave Macmillan, London*, p. 9–23, 2014. Acessado em: 14/10/2022. Disponível em: <https://link.springer.com/chapter/10.1057/9781137353320_2>.

25 DEUFF, O. L. L'open source intelligence (osint): origine, définitions et portée, entre convergence professionnelle et accessibilité à l'information. *I2D - Information, données & documents*, v. 1, n. 1, p. 14–20, 2021. DOI: 10.3917/i2d.211.0014. Acessado em: 12/10/2022. Disponível em: <https://www.cairn.info/revue-i2d-information-donnees-et-documents-2021-1-page-14.htm>.

26 BERGHEL, H. Robert david steele on osint. *Computer*, v. 47, n. 7, p. 1558–0814, July 2014. Pp. 76-81 ISSN. Acessado em: 14/10/2022. Disponível em: <https://ieeexplore.ieee.org/document/6861897>.

27 JANJEVA, A.; HARRIS, A.; BYRNE, J. The future of open source intelligence for uk national security. *Occasional Papers*, 2022. Acessado em: 03/05/2022. Disponível em: <https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf>.

28 HIMES, C. R. J. Rightly scaled, carefully open, infinitely agile: Reconfiguring to win the innovation race in the intelligence community. Acessado em: 14/10/2022. Disponível em: <https://intelligence.house.gov/uploadedfiles/final_start_report_v4.pdf>.

29 BRASIL. *LEI No 9.883, DE 7 DE DEZEMBRO DE 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.* 1999. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9883.htm>.

30 BRASIL. *Política Nacional de Inteligência. DECRETO Nº 8.793, DE 29 DE JUNHO DE 2016*. 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm>.

31 BRASIL. *Estratégia Nacional de Inteligência. Decreto de 15 de dezembro de 2017*. 2017. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/ENINT.pdf>.

32 HASTEDT, G. P. *Controlling Intelligence*. [S.l.]: Routledge, 2012. ISBN: 0714633941.

33 BRUNEAU, T. C. A inteligência como profissão. in: SeminÁrio atividades de inteligÊncia no brasil: Contribuições para a soberania e a democracia. 2022. Acesssado em: 12/10/2022. Disponível em: <https://www.senado.gov.br/comissoes/ccai/05-Segunda\%20Parte.pdf>.

34 KENT, S. *Strategic intelligence for American world policy*. [S.l.]: Princeton University Press, 2015. v. 2377. ISBN: 9780691650654.

35 SIANES, M. Compartilhar ou proteger conhecimentos? grande desafio no comportamento informacional das organizações. *STAREC, Cláudio; GOMES, Elisabeth; BEZERRA, Jorge. Gestão estratégica da informação e inteligência competitiva. São Paulo: Saraiva*, p. 259, 2005.

36 FERNANDES, F. d. C. Inteligência ou informações? *Revista Brasileira de Inteligência*, v. 2, n. 3, p. 7–21, set. 2006. Disponível em: <https://rbi.enap.gov.br/index.php/RBI/article/view/36>.

37 VAITSMAN, H. S. *Inteligência empresarial: atacando e defendendo*. [S.l.]: Interciência, 2001.

38 DEDIJER, S. Obvescevalna knjiznica v obvescevalnem zivcnem sistemu slovenije? *Organizacija znanja*, v. 10, n. 3, p. 124–129, 2005. Disponível em: <https://www.cobiss.si/oz/HTML/OZ_2005_3_final/6/index.html>.

39 KAY, T.; MCELREATH, D. Overview of the intelligence disciplines. 09 2020. Acessado em: 15/10/2022. Disponível em: <https://www.researchgate.net/publication/344224551_Overview_of_the_Intelligence_Disciplines>.

40 UK, M. of D. *Joint Doctrine Publication 2-00 (JDP 2-00) Understanding and Intelligence Support to Joint Operations*. 2011. Acessado em: 14/10/2022. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf>.

41 CEPIK, M. Profissionalização da atividade de inteligência: critérios de avaliação e desafios atuais. *Atividades de Inteligência no Brasil: contribuições para a soberania e a democracia*, Congresso Nacional, v. 1, n. 1, p. 179–198, 2003. Disponível em: <https://core.ac.uk/download/pdf/36735327.pdf>.

42 DINIZ, M. Profissionalização da atividade de inteligência. *Atividades de Inteligência no Brasil: contribuições para a soberania e a democracia*, Congresso Nacional, v. 1, n. 1, 2003. Disponível em: <https://core.ac.uk/download/pdf/36735327.pdf>.

43 BELLINGCAT. *About*. 2022. Acessado em: 23/04/2022. Disponível em: <https://www.bellingcat.com/about/>.

44 Human Rights Center. *About Us*. Acessado em: 22/06/2022. Disponível em: <https://humanrights.berkeley.edu/about/about-us>.

45 ABIN. *Mission, Vision and Values*. 2022. Acessado em: 11/06/2022. Disponível em: <https://www.gov.br/abin/pt-br/acesso-a-informacao/institucional/missao-visao-e-valores>.

46 AMINZADE, M. Confidentiality, integrity and availability–finding a balanced it framework. *Network Security*, Elsevier, v. 2018, n. 5, p. 9–11, 2018.

47 LITMAN, J. A.; SPIELBERGER, C. C. D. Measuring epistemic curiosity and its diversive and specific components. *Journal of Personality Assessment*, v. 80, n. 1, p. 75–86, February 2003. PMID: 12584070. Disponível em: <https://www.tandfonline.com/doi/abs/10.1207/S15327752JPA8001_16>.

48 GOOGLE. *Programmable Search Engine*. 2022. Acessado em: 23/05/2022. Disponível em: <https://programmablesearchengine.google.com/about/>.

49 GDPR.EU. *GDPR Principles relating to processing of personal data*. 2022. Acessado em: 23/05/2022. Disponível em: <https://gdpr.eu/article-5-how-to-process-personal-data/>.

50 NOBLE, S. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press, 2018. ISBN-10: 1479837245.

51 ZULKIFFLI, S. N. H.; ZAWAWI, M. N. A.; RAHIM, F. A. Passive and active reconnaissance: A social engineering case study. In: *2020 8th International Conference on Information Technology and Multimedia (ICIMU*. [s.n.], 2020. p. 138–143. Disponível em: <https://ieeexplore.ieee.org/document/9243402>.

52 ALTHOFF, M. Human intelligence. In: *The 5 Disciplines of Intelligence Collection*. [S.l.]: Mark M. Lowenthal, Robert M. Clark, Ed. Los Angeles, CA, USA: C Press, 2015. p. 45–79. ISBN: 9781452217635.

53 NOTE, W. N. Signals intelligence. In: *The 5 Disciplines of Intelligence Collection*. [S.l.]: Mark M. Lowenthal, Robert M. Clark, Ed. Los Angeles, CA, USA: C Press, 2015. p. 81–110. ISBN: 9781452217635.

54 HUGHES, P. M. Masint: An 'int' for the 21st century. no. 2. *American Intelligence Journal*, v. 36, Jun 2019. Acessado em: 15/07/2022. Disponível em: <https://www.jstor.org/stable/27066366>.

55 OMAND, D.; BARTLETT, J.; MILLER, C. Introducing social media intelligence (socmint). *Intelligence and National Security*, v. 27, p. 801–23, 2012. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/02684527.2012.716965>.

56 HERHKOVITZ, S. Crowdsourced intelligence (crosint): Using crowds for national security. *International Journal of Intelligence, Security, and Public Affairs*, v. 22, n. 1, p. 42–55, 2022. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/23800992.2020.1744824>.

57 BUBACH, R. O ciclo da inteligência e os requisitos para a produção do conhecimento. 2019. Acessado em: 16/10/2022. Disponível em: <https://repositorio.uvv.br//handle/123456789/570>.

58 HERMAN, M. *Intelligence power in peace and war*. [S.l.]: Cambridge University Press, 1996. ISBN 9780511521737.

59 CRUZ, A. Aprimoramento da capacidade analÍtica e avanÇo na atividade de inteligÊncia. *Revista Brasileira de Inteligência*, n. 15, p. 25–40, set. 2021. Acessado em: 29/10/2022. Disponível em: <https://rbi.enap.gov.br/index.php/RBI/article/view/178>.

60 SERRANO, L.; BOUZID, M.; CHARNOIS, T.; BRUNESSAUX, S.; GRILHERES, B. Events extraction and aggregation for open source intelligence: From text to knowledge. In: IEEE. *2013 IEEE 25th International Conference on Tools with Artificial Intelligence*. 2013. p. 518–523. Acessado em: 17/10/2022. Disponível em: <https://ieeexplore.ieee.org/abstract/document/6735294>.

61 LAYTON, R.; PEREZ, C.; BIRREGAH, B.; WATTERS, P.; LEMERCIER, M. Indirect information linkage for osint through authorship analysis of aliases. In: LI, J.; CAO, L.; WANG, C.; TAN, K. C.; LIU, B.; PEI, J.; TSENG, V. S. (Ed.). *Trends and Applications in Knowledge Discovery and Data Mining*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. p. 36–46. ISBN 978-3-642-40319-4.

62 USAJOBS. *Collection Manager*. 2022. Acessado em: 20/10/2022. Disponível em: <https://www.usajobs.gov/job/641982300>.

63 CIA. *Open Source Targeter*. 2022. Acessado em: 28/06/2022. Disponível em: <https://www.cia.gov/careers/jobs/open-source-targeter/>.

64 CIA. *Open Source Collection Specialist*. 2022. Acessado em: 28/06/2022. Disponível em: <https://www.cia.gov/careers/jobs/open-source-collection-specialist/>.

65 CIA. *Open Source Exploitation Officer*. 2022. Acessado em: 28/06/2022. Disponível em: <https://www.cia.gov/careers/jobs/open-source-exploitation-officer/>.

66 ONI, A. *Our Mission*. Office of National Intelligence, 2022. Acessado em: 20/10/2022. Disponível em: <https://www.oni.gov.au/about/our-mission>.

67 ONI, A. *Open Source Current Intelligence Analyst*. Office of National Intelligence, 2022. Acessado em: 20/10/2022. Disponível em: <https://bit.ly/3VcxwDf>.

68 HOLANDA. *OSINT rechercheur*. Werken bij de Rijksoverheid, 2022. Acessado em: 20/10/2022. Disponível em: <https://www.werkenvoornederland.nl/vacatures/osint-rechercheur-BD-2022-2769#0>.

69 HOLANDA. *Rechercheur OSINT Werk en Inkomen*. Werken bij de Rijksoverheid, 2022. Acessado em: 20/10/2022. Disponível em: <https://www.werkenvoornederland.nl/vacatures/rechercheur-osint-werk-en-inkomen-SZW-2022-0402#0>.

70 CANADá. *Investigator, Open-Source Intelligence (OSINT)*. College of Immigration and Citizenship Consultants, 2022. Acessado em: 20/10/2022. Disponível em: <https://college-ic.ca/whats-on/careers/Investigator-OSINT?l=en-CA>.

71 FRANçA. *Ingénieur analyste de données en cyber offensif*. DGSE, 2022. Acessado em: 20/10/2022. Disponível em: <https://www.dgse.gouv.fr/fr/le-recrutement/nos-offres-d-emploi/ingenieur-analyste-de-donnees-en-cyber-offensif-hf-31cyb20221103>.

72 LOWENTHAL, M. M. Osint: The state of the art, the artless state. *Studies in Intelligence*, v. 45, p. 63, September 2001. Acessado em: 19/05/2022. Disponível em: <https://www.cia.gov/library/readingroom/document/0006122548>.

73 BOEHM, B.; ABTS, C. Cots integration: plug and pray? *Computer*, v. 32, n. 1, p. 135–138, January 1999. Doi: 10.1109/2.738311. Disponível em: <https://ieeexplore.ieee.org/document/738311/>.

74 LOWENTHAL, M. M.; CLARK, R. M. *The five disciplines of intelligence collection*. [S.l.]: Sage, 2015. ISBN 978-4522-1763-5.

75 GIBSON, H. Acquisition and preparation of data for osint investigations. *Advanced Sciences and Technologies for Security Applications*, p. 69–93, 2016. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-319-47671-1_6>.

76 LAPERDRIX, P.; BIELOVA, N.; BAUDRY, B.; AVOINE, G. Browser fingerprinting: A survey. *ACMTrans. Web*, v. 14, p. 2, 2020. Article 8 33 pages, doi: 10.1145/3386040. Disponível em: <https://dl.acm.org/doi/10.1145/3386040>.

77 KUMAR, S.; CHENG, J.; LESKOVEC, J.; SUBRAHMANIAN, V. S. An army of me. In: *Proceedings of the 26th International Conference on World Wide Web - WWW '17*. [s.n.], 2017. p. 33. Doi: 10.1145/3038912.3052677. Disponível em: <https://dl.acm.org/doi/10.1145/3038912.3052677>.

78 BRASIL. *LEI Nº 11.776, DE 17 DE SETEMBRO DE 2008. Dispõe sobre a estruturação do Plano de Carreiras e Cargos da Agência Brasileira de Inteligência - ABIN, cria as Carreiras de Oficial de Inteligência, Oficial Técnico de Inteligência, Agente de Inteligência e Agente Técnico de Inteligência e dá outras providências*. 2008. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11776.htm>.

79 INE, B. E. Hidden in plain sight: The ever-increasing use of open source intelligence. *American Intelligence Journal*, v. 2, n. 29, p. 141–144, 2011. Acessado em: 12/06/2022. Disponível em: <http://www.jstor.org/stable/26201962>.

80 PROJET, T. T. *TOR Project*. 2022. Acessado em: 13/10/2022. Disponível em: <https://www.torproject.org/>.

81 JARDINES, E. A. *National Open Source Enterprise, April*. 2006. Accessed: Jun 30, 2022. Disponível em: <https://irp.fas.org/dni/osc/nose.pdf>.

82 NORDINE, J. *OSINT Framework*. 2022. Acessado em: 13/10/2022. Disponível em: <https://osintframework.com/>.

83 MRCL0WNLAB. *GitHub - OSINT Brazuca*. 2022. Acessado em: 13/10/2022. Disponível em: <https://github.com/osintbrazuca>.

84 SANS, I. *20 Coolest Cyber Security Careers*. 2022. Acessado em: 20/05/2022. Disponível em: <https://www.sans.org/cybersecurity-careers/20-coolest-cyber-security-careers/>.

APÊNDICES

Anexo I: Artigo submetido ao CSI 2022.

OSINT Methods in the Intelligence Cycle

Roberto Tanabe[1], Robson de Oliveira Albuquerque[1,2], Demétrio da Silva Filho[1,3], Daniel Alves da Silva[1], and João Jose Costa Gondim[1,4]

[1] Professional Post-Graduate Program in Electrical Engineering, Department of Electrical Engineering, University of Brasília, Brasília 70910-900
rtanabe@gmail.com; robson@redes.unb.br; dasf@unb.br; daniel.alves@redes.unb.br
[2] NUBANK Security Research; Brazil
security@nubank.com.br
[3] Institute of Physics, University of Brasilia, 70910-900, Brasilia, DF, Brazil
[4] Dept. of Computer Science, University of Brasilia (UnB), Brasília-DF 70910-900, Brazil
gondim@unb.br (J.J.C.G)

Abstract. The process for producing intelligence is traditionally represented by a series of steps forming a cycle. Collection is one of these stages and is characterized by the application of a set of disciplines to obtain information that will be analyzed for the production of an intelligence product. These disciplines are characterized according to the type of source, its methods and techniques. Open-Source Intelligence (OSINT) is the collection discipline focused on publicly available information. Open-source collection methods are usually represented by working diagrams that draw a flow according to the type of information. This paper makes a comparative study of the intelligence cycles of some relevant actors in the international OSINT scene, locates open-source collection in the intelligence cycle, and presents a workflow that combines this cycle with the techniques that form a method for OSINT.

Keywords: OSINT · Intelligence · Methodology.

1 Introduction

Intelligence obtained from open-sources is critical to the production of knowledge to support decision-making. Open-source intelligence (OSINT) is a discipline of gathering intelligence on publicly available information. The web and social media platforms have increased the amount of available data and facilitated access to information by promoting online searches and the rapid development of tools to facilitate information retrieval.

OSINT is usually related to a set of tools or a list of online services. Tools can be discontinued or cease to function and tend toward an automation that abstracts from understanding the techniques they enable. A technique is a specific way of performing a task, composed of processes that transform an input into an output. The information paths formed by techniques is usually called

a method. To be durable over time, OSINT methodological practice must be based on its techniques and not only on tools

Considering the above, the main contributions of this paper are:

a) Situates open-source intelligence in the intelligence cycle;

b) A comparative study of the OSINT intelligence cycles, methods and techniques of some relevant players in the global OSINT landscape; and

c) Presents a workflow that combines an intelligence cycle with the techniques that form a method for OSINT.

This paper is organized as follows: Section 2 defines some necessary background concepts and major related work in OSINT; Section 3 presents techniques and methods indicated for working with OSINT; Section 4 proposes a method for OSINT that combines a workflow of techniques with the intelligence cycle; Finally, Section 5 concludes the main observations of this paper.

2 Related Work

Intelligence refers primarily to the activities of state intelligence agencies or services that collect, analyze, and disseminate information to meet the requirements of a decision-maker.

The intelligence cycle is the process for producing intelligence. In general, it is formed by steps that: a) define the information requirements of a user; b) plan the fulfillment of these requirements; c) collect the necessary information to develop the final product; d) transform the collected information into a usable format; e) analyze the information to obtain meaning; f) create the intelligence product; g) transmit the intelligence product to the user who demanded it; and h) evaluate all these actions constantly. These general steps are usually presented as a continuous cycle (Fig. 1).

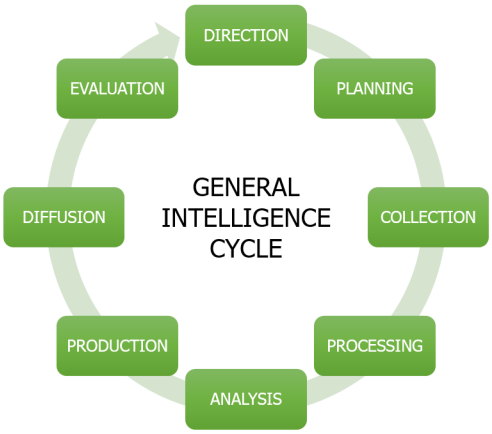

Fig. 1. A general intelligence cycle and its steps.

Collection is a step in the intelligence cycle, and is performed to collect information related to the intelligence gathering disciplines or intelligence sources in order to provide analysis of all available sources (all-source intelligence) [9].

A Discipline of Intelligence Collection (INT) is characterized by the specific methods, techniques, and type of sources for collecting information. Five disciplines are listed as classic INTs [13]. In addition to OSINT we have those of Table 1:

Table 1. Disciplines of Intelligence Collection descriptions

Disciplines of Intelligence Collection	Description
Human Intelligence (HUMINT)	The collection of information provided by a human source, where the collector interacts directly with the source, controls the discussion topics, and directs the source's actions [7].
Image Intelligence (IMINT)	Connected to the collection and analysis of images and geospatial information to describe, evaluate and represent georeferenced activities [14]
Signal Intelligence (SIGINT)	The intelligence form of collecting and processing various forms of electronically transmitted information; these forms are the communication of human language material and data derived from electronic transmission devices [15]
Measurement and Signature Intelligence (MASINT)	Produced by quantitatively and qualitatively analyzing the physical attributes of targets to characterize and identify them [12]. It uses various types of sensors, such as radiation meters.

There are many ways for collecting information from open-sources. Thus, an ordering of actions is necessary to obtain efficient results [6]. In [14,5,10], OSINT is described as one of the collection step disciplines of the intelligence cycle. The results of the collected one are then added to the results obtained from the other INTs (see Fig. 2).

Some authors have developed their own cycles for OSINT that have the advantage of working independently of being contained in a larger intelligence cycle that also considers other INTs. This is also one of the drawbacks since the absence of the other INTs makes an all-source product impossible. These cycles detail the path from identifying the decision maker's requirements to delivering the product. Some examples of these cycles are shown below:

2.1 Williams and Blum OSINT Cycle

Williams and Blum's cycle [18], has 4 stages. The first is the Collection stage, which includes identifying and obtaining potentially useful information and preserving what has been collected. The second, Processing, involves the translation, conversion and aggregation of the information into a usable format for the other steps of the cycle. In Exploration occurs the analysis that verifies the reliability

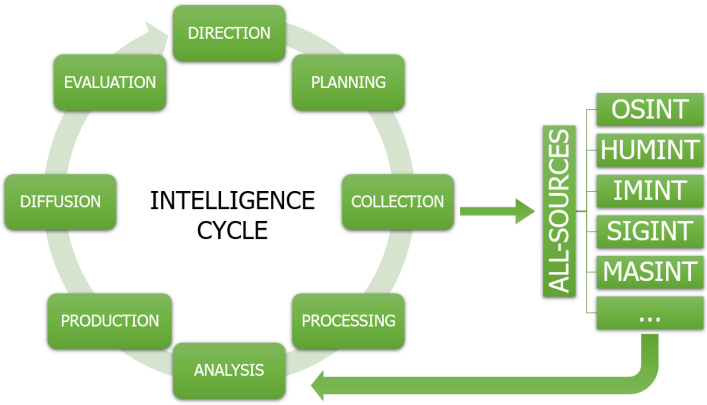

Fig. 2. OSINT as part of the Intelligence Cycle.

of the information and relates it to the interest of the decision-maker. In Production, there is the evaluation of whether the information produced should be classified and the delivery to the user. Fig. 3 refers to their cycle.

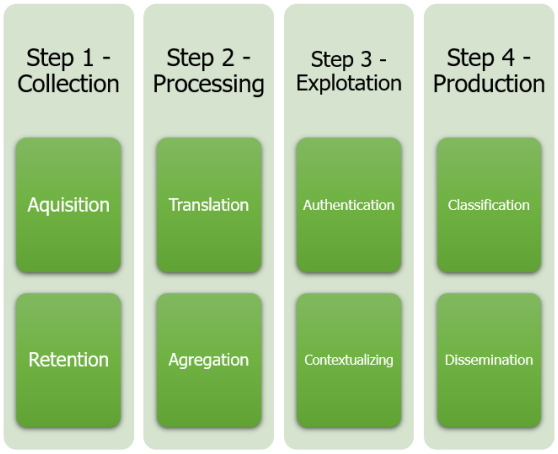

Fig. 3. Williams and Blum OSINT cycle [18].

2.2 Berkeley Protocol OSINT Cycle

The Center for Human Rights at the University of California, Berkeley, School of Law develops, in partnership with the United Nations Human Rights Office, an international protocol, the Berkeley Protocol on Digital Open Source

Investigations [17], that provides professional standards and guidelines aimed at improving its effective use in international criminal and human rights investigations [3].

The Berkeley Protocol has 6 steps: Online Inquiries to find information; Preliminary Assessment to determine if the benefits of collection outweigh the risks; Collection to capture digital items from the internet; Preservation to ensure that the information is stored and retrievable; Verification to assess the reliability of the sources and their content; and Investigative Analysis to interpret the data. The Berkeley Protocol OSINT cycle (Fig. 4) does not show a dissemination step, but it is described in the protocol.

Fig. 4. Berkeley Protocol OSINT cycle [17].

2.3 The Bellingcat OSINT Cycle

Bellingcat is an independent international group of researchers, investigators and journalists using open-sources to report on a variety of conflicts around the world [1].

The Bellingcat cycle begins in Identification with locating sources of information and determining their scope and depth. Next, Collection and Preservation occur to obtain the information and protect it from tampering and destruction. Next, in Verification, geospatial analysis tools, reverse image search, and visual data analysis are employed. In Analysis, the main questions of the case are answered. Next, in Review and Confirmation, content cross-referencing and incident classification are performed. Finally, the information is presented to the user and stored in a database. Fig. 5 shows the Bellingcat OSINT cycle. This

cycle shows that it tends to start with a large amount of not very relevant information, which in its 7 stages, would deliver to the intelligence user a small amount of very relevant information [2].

Fig. 5. Bellingcat OSINT cycle [2].

2.4 Pastor-Galindo *et al.* OSINT approaches

J. Pastor-Galindo *et al.* [16] propose a workflow that expands the amount of data about a target from social networks, email address, username, real name, location, IP address, and domain name. The execution of techniques specific to each piece of data generates an output that can be leveraged as input for another process (data transfer) that exploits another technique to generate more data. The Fig. 6 illustrates their approach.

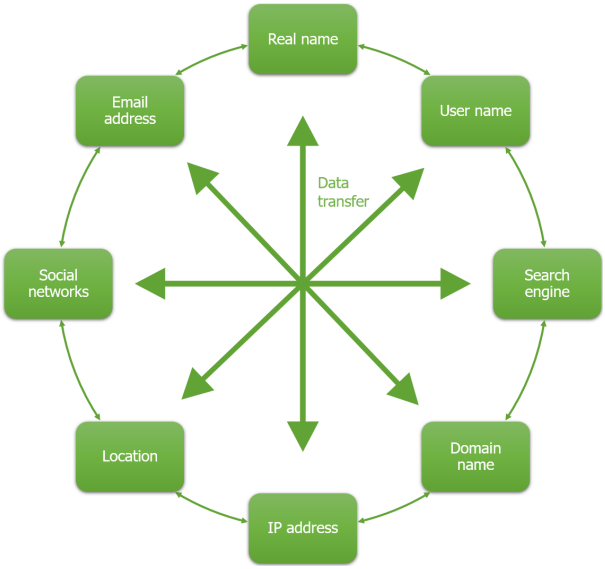

Fig. 6. From any starting point, the dataset about the target increases [16].

3 Techniques and Methods

The authors of the cycles presented in Section 2 also describe their techniques. Some techniques are focused on information gathering and others on analysis. Other authors represent the techniques through workflows or diagrams.

3.1 Techniques for gathering information according to Pastor-Galindo *et al.* [16]

J. Pastor-Galindo *et al.* present a list of techniques with a focus on collection according to the type of information one has, as shown in Table 2.

Table 2: Description of techniques for gathering information by Pastor-Galindo *et al.* [16].

Techniques	Description
Search engines	Services within the web receive a query trying to provide information that matches the input, returning information to the collector such as Google, Bing and DuckDuckGo;
Social networks	A lot of information about people or organizations can be found on social media platforms like YouTube, LinkedIn, and TikTok;
Email	An email address is unique and acts as the input for numerous web services;
Username	They are used for online services and are also a good way to collect information because the same username can be used in different web services and in each of them reveal information;
Real name	Searching for a target's real name can also reveal social media, home addresses, phone numbers, email, usernames, and more;
Location	Searching the locations related to a target can give us indications about a person's behavior. Photos, addresses, and GPS coordinates are all data that can be obtained;
Internet Protocol (IP)	IP addresses are important for digital forensics to collect information from an event; and
Domain name	They are related to the name of web services. They can reveal information about a target, such as the person who registered the site.

3.2 Techniques for analysis described in the Berkeley Protocol [17]

The Berkeley Protocol [17] segments the techniques by types of analysis, as shown in Table 3.

Table 3: Description of techniques for analysis described in the Berkeley Protocol [17]

Types of analysis techniques		Description
Techinical Analysis	Metadata	The data about other data, such as the latitude and longitude of where an image was taken
	Source Code	The programming language behind a web page (HyperText Markup Language - HTML) or software (Python, Java, PHP, etc)
Content Analysis	Geolocation	The identification of the whereabouts of an object or an activity
	Chronolocation	The identification of dates and times of an event. This can be done by analyzing the shadow projection of buildings to identify the time of day in a photo, for example.
Investigative Analysis	Image/Video comparison	The process of comparing characteristics of objects, people and/or places when at least one of them is an image
	Image/Video interpretation	Analysis of visual clues of objects and places;
	Spatial analysis	It involves examining different landscape objects and checking them against satellite or other imagery, geodata, and maps;
	Actor mapping	It is to identify the key players and their relationships;
	Social network analysis	It is the mapping and measuring of the relationships between the nodes of a network in the context of social media platforms;
	Incident mapping	It is used to establish the temporal and geographical relationships between different events.

3.3 Techniques used in social media content analysis based on Williams and Blum approach [18]

Williams and Blum [18], on the other hand, bring in the social network techniques applied to social media platforms (Table 4).

Table 4: Description of Social Network Analysis techniques by Williams and Blum [18]

Social Network Techinques	Description
Lexical analysis	It can cluster vast amounts of text and show the most earched terms in a search engine or which words appeared most frequently. At another level, it can infer information about the people involved including demographic characteristics. Common ways of doing this include Sentiment Analysis, Natural Language Processing and Machine Learning;
Social Network Analysis (SNA)	It attempts to explain relationships between individuals as a series of exchanges that can be mapped to understand the network of connected actors. SNA in the internet age has created an exponential supply of new data points in the study of network interactions. Among its techniques are: Degree, Density, Betweenness and Betweenness Centrality;
Geospatial	Social media platforms allow you to automatically link a post to a specific location. It includes Geotagging, Geolocating, Geo-inference and Georeferencing.

3.4 Methods described as workflows of techniques

Some authors prefer to describe methods as workflows of techniques through diagrams that show the path to be taken to work with each type of information.

Bazzell [8]'s diagrams map actions and tools that can show which username or social network is related to an email. Bazzell [8] also presents diagrams for real names, locations, usernames, phone numbers, and domain names.

These workflows by information type decrease the abstraction of what should be done in the collection phase, while detailing a way of doing things that takes into account the environment of each search, regionalisms, and the technical capacity of the OSINT collector.

Sinwindie [4] also uses the model presented by Bazzell to create his own diagrams. For example, Sinwindie [4] developed the diagrams for usernames, email, IP, image, person and website.

Fig. 7 shows examples of Bazzell's and Sinwindie's diagrams.

The continuous concatenation of the output obtained by one technique into an input for the next technique from several diagrams would make it possible, from one type of information, to arrive at another type. This can be illustrated in Fig. 8 by the use of Hoffman's [11] graph analyzer.

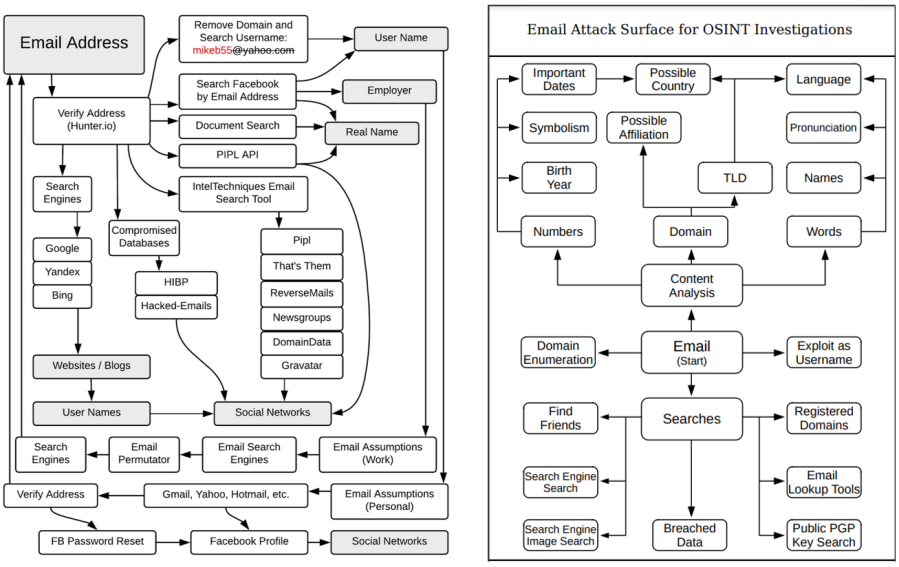

Fig. 7. Bazzell's (left) [8] and Sinwindie's (right) [4] workflows for email.

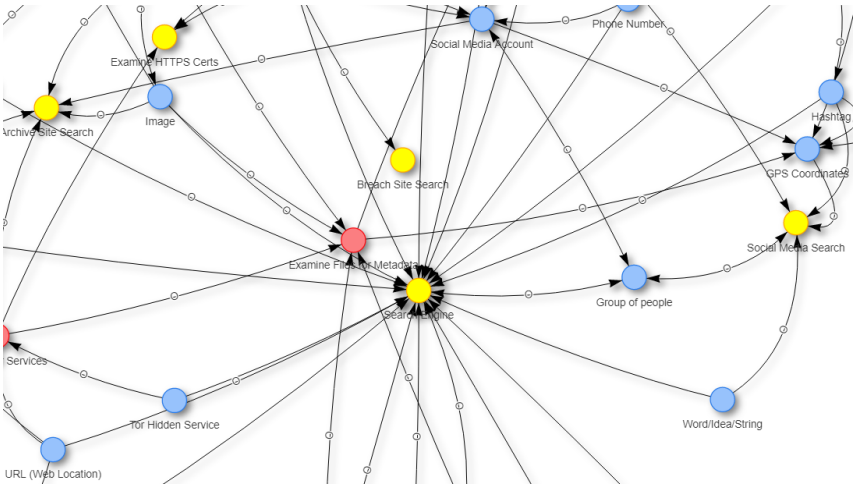

Fig. 8. Hoffman's OSINT Graphical Analyzer [11].

4 Proposed Method

Each type of information corresponds to several types of techniques. The combination of all the information paths within the OSINT discipline and the logical sequence of each technique constitutes a method for OSINT.

Open sources need to be verified, and this is an analysis function. Sometimes, for this verification to happen, the information needs to be converted, either by translating it or by transforming it into a format that can be used. Although traditionally INTs are known as collection disciplines, in practice the Processing and Analysis steps are indispensable in their execution.

Fig. 9 illustrates the detailing of the Collection, Processing and Analysis steps of the intelligence cycle with the respective OSINT techniques.

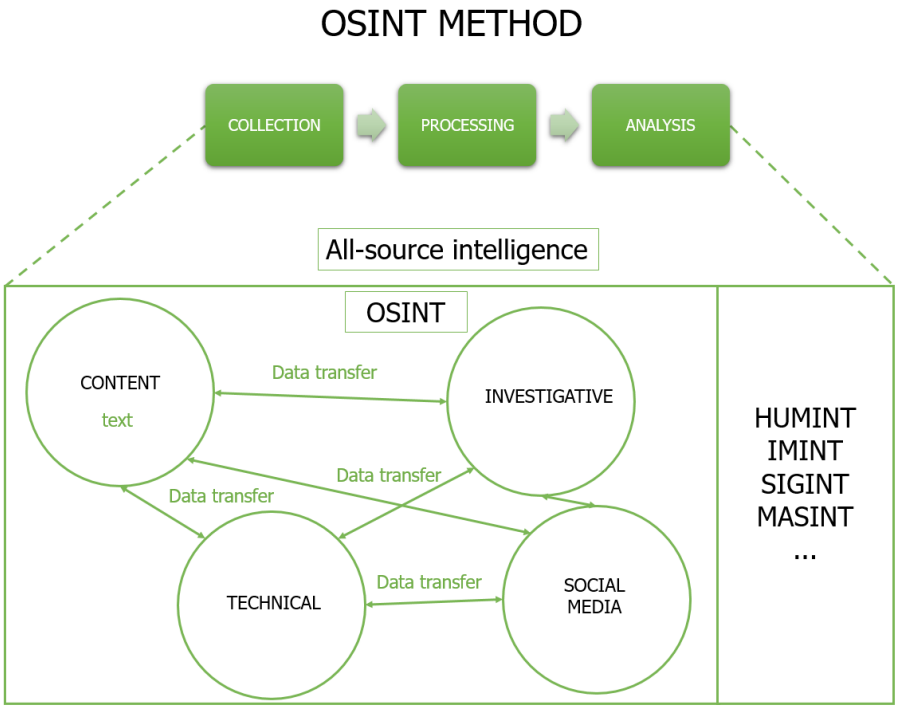

Fig. 9. OSINT Method

As we begin this major step of Collection, Processing and Analysis, we make use of all available INTs (all-source intelligence), starting with OSINT, since publicly available information is most easily obtained. The techniques presented in section 3 as analysis techniques are actually also collection and processing techniques at the same time.

In this paper, we consider the text type to be the most frequent and the most used as a starting point in OSINT collections. In this way, the text type is transformed into other types of information that then go on to technical, investigative and social media analysis.

Compared to the cycles unique to OSINT, the method proposed here excludes the Steering, Planning, Production, Dissemination and Evaluation phases, focusing only on the steps that obtain, transform and analyze information. It also places OSINT execution ahead of other INTs because of the free access characteristic of open sources. Mainly, this method contemplates the other INTs, allowing for a more complete Intelligence product considering other available sources of information.

5 Conclusion

Versions of the classic intelligence cycle are often presented as methods for OSINT which, as a collection discipline, are in the Collection phase. However, its analysis techniques and the eventual need to transform information into a useful format make OSINT, in practice, also part of Processing and Analysis, as shown in Fig. 9

OSINT techniques depend on the type of information you have, and when chained together to get more information about a target they draw paths that describe a method. Content, technical, investigative, and social media analysis techniques exchange information with each other until the publicly available information is addressed and then follow with the other INTs.

The cycles presented by J. Pastor-Galindo et al, Berkeley Protocol, Bellingcat and Williams and Blum work independently of the other INTs. The method presented in Section 4 unifies the workflow of the OSINT techniques with the general intelligence cycle and links it with the other collection disciplines.

6 Acknowledgments

The authors thankfully acknowledge the support of Brazilian Intelligence Agency - ABIN grant 08/2019; R.d.O.A. and D.A.d.S gratefully acknowledge the technical and computational support of the Laboratory of Technologies for Decision Making (LATITUDE) of the University of Brasília; the General Attorney's Office (Grant AGU 697.935/2019); the General Attorney's Office for the National Treasure – PGFN (Grant 23106.148934/2019-67); the National Institute of Science and Technology in Cyber Security – Nucleus 6 (grant CNPq 465741/2014-2); D.d.S.F gratefully acknowledges the financial support from the Edital DPI-UnB No. 02/2021, from CNPq (grants 305975/2019-6, and 420836/2018-7) and FAP-DF (grants 193.001.596/2017 and 193-00001220/2021-37); D.A.d.S gratefully acknowledges the National Department of Audit of the SUS (Grant DENASUS 23106.118410 /2020-85); the Deans of Research and Innovation and Graduate Studies at the University of Brasília (Grant 7129 FUB/AMENDA/DPI/COPEI/ AMORIS).

References

1. Bellingcat - the home of online investigations: About page, https://www.bellingcat.com/about/, last accessed 23/04/2022
2. Bellingcat: workflow page, https://yemen.bellingcat.com/methodology/workflow, last accessed 20/05/2022
3. Human rights center about us page, https://humanrights.berkeley.edu/about/\about-us, last accessed 22/06/2022
4. Sinwindie: Github - sinwindie/osint: Collections of tools and methods created to aid in osint collection, https://github.com/sinwindie/OSINT, last accessed 16/09/2017
5. National doctrine on intelligence activity - doctrinal foundations (2016), https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/Legislao3V5.pdf, "Portaria n.o 244-ABIN/GSI/PR", Coletânea de Legislação
6. Editorial standards & practices (2020), https://www.bellingcat.com/app/uploads/2020/09/Editorial-Standards-Practices.pdf, last accessed 22/06/2022
7. Althoff, M.: The five disciplines of intelligence collection, chap. Human Intelligence. Sage (2015), ISBN: 9781452217635
8. Bazzell, M.: Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. Inteltechniques.com, ninth edn. (2022), ISBN-13: 979-8794816983
9. Fingar, T.: A guide to all-source analysis. The Intelligencer. Journal of US Intelligence Studies. Association of Former Intelligence Officers **19** (2012), https://www.afio.com/publications/Fingar_All_Source_Analysis_in_AFIO_INTEL_WinterSprg2012.pdf
10. Gibson, H.: Acquisition and preparation of data for osint investigations. In: Open Source Intelligence Investigation, pp. 69–93. Springer (2016). https://doi.org/10.1007/978-3-319-47671-1_6
11. Hoffman, M.: Introducing osint yoga, https://webbreacher.com/2018/06/24/introducing-osint-yoga/, last accessed 05/06/2022
12. Hughes, P.M.: Masint. American Intelligence Journal **36**(2), 7–10 (2019), last accessed 15/06/2022
13. Kamiński, M.A.: Intelligence sources in the process of collection of information by the us intelligence community. Security Dimensions: International & National Studies (32), 02–105 (2019). https://doi.org/10.5604/01.3001.0014.0988
14. Office of the Director of National Intelligence, O.: Us national intelligence: An overview 2013 (2013), www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf, last accessed 10/06/2022
15. Nolte, W.N.: The five disciplines of intelligence collection, chap. Human Intelligence. Sage (2015), ISBN: 9781452217635
16. Pastor-Galindo, J., Nespoli, P., Mármol, F.G., Pérez, G.M.: The not yet exploited goldmine of osint: Opportunities, open challenges and future trends. IEEE Access **8**, 10282–10304 (2020). https://doi.org/10.1109/ACCESS.2020.296525
17. United Nations Office of the High Commissioner for Human Rights: Berkeley protocol on digital open source investigations. United Nations, New York, NY (Jun 2022), www.ohchr.org/Documents/Publications/OHCHR_BerkeleyProtocol.pdf, last accessed 17/06/2022
18. Williams, H., Blum, I.: Defining second generation open source intelligence (OSINT) for the defense enterprise. Tech. rep. (2018). https://doi.org/10.7249/rr1964, https://doi.org/10.7249/rr1964, last accessed 29/05/2022