Uma revisão sistemática de literatura para avaliação da OSINT (Open Source Intelligence) como ferramenta de auxílio ao combate a crimes cibernéticos.

Francisco de Assis Fialho Henriques – assishenriques@gmail.com
Computação forense e Perícia digital
Instituto de Pós-Graduação - IPOG
São Luís, MA, 10 de novembro de 2021

Resumo

O termo *Open Source Intelligence* (OSINT) ou Inteligência de Fontes Abertas é conceituado como uma análise de informações disponíveis ao público e que não possuem restrições quanto ao acesso. Refere-se à coleta e análise de inteligência com base em informações de fontes disponíveis publicamente - incluindo jornais, internet, revistas, relatórios governamentais, manuais etc. - de forma estruturada para responder perguntas específicas. A importância da coleta de inteligência a partir do crescimento tecnológico tornou-se um ponto em comum entre as literaturas especializadas. O presente estudo, através de uma revisão sistemática da literatura, busca identificar os estudos primários sobre o uso da OSINT como ferramenta de auxílio ao combate de crimes cibernéticos. A revisão sistemática de literatura é uma busca sistemática de estudos que visa deixar claro aos leitores os passos que foram feitos para definir os estudos relevantes para a pesquisa seguindo um protocolo de revisão pré-definido. O objetivo deste estudo é apresentar uma revisão sistemática da literatura sobre a OSINT (Open Source Intelligence) e como suas técnicas são aplicadas na perícia digital com o intuito de contribuir para o combate aos crimes cibernéticos. Fizeram parte do escopo dessa revisão 487 papéis obtidos de 4 bibliotecas digitais publicadas nos anos de 2017 a 2021, 43 artigos foram obtidos após a aplicação de critérios de exclusão e inclusão. Esta revisão confirma a eficiência do uso da OSINT no combate a crimes cibernéticos através dos estudos apresentados e métodos demonstrados. A importância da coleta de inteligência a partir do crescimento tecnológico tornou-se um ponto em comum entre as literaturas especializadas. Enfim, por meio de todo o estudo realizado e das metodologias apresentadas foi possível confirmar que a OSINT auxilia no combate a Crimes Cibernéticos por meio de dados existentes nas mais diversas fontes disponíveis para pesquisa.

***Palavras-chave**: Forense Digital. OSINT. Inteligência em fontes abertas. Revisão sistemática da literatura.*

1. Introdução

A informação possui grande importância na sociedade moderna. Nesse contexto, temos os desenvolvimentos tecnológicos e as informações provenientes do uso dessa tecnologia, impactando nossa sociedade de forma global e caracterizando-a como uma sociedade da informação, tornando os sistemas informáticos fundamentais para o seu funcionamento. Esse universo de conteúdos e ambientes está sujeito a um crescento aumento de pessoas e fraudes cibernéticas.

O objetivo deste artigo foi evidenciar, através de uma revisão sistematizada o uso da OSINT como instrumento necessário ao apoio aos agentes de segurança/inteligência no combate a crimes digitais.

Fazendo um paralelo com outros autores, as fontes OSINT são legalmente acessíveis pelo público sem violar quaisquer leis de direitos autorais ou privacidade e distinguidas de outras formas de inteligência por esse motivo. É por isso que eles são considerados "publicamente disponíveis", isso permite que o uso de OSINT vá além de serviços de segurança.

Conforme Hassan e Hijazi (2018), a sociedade foi transformada pelo advento da internet com bilhões de pessoas se comunicando e trocando informações. O autor deixa claro que os benefícios da era digital trouxeram diferentes tipos de riscos. Atores maliciosos como grupos terroristas, cibercriminosos ou estelionatários estão usando a internet para seus crimes.

O que existe nas fontes abertas , pode compor um grande arcabouço de conhecimentos de uma situação específica. Com métodos estruturados de pesquisa em fontes abertas, surge o processo de Inteligência digital,um processo que utiliza todos os meios tecnológicos , digitais, telemáticos e de interceptação de sinais, para de obter dados e analisá-los com o fim de produzir conhecimentos.

Devido a este cenário, foi formulada a seguinte questão de pesquisa:

1) A OSINT pode ser utilizada como ferramenta de apoio às forças de segurança em processos envolvendo Crimes Cibernéticos?

E questões secundárias:

1.1) Para quais funções a OSINT se aplica dentro do contexto da pesquisa em Computação Forense?

1.2) Quais as oportunidades da área prevista no estudo?

1.3) Quais os desafios descritos no estudo?

Nesse contexto, essa proposta de trabalho visa apresentar os conceitos de OSINT e como é utilizada como apoio à solução de crimes cibernéticos, preconizados por uma vasta compilação de artigos científicos.

O método de pesquisa adotado neste trabalho foi a revisão sistemática de literatura, que consiste em reunir evidências de material publicado anteriormente, consistindo principalmente de livros, artigos de revistas que são disponibilizados em diferentes bases de dados.

As pesquisas, do ponto de vista dos objetivos podem ser: exploratórias, descritivas e explicativas. O presente estudo é caracterizado como uma pesquisa descritiva, cujo principal objetivo é “descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. Envolve o uso de técnicas padronizadas de coleta de dados: questionário e observação sistemática. Assume, em geral, a forma de levantamento”.(GIL, 2009:42)

Este artigo está organizado da seguinte forma: seção “Resumo”, onde trataremos do objetivo geral, expondo a metodologia de pesquisa e descrevendo o método de revisão, com seus critérios.

A seção “Introdução” haverá uma contextualização de todos os tópicos abordados. No “Referencial Teórico” são apresentados os conceitos pertinentes ao tema, conceitos de OSINT e seu papel na Inteligência, o contexto histórico da cibersegurança e ferramentas de OSINT que auxiliam investigações e combate ao crime cibernético.
Em seguida, em “Metodologia de pesquisa” mostraremos todo o protocolo seguido para a elaboração da revisão sistemática. Os resultados da revisão, juntamente com uma análise detalhada e discussão de cada questão de pesquisa, dividem espaço na seção “Resultados e Discussão”, onde discutiremos o escopo desta revisão sistemática da literatura, bem como apontaremos novas pesquisas a serem exploradas sobre o uso da OSINT na aquisição da inteligência contra o crime cibernético e a sessão "Considerações finais” que apresenta considerações finais, limitações e propostas para trabalhos futuros.

2. Referencial Teórico

A revisão sistemática da literatura nos mostra que o pesquisador busca fontes atualizadas sobre os debates relacionados ao campo de conhecimento estudado. O referencial teórico que norteia esse artigo aborda os conceitos de OSINT e referencia pesquisas que abordam as metodologias de uso da OSINT na coleta de informações, além de outros trabalhos que servirão para demonstrar a eficiência da OSINT no auxílio às forças de segurança para combate a delitos, além de conceitos utilizados por pesquisadores na criação de metodologias e frameworks que usam as informações obtidas por OSINT como base de seus trabalhos.
A Cybersecurity Ventures estima que os custos globais do crime cibernético cresçam 15% ao ano nos próximos cinco anos, atingindo US $ 10,5 trilhões anualmente até 2025,fazendo com que governos invistam no desenvolvimento de ferramentas e técnicas em inteligência de código aberto (OSINT) para combater esses crimes. (MINDSECBLOG, 2021)
Como nos mostra Barreto e Wendt (2020:2) os inúmeros dados e informações disponíveis não são usados pelos operadores da segurança pública , mais especificamente os agentes de Inteligência e de investigações policiais. Embora de elaborado de forma coordenada com todas as fases de conhecimento elaboradas, por algum desconhecimento do agente de segurança na coleta e busca dos dados, o conhecimento é gerado de forma incompleta ou imprecisa.
De acordo com Silva e Menezes (2005:38), a revisão de literatura/pesquisa bibliográfica contribuirá para: obter informações sobre a situação atual do tema ou problema pesquisado; conhecer publicações existentes sobre o tema e os aspectos que já foram abordados; verificar as opiniões similares e diferentes a respeito do tema ou de aspectos relacionados ao tema ou ao problema de pesquisa.

2.1 OSINT - Conceitos Básicos

O conceito de OSINT é amplo, sua aplicabilidade dependerá de como cada investigador/pesquisador usará as fontes abertas para as consultas sobre determinado assunto. Fonte é "qualquer dado ou conhecimento que interesse ao profissional de inteligência ou de investigação para a produção de conhecimento" (BARRETO e WENDT, 2020:4).
Segundo Evangelista *et al.*, (2020) , o conceito de OSINT é um conceito que aborda a busca, coleta, processamento, análise e uso de informações de fontes abertas que podem ser acessadas legalmente por qualquer indivíduo ou organização.
Como nos assegura Cepik (2003:32), o conceito de OSINT é:

> a análise baseada na “ obtenção legal de documentos oficiais sem restrição de segurança, da observação diretae não clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países ou alvos, do monitoramento da mídia, da aquisição legal de livros e revistas especializadas de caráter técnico-científico”.

OSINT inclui todos os acessos públicos para obtenção de informação, entre eles: a Internet, mídia tradicional, jornais especializados ou informações geoespaciais.

Pode-se dizer que fontes abertas existem há muitos anos, mas com a explosão da internet houve muitos profissionais de segurança cibernética e pesquisadores publicando revistas e artigos sobre ameaças de crimes cibernéticos. Bem como pessoas comuns publicando informações de relevância, ou não, sobre particularidades de suas vidas.

Neste contexto, fica claro que muito de inteligência preditiva pode ser obtida de fontes públicas e não classificadas.

Os dados de inteligência devem ser coletados de diferentes fontes, desta forma, como preconizam Yeboah-ofori e Brimicombe (2018:88), a importância da OSINT tornou-se um conflito entre o setor privado, o governo e os militares sobre como os dados de inteligência devem ser coletados de diferentes fontes.

A coleta, exploração e divulgação da forma correta e em tempo hábil com o propósito de abordar requisitos específicos de inteligência tem sido um grande desafio.

A IDC Research, em pesquisa de 2020, informa que a “quantidade total de dados digitais criados em todo o mundo chegará a 44 zetabytes e o número aumentará mais rápido dentro de cinco anos para chegar a 180 zetabytes em 2025”. (DNA DATA STORAGE ALLIANCE, 2021)

Conforme explicado acima, concluímos que o aumento do número de pessoas que usam a Internet para fazer seus trabalhos e, consequentemente, o crescente volume de dados digitais, farão das fontes on-line a principal fonte do OSINT para tanto governos quanto corporações empresariais no futuro.

Conforme Hassan e Hijazi (2018:10), vários autores podem beneficiar-se da OSINT e suas motivações podem ser as mais diversas. Os maiores consumidores de fontes OSINT são os departamentos militares, governo e órgãos governamentais, devendo esse consumo ao enorme desenvolvimento tecnológico e o uso generalizado da Internet em todo o mundo.

Governos utilizam fontes OSINT para diversos propósitos, desde a segurança nacional à compreensão das opiniões públicas nacionais e estrangeiras sobre diferentes assuntos.

Organizações internacionais usam OSINT para proteger sua cadeia de suprimentos de grupos terroristas, analisando sites de mídia social e aplicativos de mensagens da Internet para prever futuras ações terroristas.

Os autores deixam claro que todas as metodologias têm algumas limitações e desafios, entre eles o alto volume de dados, confiança de fontes e esforços humanos.

Pode-se dizer que OSINT traz grandes responsabilidades ao agente que faz uso de suas ferramentas, neste contexto, fica claro que há preocupações legais em muitos casos. O mais preocupante, contudo, é constatar que existem formas de alguém adquirir informações por meios ilegais e como o sistema de leis deve lidar com isso.

Outra preocupação é quando algumas formas de informações públicas ocultas são coletadas e amplamente divulgadas como parte de um escândalo.

É importante considerar que os benefícios do OSINT estão em várias áreas e ninguém deve subestimar seu uso. A coleta em fontes abertas não fornece riscos quando comparada a outras formas de inteligência e seu custo é bem menor quando comparado a outras fontes, por exemplo, o uso de satélites espiões.
Hasan e Hijazi (2008:341, tradução nossa), nos mostra a importância da OSINT quando afirma:

> A era da informação resultou em uma quantidade explosiva de fontes potenciais de inteligência e moldará o futuro da coleta de OSINT. Na arena de inteligência, prevê-se que a prática de coleta de dados online para combater o terrorismo e solucionar o crime aumentará. Além disso, OSINT continuará a oferecer um método barato para adquirir inteligência sobre qualquer comunidade ao redor do globo[1].

O autor deixa claro que a OSINT é o método preferido para a obtenção de informações das agências em todo o mundo. Importante frisar que a OSINT não está limitada apenas às forças de segurança e serviços de inteligência, OSINT pode ser usada como um processo fundamental na tomada de decisões por agências não governamentais bem como pela sociedade civil.
Espera-se, dessa forma, que a OSINT seja cada vez mais inserida no cotidiano do cidadão comum para que possa obter informações além das fontes mais comuns - muitas vezes com informações manipuladas - a fim de buscar conhecimentos sobre como os criminosos agem no mundo digital e ter acesso a ferramentas que auxiliarão na proteção contra crimes cibernéticos.

2.2 Cibersegurança e OSINT

A origem da Cibersegurança data da década de 1970, quando em 1977 o governo norte-americano reconheceu que o acesso aberto aos sistemas de computador poderia gerar falhas de segurança, nessa ocasião o projeto de lei de proteção do sistema de computador federal, proposto, não foi aprovado na revisão do Congresso.(KREMLING e PARKER, 2018:57)
De acordo com Lynett (2015), a computação em rede estava surgindo, pois até o fim dos anos 80 a internet como conhecemos ainda não havia sido materializada.
As grandes organizações, especialmente os governos, estavam começando a ligar computadores via linhas telefônicas embora não houvesse uma rede mundial. Reconhecendo isso, as pessoas começaram a procurar maneiras de entrar nas linhas telefônicas conectadas aos computadores, para que pudessem roubar dados. Essas pessoas se tornaram os primeiros grupos de *hackers*.
Na década de 1980, foi lançado o filme *WarGames* e em 1983, as tentativas de *hacking* aumentaram, em parte graças a seu lançamento. Em 1987 surge a Lei de Segurança Informática para fortalecer as medidas de segurança para sistemas online.
A década de 1990 nos apresenta o início da indústria da Segurança da Informação. As redes baseadas em *Internet Protocol* (IP) mudaram o foco para a disponibilidade, surgindo nessa mesma época ameaças como vírus e ataques de negação de serviço. (NAKAMURA e GEUS, 2007)
A atividade maliciosa da Internet se transformou na primeira década do século XXI e o ganho financeiro foi visto como um negócio lucrativo. Ameaças como Code Red,

[1] The information age has resulted in an explosive amount of potential intelligence sources and will shape the future of OSINT gathering. In the intelligence arena, it is predicted that the practice of harvesting online data to counter terrorism and solve crime will increase. In addition, OSINT will continue to offer a cheap method to acquire intelligence about any community around the globe.(HASSAN; HIJAZI, 2018:341)

Nimda entre outros, começaram a tirar proveito de máquinas desatualizadas e desprotegidas.
Nos dias atuais os crimes incluem ataques aprimorados de roubo de identidade, malwares, engenharia social e ataques de negação de serviço aumentam o problema consideravelmente.
Os profissionais de segurança cibernética precisam estar capacitados para tratar os incidentes em áreas diferentes. Alencar (2010) nos diz que a abordagem é multidisciplinar e trabalhada por diferentes áreas do conhecimento como a Administração, a Ciência da Computação, a Ciência da Informação, a Economia, as Engenharias, a Tecnologia da Informação, entre outras.
Atualmente, o número de ameaças cibernéticas cresce continuamente e as técnicas usadas para o desenvolvimento dos atos ilícitos tem se tornado cada vez mais inteligentes e avançadas. Devemos compreender a ligação existente entre os ciber ataques analisando o relacionamento de dados e as técnicas utilizadas.
KIM, N. *et al.*, (2018) nos mostra que a OSINT é uma ferramenta de valor inestimável para a coleta desses dados, quando propõe em seu trabalho *Design of a Cyber Threat Information Collection System for Cyber Attack Correlation* um sistema cuja função é coletar os dados de ataque às infraestruturas de várias fontes de dados abertos (OSINT) e usa os dados coletados como um valor de entrada para coletar mais dados recursivamente.
Um sistema de coleta de informações sobre ameaças cibernéticas foi desenvolvido e testado com base na estrutura e nas funções do sistema proposto. Doze tipos de informações relacionadas à ciberataques foram coletados. Cerca de dois milhões de itens de dados relacionados a ataques cibernéticos foram coletados ao longo de um período de coleta de dados de um mês.
Com as novas ferramentas e recursos disponíveis, a investigação de código aberto tem sido uma fonte inestimável de informações para qualquer um que esteja investigando uma grande variedade de tópicos e por uma ampla gama de razões.

2.3 Ferramentas de OSINT

Como nos assegura Bielska *et al.* (2020:3) considerando que a OSINT já foi uma exclusividade de analistas de inteligência e profissionais da segurança nacional, observa-se atualmente que há uma crescente atuação de profissionais de áreas como jornalismo, segurança cibernética, direitos humanos e advocacia. Nos últimos anos, organizações, ativistas de direitos humanos e jornalistas adotaram essas novas ferramentas e recursos.
A pesquisa de fontes abertas se tornará uma parte básica do trabalho de muitos pesquisadores, independentemente de sua formação (HIGGINS,2016:195) .
Existem vários sites relacionados a OSINT que possuem um número considerável de ferramentas especializadas em realizar pesquisas em fontes abertas e em diferentes fontes para obter informações regularmente. O fundamental é saber como diferenciar as informações procuradas das inúmeras informações fornecidas por uma fonte específica.
Pedersen (2021:6) nos diz que, Open Source Intelligence não é uma ferramenta, embora muitas ferramentas excelentes estejam disponíveis como agregadores de dados para facilitar a fase de coleta. Nenhuma ferramenta será capaz de alcançar o que um analista devidamente treinado pode.
Com o advento de novas ferramentas, as pesquisas de fontes abertas se tornaram uma fonte valiosa de informações para qualquer um que esteja investigando algum assunto.

De acordo com Bielska e*t al.*, (2020) a ferramenta certa pode determinar se você colhe as informações certas e que quanto mais ferramentas você tiver em seu portfólio, mais flexíveis serão seus recursos OSINT. Seguem algumas ferramentas usadas para OSINT:

- Ferramentas de busca orientadas à Privacidade

DuckDuckGo (https://duckduckgo.com/): é uma ferramenta que reúne resultados de mais de 400 fontes, incluindo Yahoo, Bing e Wikipedia.

Swisscows (https://swisscows.com**):** Localizado na Suíça O mecanismo de busca usa seus próprios servidores privadas e não depende de infraestrutura de terceiros. Com datacenter protegido pelas leis de privacidade de dados da Suíça.

Privatelee (https://privatelee.com): Pesquisa pela web e imagens de forma privada.

- Ferramentas para coleta de informações:

CheckUserNames (https://checkusernames.com/): ferramenta online que pode ajudar a encontrar nomes de usuários em mais de 170 redes sociais.

BeenVerified (https://www.beenverified.com/): ferramenta usada para obter informações de pessoas em registros públicos.

Maltego (https://www.maltego.com/); ferramenta para reconhecimento na internet e que permite obter os resultados para o alvo especificado, como :IP, Domínios, etc.

theHarvester (https://github.com/laramies/theHarvester): ferramenta baseada em Python para ser usada nos estágios iniciais de uma investigação, aproveitando a inteligência de código aberto

3. Metodologia

Gil, (2009:17) afirma que pesquisa é o procedimento racional e sistemático que objetiva proporcionar respostas a problemas propostos. Quando não dispomos de informações para resolver um problema proposto, a pesquisa é requerida. Uma pesquisa científica pode ser classificada quanto à natureza (básica ou aplicada), aos objetivos (exploratória, descritiva e explicativo) e ao método ou abordagem (qualitativa, quantitativa ou mista). O autor nos diz que a pesquisa descritiva descreve um fenômeno ou objeto de estudo e estabelece relações entre as suas variáveis.

A pesquisa que nos traz o presente artigo caracteriza-se como descritiva, objetivando a análise da OSINT como ferramenta de apoio a agentes de segurança ou de inteligência na resolução de crimes.

O principal objetivo da pesquisa descritiva, é “descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis”.(SILVA e MENEZES, 2005:21) .

Cervo e Bervian (2002) nos diz que a referência bibliográfica “busca conhecer e analisar as contribuições culturais ou científicas existentes sobre um determinado assunto, tema ou problema.” Procura explicar um problema a partir de referências teóricas publicadas em documentos.

O presente artigo surgiu a partir de um levantamento bibliográfico sobre a inteligência de fontes abertas e seu protagonismo em pesquisas e estudos publicados em jornais e revistas especializadas. Buscou-se realizar uma análise quantitativa a partir de dados coletados de fontes bibliográficas.

3.1 Questões de pesquisa (QP)

O objetivo desta revisão sistemática é demonstrar através de estudos primários

como a OSINT é usada como ferramenta de apoio na resolução de crimes cibernéticos. Desta forma, para completar pretendemos responder à principal questão de pesquisa:

Q.P1) A OSINT pode ser utilizada como ferramenta de apoio às forças de segurança em processos envolvendo Crimes Cibernéticos?
Norteado pela questão principal da pesquisa, foram elaboradas questões secundárias:
Q.P1.1) Para quais funções a OSINT se aplica dentro do contexto da pesquisa em Computação Forense e Cibersegurança?
Q.P1.2) Quais as oportunidades da área prevista no estudo?
Q.P1.3) Quais os desafios descritos no estudo?

3.2 Estratégias e processo de busca

Dieste et al. (2009) nos diz que a revisão sistemática identifica estudos empíricos relevantes baseadas em uma estratégia de busca. Deve-se definir uma estratégia adequada para detectar estudos empíricos relevantes envolvendo várias decisões: selecionar as fontes de informação adequadas (ou seja, bases de dados bibliográficas ou bibliotecas digitais), selecionar os campos do artigo nos quais pesquisar os termos, definir a string de pesquisa para identificar estudos empíricos de interesse e executar a pesquisa.
A primeira etapa consistiu em determinar as palavras-chave para busca de trabalhos relacionados. As palavras-chave definidas foram: “OSINT”, “Digital Forensics” e "Threat Intelligence". Os operadores OR e AND, utilizados respectivamente para termos sinônimos e termos alternativos para cada palavra-chave, foram definidos como “. A partir daí obteve-se como resultado, a seguinte *string* de busca genérica: (OSINT) OR (OSINT AND "DIGITAL FORENSICS") OR (OSINT AND "THREAT INTELLIGENCE").
A string de busca foi ajustada para adequar-se às características de cada base eletrônica. As pesquisas bibliográficas sistemáticas foram realizadas para encontrar estudos relevantes com base nas seguintes bases de dados:
- ACM Digital Library (http://portal.acm.org);
- IEEE Digital Library (http://ieeexplore.ieee.org);
- Science@Direct (http://www.sciencedirect.com);
- Scopus (http://www.scopus.com).

A escolha das bases eletrônicas foi norteada pelo estudo de Dieste et al. (2009), o qual define alguns critérios como estudos primários disponíveis, conferências relevantes na área de pesquisa, busca por estudos em inglês (língua adotada nos principais eventos e revistas científicas).

3.3 Processo de seleção dos trabalhos

O processo de seleção dos trabalhos foi elaborado com a ajuda da ferramenta *Parsifal (*https://parsif.al). Que, de acordo com definições de *About Parsifal*, (tradução nossa, 2021) é :

> uma ferramenta online projetada para apoiar pesquisadores na realização de revisões sistemáticas da literatura no contexto da Engenharia de Software. Pesquisadores distribuídos geograficamente podem trabalhar juntos em um espaço de trabalho compartilhado, projetando o protocolo e conduzindo a pesquisa. Além de fornecer uma maneira de documentar todo o processo, a ferramenta o ajudará a lembrar o que é importante durante uma revisão sistemática da literatura.

Os estudos selecionados abordaram aspectos de uso da OSINT como ferramenta ou metodologia para a coleta de informações acerca de crimes digitais, sistemas desenvolvidos com metodologias OSINT, bem como estudos que abordam conceitos teóricos da OSINT na Inteligência de combate a delitos digitais.
A seleção inicial dos artigos, deu-se por análise do título do trabalho, resumo e palavras-chave. Após a seleção inicial, houve a aplicação de critérios de inclusão e exclusão, para ao final extrairmos os trabalhos de interesse.
Os seguintes critérios de inclusão dos trabalhos foram definidos:
- Critério de inclusão 1: Estudos que tratam de OSINT;
- Critério de inclusão 2: Estudos que tratam de OSINT e Crimes Cibernéticos;
- Critério de inclusão 3: Estudos que tratam de OSINT e Respostas a Incidentes;
- Critério de inclusão 4: Estudos que tratam de OSINT em Forense digital.

Os critérios de exclusão dos trabalhos foram assim definidos:
- Estudos anteriores a 2017;
- Estudos duplicados;
- Estudos que fogem ao tema;
- Estudos que não sejam em inglês ou português;
- *Short Papers* (5 páginas ou menos).

4. Resultado e análise dos dados

Após a *string* principal de busca ter sido adaptada, de acordo com as características de cada base eletrônica consultada, 487 publicações foram encontradas na etapa de seleção de estudos. Dos 487 papéis obtidos de 4 bibliotecas digitais publicadas nos anos de 2017 a 2021, 43 artigos foram obtidos após a aplicação de critérios de exclusão e inclusão.
O resultado extraído dessas bases eletrônicas foi importado na ferramenta Parsifal e apresentou os seguintes quantitativos:

- ACM Digital Library: 67 publicações
- IEEE Digital Library: 76 publicações
- Science@Direct: 126 publicações
- Scopus: 218 publicações

Destes trabalhos, 444 resultados foram desconsiderados, sendo 133 trabalhos duplicados e 311 trabalhos rejeitados por serem assuntos que não se enquadram no tema OSINT, estudos anteriores a 2017, estudos em outras línguas que não sejam o inglês e o português - esta última incluída na busca para avaliar a existência de trabalhos desenvolvidos no Brasil relacionados ao tema - e *Short Papers* (publicações com menos de cinco páginas).

Esta seleção inicial pode ser observada nas figuras 1 e 2, abaixo:

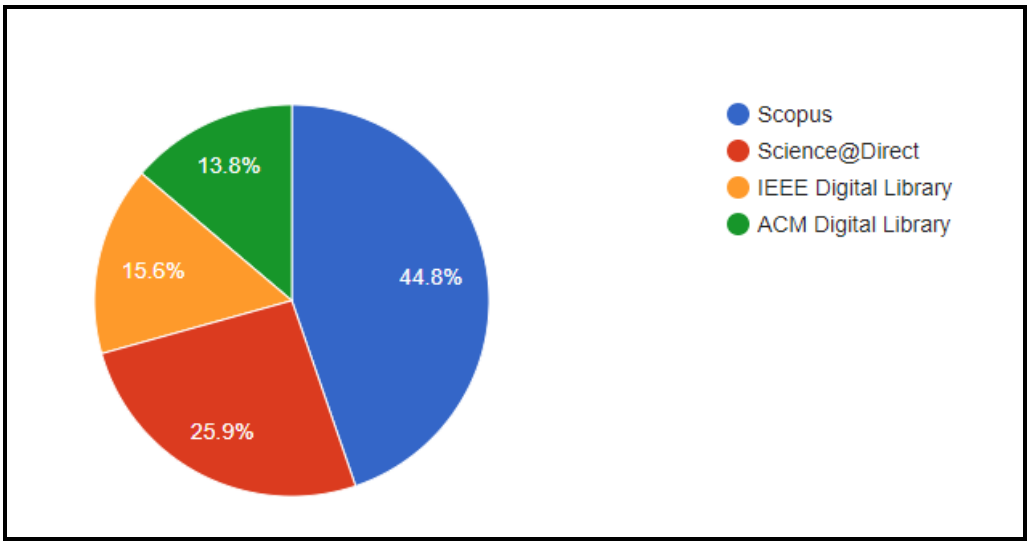

Figura 1 – Artigos por base eletrônica
Fonte: Dados produzidos pelo autor (2021)

O critério utilizado para a primeira seleção dos artigos foi buscar a ocorrência da terminologia OSINT, no título, no resumo e/ou nas palavras-chave das publicações nacionais em Revistas da base de dados.
A figura 2 mostra a quantidade de publicações sobre o tema OSINT encontradas nas bases de publicações consultadas.

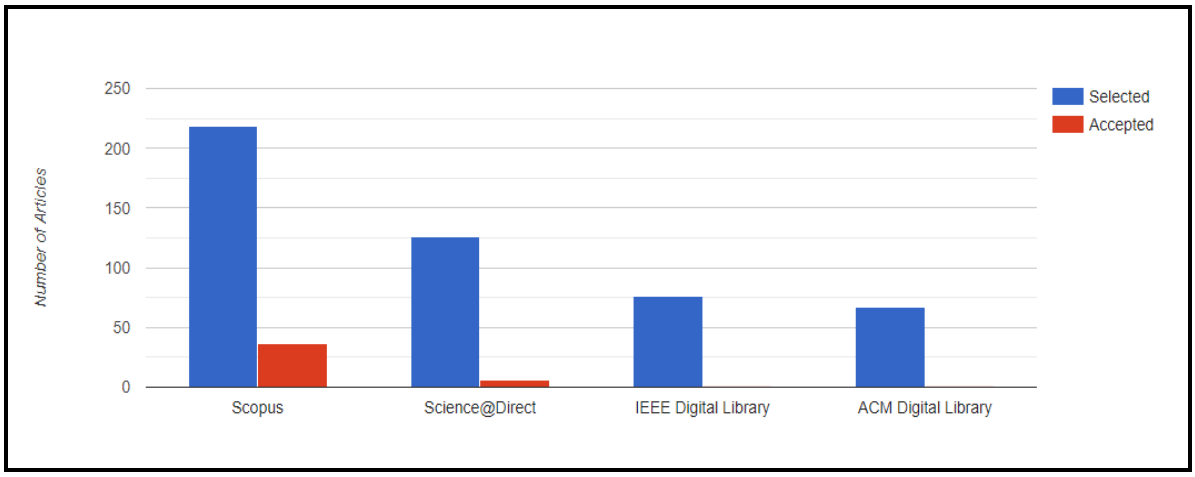

Figura 2 – Artigos selecionados x Artigos aceitos por base eletrônica
Fonte: Dados produzidos pelo autor (2021)

Após as etapas de seleção, foram encontrados 43 estudos relevantes, conforme Tabela 1, abaixo:

Títulos	Autores
• A method for teaching open source intelligence (OSINT) using personalised cloud-based exercises	• Yari, S. and Mäses, S. and Maennel, O.
• A reliability comparison method for OSINT validity analysis	• Gong, S. and Cho, J. and Lee, C.
• A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources	• Ghazi, Y. and Anwar, Z. and Mumtaz, R. and Saleem, S. and Tahir, A.

• A survey and a case-study regarding social media security and privacy on Greek future IT professionals	• Kanakaris, V. and Lampropoulos, G. and Siakas, K.
• A survey exploring open source Intelligence for smarter password cracking	• Aikaterini Kanta and Iwen Coisel and Mark Scanlon
• A system approach for evaluating current and emerging army open-source intelligence tools	• Chae, J. and Graham, D. and Henderson, A. and Matthews, M. and Orcutt, J. and Steven Song, M.J.S.
• Analyzing deviant behaviors on social media using cyber forensics-based methodologies	• Dalton, B. and Agarwal, N.
• Chapter 20 - Investigations using open source intelligence (OSINT)	• Inge {Sebyan Black} and Lawrence J. Fennelly
• Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT)	• Schwarz, K. and Schwarz, F. and Creutzburg, R.
• Crowdsourced Intelligence (Crosint): Using Crowds for National Security [Inteligencia Crowdsourced (CROSINT): utilizar a las multitudes para seguridad nacional]	• Herhkovitz, S.
• Crowd-Sourced Intelligence Agency: Prototyping counterveillance	• Gradecki, J. and Curry, D.
• Cyber-security and sustainable development: The case of Dubai	• Efthymiopoulos, M.P.
• Cybersecurity as an industry: A cyber threat intelligence perspective	• Samtani, S. and Abate, M. and Benjamin, V. and Li, W.
• Design of a Cyber Threat Information Collection System for Cyber Attack Correlation	• Kim, N. and Lee, S. and Cho, H. and Kim, B.-I. and Jun, M.
• Detecting Network Threats using OSINT Knowledge-Based IDS	• Vacas, I. and Medeiros, I. and Neves, N.
• Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix	• Quick, D. and Choo, K.-K.R.
• Enriching threat intelligence platforms capabilities	• Faiella, M. and Gonzalez-Granadillo, G. and Medeiros, I. and Azevedo, R. and Gonzalez-Zarzosa, S.
• Fusing algorithms and analysts: open-source intelligence in the age of ‘Big Data’	• Eldridge, C. and Hobbs, C. and Moran, M.
• Impact of AnonStalk (Anonymous Stalking) on users of social media: A case study	• Kanakaris, V. and Tzovelekis, K. and Bandekas, D.V.
• Knowledge creation processes between open source intelligence and knowledge management	• Fantinelli, S.
• Localising social network users and profiling their movement	• Pellet, H. and Shiaeles, S. and Stavrou, S.
• Open source intelligence (OSINT) for conflict monitoring in contemporary South Africa: Challenges and opportunities in a big data context	• Senekal, B. and Kotzé, E.
• Open source intelligence (OSINT): An oxymoron?	• Miller, B.H.
• Open source intelligence for energy sector cyberattacks	• Keliris, A. and Konstantinou, C. and Sazos, M. and Maniatakos, M.
• Open source intelligence: Performing data mining and link analysis to track terrorist activities	• Dawson, M. and Lieble, M. and Adeboje, A.
• Open-source intelligence educational resources: A visual perspective analysis	• Herrera-Cubides, J.F. and Gaona-García, P.A. and Sánchez-Alonso, S.
• Open-source intelligence for risk assessment	• Darren R. Hayes and Francesco Cappa
• OSINT by crowdsourcing: A theoretical model for online child abuse investigations	• Açar, K.V.
• OSSINT - Open Source Social Network Intelligence: An efficient and effective way to uncover “private” information in OSN profiles	• Giuseppe Cascavilla and Filipe Beato and Andrea Burattin and Mauro Conti and Luigi Vincenzo Mancini
• Perceived Risk Assessment through Open-Source Intelligent Techniques for Opinion Mining and Sentiment Analysis: The Case Study of the Papal Basilica and Sacred Convent of Saint Francis in Assisi, Italy	• Garzia, F. and Cusani, R. and Borghini, F. and Saltini, B. and Lombardi, M. and Ramalingam, S.

• Processing tweets for cybersecurity threat awareness	• Fernando Alves and Aurélien Bettini and Pedro M. Ferreira and Alysson Bessani
• PURE: Generating quality threat intelligence by clustering and correlating OSINT	• Azevedo, R. and Medeiros, I. and Bessani, A.
• Strategic information perception methods and practices in the open source intelligence	• Zeng, W. and Li, H.
• Stress level detection via OSN usage pattern and chronicity analysis: An OSINT threat intelligence module	• Miltiadis Kandias and Dimitris Gritzalis and Vasilis Stavrou and Kostas Nikoloulis
• Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence	• Evangelista, J.R.G. and Sassi, R.J. and Romero, M. and Napolitano, D.
• Technical and OSINT analysis of the TOR foundation	• Delong, M. and Filiol, E. and Coddet, C. and Fatou, O. and Suhard, C.
• TExtractor: An OSINT tool to extract and analyse audio/video content	• Magalhães, A. and Magalhães, J.P.
• The impact of preprocessing in natural language for open source intelligence and criminal investigation	• Johnsen, J.W. and Franke, K.
• The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends	• Pastor-Galindo, J. and Nespoli, P. and Gomez Marmol, F. and Martinez Perez, G.
• TorBot: Open source intelligence tool for dark web	• Narayanan, P.S. and Ani, R. and King, A.T.L.
• Using open data and Google search data for competitive intelligence analysis	• Černý, J. and Potančok, M. and Molnár, Z.
• Using soft-hard fusion for misinformation detection and pattern of life analysis in OSINT	• Levchuk, G. and Shabarekh, C.
• Utilizing air traffic communications for OSINT on state and government aircraft	• Strohmeier, M. and Smith, M. and Moser, D. and Schäfer, M. and Lenders, V. and Martinovic, I.

Tabela 1 – Artigos selecionados
Fonte: Dados produzidos pelo autor (2021)

Analisando os resultados da figura 2, podemos verificar que as bases com maior concentração de publicações sobre OSINT foram Scopus e Science Direct.
Foi realizada uma análise temporal, para identificar em que período se encontra a maior quantidade de publicações sobre OSINT. Isto foi verificado na Figura 3 que a maior concentração de publicações ocorreu no período entre 2018 e 2020, e em 2018 é a maior quantidade de trabalhos publicados com o tema OSINT.

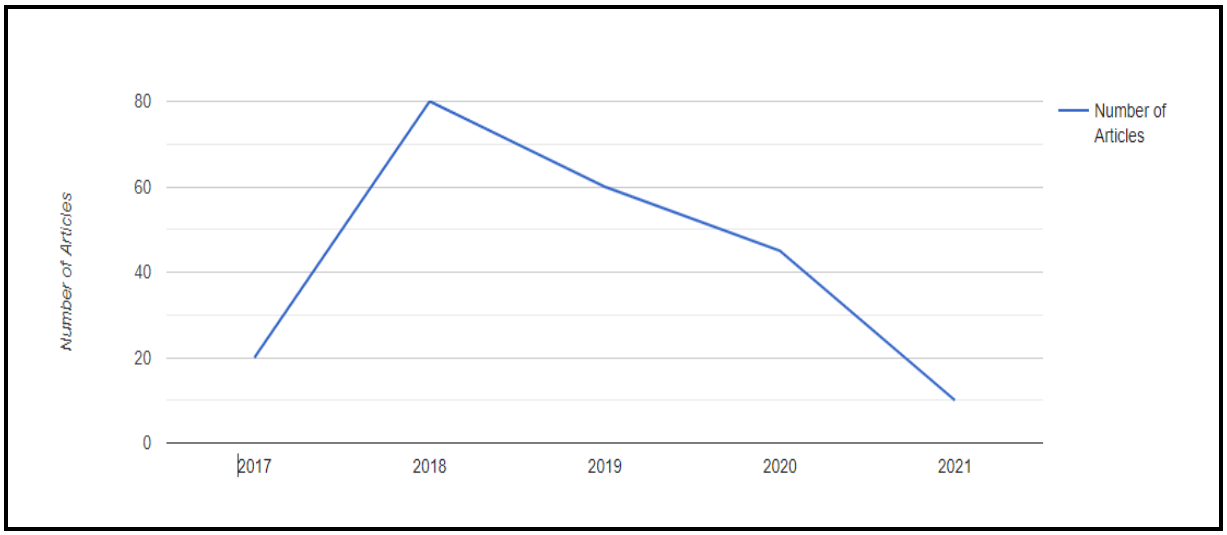

Figura 3 – Número de artigos por ano.
Fonte: Dados produzidos pelo autor (2021)

Além dos critérios de inclusão e exclusão, também foi realizada uma avaliação na qualidade dos estudos através de um questionário que buscou avaliar a metodologia dos estudos, o objetivo da pesquisa, aspectos práticos, limitações do estudo e se houve citação do estudo por outros pesquisadores. Analisados os estudos, foi respondida uma lista de avaliação de qualidade com as seguintes perguntas:

1) O estudo fornece um modelo experimental para avaliar o framework ou metodologia apresentada?
2) O objetivo da pesquisa está bem descrito?
3) O estudo realizou um experimento prático bem descrito para avaliar a proposta?
4) Os autores descrevem limitações do estudo? (Escopo)
5) O estudo foi citado por outros autores?

Para cada estudo avaliado, conforme Tabela 2, foram atribuídas as seguintes notas a partir da soma dos pesos atribuídos aos critérios definidos anteriormente:
Sim – Peso:1.0 ;
Parcialmente - Peso:0.5 e
Não - Peso: 0.0.

Estudos	Nota
A reliability comparison method for OSINT validity analysis	5.0
A survey and a case-study regarding social media security and privacy on Greek future IT professionals	5.0
A system approach for evaluating current and emerging army open-source intelligence tools	5.0
Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix	5.0
Impact of AnonStalk (Anonymous Stalking) on users of social media: A case study	5.0
Localizing social network users and profiling their movement	5.0
OSINT by crowdsourcing: A theoretical model for online child abuse investigations	5.0
OSSINT - Open Source Social Network Intelligence: An efficient and effective way to uncover “private” information in OSN profiles	5.0
Perceived Risk Assessment through Open-Source Intelligent Techniques for Opinion Mining and Sentiment Analysis: The Case Study of the Papal Basilica and Sacred Convent of Saint Francis in Assisi, Italy	5.0
Processing tweets for cybersecurity threat awareness	5.0
PURE: Generating quality threat intelligence by clustering and correlating OSINT	5.0
Stress level detection via OSN usage pattern and chronicity analysis: An OSINT threat intelligence module	5.0
The impact of preprocessing in natural language for open source intelligence and criminal investigation	5.0
Open source intelligence: Performing data mining and link analysis to track terrorist activities	4.5
A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources	4.0
Design of a Cyber Threat Information Collection System for Cyber Attack Correlation	4.0
Detecting Network Threats using OSINT Knowledge-Based IDS	4.0
Open source intelligence for energy sector cyberattacks	4.0
Open-source intelligence for risk assessment	4.0
The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends	4.0
Using open data and Google search data for competitive intelligence analysis	4.0
Using soft-hard fusion for misinformation detection and pattern of life analysis in OSINT	4.0
Utilizing air traffic communications for OSINT on state and government aircraft	4.0

A method for teaching open source intelligence (OSINT) using personalized cloud-based exercises	3.5
Enriching threat intelligence platforms capabilities	3.5
TorBot: Open source intelligence tool for dark web	3.5
Crowd-Sourced Intelligence Agency: Prototyping counterveillance	3.0
Open source intelligence (OSINT) for conflict monitoring in contemporary South Africa: Challenges and opportunities in a big data context	3.0
Open-source intelligence educational resources: A visual perspective analysis	3.0
Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence	3.0
Technical and OSINT analysis of the TOR foundation	3.0
Analyzing deviant behaviors on social media using cyber forensics-based methodologies	2.5
Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT)	2.0
Crowdsourced Intelligence (Crosint): Using Crowds for National Security [Intelligence Crowdsourced (CROSINT): utilizar a las multitudes para seguridad nacional]	2.0
Knowledge creation processes between open source intelligence and knowledge management	2.0
TExtractor: An OSINT tool to extract and analyse audio/video content	2.0
A survey exploring open source Intelligence for smarter password cracking	1.5
Cyber-security and sustainable development: The case of Dubai	1.5
Open source intelligence (OSINT): An oxymoron?	1.5
Chapter 20 - Investigations using open source intelligence (OSINT)	1.0
Cybersecurity as an industry: A cyber threat intelligence perspective	1.0
Fusing algorithms and analysts: open-source intelligence in the age of ‘Big Data’	1.0
Strategic information perception methods and practices in the open source intelligence	1.0

Tabela 2 – Notas atribuídas a cada artigo selecionado
Fonte: Dados produzidos pelo autor (2021)

5. Resultados e Discussão

Esta seção busca mostrar as evidências encontradas nos estudos que contribuem para responder às seguintes questões propostas neste trabalho:

Q.P1) A OSINT pode ser utilizada como ferramenta de apoio às forças de segurança em processos envolvendo Crimes Cibernéticos?

- Foi possível constatar que todos os 43 estudos levantados são relacionados com a OSINT e seu uso como ferramenta para o auxílio ao combate a crimes cibernéticos, é possível perceber metodologias, aplicações e conhecimentos teóricos que visam o aumento do uso de OSINT como ferramenta de análise e busca de informações. Foram encontrados diversos estudos cuja temática principal é o processamento de informações para o combate às ameaças em cibersegurança.

Q.P1.1) Para quais funções a OSINT se aplica dentro do contexto da pesquisa em Computação Forense?

- Dentre os estudos analisados, existem vários trabalhos que desenvolvem tópicos ligados à pesquisa em computação forense. Estudos trazem à tona questões

relativas à análise da rede TOR[2], conforme Narayanan *et al*., (2020) *e* Delong *et al.*, (2018).
A Inteligência forense é evidenciada nos estudos de Quick e Choo, (2018)
A análise de dados através de ferramentas de OSINT para fornecer informações comportamentais de determinado grupo pode fornecer excelentes insumos para análise comportamental de grupos extremistas em estudos de Dawson *et al*., (2018).

Q.P1.2) Quais as oportunidades da área prevista no estudo?
Estamos numa sociedade influenciada por dados e informações. A internet revolucionou a forma como as informações trafegam, como as empresas negociam e como os dados são produzidos. A OSINT – Open source Intelligence veio para explorar essas revolução, através da ampla gama de fontes de pesquisa. Tecnologias que permitem empresas coletar informações sobre a concorrência, impactam o ambiente corporativo. Tecnologias de inteligência de Estado que permitem saber mais sobre pessoas físicas ou jurídicas, essas e outras oportunidades fazem da OSINT um terreno amplo a ser explorado com inúmeras oportunidades, conforme visto em estudos de Pellet *et al*. (2019) *e* Eldridge *et al*, (2018)

Q.P1.3) Quais os desafios descritos no estudo?
A enorme oferta de informações abrangendo todas as áreas de conhecimento da humanidade, fornece um desafio grande para as atividades de inteligência e de combate ao crime cibernético. A dependência de coletas de dados de qualidade gera dificuldades que permeiam estruturas físicas, lógicas e de recursos humanos. Os resultados do estudo mostraram que diversos trabalhos estão sendo desenvolvidos para minimizar as dificuldades da OSINT no que tange à grande quantidade de dados existentes na Internet.

6. Considerações finais

O escopo desse trabalho limitou-se a evidenciar a importância da OSINT a partir de estudos primários e demonstrar as fontes de pesquisa para futuros trabalhos na área de Inteligência em fontes abertas.
Ao final deste trabalho, consideramos que ele seja uma tentativa de observação e compreensão do universo da OSINT através da análise de literaturas científicas, bem como trazer luz à dúvidas comuns às pessoas que usam a coleta em fontes abertas em seu cotidiano.
Os constantes avanços nas tecnologias de informação modificam a forma como os dados são gerados e coletados. O interesse da comunidade científica no tema permitirá a criação de ferramentas e metodologias que auxiliarão a OSINT e a qualidade de suas coletas.
Os dados provenientes dos estudos dessa RSL[3] evidenciam a importância da OSINT no combate a crimes cibernéticos e o imenso campo de pesquisa que pode ser desenvolvido.
Compete a cada um de nós refletirmos sobre os caminhos que devem ser traçados para ampliar as questões e hipóteses levantadas no campo dos dados abertos.

[2] The Onion Router. Ideia do Laboratório de Pesquisa Naval dos EUA para fornecer anonimato à usuários enquanto navegam na Internet
[3] Revisão Sistemática de Literatura

Referências

About Parsifal. **Parsifal**, 2021. Disponível em: <https://parsif.al/about/>. Acesso em: 27 out. 2021.

AKHGAR, B. **OPEN SOURCE INTELLIGENCE INVESTIGATION.** Place of publication not identified: SPRINGER INTERNATIONAL PU, 2017.

ALENCAR, G. D. **Estratégias para mitigação de ameaças internas.** 2010. 137 p. Dissertação (Ciência da Computação) — Universidade Federal de Pernambuco UFPE,Pernambuco.

ALEKSANDRA BIELSKA *et al.* **OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK 2020**. 2020. ed. [S.l.]: i-intelligence, 2020.

BARRETO, A. G.; WENDT, E. **Inteligência e Investigação Criminal em fontes abertas**. 3. ed. Rio de Janeiro: Brasport, 2020.

DAWSON, M.; LIEBLE, M.; ADEBOJE, A. Open Source Intelligence: Performing Data Mining and Link Analysis to Track Terrorist Activities. *In*: LATIFI, S. (Org.). **Information Technology - New Generations**. Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, 2018, V. 558, p. 159–163.

DELONG, M. *et al.* **OSINT Analysis of the TOR Foundation**. arXiv:1803.05201 [cs], 24 mar. 2018. Disponível em: <http://arxiv.org/abs/1803.05201>. Acesso em: 19 abr. 2021.

DNA DATA STORAGE ALLIANCE. **PRESERVING OUR DIGITAL LEGACY:AN INTRODUCTION TO DNA DATA STORAGE**. [S.l.]: DNA Data Storage Alliance, 2021. Disponível em: <https://dnastoragealliance.org/dev/wp-content/uploads/2021/06/DNA-Data-Storage-Alliance-An-Introduction-to-DNA-Data-Storage.pdf>. Acesso em: 25 out. 2021.

ELDRIDGE, C.; HOBBS, C.; MORAN, M. **Fusing algorithms and analysts: open-source intelligence in the age of 'Big Data'**. Intelligence and National Security, 16 abr. 2018. v. 33, n. 3, p. 391–406. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/02684527.2017.1406677>. Acesso em: 23 maio 2021.

EVANGELISTA, J. R. G. *et al.* **Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence.** Journal of Applied Security Research, 7 maio. 2020. p. 1–25. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/19361610.2020.1761737>. Acesso em: 19 abr. 2021.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2009.

HASSAN, N. A.; HIJAZI, R. **Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence.** *In*: HASSAN, N. A.; HIJAZI, R. (Org.). Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. Berkeley, CA: Apress, 2018, p. 1–20.

KIM, N. *et al.* **Design of a Cyber Threat Information Collection System for Cyber Attack Correlation**. *In*: 2018 INTERNATIONAL CONFERENCE ON PLATFORM TECHNOLOGY AND SERVICE (PLATCON), 2018, Jeju. Anais eletrônicos... Jeju: IEEE, 2018. p. 1–6. Disponível em: <https://ieeexplore.ieee.org/document/8472775/>. Acesso em: 13 mar. 2021.

KREMLING, J.; PARKER, A. M. S. **Cyberspace, cybersecurity, and cybercrime**. First Edition ed. Los Angeles: SAGE Publications, 2018.

MINDSECBLOG. **Crime cibernético custará ao mundo US$ 10,5 trilhões anualmente até 2025.** Minuto da Segurança, 16 mar. 2021. Disponível em: <https://minutodaseguranca.blog.br/crime-cibernetico-custara-ao-mundo-us-105-trilhoes-anualmente-ate-2025/>. Acesso em: 10 out. 2021.

NAKAMURA, E. T.; GEUS, P. L. De. **Segurança de redes em ambientes cooperativos**. São Paulo (SP): Novatec, 2007.

NARAYANAN, P. S.; ANI, R.; KING, A. T. L. **TorBot: Open Source Intelligence Tool for Dark Web**. *In*: RANGANATHAN, G.; CHEN, J.; ROCHA, Á. (Org.). Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems. Singapore: Springer Singapore, 2020, V. 89, p. 187–195.

PELLET, H.; SHIAELES, S.; STAVROU, S. **Localising social network users and profiling their movement.** Computers & Security, mar. 2019. v. 81, p. 49–57. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0167404818301524>. Acesso em: 14 mar. 2021.

QUICK, D.; CHOO, K.-K. R. **Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT + OSINT): A timely and cohesive mix.** Future Generation Computer Systems, jan. 2018. v. 78, p. 558–567. Disponível em: <https://linkinghub.elsevier.com/retrieve/pii/S0167739X16308639>. Acesso em: 6 maio 2021.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. Florianópolis: UFSC, 2005.

YEBOAH-OFORI, A.; ALLAN BRIMICOMBE. **Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media**. International Journal of Cyber-Security and Digital Forensics, 2018. v. 7, n. 1, p. 87–98. Disponível em: <http://sdiwc.net/digital-library/cyber-intelligence-and-osint-developing-mitigation-techniques-against-cybercrime-threats-on-social-media.html>. Acesso em: 9 out. 2021.