Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO EM
ECONOMIA E GESTÃO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO

TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO

CIBERCRIME NO SETOR FINANCEIRO: UMA ANÁLISE BIBLIOMÉTRICA

PEDRO HENRIQUE GIUPPONI RIBEIRO

NOVEMBRO - 2020

Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO EM
ECONOMIA E GESTÃO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO

TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO

CIBERCRIME NO SETOR FINANCEIRO: UMA ANÁLISE BIBLIOMÉTRICA

PEDRO HENRIQUE GIUPPONI RIBEIRO

ORIENTAÇÃO:
PROF. DOUTOR MANUEL FERNANDO CILIA DE MIRA GODINHO

NOVEMBRO - 2020

GLOSSÁRIO

AI - Inteligência Artificial

CNCS - Centro Nacional de Cibersegurança de Portugal

EC3 - European Cybercrime Center

EUROPOL - Serviço Europeu de Polícia

INTERPOL - Organização Internacional de Polícia Criminal

ML - Machine Learning

TI - Tecnologia da Informação

UNC3T - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

RESUMO

Tendo com base a motivação do autor em construir carreira no setor bancário, este estudo pretendeu mapear a produção científica internacional sobre a cibersegurança no setor financeiro. A partir de uma amostra de 499 artigos e *reviews* extraídos da base de dados do Web of Science, foram realizadas análises dos indicadores bibliométricos de artigos científicos publicados no período de 1995 a 2019. O que nos diz a literatura científica que relaciona a "esfera" das finanças com cibersegurança? Os resultados indicaram que (i) a pesquisa sobre cibersegurança no setor financeiro é bastante dispersa e passa por um momento de crescimento com uma tendência exponencial; (ii) a maioria dos autores prolíficos são vinculados a instituições de pesquisa norte americanas, principalmente nos EUA; (iii) as perspectivas proeminentes focam em aspectos da segurança dos dados pessoais em conexão com *Blockchain* e as relações entre as tecnologias aplicadas ao setor financeiro, com destaque para o *Internet Banking*. Algumas limitações do estudo são discutidas e servem de ponto de partida para futuras pesquisas.

Palavras-Chave: Estudo bibliométrico. Ciber-segurança. Ciberataque. Finanças. Banco.

ABSTRACT

Having as a starting point the motivation of the author to build a career in the banking sector, this study aimed to map the international scientific production on cybersecurity in the financial sector. From a sample of 499 articles and reviews extracted from the Web of Science database, analyzes of the bibliometric indicators of articles published between 1995 and 2019 were carried out. What does the scientific literature that links the "sphere" of finance with cybersecurity tell us? The results indicated that (i) research on cybersecurity in the financial sector is quite disperse and undergoes a moment of growth with an exponential trend; (ii) the majority of prolific authors are linked to North American research institutions, mainly in the USA; (iii) the prominent perspectives focus on aspects of personal data security in connection with Blockchain and the relationships between technologies applied to the financial sector, with emphasis on Internet Banking. Some study limitations are discussed and serve as a starting point for future research.

Keywords: Bibliometric study. Cybersecurity. Cyberattack. Finance. Bank.
JEL Codes: C80. F65. G20. I20. O30.

ÍNDICE

TABELA DE FIGURAS

AGRADECIMENTOS

Na realização da presente dissertação, contei com o apoio de muitas pessoas às quais sou profundamente grato. Ao querido Luiz pelo carinho, apoio e alegrias que traz a minha vida. A todos os amigos e colegas que de uma forma direta ou indireta, contribuíram na elaboração do presente estudo. Ao Rafael, Frederico, Larissa, Maria Eliza e Mirella por serem minha família em Portugal, pelas memórias e força que me prestaram em momentos menos fáceis. A querida Gabriela por toda ajuda e por sempre estar disposta a ajudar. A minha família pelo amor incondicional e por não me deixar perder o foco, mesmo com a saudade grande. Ao meu orientador, Professor Doutor Manuel Fernando Cilia de Mira Godinho, pelas orientações, atenção, dedicação e pelo incentivo frequente.

A todos o meu sincero muito obrigado!

1. INTRODUÇÃO

Nas últimas duas décadas, a segurança cibernética se tornou uma ameaça real e uma preocupação séria à medida que a Internet se tornou mais acessível e mais utilizada na vida cotidiana. Há já bastantes anos, as instituições financeiras são os alvos favoritos de quadrilhas de cibercriminosos. Em função do grande crescimento dos cibercrimes, as instituições financeiras investem cada vez mais em tecnologias avançadas para reduzir o impacto dos ataques. Porém, da mesma forma que as tecnologias de prevenção evoluem, a forma de cometer os crimes contra as instituições financeiras muda constantemente e as técnicas usadas pelos criminosos evoluem em velocidade ainda maior.

Os cibercrimes representam ameaças e têm sérias consequências para governos, empresas e cidadãos. A incidência significativa do cibercrime acompanha o aumento do uso da Internet para fazer transações online. Consequentemente, as instituições financeiras são obrigadas a melhorar constantemente seus sistemas de proteção, detecção e prevenção dos ataques.

Esse estudo se propõe a realizar um mapeamento e análise bibliométrica de artigos científicos publicados no período de 1995 a 2019, que tenham como temática a relação da "esfera" das finanças com a cibersegurança. A "esfera" das finanças compreende as instituições que fornecem serviços como intermediários dos mercados financeiros, como por exemplo, bancos, companhias de seguros, corretoras, bancos de investimento, cooperativas de crédito, fundo de pensões, entre outras. E é neste contexto que se pretende aprofundar os estudos com o objetivo de enriquecer a compreensão do universo dos cibercrimes em instituições financeiras.

Pretende-se medir a produtividade científica, avaliando o crescimento de publicações da área, o fator de impacto de autores e países, além de identificar a evolução e a obsolescência da literatura. Para tal, foram mapeadas publicações depositadas na plataforma Web of Science, com acesso final no dia 28/07/2020.

A motivação para o presente estudo se deu pelo fato de que a "esfera" das finanças sempre me gerou muita curiosidade e interesse. O meu desejo de construir carreira no setor bancário, atuando na detecção e prevenção de fraudes, teve grande influência na

realização desse estudo. Segundo Romanowski & Ens (2006), esse tipo de estudo proporciona uma visão global do que vem sendo feito na área e permite perceber a evolução das pesquisas, e também identificar as lacunas ainda existentes.

Foi colocada, em relação com os objetivos deste estudo, a seguinte questão de investigação: O que nos diz a literatura científica que relaciona a "esfera" das finanças com cibersegurança?

Para responder aos objetivos pretendidos, esta dissertação está dividida em 4 capítulos. O primeiro capítulo, apresenta o enquadramento da análise com a revisão da literatura relevante para a compreensão de todo o enquadramento da "esfera" das finanças e da cibersegurança. O segundo capítulo, apresenta o detalhamento da metodologia utilizada. O terceiro capítulo, apresenta a análise dos resultados e discussões acerca deste. Por fim, o quarto capítulo, aponta as principais conclusões e sugere recomendações para futuras investigações do tema proposto.

2. REVISÃO DA LITERATURA

2.1. Enquadramento da Análise

Têm-se vindo a verificar alterações significativas nos padrões de vida e de trabalho dos humanos, devido à imensa contribuição da tecnologia para a comunicação, o compartilhamento de informações e a realização de transações. Um marco essencial neste cenário foi o surgimento da Internet, uma inovação radical cujas origens se situam na segunda metade do século XX. No auge da Guerra Fria, nas décadas de 1960 e 1970, a Internet teve início com projetos de *networking* nos Estados Unidos e na Europa Ocidental. Pertencente ao Departamento de Defesa norte-americano, chamado de Arpanet, o antecessor da Internet era uma rede de telecomunicações de longa distância que interconectava computadores e tinha como função interligar laboratórios de pesquisa.

O uso da Arpanet tornou-se maior no âmbito acadêmico a partir de 1982. Inicialmente, seu uso estava restrito aos EUA, mas se expandiu para outros países e começou a ser chamada de Internet. Desde então, a difusão foi enorme e o crescimento da Internet foi, como se sabe, exponencial. Estima-se que, em 2019, 4,1 mil milhões de pessoas

utilizavam a Internet. O número de usuários era correspondente a 53,6% da população mundial, segundo a União Internacional de Telecomunicações, UIT.

Seguramente a Internet tornou nossa vida mais fácil e conveniente. A internet não apenas permite comunicação por e-mail e voz, mas também garante fácil acesso a informação, imagens e produtos, permite fazer negócios, ampliar rede de relacionamentos profissionais, fazer novos amigos, conhecer diferentes culturas, estudar, entre outras coisas. No entanto, além das suas vantagens e aspectos positivos, a Internet também tem desvantagens, com destaque para um seu lado obscuro, os cibercrimes. Na verdade, a Internet criou também oportunidades para criminosos, que rapidamente se adaptaram às inovações relacionadas com a Internet.

Shu, Wesley & Strassmann, Paul (2005), o setor financeiro, que tem sido uma área crescente de inovação em relação a sistemas, tecnologia da informação (TI) e desenvolvimento da oferta de produtos e serviços, por meio de plataformas e aplicativos, sofre bastante com os cibercrimes. Os cibercrimes são um problema com consequências de longo alcance no setor financeiro. A crescente dependência de novas tecnologias, como nuvem, tablets e smartphones, nos últimos anos, agravou os problemas de cibsersegurança, acabando por exigir significativos investimentos em TI com objetivo de inovar e permitir a melhoria na experiência e segurança dos clientes ao utilizar seus serviços.

De acordo com o Manual de Oslo (2005),:

> Uma inovação é a implementação de um produto (bem ou serviço) novo ou significativamente melhorado, de um processo, de um novo método de marketing, ou de um novo método organizacional nas práticas de negócio, na organização do trabalho ou nas relações externas da empresa.
>
> M. Oslo, OCDE, 2005, p. 46)

A inovação pode acontecer em diversos contextos e em dimensões diferentes, podendo ser inovação de: produto, serviço, processos, modelo de negócio, logística, marketing e tecnológica. Segundo Godinho, M. (2003), a inovação tecnológica estabelece um importante fator que determina a modificação das estruturas econômicas, a destruição

criadora. A destruição criadora ou destruição criativa é um conceito introduzido em 1942, por Joseph Schumpeter, um dos economistas e cientistas políticos mais importantes da primeira metade do século XX, em seu livro intitulado Capitalismo, Socialismo e Democracia. O autor considerava as inovações tecnológicas como impulso do desenvolvimento do mundo, pois ao surgir uma inovação, as empresas especializadas nas tecnologias maduras tendem a desaparecer e, em contrapartida, emergem empresas e indústrias ligadas às tecnologias inovadoras.

No setor financeiro, as inovações tecnológicas permitem às instituições financeiras oferecer produtos e serviços e inovar na experiência do cliente, num ambiente de negócios cada vez mais competitivo, mas desejavelmente inclusivo e seguro contra ciberataques.

Faruk Ülgen (2015) em seu livro Is the financial innovation destruction creative? A Schumpeterian reappraisal, destaca que a "esfera" financeira confirma a visão Schumpeteriana do processo de destruição criativa:

> Such a financial environment would support the Schumpeterian vision of creative destruction process by which innovations replace old methods and goods with better process, commodities, and services.It is obvious that changes occurring in money and financial markets affect the financing conditions ofirms' normal and innovative activities. Robert King and Ross Levine (1993) stated that Schumpeter might have been right about the importance of finance in economic growth as financial services would stimulate the increase of the rate of capital accumulation and improve the allocative efficiency of markets. As a result, financial intermediaries would make technological innovations and economic development possible.
>
> Faruk Ülgen (2015) p.38.

De acordo com Carvalho (2000), uma inovação financeira refere-se "(...) à produção de novos tipos de serviços financeiros ou a novas formas de produção de serviços financeiros já conhecidos". De acordo ainda com este autor uma inovação financeira é introduzida pela mesma razão que qualquer outro tipo de inovação, ou seja, as inovações representam armas competitivas nas mãos das empresas, na busca de incrementar sua fatia de mercado e obter, assim, maiores lucros.

Ao longo do tempo, uma série de inovações referentes aos processos e produtos do setor financeiro permitiu ao setor, reduzir os custos das transações, aumentar a eficiência

dos processos e agregar valor aos clientes, por meio da introdução de novos canais de distribuição para serviços existentes e o desenvolvimento de novos produtos e serviços baseados em tecnologia. Novas empresas de tecnologias aplicadas ao setor financeiro (FinTech) surgiram e trabalham para inovar e otimizar serviços do sistema financeiro, oferecendo oportunidades em termos de aumento da dinâmica concorrencial, tendo como consequência o aumento da eficiência e do bem-estar dos consumidores.

De fato, da mesma forma que a inovação no setor financeiro acontece por meio da emergência de novas tecnologias, inclusive aquelas para prevenção de ataques cibernéticos, a forma de cometer os crimes contra as instituições financeiras muda constantemente e as técnicas usadas pelos criminosos evoluem em velocidade ainda maior.

Para a Organização Internacional de Polícia Criminal – Interpol, (2020), "As formas tradicionais de crime também evoluíram à medida que as organizações criminosas recorrem cada vez mais à Internet para facilitar suas atividades e maximizar seu lucro no menor tempo possível."

Com crimes cada vez mais sofisticados e em constante evolução, a luta contra os cibercrimes é diariamente um desafio para as instituições financeiras ao redor do mundo. Em 2013, o Serviço Europeu de Polícia – EUROPOL, criou o European Cybercrime Center (EC3), para proteger as empresas, governos e cidadãos europeus contra cibercrimes. Desde então, centenas de prisões foram feitas. Em Portugal, contando com o modelo definido pelo European Cybercrime Center, da Europol, em 2016 a Polícia Judiciaria criou a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), cujo objetivo é prevenir, detectar e investigar os cibercrimes.

Os cibercrimes nas instituições financeiras centram-se sobretudo nos ataques de *phishing*. Segundo a Agência Europeia para a Segurança das Redes e da Informação, em seu Relatório de cenário de ameaças de 2018, *phishing* é um "mecanismo de elaboração de mensagens que usam técnicas de engenharia social de modo a que o alvo seja ludibriado 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os recetores de emails ou mensagens para que estes abram anexos maliciosos, cliquem em

URL inseguros, revelem as suas credenciais através de páginas de *phishing* aparentemente legítimas [*pharming*], façam transferências de dinheiro, etc."

Existem outros tipos de cibercrimes, que são caracterizados pelo Relatório Cibersegurança em Portugal - Riscos & Conflitos 2020 - CNCS, como:

- *Smishing* – é semelhante ao *phishing*, o que difere é a forma de envio, que neste caso é por SMS.
- *Ransomware* – é um tipo de extorsão cibernética onde o software malicioso impede a vítima de aceder ao seu próprio computador, com o *hacker* estipulando um valor do pagamento (resgate) para a vitima voltar a ter acesso ao seu computador.
- Ataque ao *mobile banking* – usando uma ampla série de técnicas, como aplicativos falsos de bancos e trojans bancários ocultos em aplicativos, os criminosos obtém permissões necessárias para roubar as informações da vitima.
- *Jackpotting* – é um ataque a máquinas automáticas de entrega de dinheiro ("máquinas multibanco") que tem como objetivo fazer com que essas máquinas liberem dinheiro através de um comando.

2.2. Panorama Atual

Os cibercrimes nas instituições financeiras continuam a expandir-se com o aumento da digitalização. Segundo o relatório Ninth Annual Cost of Cybercrime Study in Financial Service*s 2019* realizado pela Accenture Security, que combinou pesquisas de 11 países em 16 setores, o setor financeiro (bancos, empresas do mercado de capitais e seguradoras), tiveram que desembolsar uma média por empresa de US$18,5 milhões por ano para combater o cibercrime. O estudo revelou, que as instituições financeiras estão investindo em prevenção para a descoberta, investigação, contenção e recuperação, para se proteger contra os ciberataques. Ainda segundo este estudo, estima-se que nos próximos cinco anos, os bancos terão prejuízos de US$347 mil milhões, os mercados de capitais de US$47 mil milhões e as seguradoras de US$305 mil milhões.

Muitas empresas do setor financeiro utilizam a AI (inteligência artificial) e o ML (*machine learning*) para a prevenção e detecção de ciberataques. As tecnologias ligadas a Industria 4.0 poderão trazer muitos benefícios as instituições financeiras, sobretudo no

combate aos cibercrimes. O conceito de Industria 4.0 ou Quarta Revolução Industrial tem sido discutido nos últimos anos e originou-se a partir de um projeto do governo alemão de estratégias voltadas a tecnologia. Pode ser definido como um conceito de indústria que reúne as principais inovações tecnológicas para automação, controle e troca de dados a partir da utilização de Sistemas Cyber-Físicos, Internet das Coisas e Computação em Nuvem, proporcionando processos mais eficientes, autônomos e customizáveis. Porém, muito ainda precisa ser feito para a Industria 4.0 se tornar, de fato, uma revolução. Embora seja uma tendência, no mesmo relatório da Accenture referido acima, das instituições financeiras pesquisadas apenas 34% tinham investido em automação, AI e ML.

Os consumidores almejam que as instituições financeiras forneçam um nível de segurança adequado para proteger seus dados pessoais e realizar transações. O *Blockchain*, que é uma tecnologia de registro distribuído que visa a descentralização como medida de segurança, pode auxiliar na segurança de transações e de dados pessoais. Foi a moeda virtual *Bitcoin* que popularizou a tecnologia, com a publicação do artigo de Satoshi Nakamoto (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Por decentralizar as informações, o *Blockchain* armazena as informações com maior segurança. Os dados armazenados não podem ser apagados ou alterados, sendo assim, as transações realizadas são feitas de forma segura, transparente e autônoma.

Ao longo do tempo, muitas violações de dados tiveram como alvo instituições financeiras. Como em 2003, que a Data Processors International sofreu um ciberataque e 8 milhões de números de cartão de crédito foram roubados. [1]

A MasterCard em 2005, comunicou que 40 milhões de números de cartão de crédito foram comprometidos devido a um ciberataque a rede de computadores da CardSystems Solutions Inc. [1] Em 2010, a empresa Education Credit Management Corp. teve dados violados quando uma mídia portátil foi roubada, expondo 3.3 milhões de pessoas. [1]

[1] Ellen Zhang (2019). The Top 10 FinServ Data Breaches [Em linha]. Disponível em: https://digitalguardian.com/blog/top-10-finserv-data-breaches [Acesso em: 29/05/2020].

A Capital One Financial Corp., *holding* americana de bancos, foi atacada em 2019 por Paige Thompson, ex engenheiro da AWS (Amazon Web Services), que segundo a Capital One, a violação de dados afetou 100 milhões de clientes dos Estados Unidos e outros 6 milhões no Canadá. [2]

Em 2019, uma pesquisa divulgada pela Kaspersky [3], empresa internacional de cibersegurança, apontou a Rússia como o país que sofre mais ciberataques financeiros no mundo, com cerca de 30% dos ataques registados. Em segundo lugar a Alemanha com 7% e em terceiro a China e o Brasil com 3% cada.

No cenário atual, o CNCS - Centro Nacional de Cibersegurança de Portugal (2020) publicou o relatório de Cibersegurança em Portugal - Riscos & Conflitos que constatou que os tipos de incidentes mais registados em 2019 eram o *phishing* (31%) e a infeção por *malware*, incluindo o *ransomware* (16%). O relatório também constatou que 8% dos incidentes são direcionados a bancos, onde os agentes de ameaças são o *phishing*, e *malware* (inclui *ransomware).*

A pandemia Covid-19 tem sido um estimulante de inovação em relação com serviços via Internet, tendo vindo a provocar uma aceleração da transição para a Indústria 4.0. Porém, a pandemia, tem também favorecido agentes maliciosos que realizam ciberataques oportunistas, através de *phishing*, *smishing*, *ransomware* e fraudes. O CNCS registou um acréscimo de 85% no número de incidentes entre fevereiro e março de 2020 e um aumento de 176% comparando o mês de março de 2020 com o mês correspondente de 2019. Segundo o relatório do banco suíço Julius Baer (2020) *Cybersecurity* - Fighting Invisible Threats [4], em 2021 os crimes cibernéticos devem implicar uma perda de US$ 6 biliões (10^{12}) à economia global.

[2] Alex Scroxton (2019). Top 10 cyber crime stories of 2019- Here are Computer Weekly's top 10 cyber crime stories of 2019 [Em linha]. Disponível em: https://www.computerweekly.com/news/252475441/Top-10-cyber-crime-stories-of-2019 [Acesso em: 29/05/2020].

[3] Da redação (2020). Brasil, 4º país mais atacado por malware financeiro em 2019 [Em linha]. Disponível em: https://www.cisoadvisor.com.br/brasil-4o-pais-mais-atacado-por-malware-financeiro-em-2019/ [Acesso em: 10/06/2020].

[4] Marcelo Moura e Daniel Haidar (2020). Os ataques cibernéticos explodem durante pandemia e expõem vulnerabilidades das empresas [Em linha]. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2020/09/os-ataques-ciberneticos-explodem-durante-pandemia-e-expoem-vulnerabilidades-das-empresas.html [Acesso em: 01/11/2020].

3. METODOLOGIA

Este capítulo aborda os aspectos pertinentes relativamente à metodologia de pesquisa. Considerando o objetivo, de mapear a produção científica mundial sobre cibercrimes na "esfera" das finanças, o estudo teve caráter exploratório-descritivo, pois pretendeu compreender abrangentemente o tema proposto.

Segundo Bruyne (1991), a metodologia é a lógica dos procedimentos científicos em sua origem e em seu desenvolvimento. Isto é, a forma com que a pesquisa é conduzida, como foram coletados os dados, quais os instrumentos foram utilizados, como o trabalho foi dividido, como os dados foram tratados, ou seja, é tudo que foi feito para a realização do trabalho de pesquisa.

O presente trabalho foi dividido em 3 fases, que pode-se observar na Figura 1.

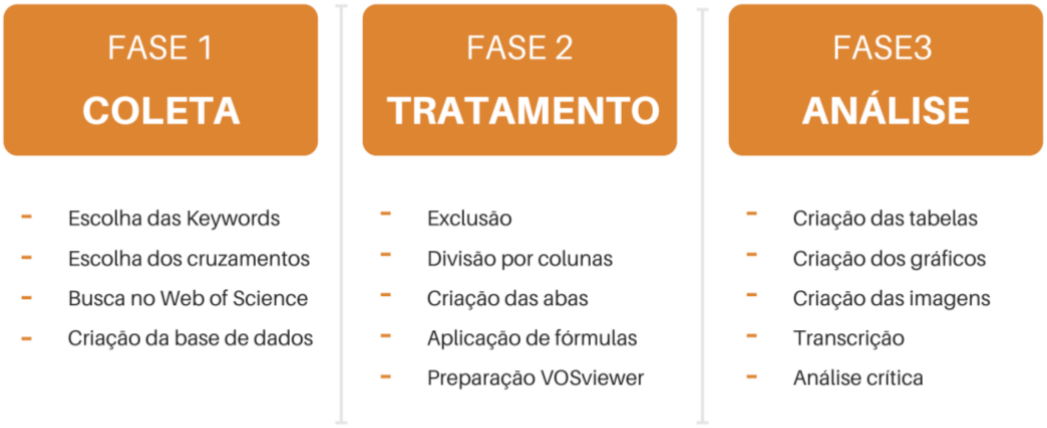

Figura 1 – Fases da Metodologia.

Fonte: Elaborado pelo autor

3.1. Fase 1

Primeiramente, foram escolhidas as palavras chaves que seriam utilizadas na busca para a criação da base de dados. A escolha das palavras chave se deu a partir da leitura na íntegra dos 10 artigos com mais citações do tema cibersegurança na "esfera" das finanças. Com isso, foram identificadas as palavras representadas na Figura 2.

Figura 2 – As Keywords de Busca.

Fonte: Elaborado pelo autor

Com as devidas palavras chaves escolhidas, foram decididos quais seriam os cruzamentos de pesquisa para a busca no Web of Science, de forma que se pudesse cruzar duas palavras na mesma busca. A busca foi feita por tópico, pois esse tipo de pesquisa abrange o título, resumo, as palavras-chave do autor e o *Keywords Plus*™. A delimitação temporal se deve ao fato de que as primeiras publicações, sobre o tema estudado, ocorreram no ano de 1995. Com isso, o período que compreende os anos de 1995 a 2019 foi o escolhido para a busca na base de dados do Web of Science. Assim, espera-se proporcionar uma visão geral do desenvolvimento, do tema abordado, desde sua primeira publicação.

Na Tabela I, pode se observar as combinações de palavras chave escolhidas para a criação da base de dados.

Tabela I
Combinações de Keywords De Busca

Keyword	+	Keyword		Keyword	+	Keyword
Cyber		Bank		Cyber Security		Bank
Cyber		Banking		Cyber Security		Banking
Cyber		Finance		Cyber Security		Finance
Cyber		Financial		Cyber Security		Financial
Cybercrime		Bank		Cyberattack		Bank
Cybercrime		Banking		Cyberattack		Banking
Cybercrime		Finance		Cyberattack		Finance
Cybercrime		Financial		Cyberattack		Financial
Cyber-Crime		Bank		Cyber-Attack		Bank
Cyber-Crime		Banking		Cyber-Attack		Banking
Cyber-Crime		Finance		Cyber-Attack		Financial
Cyber-Crime		Financial		Cyber-Attack		Financial
Cyber Crime		Bank		Cyber Attack		Bank

Tabela I
Combinações de Keywords De Busca (continuação)

Keyword	+	Keyword		Keyword	+	Keyword
Cyber Crime		Banking		Cyber Attack		Banking
Cyber Crime		Finance		Cyber Attack		Finance
Cyber Crime		Financial		Cyber Attack		Financial
Cybersecurity		Bank		Cyber-Risk		Bank
Cybersecurity		Banking		Cyber-Risk		Banking
Cybersecurity		Finance		Cyber-Risk		Finance
Cybersecurity		Financial		Cyber-Risk		Financial
Cyber-Security		Bank		Cyber Risk		Bank
Cyber-Security		Banking		Cyber Risk		Banking
Cyber-Security		Finance		Cyber Risk		Finance
Cyber-Security		Financial		Cyber Risk		Financial

Fonte: Elaborado pelo autor

Levou-se em conta possíveis variações da mesma palavra chave, com espaço e com hífen, que resultou em 48 cruzamentos. As buscas foram realizadas no dia 28/07/2020 e exportada para o Excel no mesmo dia, resultando em 4.635 publicações na base de dados.

3.2. Fase 2

A segunda fase iniciou-se com a identificação e exclusão das publicações duplicadas. As células foram verificadas a partir da identificação do Unique WOS ID, que é a identidade da publicação no banco de dados da Web of Science, e com essa exclusão o número de publicações reduziu-se a 1.041.

Em seguida, fez-se uma leitura cuidadosa do título e resumo das publicações com a finalidade de definir quais publicações deveriam ser utilizadas no estudo e quais deveriam ser descartadas, levando em conta o título e resumo das publicações. A partir da leitura, foi possível selecionar e descartar pesquisas que, apesar de tratarem de cibersegurança, não tratavam de cibersegurança na "esfera" das finanças, propósito deste trabalho. Com o descarte, a base de dados reduziu-se a 499 publicações.

Os dados relativos ao autor, geografia do autor, área de pesquisa, *keywords* e quartil precisaram ser divididos em colunas, para que se pudessem ser analisados futuramente, visto que em sua maioria apresentava mais de um valor para cada campo citado.

Para que pudesse ser estudado cada objeto de pesquisa, um levantamento das categorias a serem analisadas foi feito. De tal modo foram definidas as seguintes unidades de análise:

- Jornais e Livros;
- Ano da Publicação;
- Quartil da Categoria;
- Citações;
- Autor(es);
- Geografia do(s) Autor(es);
- Área de Pesquisa;
- *Keywords* do(s) Autor(es);
- *Keywords Plus*™.

Ambas foram colocadas em uma aba do documento para que pudessem ser analisadas individualmente.

Com os dados devidamente alinhados em cada aba, para o tratamento dos dados, foram utilizadas em todas as categorias as fórmulas:

- =ARRUMAR para poder deletar os espaços no começo de palavras;
- =ÚNICO para poder unir os dados repetidos;
- =CONT.SE para quantificar os valores dos determinados objetos de pesquisa, fornecendo a frequência absoluta.

A seguir, os dados das variáveis de texto foram colocados em ordem alfabética, para poder identificar a existência de variação de ortografia entre as variáveis e assim poder uní-los como uma única célula.

Esta fase se finalizou, com a preparação da base de dados para o software VOSviewer. VOSviewer é uma ferramenta utilizada para construção e visualização de redes bibliométricas. O passo seguinte foi a exportação do arquivo da base dados para o formato txt, que é o formato necessário para a utilização do VOSviewer.

3.3. Fase 3

Esta foi a fase dedicada a criação, no Excel e VOSviewer, dos gráficos, imagens, tabelas e também para a transcrição dos dados que foram observados na base de dados. Logo em seguida, se iniciou a análise crítica dos resultados que estão disponíveis no capítulo 3 – Análise dos Resultados.

4. ANÁLISE DOS RESULTADOS

Neste capítulo são apresentados os resultados e discussões. Primeiramente, apreciam-se os resultados gerais com as análises descritivas e frequências relativas. Logo em seguida, são apresentados os resultados dos cruzamentos de variáveis. E por fim, discutem-se as análises bibliométricas de redes de citação, com a análise das redes de co-ocorrência de termos importantes extraídos do banco de dados.

4.1. Análise Descritiva

Analisamos 499 publicações, às quais estão associados a 1.290 autores de 71 países, durante o período de 1995 a 2019. A análise descritiva que se segue, começa por identificar as fontes, os anos, os quartis da categoria e continua com a análise das citações, do autor, da geografia do autor, das áreas de pesquisa, das keyword do autor e conclui ainda com as *Keywords Plus* ™.

4.1.1. Jornais e Livros

Este estudo analisou 499 documentos, distribuídos em 393 jornais ou livros (média de 1,3 por jornal ou livro*).* A Tabela II mostra os periódicos com a maior quantidade de documentos na amostra do estudo.

Tabela II
Principais Fontes

Ranking	Fonte	Quant.	%
1º	Lecture Notes in Computer Science	12	2,40
2º	Computers & Security	8	1,60
3º	International Conference on Cyber Warfare and Security	7	1,40
3º	International Conference on Information Warfare and Security	7	1,40
5º	European Conference on Information Warfare and Security	6	1,20
5º	Future Generation Computer Systems the International Journal of Escience	6	1,20
7º	International Journal of Security and its Applications	5	1,00
Outros (10) com 3		30	6,01%
Outros (42) com 2		84	16,83%
Outros (334) com 1		334	66,93%
Total		499	100,00%

Fonte: Elaborado pelo autor

Com 47 anos de história, a fonte com mais publicações sobre o tema estudado é o Lecture Notes in Computer Science, com 12 publicações. Publicado pela Springer Science e Business Media, o Lecture Notes in Computer Science é uma série de livros de ciência da computação.

A segunda fonte com mais publicações é o Computers & Security, com 8 publicações. Computers & Security é uma respeitada revista britânica na área de segurança de TI.
Com 7 publicações cada, em terceiro lugar estão as séries de livros desenvolvidos a partir da International Conference on Cyber Warfare and Security e da International Conference on Information Warfare and Security, juntos com 2,81% das publicações.

Nota-se que das fontes com publicações com o tema de cibersegurança na "esfera" das finanças, a grande maioria (66,93%) teve apenas um único artigo abordando esse tema.

4.1.2. Anos

Nesta subseção, são apresentados os dados relativos aos anos em que o tema estudado apareceu em revistas cientificas, de acordo com a delimitação temporal definida, que compreende os anos de 1995 a 2019.

A Tabela III mostra a quantidade de publicações e a variação ao longo de todo período estudado.

Tabela III

Taxa de Crescimento Anual das Publicações

Anos	Quant.	Variação
1995	1	0%
1997	1	0,00%
1998	1	0,00%
1999	2	100,00%
2000	3	50,00%
2001	1	-66,67%
2003	1	0,00%
2004	2	100,00%
2005	4	100,00%
2006	3	-25,00%
2007	1	-66,67%
2008	4	300,00%
2009	6	50,00%
2010	11	83,33%
2011	17	54,55%
2012	13	-23,53%
2013	23	76,92%
2014	18	-21,74%
2015	57	216,67%
2016	55	-3,51%
2017	78	41,82%
2018	89	14,10%
2019	108	21,35%

Fonte: Elaborado pelo autor

Nota-se que pelo menos até ao início da década de 2010, não há uma tendência uniforme, em alguns anos tem um crescimento alto e outros anos têm um decréscimo ao longo de todo período. Podemos destacar o ano de 2008 com crescimento de 300% e o ano de 2001 e 2007 com decréscimo de 66,67%. Embora o crescimento de 2008 seja alto, vale dizer que provavelmente existem *delays*, tanto da demora para escrever, quanto da revisão da revista, devolução e publicação que podem demorar meses. Portanto,

provavelmente esse crescimento de 2008 tem a ver com muitos dos artigos que foram submetidos em 2007.

Porém, a partir de 2010, verifica-se um crescimento mais robusto, especialmente nos anos mais recentes, fazendo com que durante a década de 2010-2019 as publicações multipliquem quase por um fator de 10, passando de apenas 11 em 2010 para 108 em 2019.

4.1.3. Quartil da Categoria

O quartil refere-se ao fator de impacto da revista. Ele auxilia à comparação de uma revista com outras dentro da sua área. É calculado a partir da divisão do número total de revistas de uma categoria por quatro, assim resultando a sua classificação, que pode ser: Q1, Q2, Q3 ou Q4. Quando a revista pertencer ao Q1, significa que tem um desempenho melhor do que ao menos 75% das revistas dessa mesma área disciplinar.

A Tabela IV apresenta os resultados referentes aos quartis.

Tabela IV

Quartis da Categoria

Quartil da categoria	Quant.	%
Q1	82	31,30%
Q2	77	29,39%
Q3	44	16,79%
Q4	59	22,52%
Total	262	100,00%

Fonte: Elaborado pelo autor

Das 499 publicações analisadas neste trabalho, apenas 172 (34,47% do total) revistas disponibilizaram a classificação dos quartis nas publicações. Devido ao fato de a mesma revista estar incluída em mais de uma categoria, a soma dos quartis de todas as categorias foi 262, em que 82 pertencem ao quatil Q1 representando 31,30% da amostra, 77 ao quartil Q2, 44 no quartil Q3 e 59 no quartil Q4.

4.1.4. Citações

Nesta subseção, são apresentados os dados relativos ao número de citações das publicações estudadas. Segundo Bazerman (1988), a citação prestigia e coloca em discussão a experiência científica, ligando escritores aos seus leitores através de seus textos.

O estudo encontrou 499 publicações e desta amostra 2.093 citações foram feitas. A Figura 3, apresenta os cinco títulos com mais citações em função do número de citações que receberam de outros documentos publicados em periódicos.

Figura 3 – Títulos mais Citados.

Fonte: Elaborado pelo autor

Publicado pela Leee Transactions on Smart Grid em 2011, com a autoria de Mo, Yilin, Xie, Le e de Sinopoli, Bruno, Integrity Data Attacks in Power Market Operations, com 226 citações, foi o título mais citado.

Em segundo lugar, com 200 citações, está o título Designing Towards Emotional Usability in Customer Interfaces - Trustworthiness of Cyber-banking System Interfaces. Foi publicado pelo periódico Interacting With Computers em 1998 e escrito por Kim, J e Moon, JY.

Publicado pela Deviant Behavior em 2014, com 92 citações, An Assessment of the Current State of Cybercrime Scholarship foi o terceiro colocado e contou com autoria de Holt, TJ e Bossler, AM.

Proactive User-centric Secure Data Scheme Using Attribute-based Semantic Access Controls for Mobile Clouds in Financial Industry, publicado pelo periódico Future Generation Computer Systems, ficou no quarto lugar com 81 citações.

E por fim, na quinta posição está o título Effective Detection of Sophisticated Online Banking Fraud on Extremely Imbalanced Data, com 76 citações publicado pelo jornal World Wide Web-Internet and Web Information Systems.

4.1.5. Autor(es)

O estudo reuniu 1.290 autores, sendo um deles não identificado. A tabela seguinte apresenta os principais autores com base na quantidade de publicações existentes, representados pela frequência absoluta e pela frequência relativa.

Tabela V

Principais Autores

Ranking	Autor	Frequência Absoluta	Frequência Relativa
1º	Qiu, MK	9	0,64%
	Gai, KK	9	0,64%
3º	Leukfeldt, ER	5	0,36%
4º	Pandey, P	4	0,29%
	Memon, S	4	0,29%
	Elnagdy, SA	4	0,29%
	Kleemans, ER	4	0,29%
Outros (6) com 3 publicações			1,28%
Outros (68) com 2 publicações			9,70%
Outros (1209) com 1 publicação			86,23%
Total		1402	100,0%

Fonte: Elaborado pelo autor

Os autores com mais publicações são Qiu, Meikang e Gai, Keke, com 0,64% das publicações cada um. Ambos afiliados a Pace University, situada na cidade de Nova York nos Estados Unidos da América. Além de representar a Pace University, em duas publicações Qiu, Meikang também representa a Shenzhen University, que fica situada em Shenzhen, China.

A publicação deles com mais impacto foi a "Proactive User-Centric Secure Data Scheme Using Attribute-Based Semantic Access Controls for Mobile Clouds in Financial Industry", que teve a autoria de Gai, Keke e a co-autoria de Qiu, Meikang, com 81 citações e foi publicada pela revista Future Generation Computer Systems-The International Journal of Escience.

A segunda posição ficou com o autor Leukfeldt, E. Rutger, com 0,36% das publicações. Leukfeldt, ER está associoado ao Netherlands Inst Study Crime & Law Enforcement N, Open University Netherlands, Police Acad Netherlands, NHL Stenden University of Applied Sciences e a Vrije Universiteit Amsterdam. Nota-se que a tabela mostra os outros autores que apareceram uma, duas ou três vezes em publicações. 86,23% dos autores, apareceram apenas em uma publicação e 9,70% aparecem em duas. E por fim, 1,28% dos autores apareceram em três publicações.

4.1.6. Geografia do(s) Autor(es)

O estudo reuniu 1.290 autores e 71 países. A tabela seguinte reúne os países com mais publicações, demonstrada pela frequência absoluta, com base nos endereços de publicação dos autores.

Tabela VI
Países com mais Publicações

Ranking	País	Quant.
1º	Estados Unidos	351
2º	Índia	165
3º	Inglaterra	64
4º	China	60
5º	Rússia	56
6º	Holanda	52
7º	Coreia do Sul	50
8º	Itália	47
9º	Ucrânia	42
10º	Austrália	37
Outros (8) - entre 35 e 21 publicações		224
Outros (53) - entre 20 e 1 publicações		253
Anónimo (1)		1
Total		1402

Fonte: Elaborado pelo autor

Os Estados Unidos da América lideram o ranking de países com mais publicações sobre cibercrimes na "esfera" das finanças com 351 publicações, que representa 25,04% das publicações identificadas. Com 11,77%, em segundo lugar está a Índia, com 165 publicações. Em terceiro lugar está a Inglaterra com 64 publicações, com 4,56%. A China aparece em quarto lugar, com 60 publicações. Na sequência a Rússia, Holanda, Coreia do Sul, Itália e Ucrânia estão na casa dos 3% das publicações. Na décima posição está a Austrália, com 37 publicações. Outros 61 países foram identificados, somando 34,02%, com 477 geolocalizações dos autores.

A União Europeia conta com 22 países, com cerca de 20% do total. A Holanda é o país mais bem colocado, com 52 publicações. Portugal conta com 8 publicações e ocupa a 23º posição no ranking geral, juntamente com a Nova Zelândia e Marrocos.

O gráfico seguinte permite visualizar a frequência relativa dos 10 países com mais publicações perante a sua geolocalização do autor.

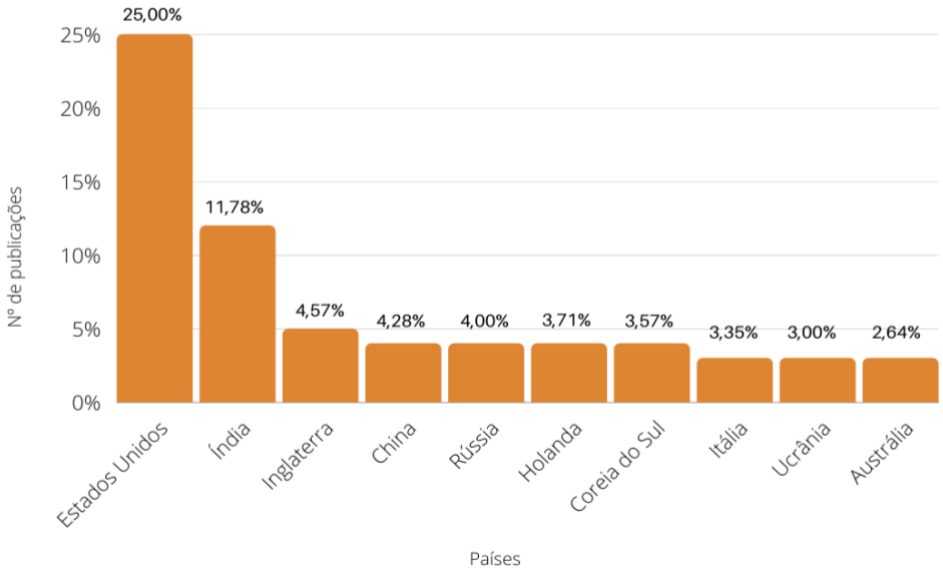

Figura 4 – Os 10 Países com mais Publicações.

Fonte: Elaborado pelo autor

Nota-se que a diferença da Índia, que aparece em segundo lugar, para os Estados Unidos da América que está em primeiro lugar é de -52,99%, um percentual expressivo. A variação dos 10 países com mais publicações pode ser encontrada no Apêndice A.

4.1.7. Área de Pesquisa

A tabela VII apresenta as 10 principais áreas de pesquisa.

Tabela VII
As Principais Áreas de Pesquisa

Ranking	Área de pesquisa	Quant.	%
1º	Computer Science	280	38,04%
2º	Engineering	132	17,93%
3º	Business & Economics	74	10,05%
4º	Telecommunications	40	5,43%
5º	Government & Law	24	3,26%
5º	Criminology & Penology	24	3,26%
7º	Information Science & Library Science	17	2,31%
8º	Operations Research & Management Science	14	1,90%
8º	Social Sciences - Other Topics	14	1,90%
10º	International Relations	13	1,77%
Outras (37) Áreas de Pesquisa		104	14,13%
Total		736	100,00%

Fonte: Elaborado pelo autor

Computer Science está em primeiro lugar, com 280 que representa 38,04% das áreas de pesquisa. Em segundo lugar está a área de pesquisa *Engineering*, com 132 publicações. Na terceira posição está a área de pesquisa *Business & Economics*, com 74 publicações. Nota-se que as três principais áreas de pesquisa, juntas, somam 66% do total.

4.1.8. Keyword do(s) Autor(es)

As *keywords* do autor são ideias e tópicos que definem o que se encontra no conteúdo da publicação. Elas são inseridas nos mecanismos de pesquisa e servem como uma ligação entre o que as pessoas procuram e o conteúdo que autor oferece do tema procurado. Neste estudo, foram identificadas 1.472 *keywords* do autor nas publicações estudadas. A tabela a seguir, destaca as 10 *keywords* mais frequentes.

Tabela VIII
Principais Keywords do(s) Autor(es)

Ranking	Keywords	Quant.	%
1º	Cybersecurity	106	4,46%
2º	Cybercrime	61	2,57%
3º	Cyberattack	35	1,47%
4º	Security	26	1,09%
5º	Phishing	24	1,01%
6º	Information Security	19	0,80%
7º	Malware	18	0,76%
8º	Blockchain	17	0,72%
8º	Risk Management	17	0,72%
10º	Machine Learning	16	0,67%
Outros (1462) Keywords		2012	85,74%
Keywords presente 1 vez		1204	50,65%
Total		2377	100,00%

Fonte: Elaborado pelo autor

A *keyword* que mais apareceu na amostra estudada, foi *Cybersecurity*, que esteve presente em 106 publicações, representando 4,46% das *keywords* encontradas. Logo em seguida, *Cybercrime* ocupa a segunda colocação com 61 publicações, com uma diferença de 42,45% em relação à primeira colocada, *Cybersecurity*. Com 35 publicações, *Cyberattack* está em terceiro lugar. Vale notar, que no *ranking* das 10 *keywords* mais frequentes, apenas uma *keyword (Blockchain)* está diretamente relacionada com a "esfera" das finanças. Outras 1.462 *keywords* foram encontradas, entre elas: *Internet of Things* com 12 e *Cyber risk* com 10 publicações. As *keywords* presentes apenas em uma publicação representam 50,65% do total da amostra.

4.1.9. Keyword Plus™

Diferente das *keywords* do autor, as *Keywords Plus™* não podem ser modificadas. Elas são geradas a partir de um algoritmo que analisa as palavras e frases que aparecem nos títulos das referências de um artigo, mas não estão no título do próprio artigo (Garfield, E. 2001).

A tabela a seguir, mostra as *Keywords Plus*™ mais frequentes.

Tabela IX
As Principais Keywords Plus™

Ranking	Autor	Quant.	%
1º	Security	19	2,97%
2º	System	18	2,81%
3º	Management	16	2,50%
4º	Internet	15	2,34%
5º	Model	14	2,19%
6º	Impact	11	1,72%
6º	Risk	11	1,72%
8º	Crime	8	1,25%
8º	Network	8	1,25%
8º	Online	8	1,25%
10º	Classification	7	1,09%
10º	Attack	7	1,09%
Outras (81) de 2 a 6		224	35,00%
Outras (274) com 1		274	42,81%
Total		640	100,00%

Fonte: Elaborado pelo autor

Nota-se que a *Keywords Plus*™ que aparece em maior número é *Security*, presente em 19 publicações, representando 2,97% do total de *Keywords Plus*™. Destaque para as *Keywords Plus*™ que apareceram apenas uma vez em publicações, representando 42,81%.

4.2. Cruzamento de Dados

4.2.1. Cruzamento de Keywords

A tabela seguinte compreende as combinações de palavras-chaves que foram utilizadas na criação do banco de dados para este estudo.

Tabela X
Combinações de Keywords de Busca

Combinações	Quant.	%
Cyber + Bank	203	40,7%
Cyber + Financial	169	33,9%
Cybersecurity + Financial	28	5,6%
Cyber + Finance	26	5,2%
Cybercrime + Financial	23	4,6%
Cybersecurity + Bank	19	3,8%
Cybercrime + Bank	17	3,4%
Cybersecurity + Finance	8	1,6%
Cybercrime + Finance	3	0,6%
Cyber + Banking	2	0,4%
Cyberattack + Financial	1	0,2%
Total	499	100,0%

Fonte: Elaborado pelo autor

A base de dados foi construída com 499 publicações, e a combinação de *keywords* que obteve mais exemplares foi: *Cyber* com *Bank*, com 40,7% dos títulos. A combinação com o menor número de publicações foi: *Cyberattack* + *Financial* com apenas uma publicação.

4.2.2. Keywords nas Áreas de Pesquisa

Nesta subseção, dados relativos as *keywords* encontradas nas principais áreas de pesquisa serão analisadas. A Figura 5 apresenta as três principais *keywords* de cada uma das três áreas de pesquisa com mais publicações na amostra estudada (*Computer Science*, *Enginnering* e *Business & Economics*).

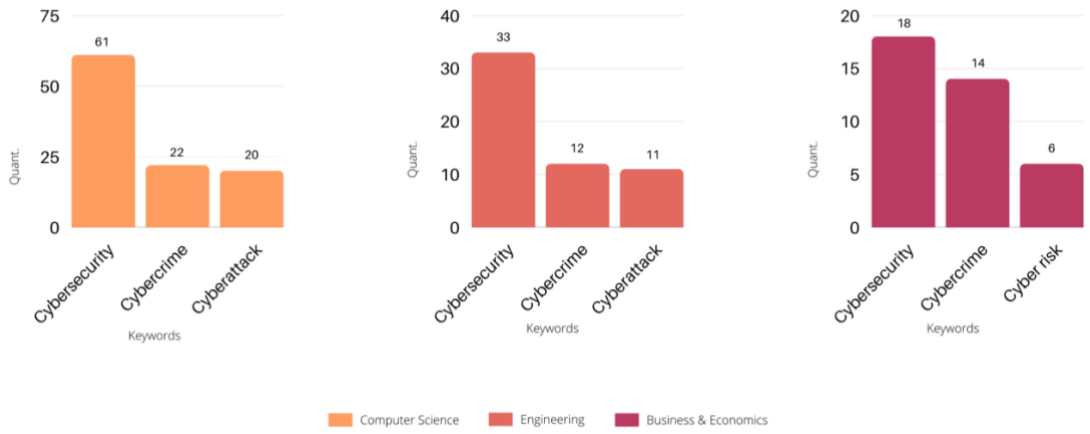

Figura 5 – Relação das Áreas de Pesquisa com as Keywords.

Fonte: Elaborado pelo autor

Observa-se que em ambas as áreas de pesquisa a *keyword Cybersecurity* esteve em primeiro lugar e a *keyword Cybercrime* em segundo lugar. Verifica-se, em paralelo com a subseção 3.1.4 *Keyword* do autor, que nas duas áreas de pesquisa com mais publicações, as *keywords* mais frequentes são as mesmas três *keywords* principais dos autores de todo estudo.

4.2.2. Citações por Ano

Durante todo o período temporal estudado, 2.093 citações foram feitas e a Tabela XI apresenta a distribuição das citações ao longo do tempo.

Tabela XI
Distribuição das Citações por Ano

Ano	Quant.
1995	3
1997	0
1998	200
1999	0
2000	11
2001	17
2003	0
2004	3
2005	15
2006	0
2007	0
2008	1
2009	5

Tabela XI
Distribuição das Citações por Ano
(continuação)

Ano	Quant.
2010	78
2011	237
2012	30
2013	159
2014	144
2015	135
2016	245
2017	325
2018	358
2019	127
Total	2093

Fonte: Elaborado pelo autor

Nota-se que a partir dos anos 2010, o crescimento no número de citações teve um crescimento expressivo, com um aumento de 15 vezes em relação ao ano anterior, tendo atingido o ápice em 2018 com 358 citações, decrescendo em 2019, para 127 citações (provavelmente relacionado coma "juventude" dessas publicações, ainda não têm muitas citações).

4.2.3. Citações por Geografia do(s) Autor(es)

Nesta subseção são apresentados dados sobre a quantidade de citações por geografia dos dez países com mais publicações. A Tabela XII, apresenta a distribuição das citações por países.

Tabela XII
Distribuição das Citações por País

País	Quant.
EUA	520
Coreia do Sul	518
Noruega	112
Índia	109
Irã	108
França	107
Inglaterra	97
China	95
Rússia	85
África do Sul	85

Fonte: Elaborado pelo autor

Nota-se que os EUA é com grande vantagem o país com o maior número de publicações citadas. A Coreia do Sul encontra-se em segundo lugar, com 518 publicações citadas. Destacam-se a Noruega, a França e a Inglaterra, representando a Europa, com respetivamente 112, 107 e 97 publicações citadas.

4.2.4. Citações por Área de Pesquisa

A Tabela XIII tem informação sobre a quantidade de citações das dez principais áreas de pesquisa.

Tabela XIII
Citações por Áreas de Pesquisa

Área de pesquisa	Quant.
Computer Science	1384
Engineering	744
Business & Economics	284
Government & Law	243
Operations Research & Management Science	140
Criminology & Penology	72
Telecommunications	68
Social Sciences - Other Topics	63
International Relations	51
Information Science & Library Science	49
Mathematics	45

Fonte: Elaborado pelo autor

Com 1.384 citações, a área de pesquisa de maior impacto foi a *Computer Science*. Em seguida, aparece a área de pesquisa *Engineering* que possui 744 citações. A terceira área de pesquisa de maior impacto na literatura foi *Business & Economics*, que obteve 284 citações no período analisado.

4.2.5. Citações por Quartil

De acordo com a posição dos quartis, essa subseção apresentará a quantidade de citações por quartil. Devido ao fato de a mesma revista estar incluída em mais de uma categoria, a soma das citações por quartil de todas as categorias foi de 3.215 citações (em comparação com 2093, o total de citações do estudo). A Tabela XIV mostra a distribuição das citações por quartil em todas as categorias.

Tabela XIV
Citações por Quartil

Quartil	Quant.
Q1	1541
Q2	775
Q3	263
Q4	636
Total	3215

Fonte: Elaborado pelo autor

É interessante verificar que os artigos sobre o nosso tema de pesquisa estão sobretudo concentrados no 1º e também no 2º quartil. O quartil Q1 apresentou a maior quantidade de citações (1.541), o quartil Q2 apresentou 775 citações e ocupou a segunda posição. O terceiro quartil com mais citações foi o quartil Q4, com 636 citações. E por fim, o quartil Q3 obteve a menor quantidade de citações (263).

4.2.5. Citações por Jornal ou Livro

Essa subseção apresenta o número de citações das três revistas que apresentaram o maior número de publicações neste estudo (presentes na subseção 3.1.5).

Tabela XV
Citações por Jornal ou Livro

Fonte	Quant.
Computers & Security	87
Lecture Notes in Computer Science	13
International Conference on Cyber Warfare and Security	7
International Conference on Information Warfare and Security	5

Fonte: Elaborado pelo autor

Com 87 citações, o jornal de maior impacto foi de longe *Computers & Security*. Em seguida, aparece o *periódico Lecture Notes in Computer Science*, com 13 citações. E por fim, *International Conference on Cyber Warfare and Security* e *International Conference on Information Warfare and Security*, apresentam menos de 10 citações. Verifica-se que a soma de citações dos quatro periódicos que ocupam os três primeiros lugares no *ranking* com mais publicações sobre a temática da cibersegurança na "esfera" das finanças, é de 112 citações. Isto representa 5,35% do total das 2.093 citações feitas das publicações estudadas neste trabalho, sugerindo que à exceção da revista *Computers & Security*, os artigos sobre o tema objeto de estudo estão bastante dispersos.

4.2.6. Frequência dos 3 Principais Autores

Na figura a seguir, pode-se observar a frequência com que os 3 principais autores publicaram ao longo dos anos.

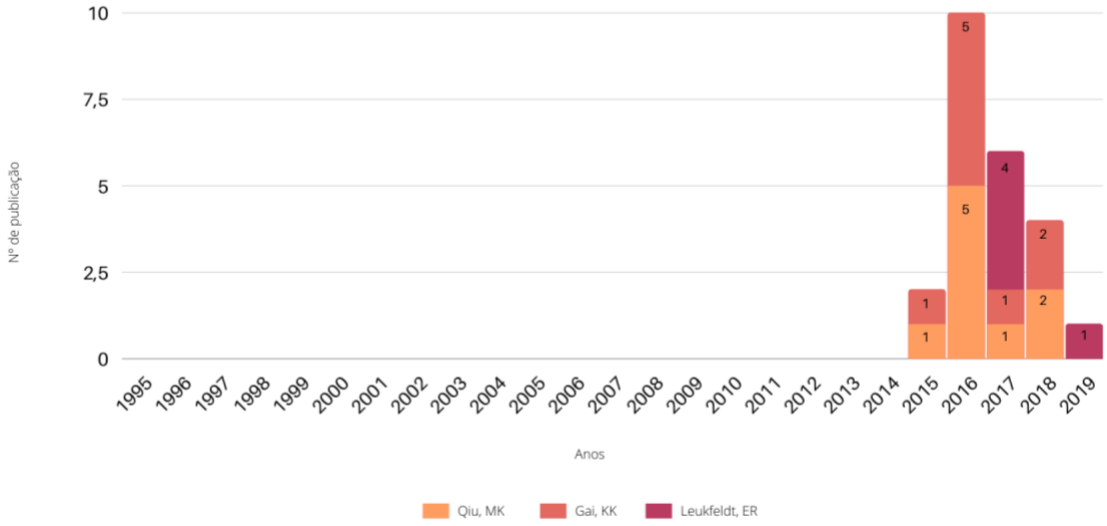

Figura 6 – Frequência dos 3 Principais Autores

Fonte: Elaborado pelo autor

Qiu, MK e Gai, KK começaram a publicar sobre cibersegurança na "esfera" das finanças em 2015. Em 2016 tiveram o maior número de publicações, somando no total cinco trabalhos. Leukfeldt, ER em 2017 publicou quatro trabalhos e em 2019 mais um. Pode-se observar a frequência completa do estudo no Apêndice B.

4.2.7. Frequência das Principais Keywords do(s) Autor(es)

Na Figura 7, é possível observar a frequência em que as três principais *keywords* do(s) autor(es) começaram a aparecer ao longo do tempo.

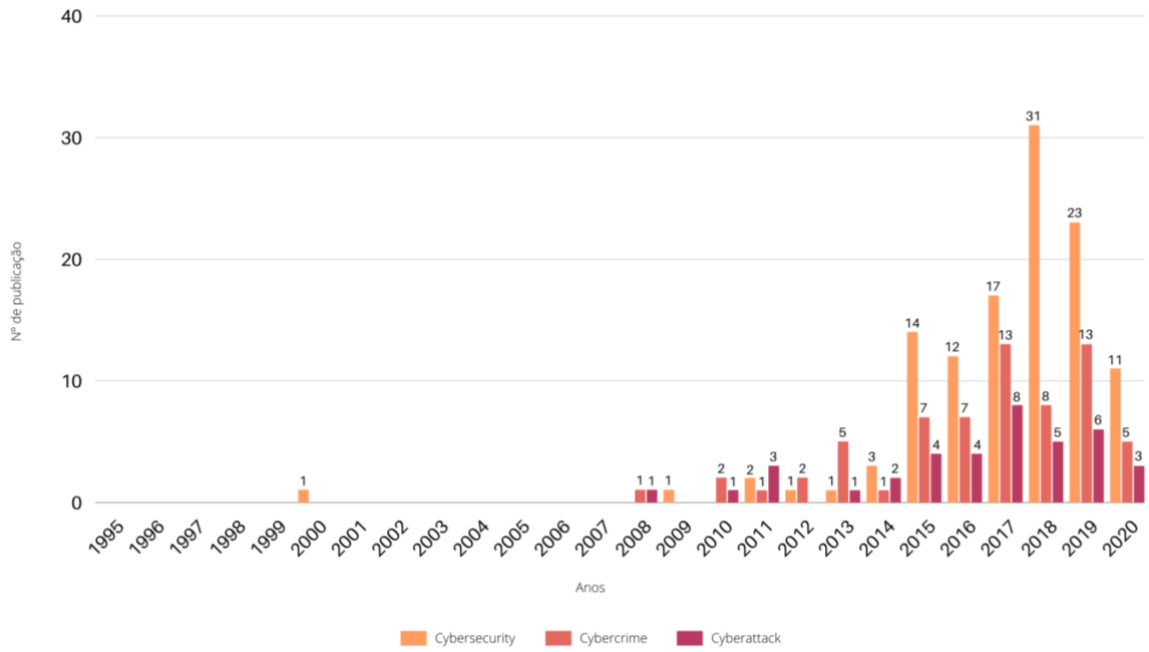

Figura 7 – Distribuição das 3 Principais Keywords do(s) Autor(es).

Fonte: Elaborado pelo autor

Podemos verificar que a *keyword Cybersecurity* começou a ser utilizada na literatura cientifica do tema estudado logo no ano 2000. Em 2014, teve um crescimento de 200% em relação ao ano anterior. Em 2015, obteve a maior taxa de crescimento, 367%, tendo como base o ano de 2014. Em 2018, com 31 publicações, teve o crescimento de 82% em relação ao ano anterior. Já em 2019, teve uma queda de 26% em comparação ao ano anterior.

A *keyword Cybercrime* teve o maior crescimento em 2017, com 13 aparições em publicações e no ano seguinte com 8 aparições. Em 2019, voltou a aparecer 13 vezes, com isso variando 63% face ao ano anterior. O ano de 2015 foi o de maior taxa de crescimento, 600% em relação ao ano anterior.

Cyberattack, em 2017, teve sua melhor pontuação, com oito aparições. Em 2018, caiu para cinco publicações e em 2019 subiu para seis. A tabela com a variação completa das três 3 *keywords* do(s) autor(es) pode ser consultada no Apêndice C.

Nota-se que o ano de 2015, foi o principal ano para as duas principais *keywords* em números de publicação (*Cybersecurity* e *Cybercrime*).

4.2.8. Frequência das Principais Keywords Plus™

A Figura 8 representa a frequência, perante os anos, das 3 *Keywords Plus*™ mais frequentes.

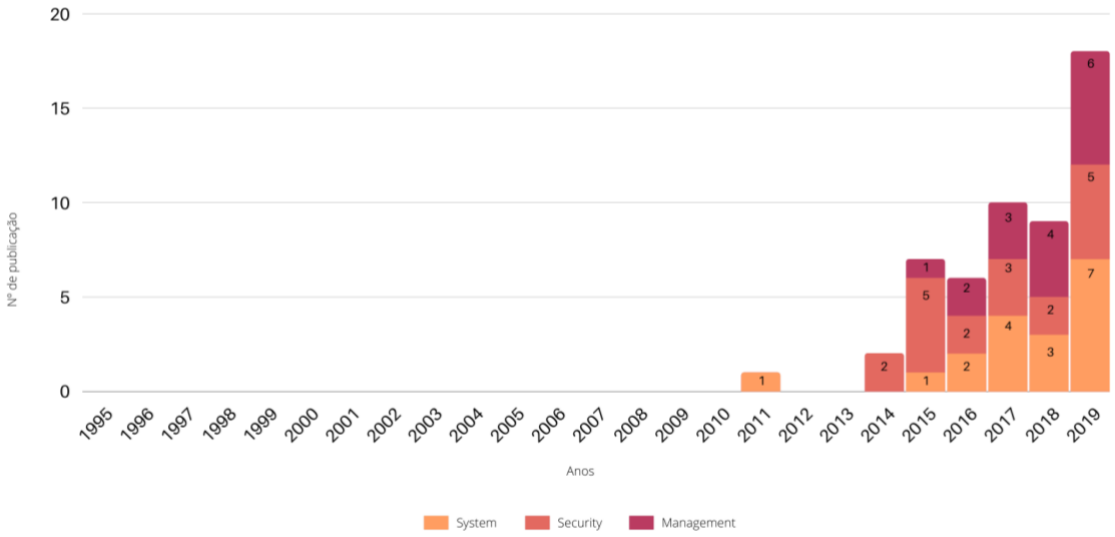

Figura 8 – A Frequência das Principais Keywords Plus™.

Fonte: Elaborado pelo autor

Nota-se que em 2011 apareceu *System*, uma das primeiras três *Keywords Plus*™ mais frequentes. A *Keywords Plus*™ mais frequente (*Security*), apareceu pela primeira vez em uma publicação em 2014. Em 2015, houve um crescimento de 150% com referência ao ano anterior. Nos anos seguintes teve um decréscimo e em 2019 voltou a crescer 150%. Constata-se que o ano de 2019 foi o ano com a maior ocorrência das três *Keywords Plus*™ mais frequentes. A tabela com a variação completa das 3 *Keywords Plus*™ mais frequentes, pode ser consultada no Apêndice D.

4.3. Análise Bibliométrica de Redes

A partir da amostra de 499 publicações extraídas da base de conhecimento Web of Science, nesta subseção apresenta-se as análises de indicadores bibliométricos relacionados com redes de citação. Por meio de análise bibliométrica, buscou-se identificar as redes de coautoria, de co-citação e de acoplamento bibliográfico, além das

principais *keywords* dos autores e *Keywords Plus*™. A análise bibliométrica mensura a produção cientifica na sua essência e auxilia no processo de tomada de decisões por permitir explorar, analisar e estruturar a análise de grandes quantidades de dados. Segundo Porter, A. (2007), identificar o número de vezes em que termos são encontrados, revela o nível de atividade de pesquisa sobre o tema.

4.3.1. Redes de Co-Citação

A análise de co-citação proporciona verificar a frequência com que periódicos ou autores são citados juntos por algum outro periódico ou autor da literatura. Em síntese, busca verificar uma medida de similaridade entre trabalhos citados, autores ou periódicos; e quanto mais dois trabalhos são citados juntos, mais seu conteúdo está relacionado. Para este estudo, optou-se por analisar as redes de co-citação entre autores, representadas pela Figura 9 criada pelo software VOSviewer com base nos autores conectados entre si. Foram encontrados 11.152 autores e o critério de corte foi o número mínimo de dez citações. Com este corte, apenas 38 atendem ao limite e somente 36 estão conectados entre si, o que levou a uma rede de co-citação de 36 autores, os chamados de nós.

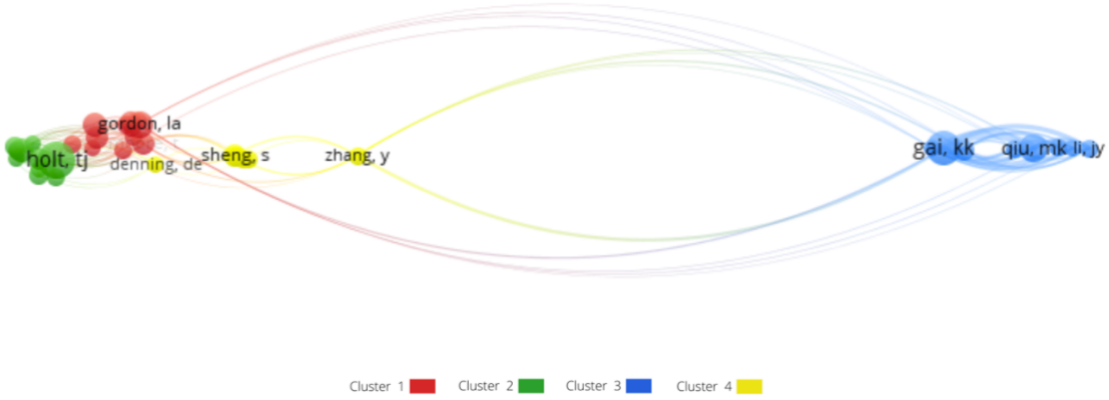

Figura 9 – Redes de Co-citação.

Fonte: Elaborado pelo autor

Nesta análise, a quantidade de citações que o respectivo autor recebeu é indicada pelo tamanho de cada nó da rede. Quanto mais próximos dois nós estão, significa que é mais forte a relação de co-citação entre eles.

A rede de co-citações do estudo foi distribuída em 4 *clusters*:

- O primeiro é composto por 12 autores, sendo os mais citados, nesta ordem, Gordon, LA. com 32 citações e Nagurney, A. com 26. Os autores com a maior força total do link são: Gordon, LA. com 125 links e Moore, T. com 99 links. Segundo Van Eck, N.J., & Waltman, L. (2010), o atributo força total do link indica a força total dos links de coautoria de um determinado pesquisador com outros pesquisadores.
- O segundo *cluster* é constituído por 10 autores, os mais relevantes são Holt, TJ. com 75 citações e Leukfeldt, ER. com 26 citações. Holt, TJ. com 372 e Bossler, AM. com 176, são os autores com a maior força total dos links.
- O terceiro *cluster* é formado por 8 autores, com destaque para os seguintes mais citados: Gai, KK. e Qiu, MK. São os mais citados, com respectivamente 61 e 41 citações. Também são os autores com a maior força total do link, Gai, KK. com 815 e Qiu, MK. com 606 links.
- O quarto *cluster* da rede de co-citação é formado por 6 autores. Os mais citados são Sheng, S. com 20 citações e Jain, AK com 14. Os autores que obtiveram a maior força total de link são: Zhang, Y. com 78 links e Sheng, S. com 60 links.

A tabela com a rede de co-citação completa pode ser verificada no Apêndice E.

4.3.2. Redes de Coautoria

Com objetivo de apontar as particularidades de colaboração entre os autores mais consideráveis, a Figura 10 indica as principais redes de coautoria mapeadas, utilizando o método de força de associação para normalizar a força das ligações entre os itens. Quanto maior a frequência de documentos produzido por um grupo de autores for, maior será a força de ligação. Para esta análise, foram consideradas publicações com até 25 autores por documento, e com isso, foram identificados 1.247 autores. Não foram utilizados critérios de corte para o número mínimo de documentos por autor e número mínimo de citações por autor. Dos 1.247 autores encontrados, apenas 31 apresentam o maior número de itens conectados, que são exibidos na figura a seguir.

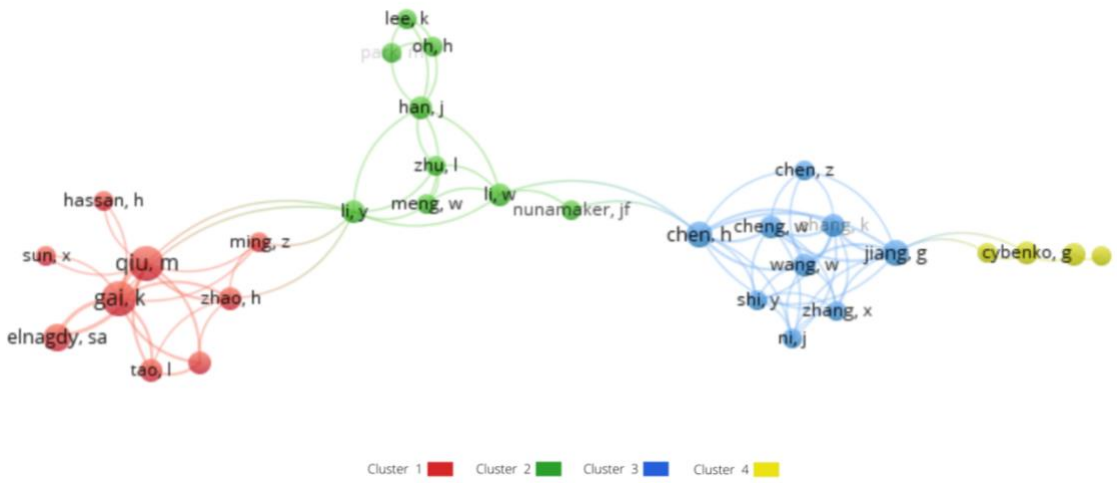

Figura 10 – Redes de Coautoria.

Fonte: Elaborado pelo autor

Os 31 nós foram distribuídos por 4 *clusters* de colaboração de pesquisa. O tamanho dos círculos representa a quantidade de artigos de cada autor na amostra, com destaque para Gal, K. e Qui, M. com a maior quantidade de artigos na amostra, ambos com 9 documentos cada:

- O *cluster* 1 é constituído por 9 autores, sendo Gal, K. e Qui, M os que possuem o maior número de links com os demais, ambos com 9 links e com a força total de link de 23.
- O *cluster* 2 é formado por 9 autores, com destaque para Li, Y. com 8 links, Han, J. com 7 links.
- O *cluster* 3 compreende 9 autores, sendo Chen, H. e Jiang, G. os autores com a maior quantidade de links, ambos com 10 links.
- Por fim, o *cluster* 4 é formado por 4 autores, onde Cybenko, G. obteve 3 links, sendo o autor com a maior quantidade de links deste *cluster*.

A tabela com a rede de coautoria completa pode ser verificada no Apêndice F.

4.3.3. Redes de Acoplamento Bibliográfico

O acoplamento bibliográfico mede a relação entre dois artigos com base no número de referências em comum a uma terceira obra comum em suas bibliografias. Segundo

Van Eck & Waltman (2014), quanto maior o número de referências que dois autores ou artigos compartilham, maior a força do acoplamento bibliográfico entre eles. A Figura 11 apresenta a rede de acoplamento bibliográfico entre os autores distribuída por *clusters*, onde cada um dos autores presentes em um determinado *cluster*, tende a citar os mesmos autores que os demais deste mesmo *cluster*.

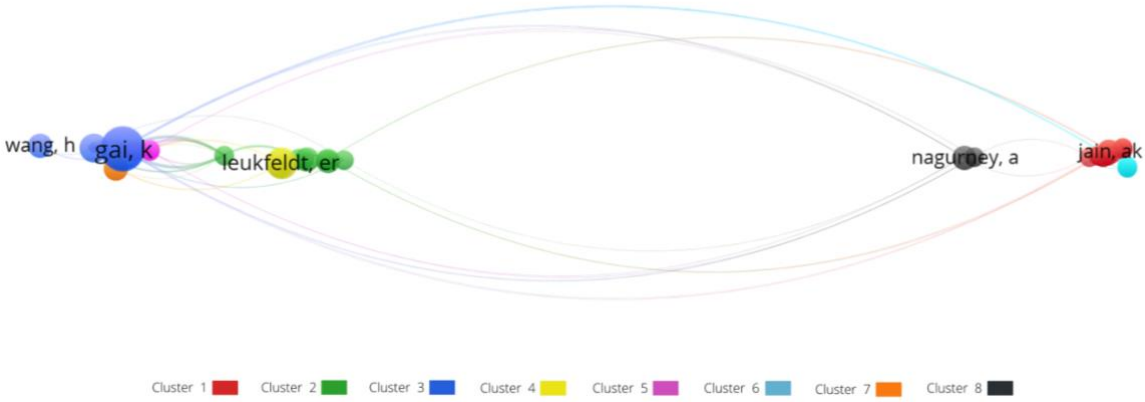

Figura 11 – Redes de Acoplamento Bibliográfico.

Fonte: Elaborado pelo autor

Foram encontrados 1.247 autores na base de dados e restringiu-se a 44 com critério de corte a autores com pelo menos de 2 documentos na amostra e com no mínimo 10 citações. Apenas 39 autores apresentaram conexão entre si, distribuídos em 8 *clusters*.

- O *cluster* 1, reuniu 14 autores, sendo Jain, AK. o autor com mais documentos, 3 no total. Os outros autores neste *cluster* apresentaram 2 documentos cada.
- O *cluster* 2, reuniu 8 autores, em que Chen, H. e Holt, TJ. são os autores que se destacam, com 3 documentos cada.
- No *cluster* 3, formado por 4 autores, Gai, K e Qiu, M são os autores com mais documentos, 9 cada.
- Outros 3 *clusters* (*cluster* 4, *cluster 5* e *cluster* 6) apresentaram 3 autores em cada um deles, destaca-se Leukfeldt, ER. com 5 documentos e Kleemans, ER. com 4 documentos. Os demais autores apresentaram 2 documentos cada.
- Os *cluster*s 7 e 8 registraram 2 autores em cada um deles. Awan, JH. e Memon, S. do *cluster* 7 reuniram 3 documentos.

- No *cluster* 8, destaca-se Nagurney, A. com 3 documentos.

A tabela completa com a rede de acoplamento bibliográfico pode ser verificada no Apêndice G.

4.3.4. Redes de Co-Ocorrências de Keywords

Definida pelo número de artigos em que ambas aparem conjuntamente, quer no título, no resumo ou na lista de *keywords*, a relação de co-ocorrência entre duas *kewwords* é estabelecida. A Figura 12 aponta as redes de co-ocorrência de *keywords* da base de dados analisada neste estudo. Foram verificadas as keywords do(s) autor(es) e as Keywords Plus™.

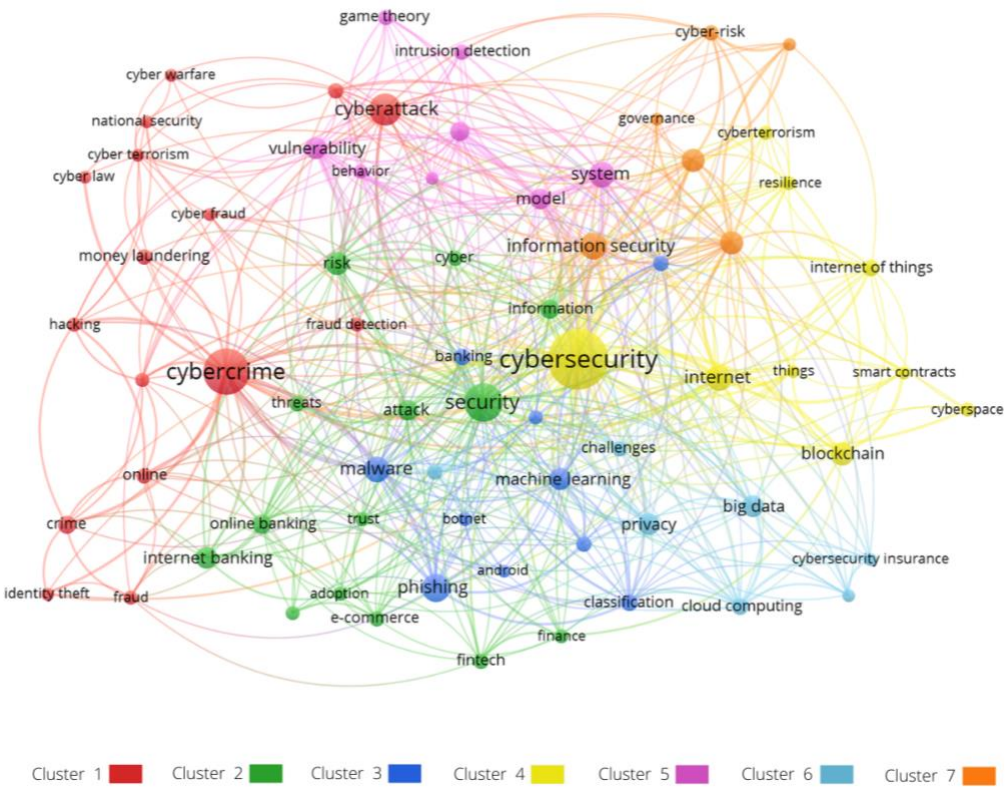

Figura 12 – Redes de Co-ocorrência de Keywords.

Fonte: Elaborado pelo autor

1.837 *keywords* do(s) autor(es) e *Keywords Plus*™ foram encontradas e para auxiliar a visualização, a construção da rede foi reduzida a *keywords* com 5 ou mais ocorrências, que resultou em 70 nós, distribuídos por 7 *clusters*:

- O *cluster* 1, contém 16 nós, verifica-se que as *keywords* com maior frequência de ocorrência são: *Cybercrime* com 62, *Cyberattack com 30* e *crime* com 10.
- No *cluster* 2, *Security* com 43, *Risk* com 16 e *internet banking* com 15, são as mais frequentes das 14 agrupadas no *cluster*.
- *Phishing* com 24 e *Malware* com 20 são as mais frequentes no *cluster* 3, que contou com 10 *keywords*.
- O *cluster* 4, agrupou 9 *keywords*, sendo a mais frequente, com 108 ocorrências, a *keyword Cybersecurity*.
- Com 8 *keywords*, o cluster 5 apontou a *keyword System* sendo a mais frequente, com 19 ocorrências.
- Entre as 7 *keywords* agrupadas no *cluster* 6, *Privacy* foi a *keyword* principal, com 15 ocorrências.
- No *cluster* 7, 6 *keywords* foram agrupadas, sendo *Information Security* a mais frequente, com 22 ocorrências.

Pode-se verificar a tabela completa com a rede de co-ocorrências de *keywords* no Apêndice H.

5. CONCLUSÃO

O presente trabalho teve como objetivo mapear a produção cientifica mundial sobre cibersegurança na "esfera" das finanças, a partir da análise de artigos depositados na plataforma Web of Science.

Em resposta à questão de investigação proposta neste estudo – O que nos diz a literatura científica que relaciona a "esfera" das finanças com cibersegurança? –, averiguou-se que a pesquisa no campo encontra-se em um período de forte crescimento, com o crescente volume de artigos publicados nos últimos anos.

Qiu, MK Gai, KK são os que publicam mais artigos que envolvem cibersegunça da "esfera" das finanças, porém nenhum deles é o autor mais citado. O autor mais citado, com base na soma de citações de todos os seus artigos, é Holt, TJ. com 75 citações. Holt, Thomas J. está associado a Michigan State University, nos Estados Unidos da América. Os referidos Gai, KK e Qiu, MK ocupam a segunda e terceira posição com 61 e 41 citações, respectivamente.

Embora o autor mais citado e com o maior número de documentos na amostra esteja vinculado a uma instituição dos Estados Unidos, é notória a presença ativa da Europa na literatura científica sobre cibersegurança na "esfera" das finanças, especificamente a Holanda com muitos dos autores mais produtivos da área de pesquisa, com um total de 52 pesquisadores e a Alemanha com a série de livros Lecture Notes in Computer Science, que foi o livro com mais publicações da área estudada com 12 publicações, resultado que corrobora a dispersão da produção no campo da ciberseguranca da "esfera" das finanças. O Computers & Security é o periódico que mais publica artigos com o tema abordado.

Constatou-se que as três áreas de pesquisa mais frequentes, também são correspondentemente as áreas de pesquisa com mais citações. Em relação as keywords do(s) autor(es), verificou-se que nas duas áreas de pesquisa com mais publicações (Computer Science e Engineering), as keywords mais frequentes são as mesmas três keywords principais dos autores de todo estudo (Cybersecurity, Cybercrime e Cyberattack). Porém as keywords do(s) autor(es) mais utilizadas não são as mesmas geradas por algoritmo para definir as *Keywords Plus*™. Com a rede de co-ocorrência de keywords, foi possível analisar e mapear as possíveis temáticas de pesquisa sobre cibercrimes na "esfera" das finanças, onde as principais encontradas também foram Cybersecurity e Cybercrime, sendo, portanto, as principais palavras que determinam a temática central.

O ano de 2018 destacou-se com o maior número de citações (358). Em relação às fontes mais frequentes, verificou-se que os três principais jornais também são os três de maior impacto com base no número de citações, com destaque para o Journal Computers & Security com 87 citações. Verificamos que a tendência de publicação de artigos

contendo a temática estudada é uma tendência exponencial e que provavelmente os trabalhos irão continuar a aumentar mais do que nos anos mais recentes.

Observou-se que o país que de acordo com a informação referida neste estudo sofre mais ciberataques financeiros no mundo (Rússia) não é o mesmo país com o maior número de publicações com o tema (Estados Unidos). A Rússia representa porém 4% dos artigos científicos na área estudada e situa-se na 5º posição dos países com mais publicações.

Com a rede de coautoria, constituída por quatro clusters, permitiu verificar os autores mais prolíficos da amostra em termos de publicações com co-autores.

A rede de co-citação foi organizada também em quatro clusters: o primeiro formado em torno dos autores Gordon, LA e Moore, T.; no segundo agrupamento destacam-se os autores Holt, TJ (autor mais citado) e Bossler, AM.; no o terceiro encontram-se o segundo e o terceiro autores mais citados do estudo, respetivamente Gai, KK e Qiu, MK., e, por fim, no quarto cluster, encontram-se com maior destaque os autores Zhang, Y e Sheng, S.. Estas informações poderão ser relevantes para uma posterior análise aprofundada da literatura sobre cibersegurança na área financeira.

Por fim, a rede de co-ocorrência de keyword mostrou sete principais linhas de pesquisa sendo conduzidas. O conjunto principal (cluster 4), sugere pesquisas que abordam as relações entre Cybersecurity e a segurança dos dados pessoais com o Blockchain, à luz da Industria 4.0 com a Internet of Things. O cluster que envolve mais a "esfera" das finanças é o número 2, no qual se registam pesquisas que abordam principalmente as relações entre as tecnologias aplicadas ao setor financeiro com destaque para o Internet Banking. Já o cluster que concentra o maior número de keywords ligados a cibersegurança é o cluster 1, onde 54% das keywords relacionadas a cibersegurança aparecem. Algumas limitações do estudo servem de ponto de partida para futuras pesquisas. Podemos destacar que a construção da base de dados que usámos não levou em conta o ano de 2020, ano em que muitos desafios, por conta da pandemia de Covid-19, ocorreram perante a temática do estudo. Segundo a COTEC Portugal (2020),

o estado de emergência em que vivemos atualmente, com a crise do Covid-19, tem estado a provocar uma aceleração da transição para a Indústria 4.0, e embora esteja funcionando também como um estimulante de inovação, a crise no entanto abriu caminho para muitos criminosos tirarem proveito desta situação, resultando em um aumento expressivo dos cibercrimes em instituições financeiras. De acordo com o Relatório Cibersegurança em Portugal - Riscos & Conflitos, no período que corresponde ao início do combate nacional à pandemia, o CERT constatou que o mês de março de 2020 teve mais 176% de ocorrências do que o de 2019.

Nestas circunstâncias, pretendo prosseguir a investigação futuramente pois creio que é possível e oportuno que surjam novas correntes de pesquisa sobre o objeto de estudo deste trabalho.

REFERÊNCIAS

Alex Scroxton (2019). Top 10 Cyber Crime Stories Of 2019- Here are Computer Weekly's Top 10 Cyber Crime Stories of 2019 [Em Linha]. Disponível Em: Https://Www.Computerweekly.Com/News/ 252475441/Top-10-Cyber-Crime-Stories-Of-2019 [Acesso Em: 29/05/2020].

Bazerman, C. (1988). Shaping Written Knowledge The Genre and Activity Of The Experimental Article in Science. Madison: The University of Wiscon- Sin Press.
Carvalho, F. J. C. Et. Al. (2000). Economia Monetária E Financeira. Rio De Janeiro.

Centro Nacional De Cibersegurança Portugal, (2020). Relatório Cibersegurança em Portugal-Sociedade. Disponível Em: https://www.cncs.gov.pt/content/files/relatorio_sociedade2020__observatoriocibersegurança_cncs.pdf [Acesso Em: 20/07/2020].

Centro Nacional De Cibersegurança Portugal, (2020). Risco e Conflitos. Disponível Em:https://www.cncs.gov.pt/content/files/relatorio_riscos.conflitos2020__observatoriocibersegurança_cncs.pdf

Da Redação (2020). Brasil, 4º País Mais Atacado por Malware Financeiro em 2019 [Em Linha]. Disponível Em: Https://Www.Cisoadvisor.Com.Br/Brasil-4o-Pais-Mais-Atacado-Por-Malware-Financeiro-Em-2019/ [Acesso Em: 10/06/2020].

Danenas, P. (2015). Intelligent Financial Fraud Detection and Analysis: A Survey of Recent Patents. Recent Patents Comput. Sci. 8. p. 13–23.

Eco (2019). Queixas Por Fraude Bancária Disparam No Ministério Público e Banco de Portugal. Disponível Em: Https://Eco.Sapo.Pt/2019/03/20/Queixas-Por-Fraude-Bancaria- Disparam-No-Ministerio-Publico-E-Banco-De-Portugal/ [Acesso Em: 20/12/2019].

Ellen Zhang (2019). The Top 10 Finserv Data Breaches [Em Linha]. Disponível Em: Https://Digitalguardian.Com/Blog/Top-10-Finserv-Data-Breaches [Acesso Em: 29/05/2020].

Erika Kraemer-Mbula, Puay Tang, Howard Rush (2013). The Cybercrime Ecosystem: Online Innovation in the Shadows?. Technological Forecasting and Social Change. Volume 80. Issue 3. p. 541-555.

European Cybercrime Centre - Ec3 (2020) Disponível em: Https://Www.Europol.Europa.Eu/About-Europol/European-Cybercrime-Centre-Ec3 [Acesso Em: 10/08/2020].

Faruk Ülgen (2015) Schumpeterian Innovations, Financial Innovations and Instability: an Institutional Perspective, Cuadernos De Economía, 106. p.38.

Garfield, E. (2001). From Bibliographic Coupling to Co-Citation Analysis Via Algorithmic Historio-Bibliography. Disponível Em: Https://Garfield.Library.Upenn.Edu/Papers/Drexelbelvergriffith92001.Pdf [Acesso Em: 11/06/2020].

Godinho, M. (2003): “Inovação: Conceitos E Perspectivas Fundamentais”, M.J. Rodrigues, A. Neves, M.M. Godinho (Orgs.). Para uma Política de Inovação em Portugal, Biblioteca ee Economia & Empresa, Dom Quixote, Lisboa, p. 29–51

Interpol (2020). Cybercrime - Future-Oriented Policing Projects. Disponível Em: Https://Www.Interpol.Int/Content/Download/5267/File/Cybercrime.Pdf. [Acesso Em: 20/10/2020].

Marcelo Moura E Daniel Haidar (2020). Os Ataques Cibernéticos Explodem Durante Pandemia e Expõem Vulnerabilidades das Empresas [Em Linha]. Disponível Em: Https://Epocanegocios.Globo.Com/Tecnologia/Noticia/2020/09/Os-Ataques-Ciberneticos-Explodem-Durante-Pandemia-E-Expoem-Vulnerabilidades-Das-Empresas.Html [Acesso Em: 01/11/2020].

Oecd (2005) Oslo Manual. Guidelines for Collection and Interpreting Innovation. 3rd Editions. Oecd Publications, Paris.

Paul Hunton (2009). The Growing Phenomenon of Crime and The Internet: A Cybercrime Execution and Analysis Model, Computer Law & Security Review. 25.Issue 6. p. 528-535.

Porter, A.L. (2007). How Tech Mining Can Enhance R&D Management. Research Technology Management.

Romanowski,J.P.; Ens, R. T. (2006) As Pesquisas Denominadas do Tipo "Estado da Arte" Em Educação. Revista Diálogo Educacional. 6. p.37-50.

Shu, Wesley & Strassmann, Paul. (2005). Does Information Technology Provide Banks With Profit?. Information & Management. 42. p. 781-787

Van Eck, N. J., & Waltman, L. (2014). Visualizing Bibliometric Networks. In Y. Ding, R. Rousseau, & D. Wolfram (Eds.), Measuring Scholarly Impact: Methods and Practice. p. 85 - 320.

Van Eck, N.J., & Waltman, L. (2010). Software Survey: Vosviewer, A Computer Program for Bibliometric Mapping. Scientometrics. 84(2). p. 523–538.

APÊNDICE

Apêndice A
Variação de Países com mais Publicações.

País	Quant.	% Variação
EUA	351	0%
Índia	165	-52,99%
Inglaterra	64	-61,21%
China	60	-6,25%
Rússia	56	-6,67%
Países Baixos	52	-7,14%
Coreia do Sul	50	-3,85%
Itália	47	-6,00%
Ucrânia	42	-10,64%
Austrália	37	-11,90%

Fonte: Elaborado pelo autor

Apêndice B
Frequência dos 3 Principais Autores

Ano	Autores		
	Qiu, MK	Gai, KK	Leukfeldt, ER
1995	0	0	0
1996	0	0	0
1997	0	0	0
1998	0	0	0
1999	0	0	0
2000	0	0	0
2001	0	0	0
2002	0	0	0
2003	0	0	0
2004	0	0	0
2005	0	0	0
2006	0	0	0
2007	0	0	0
2008	0	0	0
2009	0	0	0
2010	0	0	0
2011	0	0	0
2012	0	0	0
2013	0	0	0
2014	0	0	0
2015	1	1	0
2016	5	5	0
2017	1	1	4
2018	2	2	0
2019	0	0	1

Fonte: Elaborado pelo autor

Apêndice C
Variação das Três Principais 3 Keywords dos Autor

Cybersecurity			Cybercrime			Cyberattack		
Ano	Quant.	%	Ano	Quant.	%	Ano	Quant.	%
2000	1	0%	2008	1	0%	2008	1	0%
2009	1	0%	2009	0	-100%	2009	0	-100%
2010	0	-100%	2010	2	N/A	2010	1	N/A
2011	2	N/A	2011	1	-50%	2011	3	200%
2012	1	-50%	2012	2	100%	2012	0	-100%
2013	1	0%	2013	5	150%	2013	1	N/A
2014	3	200%	2014	1	-80%	2014	2	100%
2015	14	367%	2015	7	600%	2015	4	100%
2016	12	-14%	2016	7	0%	2016	4	0%
2017	17	42%	2017	13	86%	2017	8	100%
2018	31	82%	2018	8	-38%	2018	5	-38%
2019	23	-26%	2019	13	63%	2019	6	20%

Fonte: Elaborado pelo autor

Apêndice D
Variação das três principais Keywords Plus™

System			Security			Management		
Ano	Quant.	%	Ano	Quant.	%	Ano	Quant.	%
2011	1	0%	2014	2	0%	2015	1	0%
2015	1	0%	2015	5	150%	2016	2	100,00%
2016	2	100%	2016	2	-60%	2017	3	50,00%
2017	4	100%	2017	3	50%	2018	4	33,33%
2018	3	-25%	2018	2	-33%	2019	6	50,00%
2019	7	133%	2019	5	150%			

Fonte: Elaborado pelo autor

Apêndice E
Redes De Co-Citação

Cluster	Author	Citações	Total Link Strength
1	Gai, KK	61	815
1	Qiu, MK	41	606
1	Moore, T	22	99
1	Wall, DS	19	130
1	Gai, K	18	355
1	Kshetri, N	13	34
1	Mohammad, RM	13	31
1	Levi, M	11	38
1	Li, Y	11	156
1	Holt, T	10	96
1	Mukhopadhyay, A	10	43
1	Stone-Gross, B	10	18
2	Gordon, La	32	125
2	Leukfeldt, ER	26	140
2	Nagurney, A	26	12
2	Bossler, AM	16	176
2	Kleemans, ER	16	94
2	Zhang, Y	13	78
2	Brenner, SW	12	66
2	Li, JY	12	244
2	Michalas, A	10	0
2	Jean-Baptiste, H	10	219
3	Sheng, S	20	60
3	Bohme, R	19	65
3	Jain, AK	14	33
3	Pandey, P	12	6
3	Krebs, B	11	49
3	Langevoort, DC	10	0
3	Button, M	10	35
3	Denning, DE	10	13
4	Holt, TJ	75	372
4	Anderson, R	21	84
4	Cavusoglu, H	14	59
4	Hausken, K	11	30
4	Soudijn, MRJ	10	75
4	Yin, H	10	185

Fonte: Elaborado pelo autor

Apêndice F

Rede de Coautoria

Cluster	Autor	Documentos	Citações	Link	Total link strength
1	Gai, K	9	267	9	23
1	Qiu, M	9	267	9	23
1	Elnagdy, SA	4	45	2	8
1	Zhao, H	2	127	6	8
1	Tao, L	2	123	4	7
1	Thuraisingham, B	2	123	4	7
1	Ming, Z	1	43	4	4
1	Hassan, H	1	6	2	2
1	Sun, X	1	50	2	2
2	Han, J	2	5	7	7
2	Lee, K	1	2	3	3
2	Li, W	2	20	6	6
2	Li, Y	2	46	8	8
2	Meng, W	1	3	4	4
2	Nunamaker, JF	1	17	2	2
2	Oh, H	1	2	3	3
2	Park, M	1	2	3	3
2	Zhu, L	1	3	4	4
3	Chen, H	3	23	10	14
3	Chen, Z	1	5	5	5
3	Cheng, W	2	6	8	12
3	Jiang, G	3	6	10	14
3	Mtsweni, J	1	1	7	2
3	Shi, Y	1	1	7	7
3	Wang, W	2	6	8	12
3	Zhang, K	2	6	8	12
3	Zhang, X	1	1	7	7
4	Cybenko, G	2	0	3	3
4	Koziel, E	1	0	1	1
4	Mcgrath, D	1	0	2	2
4	Robinson, D	2	0	2	2

Fonte: Elaborado pelo autor

Apêndice G
Rede de Acoplamento Bibliográfico

Cluster	Autor	Documentos	Citações	Total link strength
1	Jain, AK	3	68	369
1	Buber, E	2	39	176
1	Choo, KKR	2	15	10
1	Diri, B	2	39	176
1	Enbody, RJ	2	15	74
1	Gupta, BB	2	47	343
1	Li, J	2	84	8
1	Mehtre, BM	2	11	3
1	Ravi, V	2	64	41
1	Sahingoz, OK	2	39	176
1	Sood, AK	2	15	74
1	Thabtah, F	2	17	51
2	Chen, H	3	23	84
2	Holt, TJ	3	134	360
2	Bossler, AM	2	104	353
2	Dupont, B	2	21	28
2	Li, W	2	20	126
2	Xie, L	2	244	2
3	Gai, K	9	267	2712
3	Qiu, M	9	267	2712
3	Elnagdy, SA	4	45	1662
3	Wang, H	3	17	5
4	Leukfeldt, ER	5	68	409
4	Kleemans, ER	4	61	375
4	Stol, WP	2	49	209
5	Tao, L	2	123	442
5	Thuraisingham, B	2	123	442
5	Zhao, H	2	127	581
6	Deane, JK	2	45	226
6	Rakes, TR	2	45	226
6	Rees, LP	2	45	226
7	Awan, JH	3	11	87
7	Memon, S	3	11	87
8	Nagurney, A	3	48	130
8	Shukla, S	2	40	129

Fonte: Elaborado pelo autor

Apêndice H
Redes De Co-Ocorrências De Keywords

Cluster	Keyword	Ocorrência	Total link strength
1	Cybercrime	62	91
1	Cyberattack	30	41
1	Crime	10	19
1	Money Laundering	8	7
1	Online	8	20
1	Critical Infrastructure	7	17
1	Fraud	6	11
1	Fraud Detection	6	10
1	Hacking	6	18
1	Victimization	6	18
1	Cyber Fraud	5	8
1	Cyber Law	5	6
1	Cyber Terrorism	5	11
1	Cyber Warfare	5	5
1	Identity Theft	5	10
1	National Security	5	7
2	Security	43	89
2	Risk	16	41
2	Internet Banking	15	22
2	Attack	13	25
2	Information	12	36
2	Online Banking	11	28
2	Fintech	8	18
2	Threats	8	18
2	Cyber	7	20
2	E-Commerce	7	17
2	Adoption	6	16
2	E-Banking	6	9
2	Finance	6	14
2	Trust	6	23
3	Phishing	24	42
3	Malware	20	47
3	Machine Learning	14	28
3	Banking	9	15
3	Classification	9	30
3	Framework	8	27
3	Social Engineering	7	19
3	Botnet	6	10
3	Data Mining	6	15
3	Android	5	9
4	Cybersecurity	108	192
4	Internet	19	68
4	Blockchain	16	33
4	Internet Of Things	9	23
4	Cyberspace	6	8
4	Cyberterrorism	6	10
4	Resilience	6	22
4	Smart Contracts	5	18
4	Things	5	22
5	System	19	60
5	Vulnerability	15	42
5	Impact	11	35
5	Model	13	37
5	Game Theory	8	14
5	Intrusion Detection	7	11
5	Behavior	6	20
5	Network Security	5	14
6	Privacy	15	35
6	Big Data	14	35
6	Cloud Computing	9	34
6	Networks	8	23
6	Challenges	7	17
6	Cybersecurity Insurance	5	19
6	Financial Industry	5	17
7	Information Security	22	41
7	Risk Management	17	36
7	Management	16	54
7	Cyber-Risk	8	21

Apêndice H
Redes De Co-Ocorrências De Keywords (continuação)

Cluster	Keyword	Ocorrência	Total link strength
7	Governance	5	12
7	Operational Risk	5	16

Fonte: Elaborado pelo autor