InterSciencePlace
International Scientific Journal – ISSN: 1679-9844
Volume 20, Article nº 04 January/December 2025
D.O.I: http://dx.doi.org/10.6020/1679-9844/v20a03
Accepted: 21/12/2024 Published: 04/07/2025

SOCIAL ENGINEERING AND VIRTUAL CRIMES: A BIBLIOMETRIC ANALYSIS OF SCIENTIFIC PRODUCTION

ENGENHARIA SOCIAL E CRIMES VIRTUAIS: UMA ANÁLISE BIBLIOMÉTRICA DA PRODUÇÃO CIENTÍFICA

Rodolfo Maravilha Franco da Silva
Mestrando em Cognição e Linguagem - UENF

Carlos Henrique Medeiros de Souza
Doutor em Comunicação - UFRJ
ORCID: 0000-0002-3774-0323

Fabio Machado de Oliveira
Doutor em Cognição e Linguagem – UENF
ORCID: 0000-0003-1336-2994

Abstract

The digital age has intensified global interconnection, but it has also driven the growth of cybercrime, highlighting social engineering as a particularly effective form of attack. Unlike exploiting technical flaws, social engineering manipulates human vulnerability through psychological and linguistic tactics, transforming the individual into the main target and, often, the weakest link in security. This article presents a bibliometric and qualitative analysis of the scientific production on the intersection between social engineering and cybercrime, with data extracted from the Scopus database and processed via VOSviewer. The study revealed a notable expansion in the interest of the scientific community from 2020 onwards, culminating in a peak of publications in 2024, which underscores the growing relevance of the topic in the global academic agenda. The predominance of areas such as Computer Science, Engineering and Social Sciences reinforces the interdisciplinary nature of the field, but also highlighted a significant gap in the scientific production dedicated to public security, a highly relevant finding that highlights the urgent need for greater engagement on the part of professionals in the field. Geographically, India and the United States lead the production, with a notable contribution from Brazil as well. The co-occurrence analysis of key terms identified conceptual clusters

covering cybersecurity, digital crime typologies (including the concept of social engineering itself) and emerging technologies, such as machine learning, highlighting the interconnectivity of defensive, offensive and technological approaches. The theoretical foundation consolidates the understanding that social engineering is a sophisticated art of manipulation that exploits human traits such as gullibility and desire for acceptance. In short, this work not only quantifies the research landscape, but also critically reinforces that the central vulnerability lies in human behavior, implying the need for more robust security policies, effective awareness programs and continuous improvement of investigation methods that consider the psychological and social dimensions of cybercrime. Future research could focus on the effectiveness of educational interventions based on cognition and language and the application of artificial intelligence to detect manipulation patterns.

Keyword: Social Engineering, Cybercrimes and Bibliometric Analysis

Resumo

A era digital intensificou a interconexão global, mas também impulsionou o crescimento da criminalidade cibernética, destacando a engenharia social como uma modalidade de ataque especialmente eficaz. Diferentemente das explorações de falhas técnicas, a engenharia social manipula a vulnerabilidade humana por meio de táticas psicológicas e linguísticas, transformando o indivíduo no principal alvo e, frequentemente, no elo mais fraco da segurança. Este artigo apresenta uma análise bibliométrica e qualitativa da produção científica sobre a interseção entre engenharia social e crimes virtuais, com dados extraídos da base Scopus e processados via VOSviewer. O estudo revelou uma notável expansão no interesse da comunidade científica a partir de 2020, culminando em um pico de publicações em 2024, o que sublinha a crescente relevância do tema na agenda acadêmica global. A predominância de áreas como Ciência da Computação, Engenharia e Ciências Sociais reforça o caráter interdisciplinar do campo, mas também evidenciou uma significativa lacuna na produção científica dedicada à segurança pública, um achado de grande relevância que destaca a necessidade premente de maior engajamento por parte dos profissionais da área. Geograficamente, a Índia e os Estados Unidos lideram a produção, com uma contribuição notável também do Brasil. A análise de co-ocorrência de termos-chave identificou clusters conceituais abrangendo cibersegurança, tipologias de crimes digitais (incluindo o próprio conceito de engenharia social) e tecnologias emergentes, como machine learning, ressaltando a interconectividade das abordagens defensivas, ofensivas e tecnológicas. A fundamentação teórica consolida a compreensão de que a engenharia social é uma arte sofisticada de manipulação que explora traços humanos como credulidade e desejo de aceitação. Em suma, este trabalho não apenas quantifica o panorama da pesquisa, mas também reforça criticamente que a vulnerabilidade central reside no comportamento humano, implicando a necessidade de políticas de segurança mais robustas, programas de conscientização eficazes e aprimoramento contínuo dos métodos de investigação que contemplem a dimensão psicológica e social do cibercrime. As futuras pesquisas poderão focar na eficácia de intervenções educativas baseadas na cognição e linguagem e na aplicação da inteligência artificial para detecção de padrões de manipulação.

Palavras-chave: Engenharia Social, Crimes Virtuais e Análise Bibliométrica

INTRODUÇÃO

A era digital, marcada pela crescente interconexão e dependência de sistemas tecnológicos, trouxe consigo um avanço sem precedentes na comunicação, no comércio e nas relações sociais. Contudo, essa evolução também pavimentou o caminho para o crescimento exponencial da criminalidade cibernética, um desafio complexo e multifacetado que transcende as barreiras geográficas e exige abordagens integradas para sua compreensão e combate. Dentre as diversas modalidades de ataques virtuais, a engenharia social emerge como um vetor particularmente insidioso e eficaz. Ao invés de explorar falhas técnicas em sistemas, a engenharia social manipula a vulnerabilidade humana, recorrendo a táticas psicológicas e linguísticas para induzir indivíduos a cometerem ações que comprometem sua própria segurança ou a de suas organizações. Essa exploração da cognição e do comportamento humano torna a engenharia social o que muitos consideram o “elixir” dos crimes cibernéticos, pois transforma o elo mais fraco da segurança – o ser humano – em seu principal ponto de ataque.

A relevância de se aprofundar na compreensão da engenharia social no contexto da criminalidade cibernética é evidente, não apenas para pesquisadores da área de segurança da informação, mas também para profissionais do direito, formuladores de políticas públicas e, especialmente, para aqueles na linha de frente do combate ao crime, como os Delegados de Polícia Civil. A perspectiva da cognição e da linguagem, fundamental para entender como a manipulação psicológica se estrutura e se efetiva, torna-se um pilar essencial para desvendar os mecanismos por trás desses crimes e atuar de forma mais proativa na prevenção e na persecução penal.

Apesar da importância crescente do tema, percebe-se uma escassez de estudos bibliométricos que explorem de forma abrangente a intersecção entre engenharia social e criminalidade cibernética no cenário acadêmico global. Mapear e analisar a produção científica existente é crucial para identificar as lacunas de pesquisa, as tendências emergentes, os principais atores e as metodologias predominantes. Tal mapeamento pode subsidiar a construção de estratégias mais

eficazes de conscientização, educação e defesa contra esses ataques que geram expressivos impactos sociais e econômicos.

Diante desse contexto, o presente artigo tem como objetivo geral realizar uma análise bibliométrica e qualitativa da produção científica sobre o papel da engenharia social na criminalidade cibernética, indexada nas bases de dados Scopus, além de executar a confecção de gráficos na plataforma VOSviewer.

Espera-se que este estudo contribua significativamente para traçar um panorama do estado da arte da pesquisa na intersecção entre engenharia social e crimes virtuais, fornecendo subsídios para pesquisadores, profissionais de segurança cibernética e formuladores de políticas públicas na identificação de lacunas de conhecimento e no direcionamento de futuras investigações e estratégias de prevenção e combate a essa modalidade criminosa.

FUNDAMENTAÇÃO TEÓRICA

A engenharia social, um vetor de ataque cada vez mais prevalente na segurança da informação, explora intrinsecamente a vulnerabilidade humana como o elo mais fraco em qualquer sistema de defesa. Conforme elucidado por Viana, Alves e Lima (2022), esta técnica se manifesta na manipulação de indivíduos para a subtração de informações ou bens, sendo particularmente perigosa por operar em interações interpessoais que sistemas computacionais dificilmente conseguem detectar. Os autores destacam a suscetibilidade humana a essa prática, atribuindo-a a características como a tendência de seguir instruções, a credulidade, o desejo de ser prestativo ou aprovado socialmente. Para compreender a dinâmica desses ataques, o estudo aponta para uma visão multidimensional, que abrange a persuasão, a fabricação de cenários e a coleta prévia de dados sobre a vítima, permitindo ao agressor aprimorar a eficácia de sua abordagem e, consequentemente, o sucesso do golpe.

Aprofundando na compreensão da engenharia social, Aramuni e Maia (2018) reforçam que essa prática consiste na "arte de manipular pessoas a fim de contornar dispositivos de segurança" (ARAMUNI; MAIA, 2018, p. 32), popularizada por figuras

como Kevin Mitnick. O cerne da questão reside na exploração das características comportamentais humanas que tornam os indivíduos suscetíveis à manipulação, como a vontade de ser útil, a busca por novas amizades e a difusão de responsabilidade. Tais traços são sistematicamente utilizados para obter informações sigilosas ou contornar as barreiras tecnológicas, confirmando a perspectiva de que "o ser humano" é o principal ponto de fragilidade nos sistemas de segurança (ARAMUNI; MAIA, 2018, p. 31). Diante desse cenário, os autores enfatizam a necessidade de políticas de segurança bem definidas e a conscientização contínua dos colaboradores como mecanismos essenciais para mitigar os riscos associados à dimensão humana da segurança da informação.

A versatilidade e a natureza multifacetada dos ataques de engenharia social são amplamente abordadas por Popper e Brignoli ([s.d.]), que a descrevem como uma "antiga técnica de roubo de informações importantes de pessoas descuidadas, através de uma boa conversa" (POPPER; BRIGNOLI, [s.d.], p. 1). O estudo detalha as diversas modalidades de ataque, que podem ser classificadas em aspectos físicos, como a obtenção de informações em locais de trabalho, por telefone ou até mesmo no lixo, e psicológicos, que envolvem técnicas de persuasão e manipulação. Além disso, os autores exploram a vertente online, que se beneficia da criação de senhas fracas e da desatenção dos usuários em ambientes virtuais. A ausência de uma fórmula definida para esses ataques, aliada à sua capacidade de explorar o fator humano negligenciado pelas empresas que investem pesadamente apenas em tecnologia, consolida a engenharia social como um perigo eminente e de difícil combate.

Complementando as discussões sobre o impacto da engenharia social, Coelho, Rasma e Morales (2013) sublinham a ameaça que essa prática representa para a sociedade da informação, especialmente por afetar o "componente mais frágil do sistema, o usuário" (COELHO; RASMA; MORALES, 2013, p. 35). O artigo ressalta que, embora a tecnologia tenha avançado significativamente, a criatividade dos criminosos e a ingenuidade das pessoas continuam a encontrar um terreno fértil para furtos e roubos virtuais. Em um contexto onde a informação é um ativo vital, a proteção se estende por todo o seu ciclo de vida – manipulação, armazenamento, transporte e descarte –, exigindo a formação de uma "cultura de segurança" (COELHO; RASMA; MORALES, 2013, p. 37) por meio de conscientização e treinamento. Essa abordagem

holística é crucial para proteger os dados pessoais e corporativos contra as vulnerabilidades comportamentais exploradas pela engenharia social.

PERCURSO INVESTIGATIVO

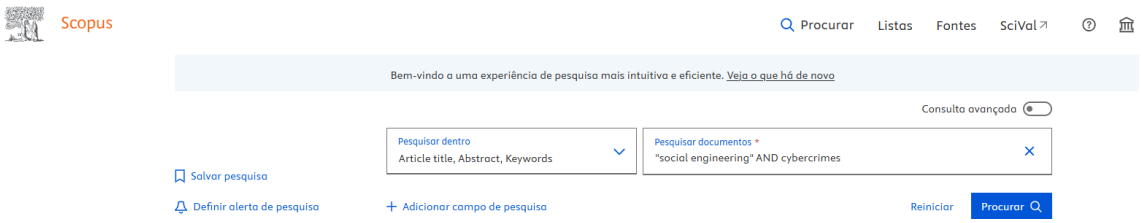
O presente estudo adota uma abordagem metodológica bibliométrica de caráter exploratório e descritivo, visando compreender a dinâmica e o panorama da produção científica em um tema tão relevante e multidisciplinar quanto a intersecção entre engenharia social e crimes virtuais. Embora o foco principal seja quantitativo, o objetivo subjacente está alinhado com a premissa de investigações sistemáticas, que buscam "reunir, avaliar criticamente e conduzir uma síntese dos resultados de múltiplos estudos primários", conforme elucidado por *Cordeiro et al. (2007)* em sua revisão sobre o tema. Ao fazer isso, o estudo contribui para a visibilidade e disseminação do conhecimento, um aspecto crucial para a ciência, como ressaltado por *Dantas (2004)* ao abordar a importância da indexação bibliográfica para "aumentar o alcance de divulgação e exposição da ciência nacional".

Para a coleta de dados desta investigação, foi empregada exclusivamente a base de dados Scopus. A seleção da Scopus se justifica por sua vasta abrangência e reconhecimento como uma das principais plataformas de indexação de literatura científica revisada por pares em diversas áreas do conhecimento. A estratégia de busca foi formulada de maneira precisa para garantir a relevância dos documentos recuperados, utilizando a combinação dos termos-chave "social engineering" e "cybercrimes" vinculados pelo operador booleano "AND" (Figura 1). Esta sintaxe foi aplicada ao campo “Article title, Abstract, Keywords” dos documentos, assegurando que os resultados estivessem diretamente relacionados ao escopo da pesquisa e, assim, contribuíssem para a melhoria da qualificação e impacto científico do trabalho, um ponto valorizado no processo de seleção e avaliação de bases de dados, conforme discutido por *Dantas (2004)*.

Após a recuperação dos documentos, os dados bibliográficos foram extraídos da Scopus e processados para análise e visualização. Para a construção de mapas de co-ocorrência e redes de colaboração, empregou-se o software VOSviewer. A

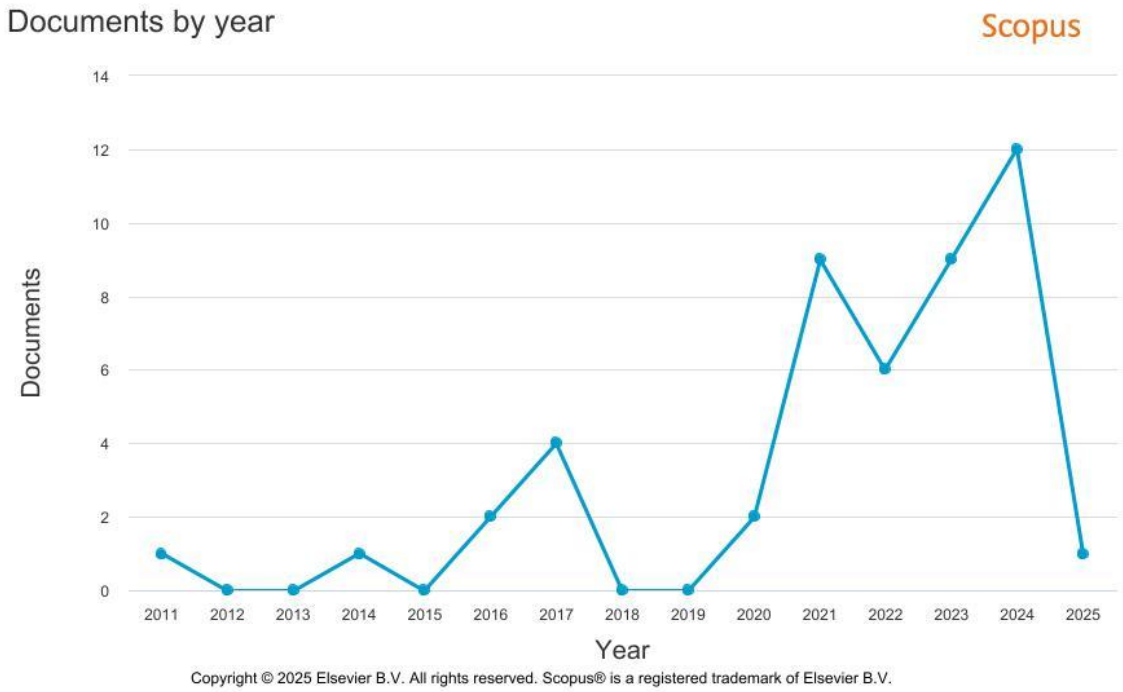
utilização dessa ferramenta é fundamental para sintetizar grandes volumes de dados e transformar informações complexas em representações visuais claras, permitindo a identificação de agrupamentos temáticos, os autores e instituições de maior relevância, e as conexões entre conceitos. Este processo de análise de dados, ao oferecer uma síntese organizada da literatura, auxilia na "tomada de decisão" sobre o estado do conhecimento, ecoando o propósito das revisões sistemáticas de fornecer a "melhor informação disponível" para a tomada de decisões, como apontado por *Cordeiro et al. (2007)*, e contribuindo para uma melhor compreensão do impacto científico, conceito central no editorial de *Dantas (2004)*.

Figura 1 – parâmetros de pesquisa na base de dados SCOPUS



A análise da distribuição temporal dos documentos indexados na base de dados Scopus, apresentada Figura 2, revela a evolução da produção científica relacionada ao tema da pesquisa no período de 2011 a 2025. Observa-se que, nos anos iniciais (2011-2019), a atividade de publicação foi bastante limitada e intermitente, com picos máximos de 4 documentos em 2017 e vários anos sem registro de publicações. No entanto, a partir de 2020, a produção científica demonstrou um crescimento notável, passando de 2 documentos para aproximadamente 9 em 2021 e 2023, atingindo seu ápice em 2024 com cerca de 12 documentos publicados. A acentuada redução para apenas 1 documento em 2025 é esperada, visto que o ano ainda está em curso e os dados para esse período estão incompletos. Essa tendência geral aponta para um aumento significativo no interesse e na consolidação da área de pesquisa a partir da última década.

Figura 2 – documentos por ano

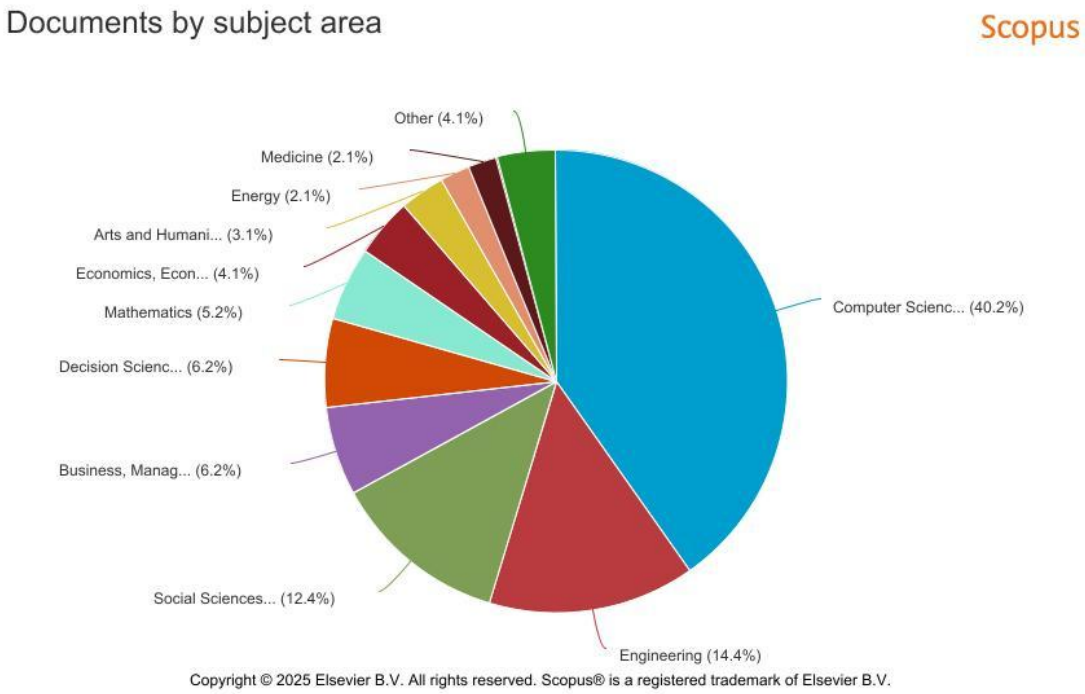


A distribuição dos documentos por área temática, conforme ilustrado na Figura 3, oferece insights sobre as disciplinas que mais contribuem para a literatura sobre engenharia social e crimes virtuais na base Scopus. Evidencia-se uma predominância notável da **Ciência da Computação**, responsável por 40,2% das publicações, o que reflete a natureza tecnológica inerente aos crimes cibernéticos. Em seguida, as áreas de **Engenharia (14,4%)** e **Ciências Sociais (12,4%)** emergem como campos significativos, ressaltando o caráter interdisciplinar do tema, que abrange tanto as vulnerabilidades sistêmicas quanto as humanas. Contribuições relevantes também são observadas em Gestão e Negócios (6,2%) e Ciências da Decisão (6,2%), indicando a preocupação com aspectos organizacionais e decisórios. A presença, ainda que em menor proporção, de outras áreas como Matemática (5,2%), Economia (4,1%), Artes e Humanidades (3,1%), Medicina (2,1%) e Energia (2,1%) reforça a complexidade do fenômeno e a necessidade de uma abordagem multifacetada para sua compreensão e combate.

Ademais, é de cardinal importância pôr em relevo o fato de que a área de segurança pública não aparece nos dados descritos no gráfico, o que demonstra que os atores da segurança pública não se dedicam à produção científica sobre o tema,

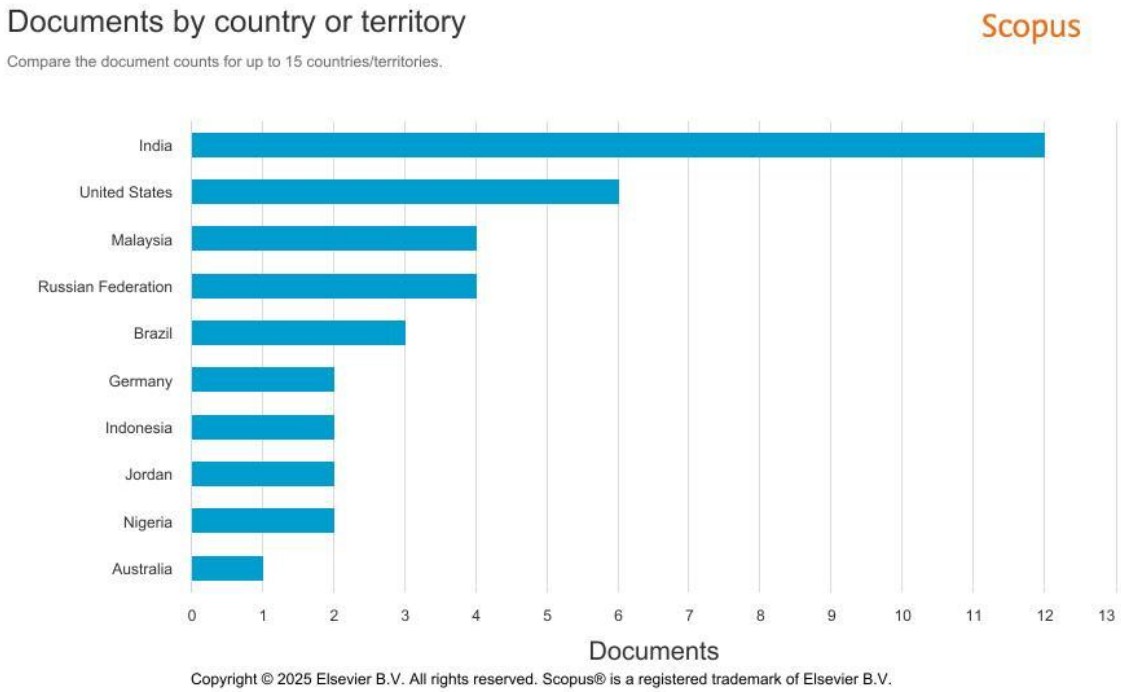
revelando, portanto, ainda mais relevância do assunto e da necessidade de ser tratado dentro deste prisma, já que diretamente relacionado a proposição de políticas públicas e desenvolvimento de estratégias para o combate a esta modalidade criminosa.

Figura 3 – distribuição por áreas temáticas



A distribuição geográfica dos documentos, conforme ilustrado Figura 4, revela os principais países ou territórios que contribuem para a produção científica sobre o tema na base de dados Scopus. Observa-se que a **Índia** se destaca como o país com a maior quantidade de publicações, registrando aproximadamente 12 documentos, o que a posiciona como um polo significativo de pesquisa na área. Os **Estados Unidos** aparecem em segundo lugar, com cerca de 6 documentos, seguidos por **Malásia** e **Rússia**, cada uma com aproximadamente 4 documentos. O **Brasil** figura na quinta posição, contribuindo com cerca de 3 documentos. Países como Alemanha, Indonésia, Jordânia e Nigéria demonstram uma participação mais modesta, com aproximadamente 2 documentos cada, enquanto a Austrália registra apenas 1 documento. Essa análise da origem dos documentos é crucial para identificar as geografias mais ativas na pesquisa e compreender a dispersão internacional do conhecimento sobre engenharia social e crimes cibernéticos.

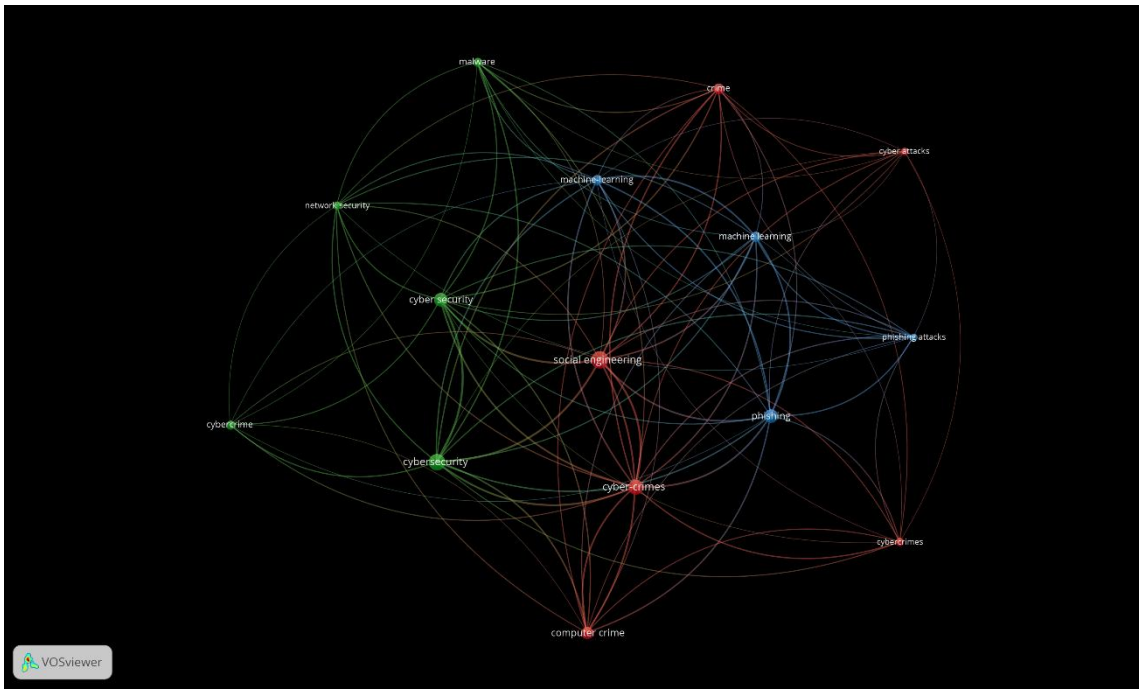
Figura 4 – distribuição países ou territórios



A análise da co-ocorrência de termos-chave, visualizada no mapa gerado pelo VOSviewer Figura 5, revela a estrutura conceitual e as interconexões temáticas predominantes na produção científica sobre engenharia social e crimes virtuais. Foram identificados três clusters principais: o **cluster verde** agrupa termos relacionados à segurança e defesa cibernética, como "cybersecurity", "network security" e "malware", indicando um foco nas medidas protetivas e de detecção. O **cluster vermelho** compreende conceitos de crimes digitais, incluindo "computer crime", "cyber-crimes" e "social engineering", delineando as atividades criminosas e suas metodologias. Por fim, o **cluster azul** destaca tipos específicos de ataques e tecnologias emergentes, com termos como "phishing", "phishing attacks", "cyber attacks", e a proeminente presença de "machine learning". Termos como "cybersecurity" e "computer crime" se destacam pelo tamanho dos nós, refletindo sua centralidade e alta frequência na literatura. É notável a interconectividade entre os clusters, evidenciada pelas ligações de "social engineering" (vermelho) com "cybersecurity" (verde), e a posição de "machine learning" (azul), que atua como ponte entre a detecção de ataques e a análise de crimes cibernéticos, sublinhando o papel crescente da inteligência artificial na segurança digital e no combate ao cibercrime. Essa visualização demonstra a natureza multifacetada do campo, conectando

aspectos defensivos, ofensivos e tecnológicos, e apontando para áreas de pesquisa interligadas e de alta relevância.

Figura 5 – *Wordmap* de palavras-chave



A revisão de literatura é reconhecida como um pilar fundamental para a construção do conhecimento científico, servindo de alicerce para a redação de trabalhos acadêmicos e para a identificação de lacunas de pesquisa. Conforme elucidado por *Ferenhof e Fernandes (2016)*, essa etapa permite ao pesquisador familiarizar-se com o campo, reconhecer autores relevantes e, crucialmente, formular ou refinar o problema de pesquisa. No contexto deste estudo sobre engenharia social e crimes virtuais, a abordagem sistemática da revisão bibliométrica adere a esses princípios, buscando não apenas mapear a produção existente, mas também sistematizar o processo de busca para garantir a repetibilidade e a mitigação de vieses, habilitando a interpretação dos dados para identificar os hiatos de conhecimento e, assim, impulsionar futuras investigações sobre um tema de crescente complexidade.

CONCLUSÃO

O presente estudo empreendeu uma investigação bibliométrica sobre a interseção entre engenharia social e crimes virtuais, com o objetivo de mapear o panorama da produção científica, identificar as lacunas de pesquisa e aprofundar a compreensão sobre a vulnerabilidade humana nesse contexto. Através de uma metodologia rigorosa, que incluiu a coleta e análise de documentos da base de dados Scopus utilizando ferramentas como o VOSviewer, foi possível traçar um panorama que reforça a natureza complexa e multifacetada do tema.

A análise temporal revelou um interesse crescente da comunidade científica no assunto, com uma notável expansão das publicações a partir de 2020, culminando em um pico de produção em 2024. Essa evolução reflete a crescente relevância da engenharia social como ameaça à segurança da informação na era digital. Geograficamente, países como a Índia e os Estados Unidos se destacam como os maiores produtores de conhecimento, embora o Brasil também apresente uma contribuição significativa, demonstrando uma preocupação global com a temática.

Em termos de áreas do conhecimento, a pesquisa confirmou o caráter interdisciplinar do campo. A Ciência da Computação e a Engenharia são as disciplinas predominantes, o que é natural dada a natureza tecnológica dos crimes virtuais. Contudo, a expressiva participação das Ciências Sociais, Gestão e Ciências da Decisão sublinha a importância do fator humano e comportamental, validando a premissa central de que a engenharia social explora o "elo mais fraco" — o indivíduo. Outrossim, o trabalho também revelou a carência de produção científica no campo da segurança pública, revelando que os profissionais da área ainda não se debruçaram sobre o tema. O mapeamento conceitual, por sua vez, evidenciou clusters temáticos que englobam desde a cibersegurança e defesa cibernética até os métodos de ataques específicos, como o *phishing*, e a emergência de tecnologias como *machine learning* no combate e na análise desses fenômenos.

A fundamentação teórica consolidou a compreensão de que a engenharia social se manifesta como uma sofisticada arte de manipulação. Autores como Viana, Alves e Lima (2022) e Aramuni e Maia (2018) detalharam como a persuasão, a fabricação de cenários e a coleta de dados são empregadas para explorar traços

humanos como a credulidade, a vontade de ser útil e a busca por aceitação social. Popper e Brignoli ([s.d.]) e Coelho, Rasma e Morales (2013) complementam essa visão ao destacar a versatilidade dos métodos, sejam eles físicos ou online, e a imperativa necessidade de uma "cultura de segurança" que transcenda as soluções tecnológicas para focar na conscientização e treinamento contínuo dos usuários.

Em suma, este trabalho não apenas quantificou a produção científica e desvendou a estrutura conceitual da engenharia social e crimes virtuais, mas também reforçou a crítica fundamental de que a principal vulnerabilidade reside no comportamento humano.

As implicações deste estudo são vastas, abrangendo a necessidade de políticas de segurança mais robustas nas organizações, programas de conscientização eficazes para o público em geral e, no âmbito da segurança pública, o aprimoramento de métodos de investigação que levem em conta a dimensão psicológica e social dos cibercriminosos. Sugere-se que futuras pesquisas possam aprofundar na eficácia de intervenções educativas baseadas em cognição e linguagem para aumentar a resiliência humana contra a engenharia social, bem como explorar o uso de IA na detecção precoce de padrões de manipulação. A proteção da informação, nesse cenário, é uma tarefa contínua que demanda a harmonização entre avanços tecnológicos e a constante elevação da consciência humana.

REFERÊNCIAS

FERENHOF, H. A.; FERNANDES, R. F. Desmistificando a revisão de literatura como base para redação científica: método SSF. **Revista ACB: Biblioteconomia em Santa Catarina**, Florianópolis, SC: v. 21, n. 3, p. 550-563, ago./nov., 2016.

CORDEIRO, Alexander Magno et al. Revisão sistemática: uma revisão narrativa. **Revista Colégio Brasileiro de Cirurgiões**, Rio de Janeiro, v. 34, n. 6, p. 428-431, 2007.

DANTAS, Paulo Elias. Indexação bibliográfica em bases de dados: O que é? Para que serve? Onde estamos?. Arq. Bras. Oftalmol., São Paulo , v. 67, n. 4, p. 569-570, Aug. 2004 . Available from . access on 26 Oct. 2017. http://dx.doi.org/10.1590/S00042749200400040001

ARAMUNI, João Paulo; MAIA, Luiz Cláudio. O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa. **AtoZ: novas práticas em informação e conhecimento**, Belo Horizonte, v. 7, n. 1, p. 31-37, jan./jun. 2018. DOI: 10.5380/atoz.v7i1.64640.

COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. Engenharia Social: uma ameaça à sociedade da informação. **Perspectivas Online: Ciências Sociais Aplicadas**, [s. l.], v. 3, n. 9, p. 34-44, 2013.

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. **ENGENHARIA SOCIAL: Um Perigo Eminente**. [S.l.]: Instituto Catarinense de Pós-Graduação, [s.d.].

VIANA, José Augusto Lopes; ALVES, Antônio José Costa; LIMA, Pedro Gustavo Santos de. Vulnerabilidade à Engenharia Social: um estudo com alunos do Instituto Federal da Paraíba (IFPB). **Revista Principia**, João Pessoa, v. 59, n. 4, p. 1344-1357, 2022. DOI: 10.18265/1517-0306a2021id5834.