CIBERCRIME E CIBERSEGURANÇA — DESAFIOS DA IV REVOLUÇÃO INDUSTRIAL

Enzo de Assis Bezerra – enzobezerra10@gmail.com
Bacharelado em Ciências e Tecnologia - Escola de Ciências e Tecnologia – ECT
Universidade Federal do Rio Grande do Norte – UFRN – Natal/RN – Brasil
Gustavo Henrique Lima de Araújo – gustavohenriquelima1@hotmail.com
Bacharelado em Ciências e Tecnologia - Escola de Ciências e Tecnologia – ECT
Universidade Federal do Rio Grande do Norte – UFRN – Natal/RN – Brasil
Daniel Araújo de Almeida – daniel.almeida.099@ufrn.edu.br
Bacharelado em Ciências e Tecnologia - Escola de Ciências e Tecnologia – ECT
Universidade Federal do Rio Grande do Norte – UFRN – Natal/RN – Brasil
Sidiale Marreiros de Lima – sidiale@ufrn.edu.br
Bacharelado em Ciências e Tecnologia - Escola de Ciências e Tecnologia – ECT
Universidade Federal do Rio Grande do Norte – UFRN – Natal/RN – Brasil
Líbia Emanoela Gomes Carvalho – libiaemanoela@ufrn.edu.br
Bacharelado em Ciências e Tecnologia - Escola de Ciências e Tecnologia – ECT
Universidade Federal do Rio Grande do Norte – UFRN – Natal/RN – Brasil
Samuel Victor Maciel da Silva – samuelvictor7@ufrn.edu.br
Bacharelado em Ciências e Tecnologia - Escola de Ciências e Tecnologia – ECT
Universidade Federal do Rio Grande do Norte – UFRN – Natal/RN – Brasil
Zulmara Virgínia de Carvalho – zulmara@ect.ufrn.br
Programa de Pós-Graduação em Ciência, Tecnologia e Inovação – PPgCTI
Universidade Federal do Rio Grande do Norte – UFRN – Natal/RN – Brasil

Resumo— *Desde o advento da III Revolução Industrial, informação é ativo estratégico de crescimento econômico. A Transformação Digital, derivada do paradigma tecnoeconômico das tecnologias de informação e comunicação, redimensionou tendências tecnológicas, bem como comportamentos econômicos e sociais: surge a IV Revolução Industrial. Nesse cenário, os crimes cibernéticos configuram-se uma das principais ameaças do paradigma tecnoeconômico 4.0. Além de comprometer a confiança digital, as práticas geram prejuízos da ordem de trilhões de dólares à economia global. Este contexto alicerça o objetivo deste estudo: identificar a dinâmica de desenvolvimento tecnológico integrado da Cibersegurança com as demais tecnologias habilitadoras 4.0, assim como analisar sua cena mercadológica. A partir de prospecção patentária nos bancos de dados Espacenet, Google Patents e The Lens e, adicionalmente, de análise de tendências de dados derivados do Google Trends, a pesquisa identificou os principais inventores e líderes patentários, diagnosticou suas dinâmicas econômicas e suas inserções no mercado brasileiro. A análise realizada oferece uma cenarização de desafios encontrados na área de segurança cibernética, assim como os principais investidores no cenário tecnomercadológico, a fim de explorar as divergências nos cenários mercadológicos internacional e nacional com intuito de especular oportunidades acerca da segurança da informação.*
Palavras-chave— *Crime cibernético, Indústria 4.0, Segurança.*

Abstract— *Since the advent of the III Industrial Revolution, information has been a strategic asset for economic growth. Digital Transformation, derived from the techno-economic paradigm of information and communication technologies, has reshaped technological trends, as well as economic and social behaviors: the IV Industrial Revolution appears. In this scenario, cybercrime is one of the main threats of the 4.0 techno-economic paradigm. In addition to undermining digital trust, the practices generate losses in the order of trillions of dollars for the global economy. This context underlies the objective of this study: to identify the dynamics of integrated technological development of Cybersecurity with the other enabling technologies 4.0, as well as to analyze its market scene. From patent prospecting in the Espacenet, Google*

Patents and The Lens databases and, in addition, from analyzing trends in data derived from Google Trends, the survey identified the main inventors and patent leaders, diagnosed their economic dynamics and their insertions in the market Brazilian. The analysis carried out offers a scenario of challenges finds in the cybersecurity area, as well as the main investors in the techno-market scenario, in order to explore the divergences in the international and national market scenarios in order to speculate opportunities about information security.
Keywords— *Cyber crime, Industry 4.0, Security.*

1 INTRODUÇÃO

Conforme afirmado em um artigo do *site* Shield Consulting (2018), "À medida que o mundo se torna mais interconectado digitalmente, manter a segurança cibernética se tornará mais difícil". As ferramentas digitais estão cada vez mais sendo conectadas à infraestrutura física, e a proteção adequada dos sistemas críticos resultantes é essencial. As organizações terão que fazer uso do aprendizado de máquina e da inteligência artificial para medir e relatar melhor o risco cibernético, enquanto enfrentam problemas associados à proliferação de dispositivos que alimentam as cidades inteligentes e a Internet das Coisas (WEF, 2021).

É dentro desse cenário que este trabalho se encarrega de analisar e prospectar os dados sobre a relevância de cibersegurança no mercado, quais partes do mundo já estão realizando pesquisas sobre esse assunto e como isso está relacionado à quarta revolução industrial.

O crime cibernético é um dos maiores riscos para a prosperidade na Quarta Revolução Industrial. As atividades cibernéticas do estado-nação tendem a atrair mais atenção internacional, mas, na verdade, os cibercriminosos são responsáveis pela maioria das atividades cibernéticas maliciosas – cerca de 80%, segundo algumas estimativas (PASSERI, 2019). Além dos danos diretos, que devem custar à economia global US $6 trilhões ao ano até 2021, o crime cibernético é uma barreira colossal para a confiança digital. Isso prejudica drasticamente os benefícios do ciberespaço e prejudica os esforços internacionais de estabilidade cibernética. (STOCK, 2020).

De acordo com um estudo recente da Xerfi (2020), esta modalidade de crime teria custado às empresas em todo o mundo cerca de 350 bilhões de euros em 2017 e 885 bilhões de euros em 2020. A empresa Accenture estima, ainda, para a projeção do período 2019-2024, o custo do cibercrime para as empresas à escala global em 4,600 mil milhões de euros (LOLLIA, 2021).

2 FUNDAMENTAÇÃO TEÓRICA

2.1 IV Revolução Industrial

Atualmente, a indústria encontra-se em um estado marcado por novas tecnologias. Chamado de Quarta Revolução Industrial, é considerada a maior revolução desde a ocorrência da Revolução Industrial no século XVIII (BEZERRA, 2019).

"Indústria 4.0 é um termo que se refere às novas tecnologias trazidas por esse movimento, como é o caso das inovações de *internet*, computação, robótica, automatização industrial, mundo virtual, entre outras" (BEZERRA, 2019). Ela é caracterizada pelo desenvolvimento de tecnologias em áreas como genética, física, tecnologias e avanços digitais, o que implica uma necessidade de avançar em segurança (BEZERRA, 2019).

2.2 Cibersegurança

Visto isso, deve-se entender precisamente o assunto tratado. Dito isso, "cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra-ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas" (CONSULTUS, 2021). "O termo é aplicável a uma variedade de contextos, desde negócios até computação móvel" (KASPERSKY, 2021).

A cada ano, a urgência por uma boa proteção virtual cresce. "Um relatório da Risk Based Security (2019) revelou um número impressionante de 7,9 bilhões de registros que foram expostos por violações de dados somente nos primeiros nove meses de 2019" (KASPERSKY, 2021).

Logo, não é surpreendente afirmar que, "com a escala da ameaça virtual crescente, a International Data Corporation prevê que os gastos mundiais com soluções de cibersegurança chegarão a 133,7 bilhões de dólares até 2022" (KASPERSKY, 2021).

2.3 Armazenamento de nuvem

A computação em nuvem pode ser definida como "um conjunto de recursos como capacidade de processamento, armazenamento, conectividade, plataformas, aplicações e serviços disponibilizados na *internet*" (TAURION, 2011).

Quase todas as empresas de tecnologia moderna estão pagando para terceirizar seus serviços de armazenamento e computação, no todo ou em parte, para a nuvem. Essa configuração permite que as *startups* surjam com muita pouca sobrecarga e que grandes empresas funcionem com mais eficiência, evitando o investimento em *hardware* físico. Isso gerou uma geração de empresas que planejam usar a nuvem para oferecer tudo como um serviço. (WOOD, 2020).

3 METODOLOGIA

Este trabalho de propósito exploratório e descritivo e com abordagem quantitativa, busca analisar o cenário tecnomercadológico referente a palavra-chave cybersecurity (cibersegurança) e as principais empresas que utilizaram e utilizam essa tecnologia no decorrer do tempo, tendo como base a pesquisa de dados através de base de dados patentários, sites e artigos científicos.

Para realizar as prospecções patentárias, retirando dados e gráficos, foram utilizadas as plataformas de pesquisa: Espacenet, Google Patents e The Lens e as informações para as prospecções mercadológicas, foram retiradas das plataformas: INPI e World Economic Forum.

Levando em conta a influência do mundo digital no cotidiano das empresas, seja para guardar informações, realizar processos ou fornecer serviços, esse trabalho tem como objetivo realizar um mapeamento tecnológico informacional sobre o investimento na proteção dessa infraestrutura virtual, mostrando o quão relevante é essa segurança no mercado. A pesquisa foi realizada utilizando as ferramentas Espacenet, Google Patents e The Lens para verificar a quantidade de patentes de Cibersegurança registradas. Isso mostrou resultados bastante variados entre as três bases de dados patentários que no total somam 29.308 patentes. A pesquisa também foi feita relacionando o tema com diversas tecnologias da 4° revolução industrial. Isso foi feito para verificar o interesse das empresas em cibersegurança, além de mostrar quais as novas tecnologias mais relacionadas com ela.

Além disso, foi feita uma busca adicional nessas 3 plataformas para determinar quais nações mais protegem invenções no campo da cibersegurança. Essas informações foram disponibilizadas em formato de um mapa de calor, demonstrando os países claramente. Adicionalmente, os principais inventores também foram prospectados, revelando os intelectuais mais envolvidos no assunto de cibersegurança.

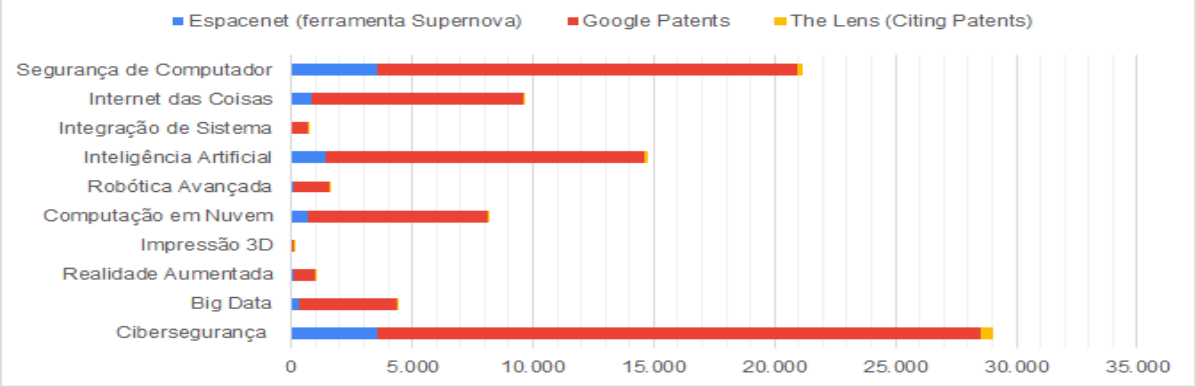
A partir desses dados, parte-se para uma análise do interesse ao longo do tempo relacionado a cada uma dessas tecnologias, utilizando ferramentas do Google Trends e sempre relacionando elas à cibersegurança. Os dados representam o interesse do mundo todo, de 2004 até a primeira semana de março de 2021.

4 RESULTADOS E DISCUSSÃO

4.1 O Cenário Tecnológico 4.0

A Figura 1 mostra o registro das patentes de cibersegurança relacionadas com as tecnologias da 4° revolução industrial. Nele é possível visualizar que Segurança de Computador, Internet das Coisas, Inteligência artificial e Computação em nuvem são os que mais se repetem, com respectivamente 21.159, 9.673, 14.780 e 8.196 patentes relacionadas.

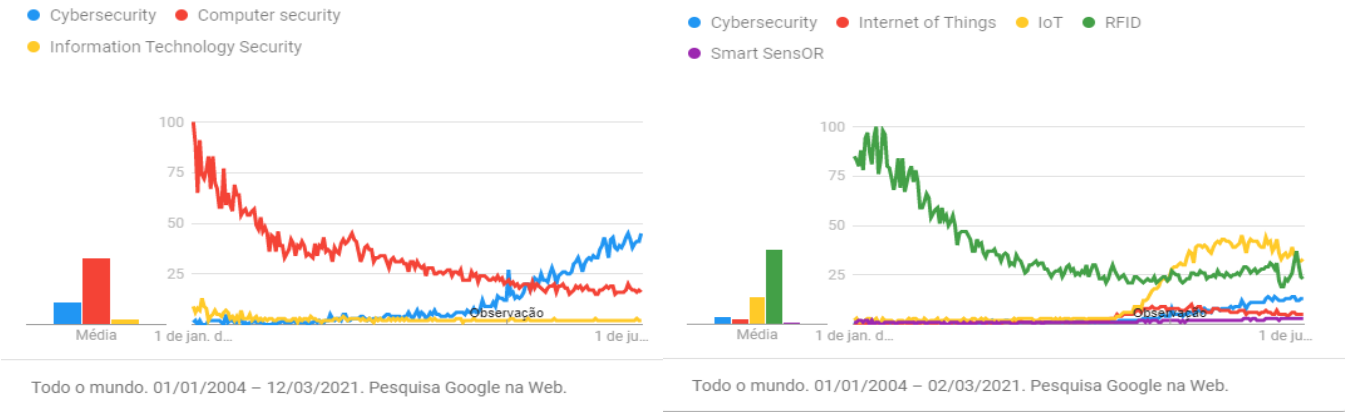
Figura 1: Registro de Patentes de Cibersegurança



Fonte: Elaboração a partir de dados do Espacenet, Google Patents e The Lens (2021)

Na figura 2 (à esquerda), verifica-se a evolução da prioridade de segurança, onde eventualmente a Segurança do Computador foi substituída por Cybersecurity, mostrando a relevância que a segurança na rede ganhou sobre a proteção do computador em si, mas isso não anula o fato de que as patentes relacionadas a ambos ainda são bem relevantes uma vez que são objetos de estudo complementares.

Figura 2: (À esquerda) Interesse ao longo do tempo de Cibersegurança(Azul), Segurança de computadores (vermelho) e Segurança em Tecnologia da Informação. (À direita) Interesse ao longo do tempo de Cibersegurança (azul), Internet das Coisas (vermelho), IoT (amarelo), Identificador de Radiofrequência (verde), Sensor Inteligente (roxo)

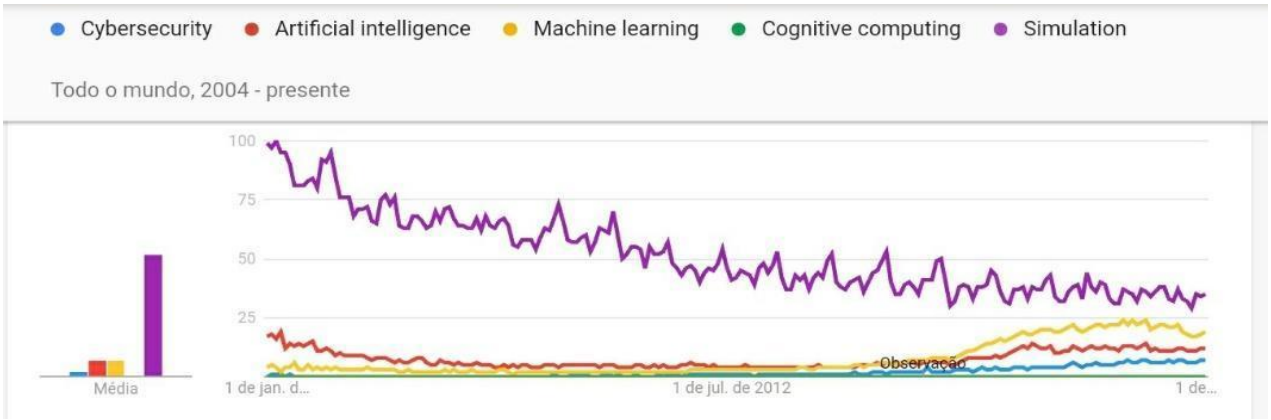


Fonte: Captura de tela do Google Trends

Já na Figura 2 (à direita), nota-se que inicialmente o Identificador de Radiofrequência, tecnologia utilizada para identificação de objetos a curta distância, bastante relevante na época, mas acabou perdendo interesse ao longo dos anos, sendo atualmente muito usado em celulares, no rastreamento de animais e em identificação biométrica. No entanto, as tecnologias que acabaram crescendo foram as de Internet das Coisas (IoT) e a cibersegurança na última década, potencialmente se tornando uma nova tendência no mercado.

Ao se observar a figura 3, é possível identificar que apesar do interesse em simulação ter caído consideravelmente no decorrer dos anos, o assunto consegue se manter bem constante, mas ainda é possível notar que houve uma diminuição na sua queda quando o interesse nos outros assuntos começou a subir, mostrando uma possível relação bem forte entre eles. Além disso, é interessante notar que a cibersegurança começou a crescer pouco tempo depois que a computação cognitiva e a inteligência artificial.

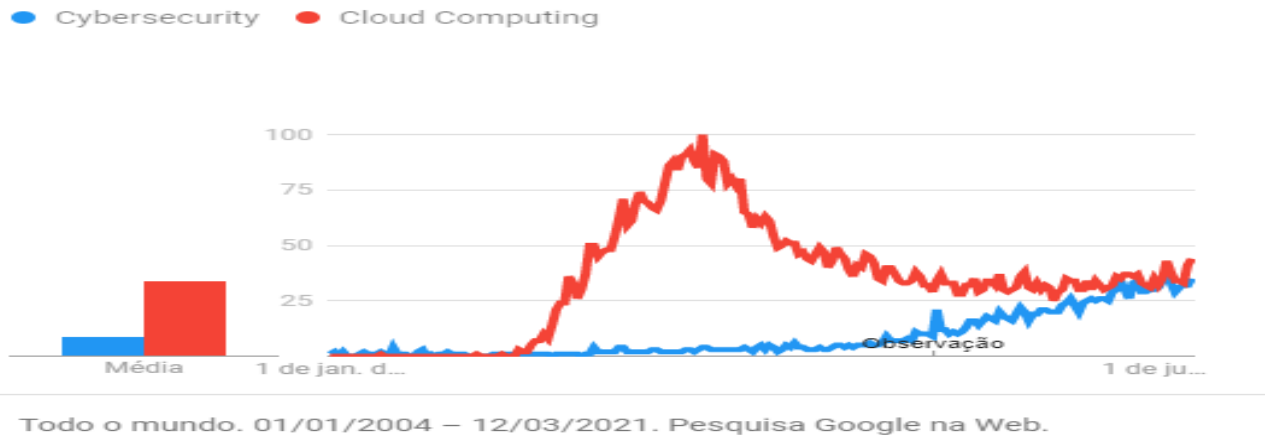
Figura 3: Interesse ao longo do tempo de Cibersegurança (azul), Inteligência artificial (vermelho), Aprendizado de máquina (amarelo), Computação Cognitiva (verde), Simulação (roxo)



Fonte: Captura de tela do Google Trends

Como é perceptível na Figura 4, enquanto o índice de cibersegurança permanece baixo entre o início de 2004 e o final de 2014, o interesse por computação em nuvem tem um grande aumento no início de 2008 atingindo seu maior índice em junho de 2011 e se igualando a Cybersecurity em 2021. Tal crescimento da foi devido às grandes empresas começarem a implementá-la em suas tecnologias, como a Apple com o iCloud, a Google com o Google Music, Hulu, Netflix e o OnLive, inaugurado no início de 2011.

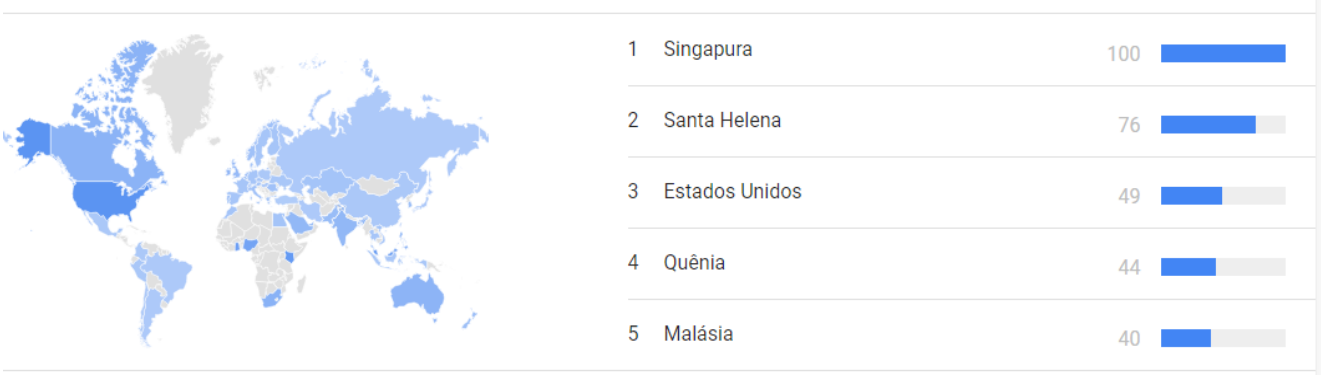
Figura 4: Interesse ao longo do tempo de Cibersegurança (Azul) e Computação em Nuvem (vermelho)



Fonte: Captura de tela do Google Trends

Além de pesquisar sobre a relevância dessas tecnologias no passar dos anos, também foi realizado um levantamento de quais regiões do mundo pesquisam mais sobre cibersegurança, também utilizando a ferramenta do Google Trends. Na figura 5 podemos observar que temos dois países Africanos (Quênia e Santa Helena), dois Asiáticos (Singapura e Malásia) e os Estados Unidos, isso ajuda a mostrar que vários lugares do mundo se preocupam com a segurança na rede, mesmo que nem todos deem tanta importância ao assunto.

Figura 5: Interesse de cybersecurity por região



Fonte: Captura de tela do Google Trends

Observa-se nas tabelas 1, 2 e 3 e na figura 6 que a maior quantidade de patentes relacionadas à cibersegurança estão concentradas nos Estados Unidos, com a China sendo a segunda região mais aparente, embora com uma intensidade significativamente menor aos EUA.

Tabelas 1,2 e 3 (Respectivamente, da esquerda para a direita): Principais nações com patentes de acordo com o Espacenet (Esquerda), com o Google Patents (Centro), com o The Lens (Direita)

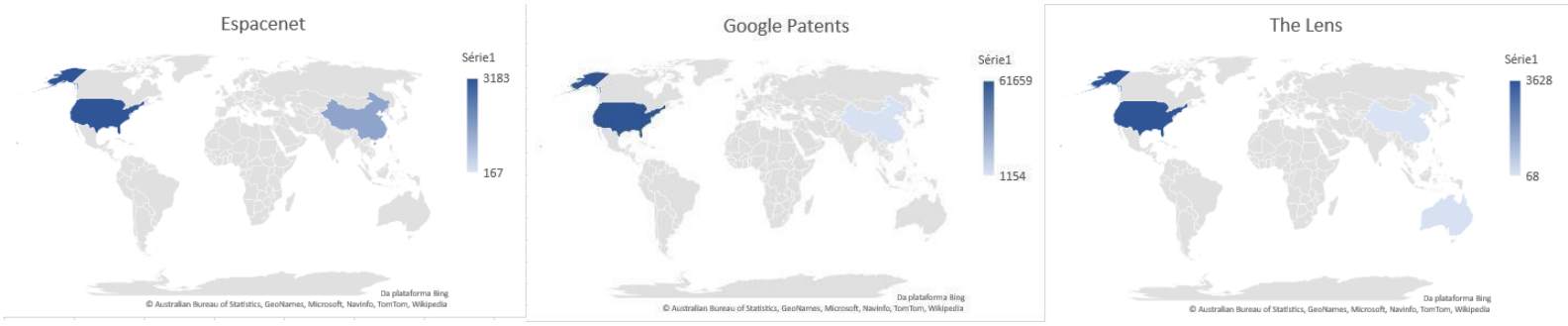
País	Qtd de patentes
Estados Unidos	3183
China	1510
WO	740
EP	259
Coréia do Sul	167

País	Qtd de patentes
Estados Unidos	61659
Japão	3926
EP	2329
China	1627
Coréia do Sul	1154

País	Qtd de patentes
US	3628
WO	705
Europeia	175
Austrália	111
China	68

Fonte: Adaptado de Espacenet (2021), de Google Patents (2021), de The Lens (2021)

Figura 6: Principais nações com patentes relacionadas ao tema.
Espacenet (à esquerda), Google Patents (centro) e The Lens (à direita)



Fonte: Adaptado de Espacenet (2021), Google Patents (2021), The Lens (2021)

Analisando outro aspecto, pode-se trazer à tona os principais inventores quando o assunto é cibersegurança.

Tabela 4 - Principais inventores relacionados a Cibersegurança

Espacenet	Google Patents	The Lens
Crabtree Jason	王艳辉	Tryfonas Christos
Nam Su Man	Jr	Muddu Sudhakar
Park Young Sun	沈军	Sellers Andrew
Ares Jean-Michel Raymon	杨春晖	Crabtree Jason
Jang Jiyong	III	Beecham James Douglas

Fonte: Adaptado do Espacenet, Google Patents e The Lens

Como se pode ver, estes são os 5 inventores, retirados de sua respectiva plataforma, com a maior quantidade de documentos atribuídos a seu nome.

4.2 O Cenário Mercadológico 4.0

Para o cenário mercadológico foram usadas como referências as 5 empresas que mais investem nas tecnologias 4.0. Essas foram escolhidas em consequência dos dados prospectados nas plataformas Espacenet, Google Patents e The Lens conforme os números de patentes.

Tabela 5 - Principais líderes patentários e sua inserção no Brasil

Os 5 principais players	**Valor de Mercado (US$)**	**Movimentação Financeira (US$)**	**Patentes no Brasil**
International Business Machines Corporation	107.2B	73.6B	1368
Microsoft Technology Licensing Llc	1.752,96B	143B	1356
LG Electronics Inc	24.556,54B	54,4B	1264
Splunk Inc	31.6B	791,1M	0
Intel Corporation	246,62B (2021)	US$ 16,5 B (2019)	1182

Fonte: Prospecção patentária no Brasil e dos relatórios anuais das empresas (2021)

Como se pode ver na tabela 5, os Top 5 players são compostos por empresas de grande nome, já consolidadas em suas respectivas partes do mercado. Todas em tecnologias diferentes, se especializando em coisas como segurança virtual, desenvolvimento de tecnologias de informática ou de eletrodoméstico.

A International Business Machines Corporation (IBM) é uma empresa focada em informática, que vende tanto software quanto hardware. Uma contribuição notável sua foi o desenvolvimento do IBM Watson, uma IA mostrada em 2016 que passou a ser indispensável a muitas outras organizações. Sua ajuda em hospitais para tornar o tratamento de câncer mais eficaz é um grande exemplo.

A Microsoft é uma das mais reconhecidas empresas de todo o mundo, seja pelos seus computadores ou o sistema operacional Windows, o mais usado no mundo. No entanto, não significa que tenha parado por aí. Em 2020, liberou o HoloLens 2, um aparelho semelhante a um óculos, de realidade misturada, altamente imersivo.

A LG Electronics é uma empresa com um grande foco em desenvolver novas tecnologias, mas há um claro foco para produtos de casa. Isso é refletido em suas criações reconhecidas anualmente como inovadoras pela premiação da Consumer Electronics Show (CES). Por exemplo, em 2018 foi apresentado o ThinQ, programa AI incorporado em TVs da marca para auxiliar o usuário.

A Splunk Inc é uma empresa voltada para a área de cibersegurança, onde os seus projetos são voltados para garantir a seguridade aos seus clientes com o uso da internet.

Já a Intel é altamente aclamada por seus processadores de computador, sempre aumentando o seu poder anualmente. Claro, não se mantém presa a isso. Em 2020, apresentou a tecnologia de condução autônoma RoboCar, o que irá oferecer uma segurança maior aos motoristas.

A partir destas 5 empresas, foi feita uma análise de registros patentários no INPI. No entanto, ao fazer a busca, foi descoberto que, das 5, apenas a LG apresentou transações registradas (5) entre os anos de 2016 e 2020. Através da pesquisa do INPI, quatro empresas vieram da sede da Coreia do Sul até o Brasil, em São Paulo, transportando equipamentos para informática. A última, no entanto, originou-se da VOLVO CONSTRUCTION EQUIPMENT AKTIEBOLAG(Suécia), levando materiais para fabricação de tratores, peças e acessórios, exceto agrícolas.

Com base no cenário mercadológico nacional, os dados prospectados mostram que não há muito investimento de empresas internacionais, e não há empresas nacionais consolidadas no mercado tecnológico. No segmento da cibersegurança e das tecnologias que compõem a indústria 4.0. O cenário atual é uma oportunidade para mais empresas que buscam investir no território nacional no ramo da tecnologia e suas vertentes.

Segundo o Instituto Igarapé, o Brasil está constantemente no topo do ranking global de crimes cibernéticos. Em 2014, por exemplo, ele foi classificado pela Kaspersky Lab, uma empresa de segurança cibernética, como a nação número um do mundo em ataques de malware bancário, com quase 300.000 usuários comprometidos. (Murcham, R; Thompson, N, 2018).

Em 2019, o Brasil foi o segundo país mais ameaçado no mundo por ataques de ransomware, de acordo com o estudo da empresa de segurança Trend Micro. No mesmo ano, foi responsável por 10,64% de todos os ataques de ransomware em escala global. Estando de fora frequentemente do Índice Global de Segurança Cibernética (GCI) conforme a figura 7, criado pela International Telecommunications Union (ITU), o Brasil se mostra vulnerável, visto que o índice classifica quais países estão bem preparados para evitar ataques cibernéticos, baseado nos cinco pilares da Agenda Global de Segurança Cibernética (GCA): Jurídico, técnico, organizacional, capacitação e cooperação.

Figura 7: Índice de desempenho contra ataques cibernéticos no ano 2017

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

Fonte: International Telecommunication Union (2017)

Assim, o Brasil, em 2017, se revela um país em que a cibersegurança não é levada como algo de extrema importância, relembrando mais uma vez que o Brasil ainda não tem uma forte infraestrutura, nem um alto investimento na área de tecnologia da informação (TI), tornando assim, um país muito vulnerável a ataques cibernéticos.

5 CONSIDERAÇÕES FINAIS

Após o início da IV Revolução Industrial, e a subsequente atualização para a Indústria 4.0, a cibersegurança tornou-se uma obrigação. A cada ano, sua presença é mais exigida, devido a um crescente número de crimes cibernéticos. Diante disso, o mundo como um todo passou a buscar uma segurança cibernética mais e mais confiável, países e empresas trabalhando em prol disso.

Isso levará a uma distinção muito evidente entre aqueles que investirem e os que não, especialmente considerando os gigantescos custos à qualquer empresa vítima de crimes virtuais. Prejuízos custando bilhões

em Euros seriam comuns aos despreparados, sejam empresas ou países. Para se manter em dia, faz se necessário um grande investimento em inteligência artificial e aprendizado de máquina, de modo a usufruir proveitosamente das proteções contra cibercrimes.

Dito isto, a pesquisa feita mostrou um claro avanço gradual do setor, não mostrando nenhum sinal de diminuição. O interesse pela segurança na rede digital cresceu drasticamente de poucos anos até agora, como provado por plataformas de busca como o google trends. No mundo mercadológico, grandes nomes se mostraram como ou provedores de cibersegurança, ou usuários obrigatórios, devido ao seu método de trabalho já ser altamente dependente de serviços digitais. Países que não inovam na área da cibersegurança, ficam mais vulneráveis a ciberataques. Como já citado, o Brasil está constantemente no topo do ranking global de crimes cibernéticos, devido à falta de investimentos na área da cibersegurança.

Portanto, analisando o presente trabalho, confirmamos a relevância da cibersegurança no mercado, assim como quais partes do mundo já estão realizando pesquisas sobre o assunto. Ela apenas cresce com o passar dos anos, elevando todos os investidores mostrados acima do risco ameaçado pelos crimes virtuais, os quais evoluem em seriedade. Logo, não há motivos para relaxar, já que as próprias tecnologias responsáveis pela criação dessa situação não param de avançar. Um ciclo contínuo, para que a indústria permaneça crescendo perpetuamente, situação que se repete em casos como os da inteligência artificial, a qual proporcionará futuramente a tomada de decisões automatizada com base no compliance organizacional.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

REFERÊNCIAS

AIMEUR, Esma. GAMBS, Sébastien. AI HO. UPP: User Privacy Policy for Social Networking Sites. 2009 Fourth International Conference on Internet and Web Applications and Services, Venice/Mestre, Italy, 2009, pp. 267-272, doi: 10.1109/ICIW.2009.45. Disponível em: https://ieeexplore.ieee.org/abstract/document/5072530. Acesso em: 11 mar. 2021.

BEZERRA, Juliana. Quarta Revolução Industrial. 03/12/2019. Disponível em: https://www.significados.com.br/quarta-revolucao-industrial/. Acesso em: 11 mar. 2021.

CEZAR, Taurion. Cloud computing: computação em nuvem: transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009.

CONSULTUS. O QUE É CIBERSEGURANÇA? Disponível em: https://consultus.pt/o-que-e-ciberseguranca/. Acesso em: 13 mar. 2021

CHACHAK, Elias. Top 10 Countries Best Prepared Against Cyber Attacks. Disponível em: https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/. Acesso em: 11 mar. 2021.

CIRIACO, Douglas. Como funciona a RFID?. Disponível em: https://www.tecmundo.com.br/tendencias/2601-como-funciona-a-rfid-.htm. Acesso em: 10 mar. 2021.

FERRARA, Anna Lisa et al. Policy Privacy in Cryptographic Access Control. 2015 IEEE 28th Computer Security Foundations Symposium, Verona, Italy, 2015, pp. 46-60, doi: 10.1109/CSF.2015.11. Disponível em: https://ieeexplore.ieee.org/abstract/document/7243724. Acesso em: 10 mar. 2021.

FLAVIÁN, Carlos. GUINALÍU, Miguel. Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. Emerald insight, vol. 106 n. 5, p. 601-620, 1 jun. 2006. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/02635570610666403/full/html. Acesso em: 11 mar. 2021.

INTEL. CES 2020: Intel traz inovação por meio de tecnologias inteligentes abrangendo a nuvem, a rede, a borda e o PC. 06/01/2020. Disponível em: https://newsroom.intel.com.br/news-releases/ces-2020-intel-traz-inovacao-por-meio-de-tecnologias-inteligentes-abrangendo-a-nuvem-a-rede-a-borda-e-o-pc/#gs.w0iu05. Acesso em: 08 mar. 2021.

KASPERSKY. O que é cibersegurança? Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security. Acesso em: 09 mar. 2021.

MEDINE, David. Data Protection: Consent is Dead (Long Live Privacy). 25/02/2021. Disponível em: https://www.cgdev.org/blog/data-protection-consent-dead-long-live-privacy. Acesso em: 09 mar. 2021

MUGGAH, Robert. THOMPSON, Nathan B. Brazil struggles with effective cyber-crime response. Disponível em: https://igarape.org.br/brazil-struggles-with-effective-cyber-crime-response/. 12 mar. 2021.

NYKODYM, Nick. TAYLOR, Robert. VILELA, Julia. Criminal profiling and insider cyber crime. Computer Law & Security Review. 5. ed. 2005. v. 21, p. 408-414. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364905001433. Acesso em: 11 mar. 2021.

PASSERI, Paolo. June 2019 Cyber Attacks Statistics. HACKMAGEDDON, 12 ago. 2019. Disponível em: https://www.hackmageddon.com/2019/08/12/june-2019-cyber-attacks-statistics/. Acesso em: 14 mar. 2021.

PRADA, Rodrigo. Por que 2011 será o ano da computação nas nuvens?. 15/06/2011. Disponível em: https://www.tecmundo.com.br/google/10791-por-que-2011-sera-o-ano-da-computacao-nas-nuvens-.htm. Acesso em: 10 mar. 2021.

STOCK, Jürgen. DANIEL, Michael. GOLDSTEIN, Tal. Partnerships are our best weapon in the fight against cybercrime. Here‘s why. World Economic Forum, 21 jan. 2020. Disponível em: https://www.weforum.org/agenda/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/. Acesso em: 11 mar. 2021.

SHIELD CONSULTING. Como convencer seu chefe a investir em segurança da informação. 29/10/2018. Disponível em: https://shield-consulting.com/2018/10/29/business-plan-template-for-startup-business-2/. Acesso em: 26 mar, 2021.

LOLLIA, Fabrice. THE CONVERSATION. Cyberattaques et kidnapping des données: comment protéger les organisations des rançongiciels ?. The Conversation, 22 fev. 2021. Disponível em: https://theconversation.com/cyberattaques-et-kidnapping-des-donnees-comment-proteger-les-organisations-des-rancongiciels-155384. Acesso em: 11 mar. 2021.

WENDT, Emerson. JORGE, Higor. Crimes cibernéticos: ameaças e procedimentos de investigação. 2 ed. Rio de Janeiro: Brasport, 2013.

WOOD, Molly. We Need to Talk About ‘Cloud Neutrality’. WIRED. Disponível em: https://www.wired.com/story/we-need-to-talk-about-cloud-neutrality/. Acesso em: 09 mar. 2021.