Research, Society and Development, v. 10, n. 3, 4210312937e, 2021
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v10i3.12937

Um estudo bibliométrico das publicações sobre Segurança Cibernética na Indústria 4.0

A bibliometric study of Cybersecurity in Industry 4.0 publications

Un estudio bibliométrico de la Ciberseguridad en las publicaciones de la Industria 4.0

Recebido: 13/02/2021 | Revisado: 21/02/2021 | Aceito: 25/02/2021 | Publicado: 04/03/2021

Antonio João Gonçalves de Azambuja
ORCID: https://orcid.org/0000-0002-4378-5181
Instituto Tecnológico de Aeronáutica, Brasil
E-mail: ajaazambuja@gmail.com
Vilson Rosa Almeida
ORCID: https://orcid.org/0000-0001-9077-2941
Instituto Tecnológico de Aeronáutica, Brasil
E-mail: vilsonra@ita.br

Resumo
A 4ª Revolução Industrial (4RI), caracterizada pela combinação de diferentes tecnologias, em diversos graus de maturidade, gera um conjunto de oportunidades de inovação na indústria. Essa revolução, conhecida como Indústria 4.0, teve a origem na Alemanha, dentro de uma estratégia de Estado para tornar o país líder em tecnologia, visando fortalecer a sua competitividade global. O atual ambiente tecnológico da Indústria 4.0 faz uso dos sistemas ciberfísicos interconectados por meio de um conjunto de tecnologias habilitadoras. Com a conectividade desses sistemas, surgem os desafios da Segurança Cibernética, tornando essas questões como uma das principais preocupações dos líderes empresariais. Diante de um cenário para a proteção de dados e informações, esta pesquisa realizou um estudo bibliométrico sobre a produção científica relacionada com a Segurança Cibernética na Indústria 4.0, utilizando uma abordagem quantitativa-qualitativa para mensurar as publicações e as suas características. A análise e discussão dos resultados permitiu identificar as áreas de pesquisa das publicações, os periódicos com maior número de publicações, os autores com trabalhos mais citados, os países e instituições com pesquisas mais relevantes sobre o tema, e a representatividade das palavras-chave utilizadas nas publicações identificadas nas bases de dados *Web of Science* e *Scopus*.
Palavras-chave: Indústria 4.0; Segurança cibernética; Resiliência separadas.

Abstract
The 4th Industrial Revolution (4IR), characterized by the combination of different technologies, in several degrees of maturity, generates a set of innovation opportunities in the industry. This revolution, known as Industry 4.0, originated in Germany, within a national strategy to make the country a leader in technology, aiming to strengthen its global competitiveness. The current technological environment of Industry 4.0 makes use of interconnected cyber-physical systems through a set of enabling technologies. With the connectivity of these systems, Cyber Security challenges arise, making these issues a top concern for business leaders. Faced with a scenario for the protection of data and information, this research carried out a bibliometric study on the scientific production related to Cyber Security in Industry 4.0, using a quantitative-qualitative approach to measure publications and their characteristics. The analysis and discussion of the results made it possible to identify the research areas of the publications, the periodicals with the largest number of publications, the authors with the most cited works, the countries and institutions with the most relevant research on the topic, and the representativeness of the keywords used in publications identified in the Web of Science and Scopus databases.
Keywords: Industry 4.0; Cyber security; Resilience.

Resumen
La 4ª Revolución Industrial (4RI), caracterizada por la combinación de diferentes tecnologías, en distintos grados de madurez, genera un conjunto de oportunidades para la innovación en la industria. Esta revolución, conocida como Industria 4.0, tuvo su origen en Alemania, dentro de una estrategia estatal para convertir al país líder en tecnología, con el objetivo de reforzar su competitividad global. El entorno tecnológico actual de la Industria 4.0 hace uso de sistemas ciberfísicos interconectados por medio de un conjunto de tecnologías habilitadoras. Con la conectividad de estos sistemas, surgen los desafíos de la ciberseguridad, lo que hace que estas cuestiones sean una de las principales preocupaciones de los líderes empresariales. Ante un escenario de protección de datos e información, esta investigación realizó un estudio bibliométrico sobre la producción científica relacionada con la Ciberseguridad en la

Industria 4.0, utilizando un enfoque cuantitativo-cualitativo para medir las publicaciones y sus características. El análisis y la discusión de los resultados permitieron identificar las áreas de investigación de las publicaciones, las revistas con mayor número de publicaciones, los autores con los trabajos más citados, los países e instituciones con las investigaciones más relevantes sobre el tema y la representatividad de las palabras clave utilizadas en las publicaciones identificadas en las bases de datos Web of Science y Scopus.
Palabras clave: Industria 4.0; Ciberseguridad; Resiliencia.

1. Introdução

A evolução tecnológica evidenciada pela 4ª Revolução Industrial (4RI), conhecida como Indústria 4.0, caracteriza-se pela convergência e possibilidades de combinação de diferentes tecnologias, que combinadas geram um conjunto de oportunidades de inovação na indústria (Bibby & Dehe, 2018).

Historicamente a 1ª Revolução Industrial teve início na Inglaterra, no final do século XVIII, com a introdução da energia hídrica e da máquina a vapor. Já na 2ª Revolução Industrial, ao longo da segunda metade do século XIX, foram desenvolvidas aplicações de produção em massa com o uso da energia elétrica. A 3ª Revolução Industrial na segunda metade do século XX, foi baseada no uso de componentes eletrônicos e tecnologias que possibilitaram a automação da manufatura. A 4ª Revolução Industrial, começou na virada do deste século, caracterizada pela digitalização da produção, fábricas inteligentes, customização em massa, servitização, uso de dados, sensores e equipamentos conectados em rede, associados a sistemas ciberfísicos (Anderl, 2014; Schwab, 2016).

O conceito de Indústria 4.0 teve origem na Alemanha, dentro de uma estratégia do Estado para tornar o país líder em tecnologia e fortalecer a sua competitividade global. O governo alemão apoiou o projeto "*High-Tech Strategy 2020*[1]*"* com incentivos às empresas na busca de liderança em inovação tecnológica como parte integrante do conceito da Indústria 4.0 (Kagermann; Wahlster & Helbig, 2013).

O atual ambiente tecnológico da Indústria 4.0 compreende a organização e gestão de toda a cadeia de valor do ciclo de vida dos produtos, oportunizada pela integração de tecnologias digitais no desenvolvimento, produção e logística de produtos e processos. O uso de tecnologias digitais para implementação de soluções inovadoras no contexto da 4ª Revolução Industrial contribui para incrementar a velocidade na capacidade de resiliência das empresas. Projetos relacionados à Industria 4.0 estão sendo implementados como uma resposta ao aumento da competitividade e a necessidade de lidar com a transformação digital (Schuh et al., 2020).

As recentes tecnologias aplicadas à manufatura têm o potencial de trazer mudanças significativas nas cadeias produtivas. O grau de adaptação das empresas e governos nesse cenário é um processo de aprendizagem para a implementação de novos conceitos e tecnologias que emergiram com a Indústria 4.0. A gestão da informação, a interoperabilidade dos sistemas, a internet das coisas, a inteligência artificial, a digitalização, os sistemas ciberfísicos, o *big data*, a computação em nuvem, a logística da indústria conectada com o cliente e a automação com sensores, são questões que devem ser gerenciadas pelas empresas que almejam a participação nessa revolução.

Na era da Indústria 4.0, com a presença dos sistemas ciberfísicos conectados em ambientes industriais, surgem os desafios da Segurança Cibernética (SegCiber). Os ataques cibernéticos podem gerar prejuízos financeiros e impactos na imagem da empresa (Lezzi, Lazoi & Corallo, 2018). As estratégias de SegCiber devem estar integradas às estratégias organizacionais e de tecnologias da informação e comunicação (TIC), para assegurar a segurança dos dados, informações e conhecimento com o objetivo de impulsionar o desempenho de toda a cadeia de valor da manufatura (Walso et al., 2017).

[1] *High-Tech Strategy 2020*: subiu o patamar da pesquisa e da inovação na agenda política do governo alemão, envolvendo o setor político, a indústria, a pesquisa e as pessoas. (Fonte:<https://www.automation.com/en-us/articles/2014-1/industry-40-only-one-tenth-of-germanys-high-tech-s>).

A Segurança Cibernética é uma das principais preocupações dos líderes empresariais, dada a complexidade presente nas novas tecnologias, passando para o topo da agenda (Bughin et al., 2015). Já para os autores Frost e Sullivan (2017), a integração das TIC com a tecnologia operacional traz consigo novos desafios, particularmente a SegCiber. O panorama cibernético é dinâmico, decorrente da velocidade de mudanças das tecnologias, da sua complexidade e sofisticação dos ataques nos ativos de informação (Weber & Studer, 2016).

O vazamento de informações *on-line* aumenta as preocupações dos indivíduos e empresas em relação à disseminação dados sem autorização dos titulares. Diante do contexto no qual os direitos à privacidade e proteção de dados foram elevados ao nível de direitos humanos no cenário internacional, os governos têm devotado especial atenção para lidar com esses desafios. Nesse cenário, destaca-se o Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* - GDPR), publicado em 24 de março de 2018, pela União Europeia (EU), que visa a proporcionar aos usuários um maior controle sobre seus dados pessoais e a aumentar as restrições sobre as organizações que tratam e lidam com esses dados. Por sua vez, o Governo Brasileiro publicou a Lei Geral de Proteção de Dados Pessoais (LGPD), n.º 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais. Com a entrada da LGPD, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), que no dia 03 de fevereiro recomendou para a Polícia Federal (PF) a abertura de uma investigação sobre o "megavazamento de dados" de 223 (duzentos e vinte e três) milhões de brasileiros, ocorrido no mês de janeiro de 2021(Economia, Tecnologia, 2020).

Cook, Render e Woods (2009) afirmam que uma forma para reforçar a segurança nas organizações, que lidam com sistemas complexos, é desenvolver a capacidade do sistema para detectar riscos e lidar com a sua variabilidade e incerteza. A Segurança Cibernética é uma questão central para as empresas inseridas no ecossistema da Indústria 4.0. A proteção dos dados, informações e conhecimento das empresas contra acessos não autorizados e furtos é essencial para a manutenção e incremento da competitividade (Kaplan et al., 2011).

Os fundamentos e ferramentas de Segurança Cibernética são direcionados para aplicação em sistemas complexos, de alto risco. A Indústria 4.0 aumenta a complexidade dos sistemas em relação a fabricação tradicional, dada a interconectividade entre processos, produtos e pessoas. As empresas, devido à inserção de novas tecnologias e maior ênfase dada à dimensão cognitiva do trabalho, estão enfrentando os desafios para a gestão de sistemas complexos, tornando os recursos humanos como um dos pilares da segurança (BCG, 2017; Greitzer et al., 2019).

Os conceitos, princípios, características e formas de avaliação relacionados com a Segurança Cibernética na Indústria 4.0 podem ser evidenciados na literatura. Entretanto, para entender um determinado campo do conhecimento é necessário compreender como ele está sendo gerado, pesquisado, divulgado e socializado na sua produção científica. Este trabalho busca apresentar uma análise bibliométrica das publicações sobre a produção científica relacionada com a SegCiber na Indústria 4.0, para colaborar com as pesquisas acadêmicas que pretendem estudar a temática.

Para isso, utilizou-se o portal de periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior[2] (CAPES), nas seguintes bases de dados: *Web of Science*[3] e *Scopus*[4]. O trabalho inicialmente apresenta os conceitos basilares relacionados com o tema do artigo. A seguir discorre sobre a metodologia utilizada na pesquisa, análise e discussão dos resultados. Por fim, apresenta a conclusão do estudo realizado e uma abordagem para trabalhos futuros.

[2] Portal de Periódicos da CAPES: http://www-periodicos-capes-gov-br.ez45.periodicos.capes.gov.br/;
[3] *Web of Science*: é uma plataforma referencial de citações científicas projetada para apoiar pesquisas científicas e acadêmicas com cobertura nas áreas de ciências, ciências sociais, artes e humanidades; e
[4] *Scopus*: base de resumos e citações de literatura científica e fontes de informação de nível acadêmico.

2. Indústria 4.0

O conceito da Indústria 4.0, cunhado pelo Governo Alemão, é utilizado para descrever a integração das TIC na fabricação industrial, com a digitalização de sistemas e processos industriais, conexão de equipamentos em redes, associados a sistemas ciberfísicos, dados e serviços inteligentes de Internet (Plano de CT&I para Manufatura Avançada no Brasil, 2017, ProFuturo, Ministério da Ciência, Tecnologia e Inovações; Schuh et al., 2020).

Em outras palavras, segundo a *European Union Agency for Network and Information Security* (ENISA, 2018), Indústria 4.0 significa fazer uso dos sistemas ciberfísicos interconectados por meio de um conjunto de tecnologias habilitadoras, visando automatizar desde o projeto e fabricação até a cadeia de fornecimento e manutenção de produtos e serviços.

Os autores, Dilberoglu et al. (2017), Mosterman e Zander (2015), conceituam a Indústria 4.0 como um conjunto integrado de sistemas de produção inteligentes e TIC, com um grupo de *hardwares* e *softwares* integrados. Para Khan e Turowski (2016), é um conjunto de tecnologias, denominadas tecnologias habilitadoras que têm impacto no planejamento e direcionamento dos negócios. Já para Shaabany e Anderl (2018), a Indústria 4.0 é caracterizada pela digitalização da produção com alto uso de TIC.

Com base na revisão da literatura foram identificadas 9 (nove) tecnologias habilitadoras, a saber: Robôs Autônomos, Manufatura Aditiva, Internet das Coisas, Segurança Cibernética, Simulação, *Big Data*, Computação em Nuvem, Sistemas Integrados (Horizontal e Vertical) e Realidade Aumentada (Gerbert et al., 2015). Na visão dos autores, Guoping, Yun e Aizhi (2017), a Inteligência Artificial insere-se como mais uma tecnologia habilitadora. A Inteligência Artificial é definida por Chun, Kim e Lee (2019), como uma tecnologia que gerencia o conhecimento.

As novas tecnologias utilizadas na Indústria 4.0, pavimentaram o caminho para o desenvolvimento dos sistemas ciberfísicos (Jamai et al., 2020). Esses sistemas compreendem tecnologias de redes computacionais e processos físicos que permitem a conectividade do ambiente físico e tecnológico, possibilitando o processamento e acesso aos dados por meio de tecnologias como a Internet (Liu; Xung, 2017). A conectividade dos sistemas em ambientes industriais, apresentam desafios de SegCiber (Tuptuk; Halies, 2018). O gerenciamento dos sistemas ciberfísicos demandam maior controle e segurança dos dados no ambiente cibernético (Wang; Wang, 2016).

3. Segurança Cibernética

Entre as tecnologias habilitadoras da Indústria 4.0, a Segurança Cibernética é um dos desafios enfrentados pelas empresas inseridas nesse ecossistema. Os avanços das tecnologias colocam as empresas em um patamar, no qual, os equipamentos estão conectados por meio de redes computacionais internas e externas a empresa. Tais redes requerem SegCiber para gerenciar os ataques cibernéticos, que estão cada dia mais presentes no espaço cibernético (Wu et al., 2018).

A Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (Brasil, 2015), define a Segurança Cibernética como a arte de assegurar a existência da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas. Segundo Mandarino Júnior (2010), as infraestruturas críticas são instalações, serviços, bens e sistemas que, se forem paralisados, invadidos ou destruídos, provocarão impacto social, econômico, político à segurança do Estado e da sociedade.

Para Carvalho (2010), o espaço cibernético constitui novo e promissor cenário para a prática de toda a sorte de atos ilícitos, desafia conceitos tradicionais, entre eles o de fronteiras geopolíticas e/ou organizacionais. O relatório publicado pelo

Center for Strategic and International Studies[5] (CSIS) dos Estados Unidos da América (EUA) para a 44ª Presidência, estabelece que a Segurança Cibernética é um problema nacional para o Governo e que uma compreensão estratégica do que é essa tecnologia tornará o País e as empresas mais seguras (Barros; Gomes & Freitas, 2011).

Segundo a *European Cyber Security Organization*[6] (ESCO) e a *European Union Agency for Network and Information Security*[7] (ENISA), os documentos, as diretrizes e as melhores práticas relacionadas com as questões de Segurança Cibernética, publicadas de 2010 a 2020, apresentadas no Quadro 1, formam um arcabouço normativo para Indústria 4.0 no tocante à SegCiber (Corallo; Lazoi & Lezzi, 2020).

Quadro 1 – Arcabouço normativo de Segurança Cibernética para Indústria 4.0.

Documento	Descrição	Fonte
ISA/IEC 62443	Visa melhorar a segurança, disponibilidade, integridade e confidencialidade dos componentes do *Industrial Automation and Control Systems* (IACS) (Automação Industrial e Sistemas de Controle, tradução livre).	ISA (2016)
ISO/IEC 27032:2015	Fornece diretrizes para melhorar o estado de SegCiber, orientando e determinando práticas básicas e aspectos comuns das atividades de cibersegurança e suas ramificações em outros domínios de segurança, tais como: as redes de computadores e a proteção de infraestruturas críticas.	ABNT (2015)
ISO/IEC 27001:2013	Estabelece os requisitos para a avaliação e tratamento de riscos de segurança da informação com base nas necessidades da organização, bem como monitorar e implementar ações e métodos que visam à integração das atividades de riscos, gestão de continuidade do negócio e tratamento de incidentes.	ABNT (2013)
ISO/IEC 27002:2013	Fornece diretrizes para a prática de segurança da informação, integrando a seleção, a implementação e o gerenciamento de controles, com foco nos ambientes de riscos da segurança da organização.	ABNT (2013)
IACS *Cybersecurity Certification Framework*	Propõe quatro esquemas de certificação de SegCiber: autodeclaração de conformidade, avaliação de conformidade independente, certificação de resiliência do produto e certificação de resiliência cibernética. Fortalece o uso de componentes certificados, para melhorar a defesa cibernética do IACS.	THERON; LAZARI (2018)
ANSSI *Cybersecurity for Industrial Control Systems*	A *French Network and Information Security Agency*[8] (ANSSI) tem publicado guias sobre SegCiber na indústria para analisar as vulnerabilidades do *hardware*, do *software*, dos procedimentos e fatores humanos relacionados com os sistemas, visando implementar medidas de segurança e continuidade das funções	ANSSI (2012); ANSSI (2014a); ANSSI (2014b)

[5] *Center for Strategic and International Studies*: organização bipartidária de pesquisa política sem fins lucrativos, focada no desenvolvimento de ideias práticas para gerenciar os maiores desafios do mundo (Fonte: <https://www.csis.org/topics/cybersecurity-and-technology>).
[6] *European Cyber Security Organization*: organização sem fins lucrativos, integrante da Comissão Europeia, com o objetivo de desenvolver um ecossistema europeu de cibersegurança competitivo, para apoiar o mercado digital europeu (Fonte: <https://ecs-org.eu/>).
[7] *European Union Agency for Network and Information Security*: é uma agência da União Europeia dedicada a alcançar um elevado nível de cibersegurança na Europa (Fonte: <https://www.enisa.europa.eu/>).
[8] *French Network and Information Security Agency*: responsável pela implementação de uma gama de atividades regulatórias e operacionais, visando a coordenação das questões de Segurança Cibernética na França. (Fonte: <https://www.ssi.gouv.fr/en/>).

Documento	Descrição	Fonte
	centrais das atividades industriais.	
API *Standard* 1164	Aborda controle de acesso, segurança de comunicação, distribuição da informação classificada, problemas físicos, sistemas operacionais, *design* de rede, intercâmbio de dados entre empresas e terceiros, sistemas de gerenciamento e configuração de dispositivos de campo. Fornece uma lista de práticas para fortalecer a arquitetura dos sistemas com base nas melhores práticas da indústria.	FISCHER (2004)
The Industrial Control System (ICS) *Security Compendium*	Fornece um guia de referência básico para segurança de tecnologia da informação em ICS. A primeira parte publicada pelo *German Federal Office for Information Security*[9] (BSI), em 2013, tem foco nos operadores de sistemas de controle industrial. Já a segunda parte é destinada a fabricantes de componentes de ICS.	BSI (2013)
Catalog of Control Systems Security	Documento desenvolvido pelo *U.S. Department of Homeland Security*[10] (DHS), em 2011. Apresenta uma compilação de boas práticas para a indústria aumentar a segurança dos sistemas de controle contra ataques físicos e cibernéticos. O catálogo não fica limitado ao uso específico para um setor da indústria. Pode ser utilizado por todos os setores para desenvolver uma estrutura sólida de SegCiber.	DHS (2011)
Industrial Control Systems - Cyber Emergency Response Team (ICS-CERT)	Realiza avaliações de segurança relacionadas com as infraestruturas críticas e fornece, para as partes interessadas, opções para gerenciar e mitigar os riscos de SegCiber.	ICS-CERT (2016)
National Institute of Standards and Technology (NIST) 800-82	Fornece uma visão ampla do ICS, avaliações da topologia e arquiteturas dos sistemas. Identifica as ameaças e suas vulnerabilidades, possibilitando aplicação de contramedidas recomendadas para mitigar os riscos associados à SegCiber.	STOUFFER et al. (2015)
Cyber Resiliency Design Principles – Mitre Technical Report	Fornece um conjunto de princípios de *design* de resiliência cibernética e descreve os fatores a serem aplicados aos sistemas. Busca identificar, alinhar e analisar os princípios de *design* de resiliência cibernética.	BODEAU; GRAUBART (2017)
Space Policy Directive 5 – Cybersecurity Principles for Space Systems	Segundo o documento é essencial proteger os sistemas espaciais de incidentes cibernéticos, visando evitar interrupções nas operações de infraestruturas críticas.	*NATIONAL SECURITY & DEFENSE* (2020)

Fonte: Corallo, Lazoi & Lezzi (2020) – Adaptado pelos autores.

[9] *German Federal Office for Information Security*: provedor central de serviços de segurança de tecnologia da informação (TI) para o Governo Alemão. Realiza testes de segurança de TI em cooperação com a indústria. (Fonte: <https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html>).
[10] *U.S. Department of Homeland Security*: tem como missão proteger a nação americana das ameaças que são enfrentadas pelo país, com o objetivo claro de manter a América segura. (Fonte: < https://www.dhs.gov/>).

O arcabouço normativo não esgota os guias metodológicos disponíveis na literatura para gerenciar as questões de SegCiber. No estudo das publicações acadêmicas foram identificados: i) o NIST *Framework* (2018); ii) o *Cybersecurity and Resilience Framework* (CRF) (Babiceanu & Seker, 2017); iii) o *Industrial Control Systems* (Kobara, 2016); iv) o *Impact Assessment Model* (Radanliev et al., 2018); e v) o *Vulnerabilities Assessment – Supervisory Control and Data Acquisition* (SCADA) (Januario et al., 2016).

O NIST *Framework* (2018) visa gerenciar os riscos de Segurança Cibernética relacionados com as TIC, os ICS e os sistemas ciberfísicos. O *Cybersecurity and Resilience Framework*, propõe uma estrutura para abordar os sistemas de segurança e resiliência para os aplicativos de manufatura baseados em redes (Babiceanu & Seker, 2017).

A avaliação dos riscos de segurança para os ICS pode ser realizada por um modelo hierárquico que define os limites do sistema para avaliar e identificar as vulnerabilidades na camada física, de controle, de comunicação, de rede, de supervisão e gestão (Zhu & Basar, 2011).

O modelo proposto por Radanliev et al. (2018), permite uma avaliação do impacto econômico do risco cibernético da internet das coisas, uma das tecnologias habilitadoras da Indústria 4.0. Para Januario et al. (2016) a metodologia de avaliação de vulnerabilidades no contexto dos sistemas SCADA apresenta uma representação completa da rede, a definição das funções dos componentes dos subsistemas e os recursos utilizados nas operações dos sistemas.

Os guias metodológicos desenvolvidos para abordar as questões de Segurança Cibernética não analisam os impactos econômicos da falta de cibersegurança na Indústria 4.0. Organismos internacionais que atuam em questões de SegCiber têm definido normas, documentos de orientação e metodologias de avaliação dos controles de segurança essenciais para a Indústria 4.0 (Corallo; Lazoi & Lezzi, 2020).

As empresas de manufatura estão enfrentando desafios relacionados com os conceitos disruptivos das tecnologias aplicadas no setor (Schumacher; Erol; Sihn, 2016). Essas tecnologias combinadas possibilitam um conjunto de oportunidades de produção competitiva no contexto de sistemas integrados, máquinas inteligentes e novos modelos de negócios baseados em dados.

Sendo assim, as ações de Segurança Cibernética demandam por solidez, estabilidade, resiliência, maturidade e integração à estratégia organizacional, para assegurar a segurança de toda a cadeia de valor da Indústria 4.0.

4. Resiliência

O termo resiliência pode ser definido como a capacidade de manter ajustes positivos sob condições desafiadoras (Ismail; Poolton; Sharif, 2011). Para Leveson (2011) é a habilidade do sistema de adaptar-se às circunstâncias visando manter o controle sobre uma propriedade do sistema, a segurança ou o risco.

Segundo Hollnagel (2013), a resiliência é a capacidade intrínseca de um sistema em ajustar o seu funcionamento antes, durante e após as alterações e distúrbios, com o objetivo de sustentar as operações necessárias sob condições esperadas e inesperadas. A resiliência é uma característica de como os sistemas realizam o seu desempenho diário.

As organizações devido à inserção de novas tecnologias e maior ênfase dada à dimensão cognitiva do trabalho, estão enfrentando os desafios para a gestão de sistemas complexos na Indústria 4.0.

Para fazer frente à complexidade dos sistemas, a Engenharia de Resiliência (ER) se destaca como um novo paradigma na perspectiva de estudo e gestão da segurança (Hollnagel; Woords & Levenson, 2006). A ER se concentra no equilíbrio e produtividade de *safety* dos sistemas complexos. Fornece ferramentas para gerenciar de forma proativa o reconhecimento da complexidade inerente ao funcionamento do sistema e a necessidade correspondente da variabilidade de desempenho.

A ER usa os *insights* da pesquisa sobre falhas em sistemas complexos, incluindo riscos e fatores que afetam o desempenho humano, para desenvolver ferramentas que permitem gerenciar os riscos de forma proativa (Woods, 2003). A flexibilidade, diversidade, conectividade, conhecimento, redundância e robustez são características associadas à resiliência na Indústria 4.0 (Morisse & Prigge, 2017).

Diante dos desafios relacionados à Segurança Cibernética inerentes na Indústria 4.0, a ER focada nas ameaças cibernéticas pode ser caracterizada como Engenharia de Resiliência Cibernética (ERC), com práticas e mecanismos para melhorar a resiliência cibernética. A ERC com base na segurança de sistemas de informação implementa controles de segurança que permitem aos sistemas atenderem os objetivos da política de segurança de confidencialidade, integridade e disponibilidade (Goldman, 2010).

5. Sistemas Ciberfísicos

Nos sistemas ciberfísicos existe uma combinação de processos físicos integrados em rede, com os componentes cibernéticos, sensores e atuadores, que interagem em um ciclo de monitoramento dos processos, fornecendo informações para embasar a intervenção humana que pode mudar o funcionamento de determinada máquina ou sistema quando necessário (Ashibani; Mahmoud, 2017).

Os ataques cibernéticos, cada vez mais sofisticados, estão presentes nos sistemas gerenciados por *softwares*. A exploração das vulnerabilidades nos sistemas ciberfísicos integrados e conectados, devido à evolução tecnológica, impulsionam a área de *Cyber Physical Security* (CPS) (Dimase et al., 2015).

A segurança dos sistemas ciberfísicos, em geral é classificada em 2 (duas) áreas: i) segurança das informações; e ii) segurança de controle. A segurança da informação foca na proteção dos dados, enquanto a segurança de controle busca proteger o processo dos sistemas de controle contra ataques cibernéticos (Lu et al., 2015). O foco da segurança dos sistemas ciberfísicos passou da avaliação do risco do computador para o risco na rede computacional, na qual a presença crescente de sensores e equipamentos conectados em rede na Indústria 4.0, aumenta a superfície de ataques cibernéticos (Zalewski et al., 2013; Anderl, 2014; Schwab, 2016).

A avaliação de riscos dos sistemas ciberfísicos pode ser realizada em 3(três) fases: i) a primeira busca definir o que acontecerá com o sistema; ii) a segunda visa avaliar a probabilidade do evento de risco; e iii) a terceira tem como objetivo estimar as consequências (Lu et al., 2013). Os sistemas ciberfísicos combinam processos cibernéticos e físicos, o que aumenta a complexidade para a proteção de segurança necessária (Mahmoud et al., 2015).

Os desafios de segurança demandam por mecanismos de prevenção, detecção e mitigação (Goldman, 2010). Detectar os ataques cibernéticos não é uma tarefa simples, já que existe uma interação entre o espaço físico e o cibernético, que demandam técnicas de detecção para as camadas de aplicação, transmissão e percepção dos sistemas ciberfísicos (Ashibani; Mahmoud, 2017).

6. Metodologia

A presente pesquisa classifica-se como aplicada, quanto à sua natureza, a qual permite maior familiaridade com o problema, visando torná-lo mais explícito e construir hipóteses. Com uma abordagem qualitativa, que segundo Pereira et al. (2018), possibilita uma análise das informações e dados descritivos do conteúdo teórico para fundamentação da pesquisa. A metodologia seguiu incialmente com a etapa de revisão da literatura e na sequência com o processo de busca dos dados. Sob o ponto de vista de procedimentos técnicos de busca, foi realizado o estudo bibliométrico, para mensurar as publicações, suas características e assegurar maior conformidade da análise dos resultados apresentados (Richardson, 1999; Bardin, 2011; Gil,

2010). As quantificações reforçam os argumentos e constituem indicadores significativos para análises qualitativos (Grácio; Garrutti, 2005).

O termo bibliometria, surgiu no ano de 1917 e é oriundo da fusão do sufixo metria e de bibliografia, informação, ciência e biblioteca. A bibliometria trata de um conjunto de metodologias, com leis e princípios do campo das Ciência da Informação (CI), que emprega a análise de dados para medir e pesquisar o arcabouço de uma área científica para enriquecimento de pesquisas e estudos futuros (Guedes; Borschiver, 2005). Os conceitos da CI apresentam o escopo voltado para a produção, a organização, o armazenamento, a disseminação e o uso da informação. A bibliometria permite que com o levantamento das informações seja realizada uma análise dos atributos de pesquisa de forma quantitativa e qualitativa para fundamentar o estudo (Mugnaini, 2003).

Possui, como uma característica relevante, elaborar os índices de produção do conhecimento científico. A análise bibliométrica em pesquisas científicas está relacionada com o estudo do conhecimento e da literatura como parte do processo de comunicação (Marcelo & Hayashi, 2013). A bibliometria dispõe de várias leis e princípios empíricos que usam métodos matemáticos e estatísticos (Guedes & Borschiver. 2005). Segundo os autores, as leis mais utilizadas são:

- **Lei de *Bradford*:** que dispõe sobre produtividade dos periódicos. Também conhecida como Lei da Dispersão, na qual é possível estabelecer um núcleo dos periódicos com maior relevância e qualidade na área de interesse do pesquisador, facilitando estabelecer critérios para aquisição e descarte dos periódicos (Vanti, 2002; Guedes; Borschiver, 2005);

  Métrica: grau de atração do periódico;
  Critério: reputação do periódico;
  Objetivo: identificar os periódicos mais relevantes para publicação de determinado tema;

- **Lei de *Lotka*:** que dispõe sobre a produtividade científica dos autores. Também conhecida como Lei dos Quadrados Inversos, na qual um determinado grupo de autores com prestígio apresenta "n" contribuições em um determinado campo científico, enquanto, autores com menor prestígio apresentam "1/n" contribuições (Vanti, 2002);

  Métrica: produtividade do(s) autor(es);
  Critério: número de publicações;
  Objetivo: identificar o impacto da produção científica do(s) autor(es) em uma área de conhecimento;

- **Lei de *Zipf* ou Mínimo Esforço:** que dispõe sobre a quantidade de vezes que palavras aparecem em um texto, gerando uma lista de termos de alta e baixa frequência (Vanti, 2002). Segundo Guedes (2012), a palavra com maior número de ocorrências no texto recebe a classificação 1 (um) e a próxima é classificada como 2 (dois), e assim por diante para as outras palavras;

  Métrica: frequência das palavras-chave;
  Critério: lista de frequência das palavras-chave;
  Objetivo: identificar as palavras-chave mais recorrentes no texto relacionadas a uma área do conhecimento;

As 3 (três) leis mencionadas lidam com a distribuição e levantamento de documentos científicos que possuem temática similar. Para reconhecer a similaridade entre os documentos se faz necessário uma organização padronizada em bases

de dados que possibilitam a recuperação da produção científica.

6.1 Revisão da literatura

As fontes de coleta foram as bases de dados *Web of Science* e *Scopus*, já que são bases consolidadas e com acesso disponível pelo portal de periódicos da CAPES. A escolha das 2 (duas) bases de dados foi embasada nos seguintes aspectos: i) as bases permitem recuperar uma maior diversificação de metadados relevantes para a pesquisa; ii) as pesquisas podem ser pelo tópico, título, autor, resumo (*abstract*), palavras-chave, ano de publicação, país, área de pesquisa, nome da publicação e editor; e iii) as bases fornecem contribuições na produção de indicadores, por meio de indexação de revistas científicas (Rodrigues; Quartiero; Noubert, 2015).

Na revisão da literatura foram utilizadas as palavras-chave em inglês: *Industry 4.0*, *Cybersecurity* e *Resilience* nas *queries* empregadas nas bases no período de 2015 a 2020. A Tabela 1 apresenta os resultados das pesquisas das palavras-chave com a quantidade de publicações identificadas na base de dados *Web of Science*. Para apresentar as ocorrências de determinado termo no título, resumo, palavras-chave e *keywords plus* foi utilizado o rótulo do campo tópico "TS", com a seguinte estrutura na pesquisa avançada: TS=("palavra-chave 1" AND "palavra-chave 2").

Tabela 1 - Resultados das pesquisas – *Web of Science.*

Expressão de busca	No. de publicações	No. de palavras-chave	No. de autores
TS=("industry 4.0" AND "cybersecurity")	50	244	171
TS=("industry 4.0" AND "resilience")	72	479	246

Fonte: Autores.

Os resultados das pesquisas realizadas na base de dados *Scopus* estão apresentados na Tabela 2. Na referida base foi utilizado o parâmetro TITLE-ABS na expressão de busca para apresentar os resultados das palavras-chave no resumo e título dos artigos, com a seguinte estrutura na pesquisa avançada: TITLE-ABS("palavra-chave 1" AND "palavra-chave 2").

Tabela 2 - Resultados das pesquisas – *Scopus.*

Expressão de busca	No. de publicações	No. de palavras-chave	No. de autores
TITLE-ABS("industry 4.0" AND "cybersecurity")	100	748	250
TITLE-ABS("industry 4.0" AND "resilience")	73	734	210

Fonte: Autores.

6.2 Processo de busca

A bibliometria foi usada para apurar as publicações sobre a temática. Para delimitar um corte nas publicações foram utilizadas as seguintes combinações dos termos das palavras-chave: *"industry 4.0" AND "cybersecurity"* e *"industry 4.0" AND "resilience*.

A pesquisa realizada nas bases de dados no período de 2015 a 2020, utilizou o campo tópico, que incluí as ocorrências dos termos selecionados nos campos título, resumo (*abstract*), palavras-chave dos autores e *keywords plus*, apresentou um total de 295 (duzentos e noventa e cinco) publicações. Sendo 122 (cento e vinte e dois) publicações na *Web of Science* e 173 (cento e setenta e três) publicações na *Scopus*. Foi aplicado um filtro para identificar as publicações repetidas nas bases de dados. Para tanto, o referido filtro permitiu a identificação de 43 (quarenta e três) publicações repetidas. Sendo assim, do total de 295 (duzentos e noventa e cinco) publicações foram subtraídas as repetições ficando com uma amostra de 252 (duzentos e cinquenta e dois) trabalhos.

7. Análise dos Resultados

Esta seção apresenta os resultados da análise bibliométrica, da amostra da produção científica do tema estudado, utilizando as funcionalidades de análise disponíveis nos portais das bases de dados e os *softwares* para análise dos dados e o *VOSviewer*[11] que permite criar mapas para análise de redes bibliométricas. Essas redes podem incluir, por exemplo, áreas e instituições de pesquisa, periódicos, pesquisadores ou publicações individuais, palavras-chave, e podem ser construídas com base em relações de citação, acoplamento bibliográfico, ocorrência, cocitação ou coautoria. Para a análise dos dados foram considerados os princípios da Lei de *Bradford* para analisar a produtividade dos periódicos, da Lei de *Lotka* para analisar a produtividade científica dos autores e da Lei de *Zipf* para analisar a quantidade de vezes que palavras são citadas em um texto.

7.1 Áreas de pesquisa

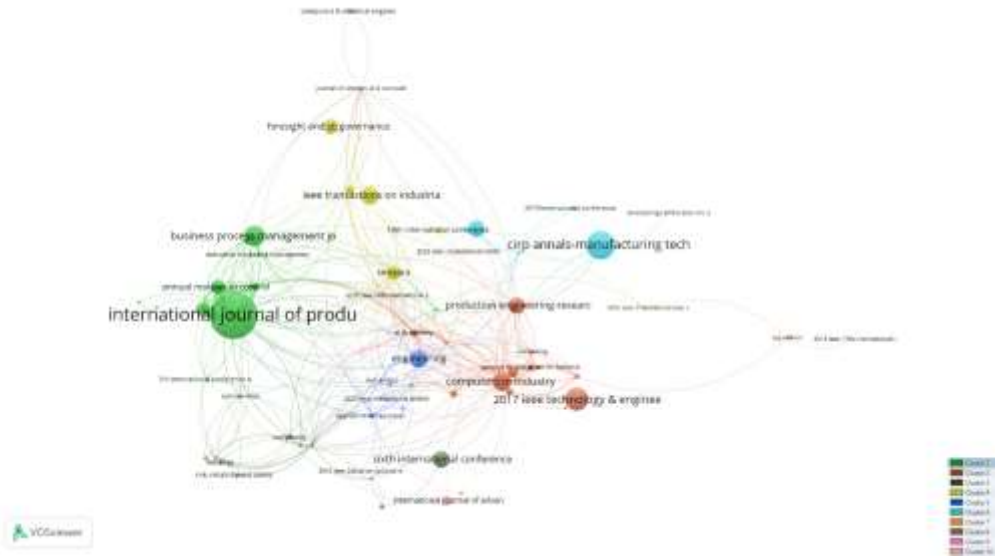
Na análise dos resultados, incialmente procurou-se identificar as áreas de pesquisa com maior concentração das publicações. Na base de dados *Web of Science* as publicações foram agrupadas em 25 (vinte e cinco) áreas, com a seguinte sequência de importância para as 6 (seis) áreas com maior número de publicações: engenharia elétrica eletrônica (20,1 %), engenharia industrial (18,4%), sistemas de controle e automação (14,2%), ciência da computação (13,4%), engenharia de manufatura (12,6%) e telecomunicações (10,9%). Já na base de dados *Scopus* as publicações foram agrupadas em 16 (dezesseis) áreas, com a ordem de relevância para as 6 (seis) áreas que tiveram o maior número de publicações, a saber: ciência da computação (28,4%), engenharias (23,9%), ciência de dados (8,5%), gestão de negócios (8,5%), matemática (8,2%) e física (4,0%).

7.2 Periódicos

As publicações da base de dados *Web of Science* apresentam uma predominância de artigos (46,7%), seguida de publicações em conferências (37,7%). Na base de dados *Scopus* o percentual foi maior para as publicações em conferências (44,0%), seguida das publicações de artigos (36,3%). A Figura 1 apresenta 10 (dez) *clusters* dos periódicos da *Web of Science*, com destaque para o "*International Journal of Production Research*" (cor verde – *cluster* 1 com maior densidade das citações).

[11] *VOSviewer*: https://www.vosviewer.com

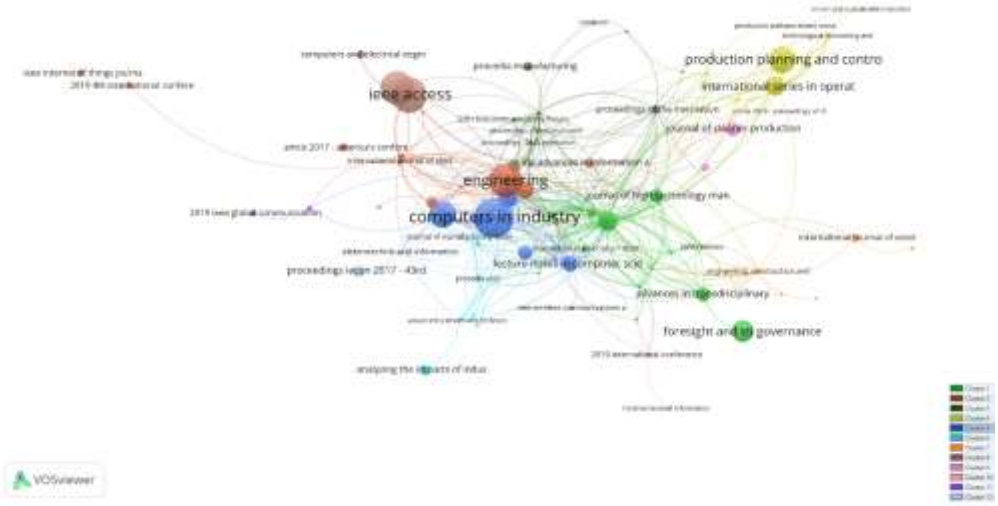
Figura 1 – Periódicos da *Web of Science.*



Fonte: *Web of Science.*

A Figura 2 apresenta 12 (doze) *clusters* dos periódicos da *Scopus*, tendo o periódico "*Computers of Industry*" a maior densidade das citações (cor azul – *cluster* 5). O tamanho da imagem representada no *cluster* demonstra sua densidade, desse modo, o círculo maior reflete a representatividade do item na amostra (Chen; Ibekwe-Sanjuan; Hou, 2010).

Figura 2 – Periódicos da *Scopus.*



Fonte: *Scopus*

O *International Journal of Production Research* tem um Fator de Impacto[12] de 4.577, com domínios de pesquisa nas áreas de engenharia, pesquisa operacional e gestão da ciência. Já o periódico *Computers in Industry* tem o seguinte indicador bibliométrico capaz de medir o prestígio do periódico científico: 1.077, denominado de JCR[13] na base de dados *Scopus*, nas áreas de engenharia e ciência da computação.

[12] Fator de Impacto: identifica a frequência média com que um artigo de um periódico é citado em um determinado período (Fonte: *Web of Science*).
[13] JCR: mede as citações ponderadas recebidas pelo periódico (Fonte: *Scopus*).

7.3 Países e instituições de pesquisa

As buscas realizadas demonstram uma liderança dos pesquisadores da Alemanha, seguidos dos pesquisadores dos Estados Unidos da América (EUA), no conjunto das publicações identificadas com a aplicação das expressões de busca, apresentadas na Tabela 1. Esses países têm maior contribuição para o desenvolvimento de um corpo teórico de pesquisa sobre o tema. A Tabela 3 mostra os 15 (quinze) países com maior número de publicações nas bases de dados pesquisadas.

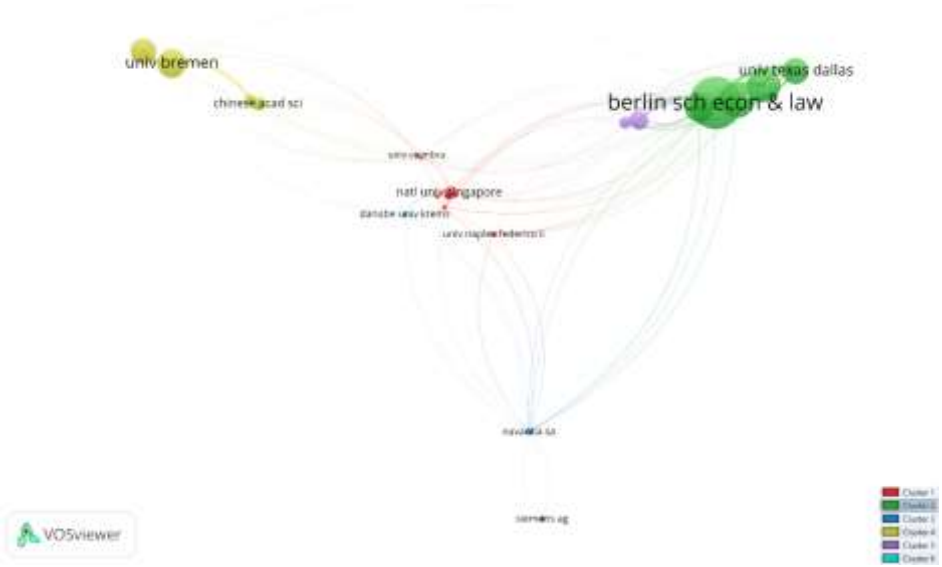
Tabela 3 – Publicações por país e base de dados.

País	*Web of Science*	*Scopus*	Total
Alemanha	29	14	43
Estados Unidos da América	18	23	41
França	14	13	27
Itália	11	14	25
Espanha	10	13	23
Inglaterra	9	12	21
China	7	9	16
Rússia	8	7	15
África do Sul	2	9	11
Austrália	4	7	11
Áustria	7	4	11
Índia	5	6	11
Brasil	2	5	7
Malásia	2	5	7
Turquia	0	5	5

Fonte: *Web of Science* e *Scopus.*

No contexto das instituições de pesquisa foram identificados 6 (seis) *clusters* com acoplamento bibliográfico entre as 30 (trinta) instituições com maior número de publicações, tendo como fonte a base de dados *Web of Science*. O *cluster* 2 (cor verde) apresenta a maior densidade das citações dos trabalhos publicados, com um total de 311 (trezentos e onze) citações. A Figura 3 apresenta a distribuição dos *clusters*.

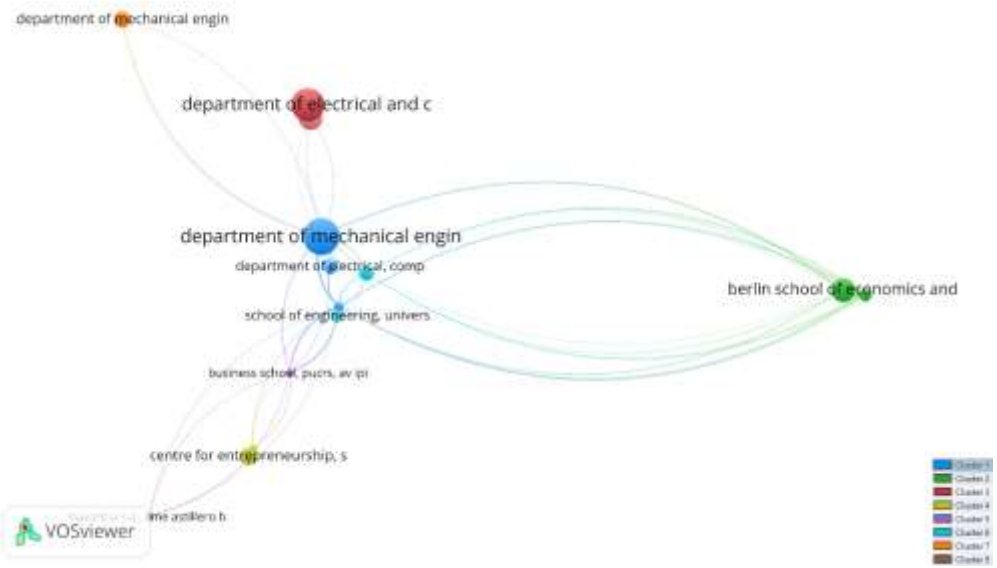
Figura 3 – Instituições de pesquisa – *Web of Science.*



Fonte: *Web of Science.*

A Figura 4 apresenta o acoplamento bibliográfico das 30 (trinta) instituições que tiveram a maioria dos trabalhos publicados na base de dados *Scopus*. A maior densidade de citações das publicações está no *cluster* 1 (cor azul) com destaque para os trabalhos do Departamento de Engenharia Mecânica da Universidade de Singapura, com 63 (sessenta e três) citações.

Figura 4 – Instituições de pesquisa – *Scopus.*

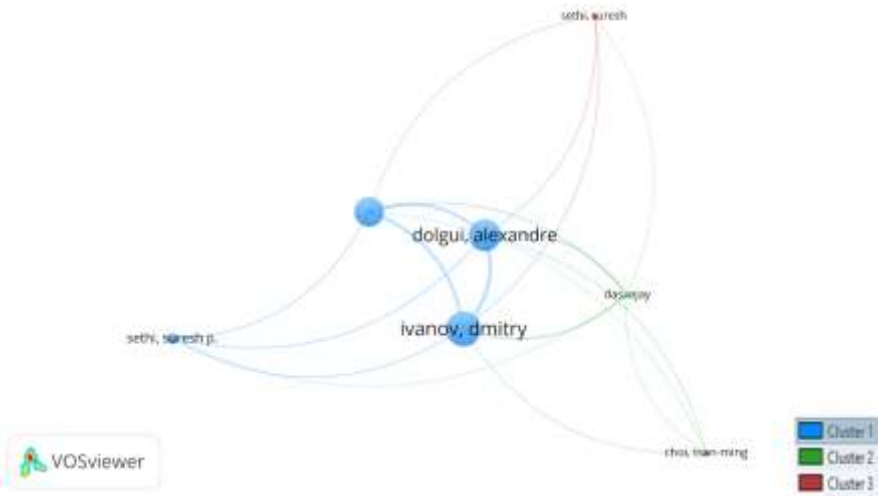


Fonte: *Scopus.*

7.4 Países e instituições de pesquisa

Na sequência da análise das instituições de pesquisa, os dados *Web of Science* permitiram realizar um estudo dos autores que mais publicaram sobre o tema no período de 2015 a 2020. A Figura 5 apresenta os 3 (três) *clusters* dos 7 (sete) autores, de um total de 412 (quatrocentos e doze), que tiveram mais de 10 (dez) citações dos seus trabalhos. O pesquisador Ivanov Dmitry, da instituição de pesquisa "*Berlim School of Economics and Law*", na Alemanha, apresenta a maior densidade relacionada tanto ao número de publicações como ao número de citações (*cluster* da cor azul), nos anos de 2019 e 2020.

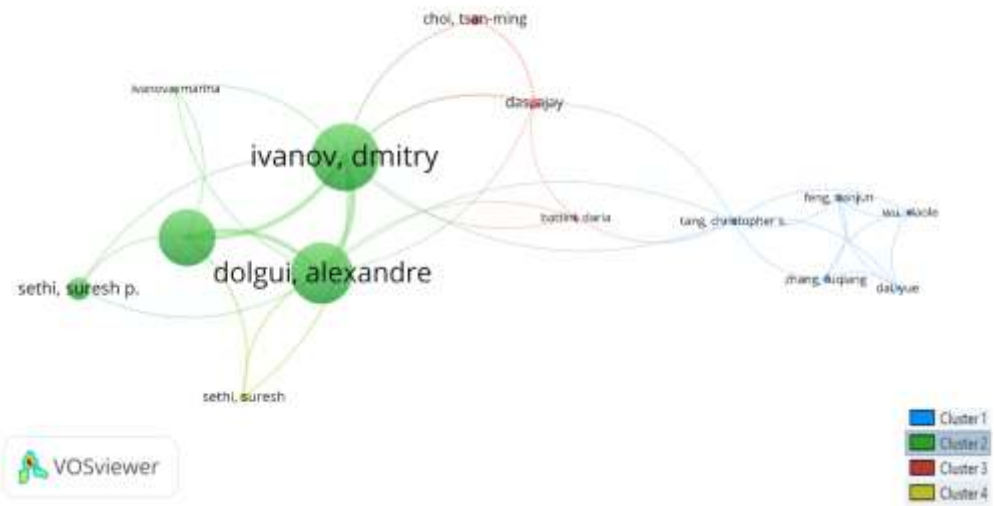
Figura 5 – Autores – *Web of Science*.



Fonte: *Web of Science*

No grupo dos autores foram identificados 4 (quatro) *clusters* de coautoria, como apresentado na Figura 6. A análise de coautoria permite uma visão da produção intelectual do conhecimento científico em termos de agrupamento (Chen; Ibekwe-Sanjuan; Hou, 2010). O *cluster* 2 (dois) tem a maior densidade de colaboração dos autores: Ivanov Dmitry (*Berlim School of Economics and Law*, Alemanha), Alexandre Dolgui (*Centre National de la Recherche Scientifique*, França), Boris Sokolov (*St. Petersburg Federal Rsearch Center of the Russian Academy of Sciences*, Rússia) e Suresh P. Sethi (*University of Texas Dallas*, EUA). As linhas que ligam os *clusters* representam as relações dos autores. A maior espessura significa elos mais fortes de colaboração dos autores nas publicações.

Figura 6 – Coautoria – *Web of Science*.



Fonte: *Web of Science.*

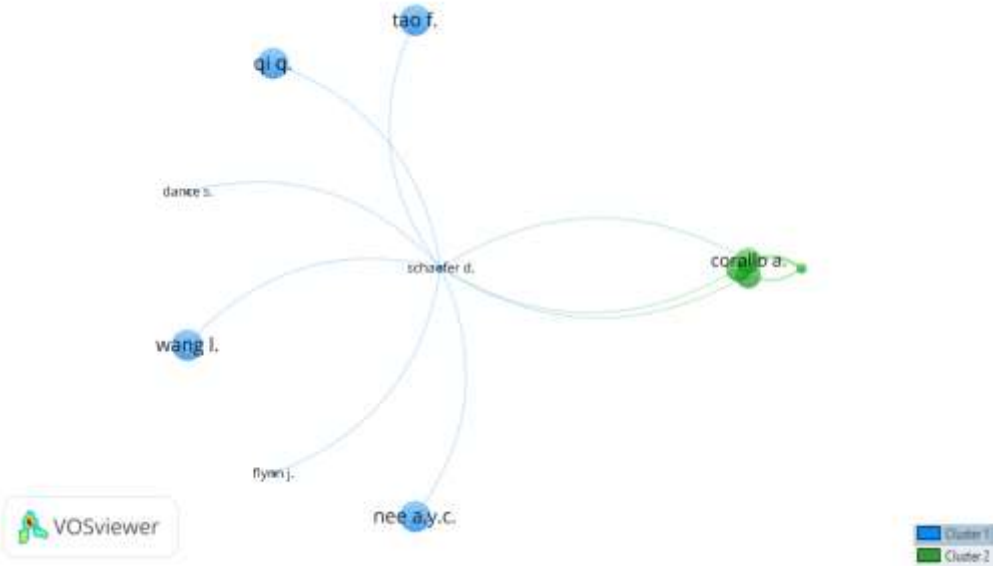
Passando para uma análise do período das publicações pode-se visualizar que os autores identificados com as cores que tendem para o azul são os que têm publicações mais recentes. A Figura 7 apresenta a distribuição dos trabalhos publicados por ano.

Figura 7 – Autores por ano – *Web of Science*.

Fonte: *Web of Science*

No estudo dos autores tendo como fonte a base de dados *Scopus* identificou-se, de um total de 459 (quatrocentos e cinquenta e nove) autores, 2 (dois) *clusters* formados por 11 (onze) autores que tiveram mais de 10 (dez) citações dos seus trabalhos. Os *clusters* podem ser visualizados na Figura 8.

Figura 8 – Autores – *Scopus.*



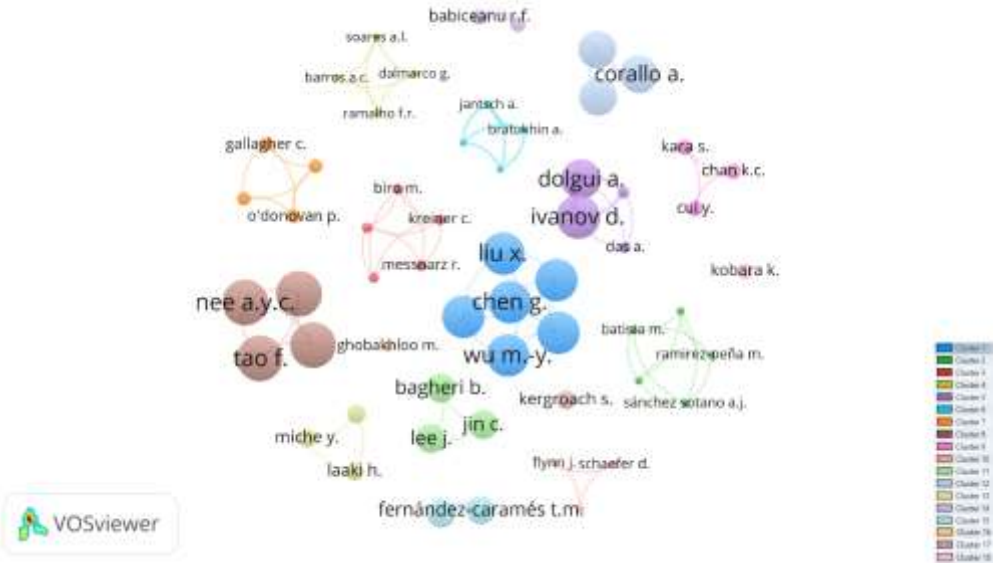
Fonte: *Scopus*

Os autores Tao, F (*School of Automation Science and Electrical Engineering*, China), Qi, Q (*School of Automation Science and Electrical Engineering*, China), Wang, L. (*Department of Production Engineering, KHT Royal Institute of*

Technology, Suécia) e Nee, A.Y.C. (*Department of Mechanical Engineering*, *National University*, Singapura), foram os que tiveram o maior número de citações.

Na análise de coautoria dos autores na base de dados *Scopus*, foram identificados 18 (dezoito) *clusters* de coautores, como apresentado na Figura 9, com destaque para o *cluster* 1 (um) que tem a participação de 6 (seis) autores.

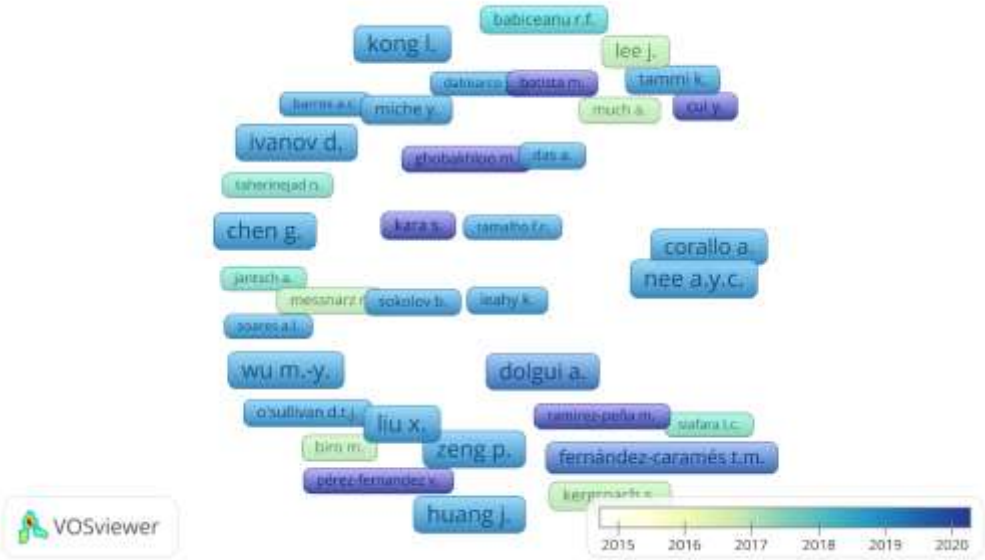
Figura 9 – Coautoria – *Scopus.*



Fonte: *Scopus.*

A Figura 10 apresenta os autores com publicações no período de 2015 a 2020, com uma tendência para o maior número de publicações nos anos de 2018, 2019 e 2020.

Figura 10 – Autores por ano.



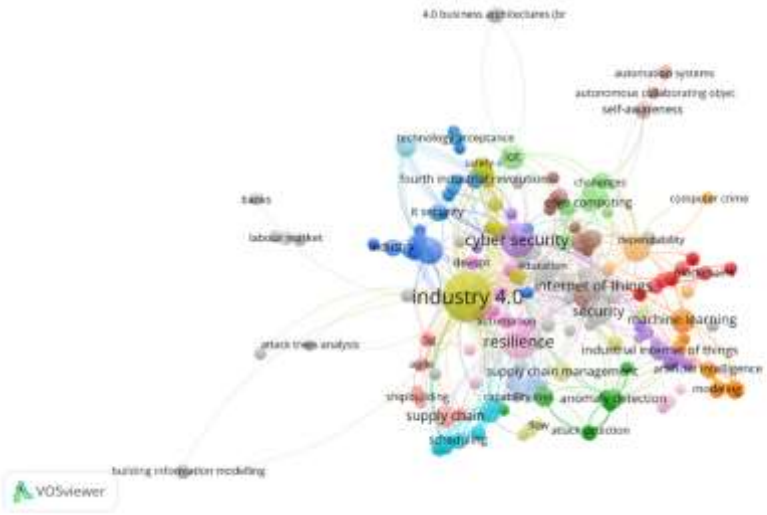
Fonte: *Scopus.*

7.5 Palavras-chave

As bases de dados *Web of Science* e *Scopus* utilizam palavras-chave ou frases como parâmetro de busca das publicações. Segundo Lebrun (2007), as palavras-chave são definidas pelos autores visando atrair os leitores, com termos gerais, intermediários ou específicos sobre a pesquisa. A análise das palavras-chave fornece informações relevantes sobre o tema da pesquisa. Nesse sentido, a co-ocorrência das palavras-chave orienta o leitor sobre o conteúdo da publicação (Feng et al., 2015).

Na Figura 11 é possível identificar a representatividade das palavras-chave utilizadas nas publicações da *Web of Science*, considerando o tamanho do círculo e as relações nos *clusters.*

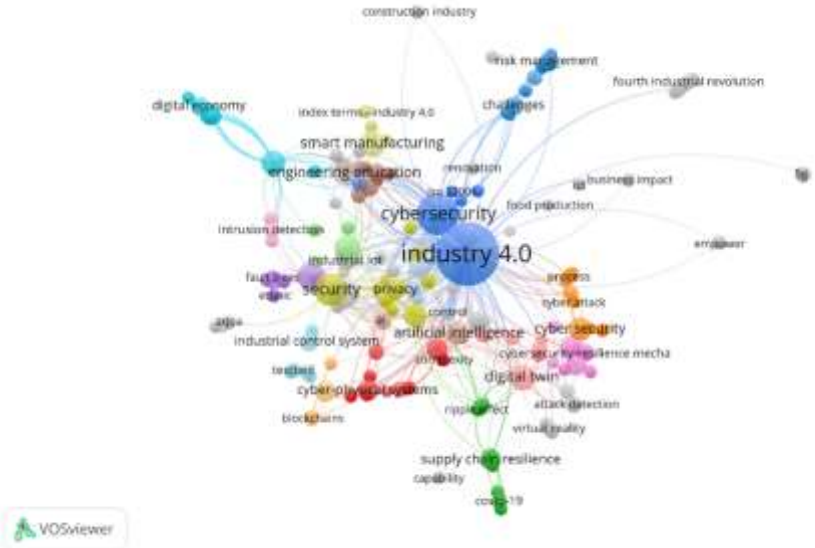
Figura 11 – Palavras-chave – *Web of Science*.



Fonte: *Web of Science.*

Nas publicações da base de dados *Scopus*, as palavra-chave identificadas podem ser visualizadas na Figura 12, seguindo o critério do tamanho do círculo que demonstra a sua representatividade na amostra.

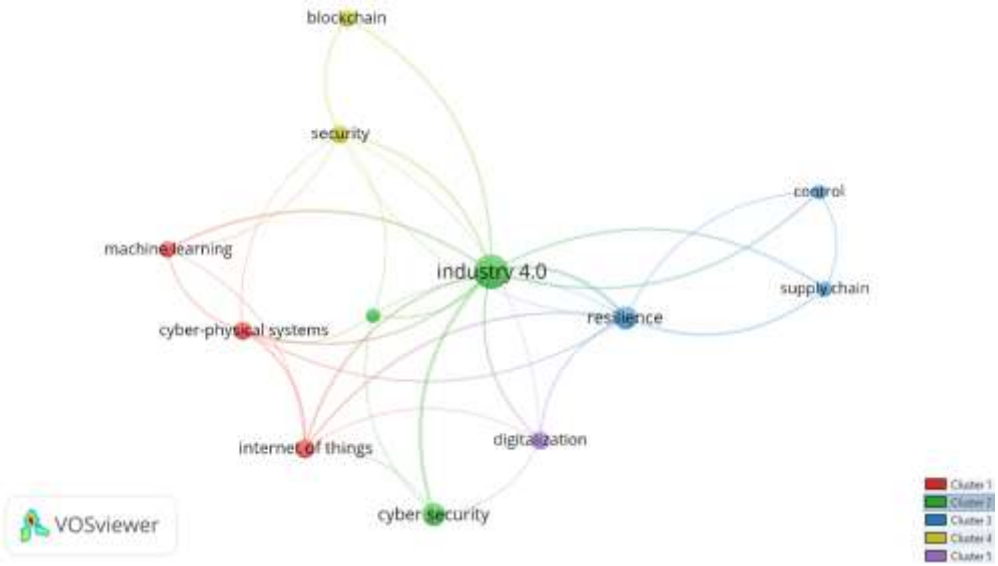
Figura 12 – Palavras-chave – *Scopus.*



Fonte: *Scopus.*

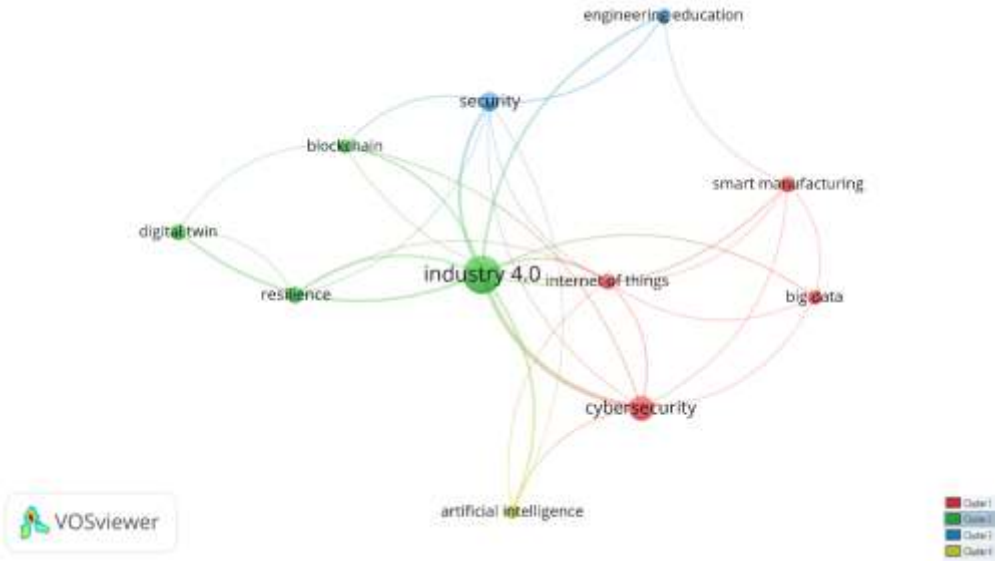
Aplicando um filtro nas palavras-chave com mais de 5 (cinco) ocorrências, identifica-se 5 (cinco) *clusters* na base de dados *Web of Science* e 4 (quatro) *clusters* na base de dados *Scopus*, como pode ser visualizado na Figura 13 e Figura 14. Nas duas figuras as linhas de ligação das palavras-chave *industry 4.0* e *cyber security*, *industry 4.0* e *resilience* têm maior espessura, indicando uma relação mais forte das palavras-chave em comparação com as demais. Na análise não foi identifica relação na combinação das 3 (três) palavras-chave: *industry 4.0*, *cyber security* e *resilience*.

Figura 13 – Palavras-chave – Ocorrências – *Web of Science.*



Fonte: *Web of Science.*

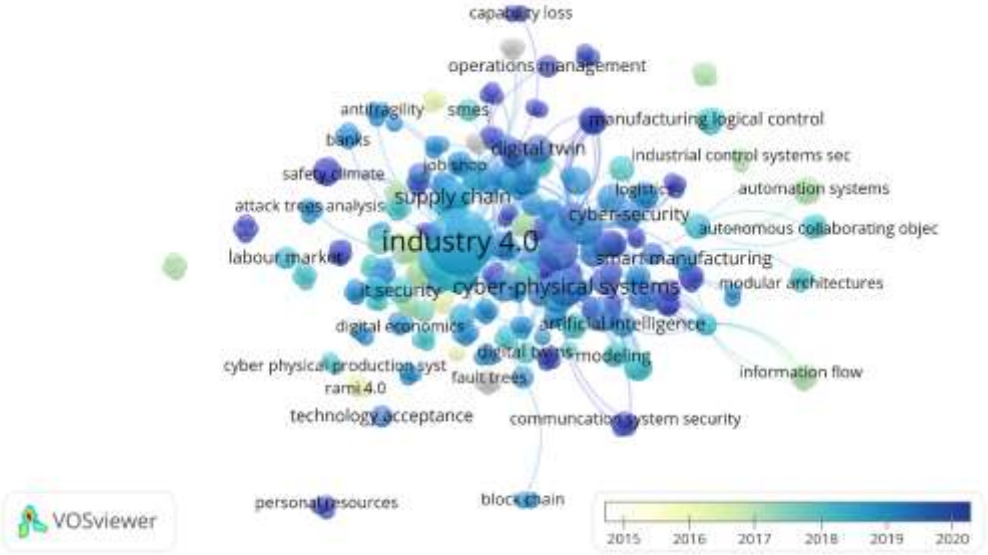
Figura 14 – Palavras-chave – Ocorrências – *Scopus.*



Fonte: *Scopus.*

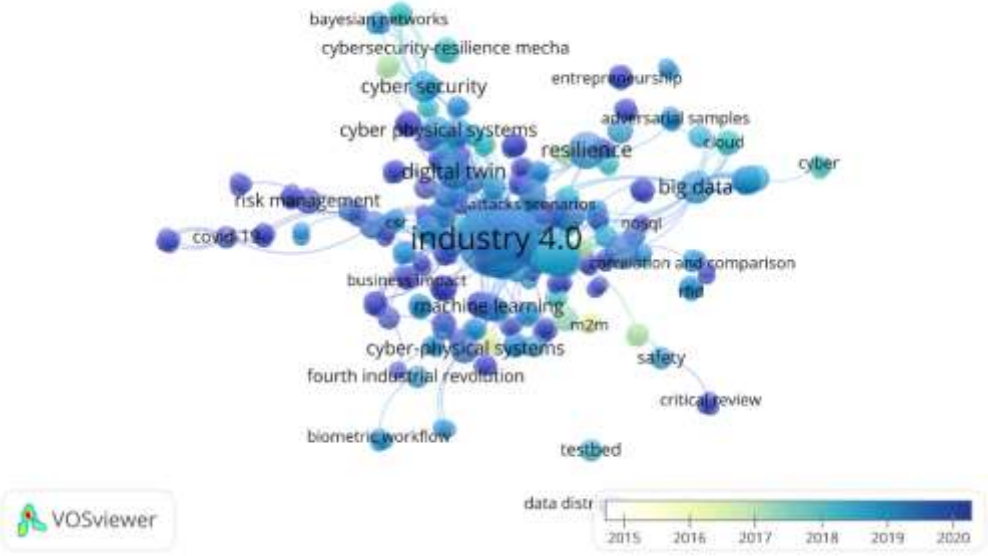
Na sequência da pesquisa, as Figuras 15 e 16 apresentam os termos das palavras-chave no período de 2015 a 2020. Os termos com tendência para a cor azul estão presentes nas publicações mais atuais de 2018, 2019 e 2020.

Figura 15 – Palavras-chave por ano – *Web of Science.*



Fonte: *Web of Science.*

Figura 16 – Palavras-chave por ano – *Scopus.*



Fonte: *Scopus.*

7.6 Publicações

Essa seção apresenta uma análise das publicações com mais citações nas duas bases de dados, visando sintetizar as principais ideias desses autores sobre o tema em estudo. Na Tabela 4 estão listadas 10 (dez) publicações com o seu respectivo número de citações.

Tabela 4 – Publicações.

Publicação / Autor(es) / Periódico / Ano / Base de dados	No.
The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. Por: Ivanov, Dmitry; Dolgui, Alexandre; Sokolov, Boris INTERNATIONAL JOURNAL OF PRODUCTION. 2019. *Web of Science*	138
Continuous maintenance and the future - Foundations and technological challenges. Por: Roy, R.; Stark, R.; Tracht, K.; *et al*. CONFERENCE: 66TH GENERAL ASSEMBLY OF THE INTERNATIONAL-ACADEMY-FOR-PRODUCTION-ENGINEERING. 2016. *Web of Science*	96
Scheduling in production, supply chain and Industry 4.0 systems by optimal control: fundamentals, state-of-the-art and applications. Por: Dolgui, Alexandre; Ivanov, Dmitry; Sethi, Suresh P.; *et al*. INTERNATIONAL JOURNAL OF PRODUCTION RESEARCH. 2019. *Web of Science*	84
Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison. Por: Tao, F., Qi, Q., Wang, L., Nee, A.Y.C. Engineering. 2019. *Scopus*	64
Blockchain Technology Innovations. Por: Ahram, Tareq; Sargolzaei, Arman; Sargolzaei, Saman; *et al*. Conference: IEEE-TECHNOLOGY-AND-ENGINEERING-MANAGEMENT-SOCIETY CONFERENCE. 2017. *Web of Science*	61
Towards secure industrial iot: Blockchain system with credit-based consensus mechanism. Por: Huang, J.; Kong, L.; Chen, G.; Liu, X.; Zeng, P. IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. 2019. *Scopus*	57
Towards Industry 4.0 Mapping digital technologies for supply chain management-marketing integration. Por: Ardito, Lorenzo; Petruzzelli, Antonio Messeni; Panniello, Umberto; *et al*. BUSINESS PROCESS MANAGEMENT JOURNAL. 2019. *Web of Science*	49
Cybersecurity for Industry 4.0 in the current literature: A reference framework. Por: Lezzi, M.; Lazoi, M.; Corallo, A. COMPUTERS IN INDUSTRY. 2018. *Scopus*	40
A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. Por: Ivanov, D., Dolgui, A. PRODUCTION PLANNING AND CONTROL. 2020. *Scopus*	39
Cyber physical systems for predictive production systems. Por: Lee, J.; Jin, C.; Bagheri, B. PRODUCTION ENGINEERING. 2017. *Scopus*	39

Fonte: *Web of Science* e *Scopus.*

O trabalho dos autores Ivanov, Dolgui e Sokolov (2019), com o título "*The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics*", discorre sobre as inovações disruptivas na Indústria 4.0 e os impactos da digitalização na gestão da cadeia de suprimentos. Os autores Roy et al. (2016), apresentam no trabalho "*Continuous maintenance and the future - Foundations and technological challenges*", os fundamentos e tecnologias para manutenção contínua no ciclo de vida dos produtos no contexto da Indústria 4.0 e os padrões de Segurança Cibernética. O segundo trabalho dos autores Dolgui, Ivanov, Sethi e Sokolov (2019), "*Scheduling in production, supply chain and Industry 4.0 systems by optimal control: fundamentals, state-of-the-art and applications*", apresenta uma pesquisa sobre as aplicações de controle e segurança para a programação em sistemas de produção e cadeia de suprimentos na Indústria 4.0.

Para Tao et al. (2019) as tecnologias de ponta, como a internet das coisas, computação em nuvem, *big data* e inteligência artificial estão relacionadas com o desenvolvimento da manufatura inteligente. Os autores, no trabalho "*Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison*", abordam e analisam a integração dos sistemas ciberfísicos e os gêmeos digitais sob múltiplas perspectivas, incluindo a sua origem,

mapeamento ciberfísicos, modelagem hierárquica e elementos centrais. Segundo Parrot e Warshaw (2017), gêmeos digitais podem ser definidos como um modelo digital de um objeto real. O termo foi criado pelo Dr. Michael Grieves, em 2003, na Universidade de Michigan.

Na publicação "*Blockchain Technology Innovations*", os autores Ahram et al. (2017), abordam a aplicação da tecnologia *Blockchain* no mundo digital desenvolvendo uma nova perspectiva para segurança, resiliência e eficiência dos sistemas tecnológicos na indústria. Segundo Huang et al. (2019), a internet das coisas industrial (IIoT) desempenha um papel fundamental para a Indústria 4.0. Os autores apresentam no trabalho "*Towards secure industrial iot: Blockchain system with credit-based consensus mechanism*", um sistema de *Blockchain* como mecanismo para assegurar segurança e eficiência no gerenciamento dos dispositivos da IIoT.

Ardito et al. (2019), citam no trabalho "*Towards Industry 4.0 Mapping digital technologies for supply chain management-marketing integration*", um conjunto de tecnologias habilitadoras da Indústria 4.0. Tecnologias que podem ser consideradas como relevantes para assegurar a segurança na integração da cadeia de suprimentos-*marketing* e o processamento da informação, segundo os autores. Para Lezzi, Lazoi e Corallo (2018), as questões de Segurança Cibernética representam um desafio complexo para empresas inseridas no ecossistema da Indústria 4.0. No trabalho "*Cybersecurity for Industry 4.0 in the current literature: A reference framework*", esses autores propõe analisar, por meio de uma abordagem de revisão sistemática da literatura, como o estado da arte aborda as questões de SegCiber no contexto da Indústria 4.0. Na análise são definidos os conceitos de SegCiber, Indústria 4.0 e as características da gestão da cibersegurança.

No terceiro trabalho publicado por Ivanov e Dolgui (2020), na amostra das publicações mais citadas, os autores apresentam uma análise da implementação dos gêmeos digitais no gerenciamento de risco na cadeia de suprimentos. O trabalho "*A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0*" contribuí para a pesquisa e prática da gestão de risco, para assegurar a continuidade do negócio. Lee, Jin e Bagheri (2017) realizam uma abordagem sistemática no trabalho "*Cyber physical systems for predictive production systems*", para implementar a resiliência e interoperabilidade para otimizar a produtividade na manufatura. A análise das publicações demonstra o desenvolvimento de aplicações técnicas para a Indústria 4.0.

8. Conclusão

Este trabalho apresenta um estudo bibliométrico sobre a produção acadêmica do tema da Segurança Cibernética na Indústria 4.0. O estudo foi realizado em uma amostra de 252 (duzentos e cinquenta e dois) publicações no período de 2015 a 2020, nas bases de dados *Web of Science* e *Scopus*. A análise possibilitou identificar as áreas de pesquisa mais relevantes relacionadas com o tema, periódicos com impacto acadêmico, autores e artigos altamente citados, palavras-chave significativas, instituições e países que contribuem para o corpo técnico de pesquisa sobre segurança na Indústria 4.0.

Como evidenciado na pesquisa, o tema de estudo tem tido uma abordagem sob uma nova perspectiva de evolução tecnológica com a presença dos sistemas ciberfísicos conectados em ambientes industriais que demandam Segurança Cibernética. Sendo assim, a SegCiber emerge como desafio para organizações, considerando a complexidade e dinâmica do panorama cibernético, passando para o topo da agenda do setor público e privado.

A análise bibliométrica desenvolvida neste trabalho indica a liderança da Alemanha nas pesquisas com o tema da Indústria 4.0, com uma abordagem de segurança e resiliência. As publicações cobriram 25 (vinte e cinco) e 16 (dezesseis) áreas de pesquisa categorizadas nas bases de dados *Web of Science* e *Scopus*, respectivamente. As áreas de pesquisa identificadas como mais importantes foram: engenharia, ciência da computação, ciência de dados e telecomunicações, com maior concentração de publicações nos anos de 2018, 2019 e 2020. Com base na análise foi possível identificar os autores com

os trabalhos mais citados na amostra, a saber: Ivanov Dmitry, Alexandre Dolgui, Boris Sokolov, Suresh P. Sethi, Tao F., Qi Q., Wang L. e Nee, A.Y.C. O estudo apontou que as palavras-chave *industry 4.0* e *cyber security* tem o maior número de ocorrências nas publicações mais recentes.

Os procedimentos metodológicos aplicados na pesquisa apresentam uma visão técnica das publicações sobre a Segurança Cibernética na 4ª. Revolução Industrial por meio da bibliometria. No entanto, a falta de uma abordagem sobre as habilidades e competências necessárias para Indústria 4.0, por parte dos autores estudados, pode ser considerada uma limitação deste artigo. Como trabalhos futuros, baseados na metodologia aplicada nesta pesquisa, podem ser analisadas as necessidades de capacitação de recursos humanos para lidar com as tecnologias habilitadoras da Indústria 4.0 de forma seletiva e/ou detalhada.

Referências

ABNT – (2013) – *NBR ISO/IEC 27001:2013: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação*: Associação Brasileira de Normas Técnicas.

ABNT – (2013) – *NBR ISO/IEC 27002:2013: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação*: Associação Brasileira de Normas Técnicas.

ABNT – (2015) – *NBR ISO/IEC 27032:2012: Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética*: Associação Brasileira de Normas Técnicas.

Ahram, T., Sargolzaei, A., Sargolzaei, S., et al. (2017). *Blockchain Technology Innovations.* Conference: IEEE-technology-and-engineering-management-society conference.

Anderl, R. (2014). *Industrie 4.0: advanced engineering of smart products and smart production*. Conference: 19th International Seminar on High Technology, Piracicaba, Brazil, pp. 1-14.

ANSSI. (2012). *Managing Cybersecurity for Industrial Control Systems.* ANSSI.

ANSSI, 2014a. (2014). *Classification Method and Key Measures.* ANSSI.

ANSSI, 2014b. (2014). *Detailed Measures.* ANSSI.

Ahram, T., Arman, S., Saman, S., Daniels, J., & Amaba, B. (2017). *Blockchain Technology Innovations.* Conference: IEEE-Technology-and-Engineering-Management-Society Conference.

Ardito, L., Petruzzelli, A. M., & Panniello, U. (2019). *Towards Industry 4.0 Mapping digital technologies for supply chain management-marketing integration.* Business Process Management Journal, 25, 323-346.

Ashibani, Y.. & Mahmoud, H. M. (2017). *Cyber physical systems security: Analysis, challenges and solutions.* Computers & Security, 68, 81-97.

Babiceanu, R. F., & Seker, R. (2017). *Cybersecurity and resilience modelling for software-defined networks-based manufacturing application.* In: Service Orientation in Holonic and Multi-Agent Manufacturing. Studies in Computational Intelligence. Springer, Cham, 167–176.

Bardin, L. (2011). *Análise de conteúdo*: Edições 70.

Barros, O. S. R., Gomes, U. M., & Freitas, W. L. (2011). *Desafios estratégicos para segurança e defesa cibernética*. Biblioteca da Presidência da República. Secretaria de Assuntos Estratégicos da Presidência da República. Brasília.

BCG. (2017). *Report from Davos: Board oversight of cyberresilience.* https://www.bcg.com/it-it/publications/2017/technology-digital-reportdavos-board-oversight-cyberresilience.aspx

Bibby, L., & Dehe, B. (2018). *Defining and assessing Industry 4.0 maturity levels-case of the defence sector*. Production Planning and Control, 29(12), 1.030-1.043.

Bodeau, D., & Graubart, R. (2017). *Cyber resiliency design principles. Technical report.* The MITRE Corporation. https ://www.mitre .org/publications/technical-papers/cyber -resiliency-design-principles

BSI – (2013) – Federal Office for Information Security. *ICS Security Compendium.* Version 1.23.

Bughin, J., Chui, M., & Manyika, J. (2015). *An executive's guide to the internet of things*. McKinsey Quarterly, 4, 92-101, 2015.

Carvalho, P. S. M. (2010). *A defesa cibernética e as infraestruturas críticas nacionais.* Brasília.

Chen, C., Ibekwe-Sanjuan, F., & Hou, J. (2010). *The structure and dynamics of cocitation clusters: A multiple - perspective cocitation analysis.* Journal of the American Society for Information Science and Technology, 61(7), 1386-1409.

Chun, K. W., Kim, H., & Lee, K. (2019). *A Study on Research Trends of Technologies for Industry 4.0; 3D Printing, Artificial Intelligence, Big Data, Cloud Computing, and Internet of Things.* Advanced Multimedia and Ubiquitous Engineering, Lecture Notes in Electrical Engineering, 518 (1), 397-403.

Cook, R. I., Render, M., & Woods, D. D. (2009). *Resilience Engineering in Practice.* International Standard Book, Number-13.

Corallo, A., Lazo,i M., & Lezzi, M. (2020). *Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts.* Science Direct, Elsevier, Computers in Industry, 114, 1-15.

Dilberoglu, U. M., Gharehpapagh, B., Yaman. U., & Dolen, M. (2017). *The role of additive manufacturing in the era of industry 4.0.* Procedia Manufacturing, 11, 545-554.

Dimase, D., Collier, Z. A., Heffner, K., et al. (2015). *Systems engineering framework for cyber physical security and resilience.* Environ Syst Decis 35**,** 291–300.

Dolgui, A, Ivanov, D., Sethi, S. P., & Sokolov, B. (2019). *Scheduling in production, supply chain and Industry 4.0 systems by optimal control: fundamentals, state-of-the-art and applications.* International Journal of Production Research, 57:2, 411-432.

Drinkwater, D. (2016). *Does a data breach really affect your firm's reputation?* http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-reallyaffect-your-firm-s-reputation.html

Economia, Tecnologia. (2020). *Megavazamento de dados de 223 milhões de brasileiros.* https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml

European Union Agency for Network and Information Security (ENISA). (2018). *Good Practice for Security of Internet of Things in the Context of Smart Manu-facturing***,** ENISA.

Feng, F. et al. (2015). *Visualization and quantitative study in bibliographic databases: a case in the field of university–industry cooperation*. Journal of informetrics, 9(1), 118-134.

Fisher. R. (2004). *Supervisory Control and Data Acquisition (SCADA) Systems White Paper.* Prepared by Argonne National Laboratory for DPO.

Frost, & Sullivan. (2017). *Cyber Security in the Era of Industrial IoT.* Frost & Sullivan White Paper, Germany.

Grácio, M. M. C., & Garrutti, É. A. (2005). *Estatística aplicada à educação: uma análise de conteúdos programáticos de planos de ensino de livros didáticos.* Revista de Matemática e Estatística, São Paulo, 23(3), 107-126, abr.

Gerbert, P., Lorenz, M., Rügmann, M., Waldner, M., Justus, J., Hengel, P., & Harnisch, M. (2015). *Industry 4.0: the future of productivity growth in manufacturing industries.* Munich: The Boston Consulting Group.

Gil, A. C. (2010). *Como elaborar projetos de pesquisa.* (5a. ed.), Atlas.

Goldman, G. H. (2010). *Building Secure, Resilient Architectures for Cyber Mission Assurance*: The MITRE Corporation, #10-3301. https://www.mitre.org/sites/default/files/pdf/10_3301.pdf

Greitzer, F. L., J., Purl, Y. M., & Leong P. J. S. (2019). *Positioning your organization to respond to insider threats.* IEEE Engineering Management Review, 47(2), 75–83.

Guedes, V. F. S. (2012). *A bibliometria e a gestão da informação e do conhecimento científico e tecnológico: uma revisão da literatura.* Ponto de Acesso, Salvador, 6(2), 74-109.

Guedes, V. F. S., & Borschiver, S. (2005). *Bibliometria: uma ferramenta estatística para a gestão da informação e do conhecimento, em sistemas de informação, de comunicação e de avaliação cientifica e tecnológica.* In: Encontro Nacional de Ciências da Informação (CINFORM), 6, Salvador, Anais do VI Encontro Nacional de Ciências da Informação, Salvador, UFBA.

Guoping, L., Yun, H., & Aizhi, W. (2017). *Fourth Industrial Revolution: Technological Drivers, Impacts and Coping Methods.* Chinese Geographic Science, 27(4), 626-637.

Hollnagel, E. (2013). *A tale of two safeties.* Nuclear Safety and Simulation, 4(1), Mar.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts.* Aldershot: Ashgate.

Huang, J., Kong, L., Chen, G., Wu, M., Liu, X., & Zeng, P. (2019). *Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism.* IEEE Transactions on Industrial Informatics, 15(6), 3680-3689.

Industrial Control Systems Cyber Emergency Response Team. (2016). ICS-CERT. *Annual Assessment Report.* National Cybersecurity and Communications Integration Center (NCCIC).

International Society of Automation – ISA. (2016). North Carolina. *The 62443 Series of Standards***,** ISA.

Ismail, H. S., Poolton, J., & Sharifi, H. (2011). *The role of agile strategic capabilities in achieving resilience in manufacturing-based small companies.* International Journal of Production Research, Taylor & Francis Group, pp. 5469–5487.

Ivanov, D., Dolgui, A., & Sokolov, B. (2019***).*** *The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics.* International Journal of Production Research, 57(3), 829-846.

Ivanov, D., & Dolgui, A. (2020). *A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0.* Production Planning & Control.

Jamai, I., Ben Azzouz, L., & Saïdane, L. A. (2020). *Security issues in Industry 4.0.* International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 2020, 481-488.

Januario, F., Carvalho, C., Cardoso, A., & Gil, P. (2016). *Security challenges in SCADA systems over wireless sensor and actuator networks.* International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops.

Kagermann H., Wahlster, W., & Helbig, J. (2013). *Recommendations for implementing the strategic initiative Industrie 4.0*, Final report of the Industrie 4.0 Working Group, 1-84.

Kaplan J., Weinberg, A., & Sharma, S. (2011). *Meeting the cybersecurity challenge.* Digit. McKinsey.

Khan, A., & Turowski, K. A. (2016). *Perspective on Industry 4.0: From Challenges to Opportunities in Production Systems.* In: Proceedings of The International Conference on Internet of Things and Big Data – IoTBD, Rome: IoTBD, 441-448.

Kobara, K. (2016). *Cyber physical security for industrial control systems and IoT.* IEICE Trans. Inf. Syst. E99D (4), 787–795.

Lebrun, J. L. (2007). *Scientific writing: A reader and a writer's guide*: World Scientific.

Lee, J., Jin, C., & Bagheri, B. (2017). *Cyber physical systems for predictive production systems.* Production Engineering.

Leveson, N. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety.* MIT press.

Lezzi, M., Lazoi, M., & Corallo, A. (2018). *Cybersecurity for Industry 4.0 in the current literature: a reference framework.* Computers in Industry, 103, 97–110.

Liu, Y., & Xu, X. (2017). *Industry 4.0 and cloud manufacturing: A comparative analysis.* Journal of Manufacturing Science and Engineering, 139(3), 034701.

Lu, T., Lin J., Zhao, L., Li, Y., & Peng, Y. (2015). *A security architecture in cyberphysical systems: security theories, analysis simulation and application fields.* Int J Secur Appl; 9(7):1–16.

Lu, T., Xu, B., Guo, X., Zhao, L., & Xie F. (2013). *A new multilevel framework for cyber-physical system security***,** 2–3.

Mahmoud, R., Yousuf, T., Aloul, F. & Zualkernan, I. (2015). *Internet of things (IoT) security: Current status, challenges and prospective measures.* 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, 336-341.

Mandarino, J. R. (2010). *Segurança e defesa do espaço cibernético brasileiro.* Recife, Cubzac.

Marcelo, J. F., & Hayashi, M. C. P. I. (2013). *Estudo bibliométrico sobre a produção científica da área da sociologia da ciência*; Estudio bibliométrico en la producción científica del campo de la sociología de la ciencia. Informação & Informação, 18(3), 138.

Morisse, M., & Prigge, C. (2017). *Design of a Business Resilience Model for Industry 4.0 Manufacturers.* Twenty-third Americas Conference on Information Systems, Boston, AMCIS.

Mosterman, P. J., & Zander J. (2015). *Industry 4.0 as a Cyber-Physical System study.* Springer-Verlag, 15, 17-29.

Mugnaini, R. (2003). *A bibliometria na exploração de bases de dados: a importância da Linguística.* TransInformação. 15. 45-52.

National Security & Defense. (2020). *Memorandum on Space Policy Directive 5 – Cybersecurity.* https://www.whitehouse.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* National Institute of Standards and Technology.

Oliveira, S. C. M., et al. (2013). *Bibliometria em artigos de contabilidade aplicada ao setor público.* In: Congresso Brasileiro de Custos, 20., Uberlândia. Anais: Associação Brasileira de Custos.

Parrot, A., & Warshaw, L. (2017). *Industry 4.0 and the digital twin: Manufacturing meets its match.* Copyright© Deloitte Insights.

Presidência da República. Gabinete de Segurança Institucional. *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018*, versão 1.0 / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. Brasília.

Pereira, A. S., Shitsuka, D. M., Parreira, F. J., & Shitsuka, R. (2018). *Metodologia da pesquisa científica.* UFSM. https://repositorio.ufsm.br/bitstream/handle/1/15824/Lic_Computacao_Metodologia-Pesquisa-Cientifica.pdf?sequence=1

Plano de CT&I para Manufatura Avançada no Brasil. (2017). *PROFUTURO.* Ministério da Ciência, Tecnologia e Inovações. https://www.mctic.gov.br/mctic/export/sites/institucional/tecnologia/tecnologias_convergentes/arquivos/Cartilha-Plano-de-CTI_WEB.pdf

Radanliev, P., De Roure, D., Nurse, J. R., Nicolescu, R., Huth, H., Cannady, S., & Montalvo, R. M. (2018). *Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0.* In: Livingin the Internet of Things: Cybersecurity of the IoT - 2018, London.

Richardson, R. J. (1999). *Pesquisa social: métodos e técnicas*: Atlas.

Rodrigues, R. S., Quartiero, E., & Neubert, P. (2015). *Periódicos científicos brasileiros indexados na Web of Science e Scopus: estrutura editorial e elementos básicos.* Informação & Sociedade: Estudos, 25(2), 138.

Roy, R., Stark, R., Tracht, K., Takata, S., & Mori, M. (2016). *Continuous maintenance and the future – Foundations and technological challenges.* CIRP Annals, 65(2), 667-688, ISSN 0007-8506.

Schuh, G., Anderl, R., Dumitrescu, R., Krüger, A., & Ten Hompel, M. (2020). (Eds.): *Industrie 4.0 Maturity Index.* Managing the Digital Transformation of Companies – UPDATE 2020 – (Acatech STUDY), Munich.

Schumacher, A., Erol, S. & Sihn, W. (2016). *A Maturity Model for Assessing Industry 4.0 Readiness and Maturity of Manufacturing Enterprises.* Procedia CIRP, 52, 161-166, ISSN 2212-8271.

Schwab, K. (2016). *A Quarta Revolução Industrial.* Tradução: Daniel Moreira Miranda, EDIPRO.

Shaabany, G., & Anderl, R. (2018). *Security by Design as an Approach to Design a Secure Industry 4.0-Capable Machine Enabling Online-Trading of Technology Data*. International Conference on System Science and Engineering (ICSSE), New Taipei, 1-5.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security.* National Institute of Standard and Technology (NIST).

Tao, F., Qi, Q., Wang, L., & Nee, A.Y.C. (2019). *Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison.* Engineering.

Theron, P., & Lazari, A. (2018). *The IACS Cybersecurity Certification Framework (ICCF).* Lessons from the 2017 study of the state of the art., EUR 29237 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-79-85968-7, 10.2760/856808, JRC111611.

Tuptuk, N., & Hailes, S. (2018). *Security of smart manufacturing systems.* J. Manuf. Syst.47, 93–106.

U.S. Department of Homeland Security – DHS. (2011). *Catalog of Control System Security: Recommendations for Standards Developers.* Homeland Security.

Vanti, N. A. P. (2002). *Da bibliometria à webometria: uma exploração conceitual dos mecanismos utilizados para medir o registro da informação e a difusão do conhecimento.* Ciência da Informação, Brasília, 31(2), 369-379, maio/ago.

Wang, L., & Wang, G. (2016). *Big data in cyber-physical systems, digital manufacturing and Industry 4.0.* International Journal of Engineering and Manufacturing (IJEM), 6(4), 1-8.

Waslo, R., Lewis, T., Hajj, R., & Carton, R. (2017). *Industry 4.0 and Cybersecurity. Man-aging Risk in an Age of Connected Production.* Deloitte University Press.

Weber, R. H., & Studer, E. (2016). *Cybersecurity in the internet of things: legal aspects.* Comput Law Secur Rev 32:715–728.

Woods, D. (2003). *Creating foresight: how resilience engineering can transform NASA's approach to risky decision making.* Testimony on the future of NASA for Committee on Commerce, Science and Transportation. John McCain, Chair; 29 October.

Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P. & Fu, X. (2018). *Cybersecurity for digital manufacturing*. J. Manuf. Syst. 48, 3–12.

Zalewski, J., Drager, S., Mckeever W., & Kornecki, A. J. (2013). *Threat modeling for security assessment in cyber physical systems.* Proc. Eighth Annual. Cyber Security. Inf. Intell. Res. Work. - CSIIRW '13, p. 1.

Zhu, Q., Craig, R., & Basar, T. (2011). *A hierarchical security architecture for cyber-physical systems.* In: 2011 4th International Symposium on Resilient Control Systems, Boise, ID, USA.