UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS

DEPARTAMENTO DE CIÊNCIA POLÍTICA

JÚLIA COSTA AMANCIO SANTOS CORIOLANO

CIBERSEGURANÇA E ESTABILIDADE ESTRATÉGICA: UMA REVISÃO SISTEMÁTICA DA LITERATURA

RECIFE

2024

UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS

DEPARTAMENTO DE CIÊNCIA POLÍTICA

JÚLIA COSTA AMANCIO SANTOS CORIOLANO

CIBERSEGURANÇA E ESTABILIDADE ESTRATÉGICA: UMA REVISÃO SISTEMÁTICA DA LITERATURA

TCC apresentado ao Bacharelado em Ciência Política da Universidade Federal de Pernambuco, Centro Acadêmico de Recife, como requisito parcial para a obtenção do título de Bacharel em Ciência Política.

Orientador(a): Profº. Dr. Marcos Aurélio Guedes de Oliveira
Coorientador(a): Profº. Dr. Dalson Britto Figueiredo Filho

RECIFE

2024

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Coriolano, Júlia Costa Amancio Santos.
Cibersegurança e estabilidade estratégica: uma revisão sistemática da literatura / Júlia Costa Amancio Santos Coriolano. - Recife, 2024.
56 p. : il.

Orientador(a): Marcos Aurélio Guedes de Oliveira
Cooorientador(a): Dalson Britto Figueiredo Filho
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Filosofia e Ciências Humanas, Ciência Política, 2024.
Inclui referências.

1. Cibersegurança. 2. Ciberataque. 3. Dissuasão nuclear. 4. Estabilidade estratégica. 5. Revisão sistemática. I. Oliveira, Marcos Aurélio Guedes de. (Orientação). II. Filho, Dalson Britto Figueiredo. (Coorientação). IV. Título.

320 CDD (22.ed.)

JÚLIA COSTA AMANCIO SANTOS CORIOLANO

CIBERSEGURANÇA E ESTABILIDADE ESTRATÉGICA: UMA REVISÃO SISTEMÁTICA DA LITERATURA

TCC apresentado ao Bacharelado em Ciência Política da Universidade Federal de Pernambuco, Centro Acadêmico de Recife, como requisito parcial para a obtenção do título de Bacharel em Ciência Política.

Aprovado em: 08 / 03 / 2024.

BANCA EXAMINADORA

_____
Profº. Dr. Marcos Aurélio Guedes de Oliveira (Orientador)
Universidade Federal de Pernambuco

_____
Profª. Drª. Graciela de Conti Pagliari (Examinadora Externa)
Universidade Federal de Santa Catarina

_____
Profª. Drª. Thays Felipe David de Oliveira (Examinadora Externa)
Universidade Federal da Paraíba

AGRADECIMENTOS

Primeiramente, toda honra e glória a DEUS, por ser o meu principal suporte, pelas bênçãos, e provisão em minha vida. Agradeço à Ele pela saúde, família, e vida que eu tenho, e portas abertas nestes últimos anos. A bondade dEle me acompanha a todo instante.

Em segundo, à minha mãe, Luana, e minha avó, Clélia, por todo o apoio e esforços envolvidos em minha criação. Agradeço profundamente por sempre terem me proporcionado uma educação de qualidade, pelos incentivos em meus estudos, e pelas motivações para ir atrás dos meus sonhos. Mãe, eu admiro muito a sua personalidade forte e resiliente. Obrigada por ser o meu maior apoio, e por me ensinar que "todas as coisas cooperam para o bem daqueles que amam a DEUS" (Romanos 8:28); sempre guardarei este ensinamento.

Ao meu tio, Alexandre, que me deu suporte durante todo o período que estive em Recife. Aos meus amigos de graduação, Isabela, Eveline, Jayane, José, Luciano, e Rebeca. Os meus anos de faculdade se tornaram muito mais leves e divertidos com a presença e amizade de todos vocês. Ao Renato Lira Brito, pelo apoio e incentivos para oportunidades acadêmicas.

Ao meu pai, por suas orações. Ao meu grande amigo de longa data, Flávio Roberto, pela companhia e amizade durante os anos de escola e de faculdade, apesar da distância física. Obrigada pela valiosa amizade, debates instigantes e conselhos frutíferos. A sua atenção e respeito extremos em nossas conversas são ímpares. Admiro muito a sua pessoa.

Ao meu orientador, professor Marcos Guedes, pelos *insights* para o meu trabalho de conclusão de curso, e por me mostrar o mundo acadêmico de cibersegurança, pelo qual me identifiquei bastante, resultando em meu desejo em seguir carreira na área. Ao meu professor e co-orientador Dalson Figueiredo, pelas oportunidades acadêmicas e profissionais no decorrer dos anos, pelo aperfeiçoamento deste trabalho, e pelos incentivos para aprender programação e ciência de dados, algo que fará total diferença em meu futuro profissional.

À professora Nara Pavão, pelas aulas de Comportamento Político e oportunidade de monitoria nesta disciplina, duas experiências muito enriquecedoras e fascinantes. Ao professor Adriano Oliveira, por me mostrar o quão incríveis são pesquisas de mercado, e por ter contribuído para a minha primeira experiência de estágio, da qual guardo muito carinho e aprendizados. Obrigada a Beninho, por me deixar sempre à vontade para usar o cantinho de estudos do seu estúdio de treino. Por último, mas não menos importante, agradeço aos meus quatro lindos gatinhos, que sempre me fazem companhia e alegram o meu dia; amo vocês.

RESUMO

Qual a relação entre cibersegurança e estabilidade estratégica? A partir de uma amostra de 40 trabalhos publicados entre 2010 e 2023, esta monografia apresenta uma revisão sistemática da literatura com o objetivo de entender como tópicos específicos de cibersegurança se relacionam com o equilíbrio nuclear, no geral, e os incentivos para mantê-lo. Em particular, examinamos quatro aspectos substantivos da produção científica sobre o tema, com ênfase em vulnerabilidades cibernéticas e ciberataques. A escolha do tema se justifica por dois motivos principais: a) quaisquer sistemas de computadores, inclusive os responsáveis pelo lançamento de armas nucleares, estão suscetíveis à ação e controle de *hackers*, e b) porque queremos descobrir se a literatura propõe soluções para diminuir os riscos cibernéticos que podem provocar uma escalada nuclear. Para isso, optamos pela metodologia de revisão sistemática da literatura, criando quatro variáveis substantivas (de um total de 17 gerais) para mensurar o que tem sido discutido neste campo. As principais evidências indicam que: 1) 100% da literatura está no idioma inglês, sugerindo uma prevalência do tema no hemisfério norte; 2) apenas 2,5% da amostra possui metodologia, indicando que, possivelmente, este campo de estudos é emergente e ainda exploratório; 3) a literatura concebe a retaliação nuclear a ciberataques como uma resposta desproporcional, mas um cenário provável; 4) sistemas de comando, controle e comunicações nucleares (sistemas NC3) podem ser danificados por ataques cibernéticos, o que diminui a capacidade de dissuasão nuclear e, por consequência, a estabilidade estratégica; 5) a modernização e desenvolvimento de *softwares* de sistemas nucleares precisam prezar pela simplicidade, uma vez que sistemas complexos dificultam a detecção de vulnerabilidades, piorando a sua cibersegurança, e aumentando a superfície de ciberataques; e 6) é necessário que potências nucleares firmem acordos que coíbam o emprego de operações cibernéticas ofensivas contra os sistemas de comando e controle nucleares de um país adversário, uma vez que estas comprometem a tomada de decisão, gerando confiança em dados falsos transmitidos pelos computadores – como confiar num falso alarme de ataque nuclear inimigo vindouro – ou minando a confiança na integridade dos sistemas NC3, mesmo na presença de alarmes verdadeiros. Os resultados desta pesquisa são importantes para fundamentar outros estudos sobre o tema, e podem ser úteis para subsidiar decisões governamentais sobre o papel da cibersegurança como instrumento estratégico de defesa.

Palavras-chave: cibersegurança; ciberataque; dissuasão nuclear; estabilidade estratégica; revisão sistemática

ABSTRACT

How cybersecurity relates to strategic stability? From a sample of 40 works published between 2010 and 2023, this monograph presents a literature systematic review with the purpose to understand how specific cybersecurity topics relate to nuclear stability, broadly speaking, and the incentives to maintain it. In particular, we examine four substantive aspects from the scientific production on the topic, with an emphasis on cyber vulnerabilities and cyber attacks. The choice for the topic is justified for two main reasons: a) any computer systems, including those responsible for nuclear weapons' launching, are susceptible to the action and control of hackers, and b) because we want to find out whether the literature proposes solutions to reduce cyber risks that could lead to nuclear escalation. To achieve this, we opted for the systematic review of the literature methodology, creating four substantive variables (out of a total of 17) to measure what has been discussed in this field. The main evidences indicates that: 1) 100% of the literature is in English, suggesting a high prevalence of the topic in the Northern Hemisphere; 2) only 2,5% of the sample has methodology, indicating that the field of study is probably emergent and still exploratory; 3) the literature conceives nuclear retaliation to cyberattacks as a disproportionate response, but a likely scenario; 4) nuclear command, control and communications systems (known as NC3) can be damaged by cyber attacks, which reduces nuclear deterrence capacity and consequently, strategic stability; 5) the modernization and development of nuclear systems software needs to focus on simplicity, since complex systems make it difficult to detect vulnerabilities, worsening their cybersecurity, and increasing the surface area for cyberattacks; and 6) it is necessary for nuclear powers to sign agreements that prohibit the use of offensive cyber operations against nuclear command and control systems of adversary countries, as these compromise decision-making, resulting in confidence in false data transmitted by computers – such as believing in a false alarm of an incoming enemy nuclear attack – or undermining confidence in the integrity of NC3 systems, even if they display true warning messages. The results of this research are important to support other studies on the topic, and might be useful to support government decisions on the role of cybersecurity as a strategic defense tool.

Keywords: cybersecurity; cyberattack; nuclear deterrence; strategic stability; systematic review.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

O objetivo deste trabalho é apresentar uma revisão sistemática da produção acadêmica que relaciona cibersegurança com estabilidade estratégica, um tema amplamente explorado por autores do norte global, das relações internacionais, mas ainda inédito na literatura brasileira. Resumidamente, e em termos substantivos, os estudiosos têm relacionado aspectos específicos da cibersegurança – como ciberataques aos sistemas de comando, controle e comunicações nucleares (NC3) – e os seus impactos sobre os riscos de uma escalada nuclear – que pode se dar por meio do comprometimento desses sistemas, facilitando lançamentos não-autorizados de mísseis, ou motivando a retaliação nuclear por preempção.

Para além dos ciberataques, os acadêmicos reconhecem que, se exploradas por atores maliciosos, as vulnerabilidades de segurança intrínsecas aos sistemas NC3 – principalmente os sistemas modernizados – são capazes de minar a capacidade de dissuasão nuclear – o que, por consequência, diminui a estabilidade estratégica. As quatro variáveis substantivas avaliam como outras relações são feitas pelos estudiosos da área.

As buscas foram feitas em janeiro de 2024, e o recorte temporal é de 2010 a 2023, pois 2010 foi o ano em que ocorreu o Caso Stuxnet, um *malware* que gerou o mal funcionamento das centrífugas de uma usina nuclear em Natanz, no Irã. O *worm* Stuxnet foi considerado uma das armas cibernéticas mais sofisticadas e, segundo Shoaib (sem ano), possivelmente, o primeiro caso de guerra eletrônica.

Em termos metodológicos, o desenho de pesquisa reproduz as sete etapas sugeridas por Cooper (2010) para a condução de uma revisão sistemática: (1) formular o problema ou questão de pesquisa, (2) pesquisar pela literatura, (3) coletar as informações sobre os estudos, (4) avaliar a qualidade dos trabalhos, (5) analisar os seus resultados, (6) interpretar os resultados, e (7) apresentar as conclusões. Além disso, uma minoria dos artigos sul-americanos publicados, no campo das Relações Internacionais, explicita o seu método de pesquisa (ALBUQUERQUE, MESQUITA, LIRA-BRITO. 2022) revelando uma "obscuridade metodológica". Portanto, optamos pela revisão sistemática por, pelo menos, três razões.

A primeira razão é (1) difusão da metodologia, raramente adotada por acadêmicos internacionalistas; a segunda, (2) compensação da falta de clareza metodológica nas Relações Internacionais; por fim, a terceira (3) é sistematizar os achados da literatura que relaciona cibersegurança com estabilidade estratégica, que, salvo melhor juízo, ainda não possui uma revisão sistemática, conforme as pesquisas feitas no *Publish or Perish* (PoP) com as palavras-chave "cibersegurança", "estabilidade estratégica", "dissuasão nuclear" e "revisão sistemática", em inglês e em português.

2. JUSTIFICATIVA TEÓRICA

O presente trabalho justifica-se pela premissa teórica de que ameaças cibernéticas podem gerar consequências indesejáveis para a segurança global, conforme o relatório de 2018 do *Nuclear Threat Initiative* (NTI). A partir desta premissa, justificamos a necessidade de compilar, sistematicamente, as principais discussões da literatura, a fim de descobrir como uma escalada nuclear pode ocorrer a partir de interferências cibernéticas, e o que podemos fazer para evitar este cenário.

O referido relatório do NTI traz algumas recomendações, e alerta para o aumento do risco de uso de armas nucleares, devido ao surgimento de ameaças cibernéticas, além de apontar para as consequências de um ciberataque num sistema NC3. É importante salientar que a natureza da ameaça cibernética não se restringe ao *hacking* de sistemas e o roubo de informações, mas envolve, também, o comprometimento dos computadores e segurança da informação (Futter, 2016a).

Avin e Amadae (2019, p. 12) reconhecem a cibersegurança como "um grave desafio para a credibilidade de dissuasão nuclear de um país". Shoaib (2018), por sua vez, demonstra claramente a intersecção entre as duas variáveis presentes no título deste artigo: "as ameaças cibernéticas, dentro do domínio nuclear, podem ser estudadas em dois níveis: (1) a segurança das armas nucleares e suas instalações, e (2) ameaças à estabilidade estratégica" (p. 31).

Sistemas de comando e controle nucleares possuem vulnerabilidades de segurança que podem ser exploradas por *hackers* (FUTTER, 2018). Muitos dos artigos acadêmicos e relatórios governamentais que avaliam a interação entre cibersegurança, armas nucleares, e estabilidade estratégica alertam para a suscetibilidade desses sistemas à invasões (SCHNEIDER; SCHECHTER; SHAFFER, 2023; SHOAIB, 2018; FUTTER, 2016; VELEZ-GREEN; HOROWITZ; SCHARRE, 2019; HOROWITZ; SCHARRE, 2019).

Países como China, Rússia, Coreia do Norte e Estados Unidos desenvolveram programas de ataque aos sistemas de comando nucleares de outros países, com o objetivo de implantar vírus e "desabilitar, confundir, e atrasar o comando nuclear e os processos de avisos", conforme o *Global Zero Commission for Nuclear Risk* (2015, p. 30), o qual referencia as estimativas de Herbert (2005). Portanto, o risco de ciberataques aos sistemas de comando e controle nucleares não é apenas uma construção teórica, mas uma realidade em potencial.

Segundo Futter (2015), ao considerarmos o número de acidentes nucleares, assume-se que *hackers* já tenham interferido em sistemas dessa categoria num passado recente – não somente nos Estados Unidos, mas em outras potências que possuem essas armas de destruição em massa. Para o autor, ameaças cibernéticas – incluindo ciberataques aos sistemas de

comando, controle, e comunicações – podem impactar a relação nuclear entre as potências que possuem este arsenal – como a Rússia e os Estados Unidos. As consequências desse tipo de atividade cibernética serão exploradas na seção de resultados.

Poucos são os ciberataques que causaram destruição física e que sejam publicamente conhecidos; o Stuxnet é um deles, danificando uma instalação nuclear do Irã (FUTTER, 2016a). É provável que o *worm* tenha acessado o sistema – não conectado às redes externas – através de um drive USB infectado ou similar, atrasando o desenvolvimento de uma possível bomba nuclear iraniana, e mostrando ser possível infectar e danificar sistemas físicos separados da internet, *hackeando* os computadores e redes que os controlam (SHOAIB, 2018).

Segundo Futter (2016a), embora haja poucos casos de ciberataques que tenham causado grandes danos – como o Stuxnet – existe um potencial para essas atividades aumentarem no futuro – inclusive, em sistemas nucleares. Em suma, a literatura aponta que invadir sistemas NC3, e não somente os outros tipos de infraestruturas críticas, pode diminuir a estabilidade estratégica – conforme veremos nos achados.

3. CONCEITOS

Nos próximos parágrafos, conceituamos os termos mais recorrentes nos trabalhos que constituem a amostra da revisão sistemática, a fim de contextualizar para um leitor possivelmente leigo no assunto.

Segundo a empresa russa de desenvolvimento de *softwares* de segurança, *Kaspersky*, a cibersegurança[1] é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos. Ao mesmo tempo, cibersegurança não é meramente um campo da computação, se tornando, também, um dos mais significantes campos para acadêmicos das Relações Internacionais, uma vez que ameaças cibernéticas são críticas para a agenda internacional (VALERIANO; MANESS, 2018), especialmente por serem capazes de gerar crises diplomáticas (VELEZ-GREEN; HOROWITZ; SCHARRE, 2019).

Ciberataques[2] são tentativas de roubar, expor, modificar, desativar ou destruir ativos de terceiros por meio de acesso não autorizado a sistemas de computador, conforme a *International Business Machines Corporation* – a IBM; as motivações por trás desses ataques variam, mas se dividem em três categorias principais: criminoso, pessoal e político.

Ciberataques representam ameaças que vão desde à espionagem dos sistemas nucleares, até à sabotagem ou risco de uso não-autorizado dessas armas (SHOAIB, 2018). Termos como "guerra cibernética" (SHOAIB, 2018), "capacidades cibernéticas ofensivas", "armas cibernéticas ofensivas", e até "operações cibernéticas ofensivas" abarcam ciberataques e, para os fins deste trabalho, assumimos que podem ser interpretadas diretamente como tal – por exemplo, se seguirmos as definições legais de Johnson (2019), ou Hanson e Uren (2018), conforme a seguir.

Há certas definições legais de operações cibernéticas ofensivas, como *hacking*, *data-poisoning attacks*, e *spoofing* (JOHNSON, 2019). Essas operações são atividades conduzidas no ciberespaço que "manipulam, perturbam, degradam, ou destroem alvos como computadores, sistemas da informação, ou redes" (HANSON; UREN, 2018, p. 6).

Cyber Warfare[3] – ou guerra cibernética – é normalmente definido como um ciberataque ou uma série de ataques direcionados a um país, com o potencial de comprometer sistemas críticos (Imperva). Dentre os tipos de sistemas críticos, estão os sistemas de comando e controle nucleares. Rautenbach (2019) traz que *cyberwar* é o meio pelo qual se reduz a efetividade de combate do oponente, distorcendo a informação e fragmentos de seus sistemas

[1] https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security. Acesso em 3 de março de 2024.
[2] https://www.ibm.com/br-pt/topics/cyber-attack. Acesso em 3 março de 2024.
[3] https://www.imperva.com/learn/application-security/cyber-warfare/. Acesso em 3 março de 2024.

de comando e controle (TIMOTHY, 2014 *apud* RAUTENBACH, 2014, p. 103).

Dissuasão nuclear[4] (em inglês, *nuclear deterrence*), também conhecida como teoria da intimidação, refere-se ao princípio das relações internacionais onde a força destrutiva das armas nucleares é capaz de prevenir outras nações de lançar um ataque nuclear, conforme o *Carnegie Council for Ethics in International Affairs*. Dissuasão nuclear mantém a estabilidade estratégica uma vez que, se aquela é prejudicada, esta também é (KLARE, 2019).

A dissuasão depende da certeza de que um agressor será retaliado com uma resposta grande o suficiente para que ele não obtenha quaisquer ganhos (RAUTENBACH, 2019). A estabilidade estratégica (em inglês, *strategic stability*), por sua vez, consiste na falta de incentivos de se lançar o primeiro ataque nuclear (KUMAR, 2023).

[4] https://www.carnegiecouncil.org/explore-engage/key-terms/nuclear-deterrence. Acesso em 3 março de 2024.

4. METODOLOGIA

Uma revisão sistemática identifica, avalia e sintetiza todas as evidências empíricas que atendem a critérios de elegibilidade pré-especificados para responder uma questão de pesquisa (Colaboração Cochrane[5]). Esta rigorosidade minimiza os vieses de seleção, e promove achados mais confiáveis para a tomada de decisões.

Portanto, escolhemos essa metodologia porque ela promove clareza e rigor de método, além de reduzir o potencial de viés de uma revisão da literatura (PAPAIOANNOU; SUTTON; BOOTH, 2016), e facilitar a reprodutibilidade dos achados. Também, porque ela é um método reproduzível, capaz de sintetizar os estudos feitos por pesquisadores (FINK, 2005), e o melhor conjunto de evidências possível sobre determinado tópico, conforme a pirâmide da qualidade hierárquica de evidências, comumente adotada entre pesquisas na área de saúde.

Figura 1 – Pirâmide hierárquica de evidências

Pirâmide da hierarquia de evidências (YETLEY *et al*, 2016). Acesso em 16 de fevereiro de 2024.

Também, optamos pela revisão sistemática porque cientistas políticos tendem a ignorar ou marginalizar este método (DACOMBE, 2017), ainda que sejam os trabalhos que melhor sintetizam, criteriosamente, o estado da literatura de um campo do conhecimento. Ainda, "revisar sistematicamente e integrar a literatura de um campo pode ser considerado um tipo de pesquisa em si mesmo – usando um característico conjunto de técnicas de pesquisa e métodos" (FELDMAN, 1971).

No geral, uma revisão da literatura – ainda mais a sistemática – contribui para entender

[5] https://www.cochranelibrary.com/about/about-cochrane-reviews. Acesso em 3 março de 2024.

o tema sob análise, identificar lacunas em pesquisas prévias, e descobrir o que já foi abordado por outros pesquisadores, a fim de evitarmos a duplicação dos seus esforços (PAPAIOANNOU; SUTTON; BOOTH, 2016). O Quadro 1 descreve as principais características do desenho de pesquisa.

Quadro 1 – Desenho de Pesquisa

Pergunta de Pesquisa	Como a literatura tem estudado a relação entre cibersegurança e estabilidade estratégica?
Metodologia	Revisão sistemática da literatura
Palavras-chave utilizadas nas buscas	cibersegurança AND estabilidade estratégica AND dissuasão nuclear (em inglês e em português)
Objetivo geral	Descrever o estado da literatura que traz uma relação entre cibersegurança e estabilidade estratégica
Objetivos específicos	(1) Criar variáveis que identificam a frequência de blocos temáticos que relacionam cibersegurança e estabilidade estratégica (2) Descrever, a partir desses blocos temáticos, a forma como se dá a interação entre tópicos de cibersegurança e estabilidade estratégica (3) Descobrir se a literatura propõe boas práticas ou outras recomendações a fim de mitigar riscos de cibersegurança que possam diminuir a estabilidade estratégica
Justificativas teóricas	(1) A premissa de que ameaças cibernéticas podem gerar consequências indesejáveis para a estabilidade estratégica, ou equilíbrio nuclear, conforme alertas de relatórios governamentais e de institutos de pesquisa (2) A capacidade de risco ambiental, bem como de risco existencial à humanidade, em decorrência do emprego de armas nucleares (3) Necessidade de uma compilação de boas práticas e recomendações que fomentem a cibersegurança de infraestruturas críticas, como as de comando e controle de armas nucleares (4) Falta de estudos em língua portuguesa, na área
Unidade de Análise	Artigos (publicados e *grey literature*), relatórios e *proceedings* (atas de conferência)

Delimitação Temporal	2010 - 2023 (devido ao Caso *Stuxnet*, de 2010)
Técnica	Estatística Descritiva
Fontes	*Google Scholar*
Softwares	*Google Planilhas, Harzing's Publish or Perish 8.9, e ChatGPT*
Repositório de Dados	*Open Science Framework (OSF)* - link para o OSF

Fonte: elaboração própria com base no modelo de Rodrigues (2023).

Os trabalhos precisam ser artigos, relatórios, e *proceedings*. Os artigos podem ser publicados em revistas, não-publicados (*grey literature*) – podendo ser de institutos de pesquisa ou *think-tanks* – ou publicados em livros que sejam uma coletânea de artigos. Os tipos de trabalhos que foram excluídos serão apresentados no Quadro 2.

Decidimos que o recorte temporal seria de 2010 a 2023, pois 2010 foi o ano em que ocorreu o Caso Stuxnet, onde um *malware* gerou o mau-funcionamento das centrífugas de uma usina nuclear em Natanz, no Irã. O incidente levantou discussões sobre a segurança de computadores industriais, e as consequências estratégicas de ciberataques – segundo Shoaib (sem ano), pode ter sido o primeiro caso de guerra eletrônica. Por isso, utilizamos esse ano como ponto de partida para as nossas consultas pelo *software Publish or Perish*.

4.1. Coleta e critérios de elegibilidade

Toda revisão sistemática constitui-se de critérios de inclusão e exclusão, uma vez que afunilar os seus critérios de inclusão reduzirá o número de estudos elegíveis (PAPAIOANNOU; SUTTON; BOOTH, 2016), nos dando menos trabalho ao analisar todos esses estudos. O Quadro 2 esquematiza os critérios de elegibilidade de nossa pesquisa.

Quadro 2 – Critérios de elegibilidade para a Revisão Sistemática

Critérios	Descrição
De inclusão	(1) Trabalhos cujos títulos combinem duas palavras-chave de interesse (2) O *abstract* precisa relacionar cibersegurança ou, pelo menos, alguma tecnologia emergente (como Inteligência Artificial) com estabilidade estratégica ou dissuasão nuclear. (3) O corpo do texto precisa estabelecer, pelo menos, uma relação entre cibersegurança e estabilidade estratégica

De exclusão	(1) Livros convencionais, artigos de jornal, *briefs*, teses, dissertações, trabalhos de conclusão de curso, monografias, resenhas de livros e bibliografia anotada, introduções à *special issues* (que são uma introdução à coleções de artigos sobre um mesmo tema) (2) Trabalhos em idiomas que não o inglês e o português (3) Trabalhos da área do Direito/Direito Internacional, Ciência da Computação, Segurança Nacional (ao invés de Segurança Internacional), sobre instalações de energia nuclear (nuclear facilities) ao invés de infraestruturas de armas nucleares (4) Trabalhos cujos títulos contenham as seguinte palavras-chave, ainda que apresentem *keywords* de interesse: stuxnet, law, treaty, agreements, norms, rules, national, national security, nuclear facility (5) Estar fora da delimitação temporal (antes de 2010 e depois de 2023)
De idiomas	Português e Inglês

Fonte: Elaborado pela autora, com base no modelo de Rodrigues (2023).

O primeiro e mais fundamental critério de inclusão é o título do trabalho apresentar uma combinação específica de, pelo menos, duas palavras-chave. Esta combinação indica se os *abstracts* e o restante do trabalho devem ser lidos ou não. Uma palavra-chave, necessariamente, precisa estar relacionada à "cibernética" (como *cyber*, ciberataque, inteligência artificial, ou operações cibernéticas). A outra, precisa estar relacionada ou às "armas nucleares" (como *command-and-control),* ou à estabilidade estratégica (como *stability*, *instability*, e *nuclear deterrence).* O Quadro 3 ilustra as possíveis combinações entre os termos frequentemente vistos na literatura que relaciona cibersegurança com estabilidade estratégica.

Quadro 3 – Lista de palavras-chave que atendem aos critérios de inclusão

Categoria de palavras-chave	Palavras-chave derivadas de cada categoria
1. Armas nucleares	arma nuclear, nuclear, NC3, comando e controle (*command-and-control*), comando, controle, e comunicações (*command, control, and communications*), *cyber-nuclear*.
2. Cibernética	ciber, cibersegurança, inteligência artificial, *autonomy* (autonomia), *machine learning*, modern*, tecno*, *information* (informação), *hybrid warfare* (guerra híbrida, pois envolve guerra cibernética), sistemas.
3. Estabilidade Estratégica	dissuasão nuclear, dissuasão, estabilidade estratégica, estabilidade, instabilidade, segurança internacional, segurança, internacional, escalada (*escalation*), dissuasão estratégica, diplomacia, política (*politics*), poder (*power*), *mutually assured*

	destruction.

Fonte: elaborado pela autora (2024).

Na ausência de duas *keywords*, de cada categoria, combinadas num mesmo título, não selecionamos o trabalho para a revisão sistemática; porque, a partir de nossas pesquisas primárias, percebemos que títulos com termos oriundos de cibernética, que estejam combinados a termos oriundos de armas nucleares, ou de estabilidade estratégica, têm grandes chances de responderem à nossa pergunta de pesquisa (do tipo exploratória).

Além disso, percebemos que existem dois tipos de palavras-chave: simples e compostas. Uma palavra-chave simples é composta de apenas um termo – como nuclear. Uma composta, por sua vez, é composta de dois – como *cyber deterrence*. *Cyber deterrence* não são duas palavras-chave separadas – isto é, *cyber* e *deterrence* – mas sim, uma única palavra-chave. Desta forma, se encontrássemos títulos com apenas *cyber deterrence* em seu nome, ou qualquer outra palavra-chave composta que não estivesse combinada com uma segunda palavra de interesse, não selecionamos o trabalho para a nossa base de dados.

Conforme o Quadro 1, utilizamos três *keywords* para realizar as consultas: cibersegurança, dissuasão nuclear, e estabilidade estratégica. No entanto, para que decidíssemos quais trabalhos incluir em nossa revisão sistemática, abrangemos a quantidade de palavras-chaves que desejamos encontrar nos títulos retornados pelo *Publish or Perish*, conforme os termos vistos no Quadro 3.

O Quadro 4 apresenta dois exemplos de títulos que combinam, pelo menos, uma palavra relacionada à cibernética, e outra relacionada à armas nucleares, ou estabilidade estratégica (seguindo o conjunto de *keywords* apresentado no Quadro 3).

Quadro 4 – Dois exemplos de títulos que combinam as palavras-chave de interesse

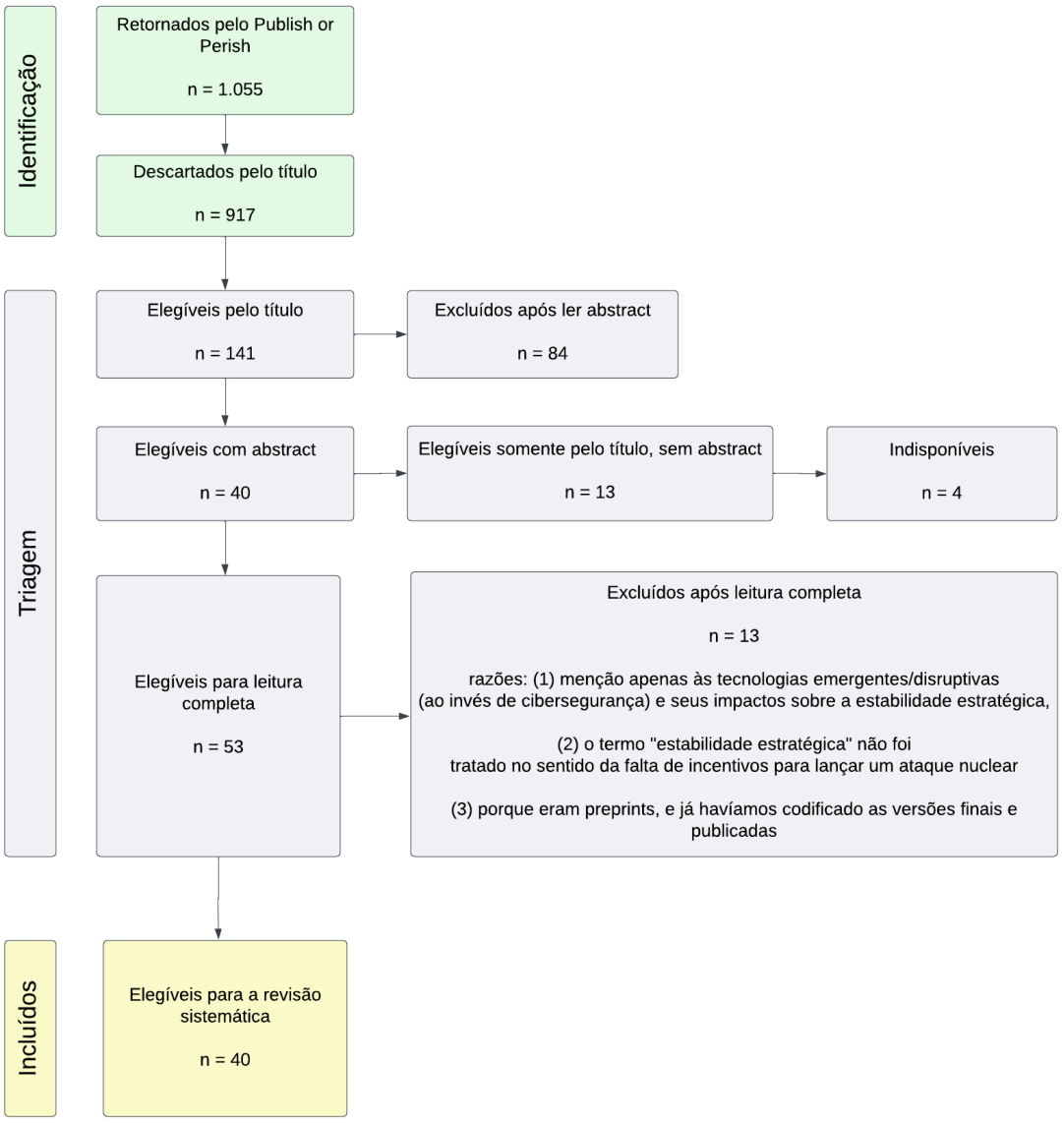
Título	Palavras-chave de interesse presentes
Thermonuclear Cyberwar	“nuclear” e “cyber”
Cyber Factors of Strategic Stability: How the Advance of AI Can Change the Global Balance of Power	“cyber” e “strategic stability”

Fonte: elaborado pela autora (2024).

A Figura 2 consiste no fluxograma PRISMA que usamos para ilustrar o número de trabalhos retornados, elegíveis e excluídos por etapa. Identificamos 1.055 trabalhos após

realizar pesquisas com as palavras-chave cibersegurança, dissuasão nuclear, e estabilidade estratégica – 1.000 retornos em inglês, e 55 em português. Restaram 40 trabalhos elegíveis para a revisão sistemática. Todos os trabalhos retornados estarão disponíveis no Google Planilhas; algumas páginas da planilha possuem os trabalhos excluídos ou selecionados por etapas (por exemplo, há uma página para os elegíveis a partir da leitura dos *abstracts*, outra para os excluídos após leitura completa, e outra para os trabalhos indisponíveis). O *link* para a planilha está presente em nosso OSF.

Figura 2 – Fluxograma PRISMA para revisões sistemáticas



Fluxograma PRISMA para revisões sistemáticas. Elaborado pela autora (2024), por meio do Lucidchart.

4.2. *Abstracts*[6]

Decidimos que não seria obrigatório que os *abstracts* tratassem sobre cibersegurança, para que os trabalhos fossem, num primeiro momento, incluídos na revisão sistemática. Porém, obrigatoriamente, os resumos precisariam tratar de, pelo menos, alguma tecnologia emergente – como Inteligência Artificial – e relacioná-la com estabilidade estratégica ou dissuasão nuclear. Isso porque, conforme pesquisas primárias, as vulnerabilidades cibernéticas

[6] Para evitarmos a repetição de termos durante o trabalho, nos referimos, ocasionalmente, a resumos como '*abstracts'*, palavras-chave como '*keywords'*, e *Publish or Perish* como 'PoP'.

são exacerbadas com a adoção dessas novas tecnologias, facilitando a ação de *hackers* que podem desestabilizar o equilíbrio nuclear. Desta forma, haveria grandes chances do artigo em questão tratar sobre ameaças cibernéticas.

Ainda, o trabalho precisaria tratar sobre operações não-cinéticas – que podem incluir ciberataques – e também relacioná-los ao equilíbrio estratégico. Por exemplo, um *abstract* que fale sobre escalada militar é insuficiente, uma vez que não revela se o artigo tratará sobre a escalada nuclear. Caso contrário, o documento era automaticamente excluído. Isto serviu para ampliar o escopo de trabalhos válidos para a revisão.

Para os trabalhos que não possuíssem resumo, sumário, ou seção de introdução, nós o incluímos na revisão sistemática antes de realizar a leitura por inteiro, uma vez que o título em si atendia aos critérios de inclusão. Caso o texto não respondesse a pelo menos uma de nossas variáveis, o excluímos, e o inserimos na base de dados de excluídos após leitura completa.

Para as situações em que o *abstract* esteve presente, o lemos para averiguar a adequabilidade do trabalho – se o documento relaciona cibersegurança com estabilidade estratégica; em caso afirmativo, demos continuidade à leitura; do contrário, excluímos com base no *abstract*. Na ausência de *abstract*, líamos a introdução ou sumário. Caso todos esses elementos de síntese do texto completo estivessem ausentes, líamos o trabalho por completo – considerando que o título, por si só, já atendia aos critérios de elegibilidade.

4.3. Variáveis

Desenvolvemos variáveis que avaliam os diversos tipos de interações cibernéticas – dentro do campo da cibersegurança – que impactam ou se relacionam com a estabilidade estratégica. Dentre essas variáveis, por exemplo, há uma que identifica se o trabalho aborda uma relação entre ciberataques e retaliação nuclear.

As nossas 17 variáveis foram divididas entre três categorias, e cada tipo foi diferenciado por meio de cores distintas (no Google Planilhas). O primeiro tipo de variável é a bibliométrica (cor vermelha). O segundo tipo é a substantiva (cor amarela), que quantifica quais trabalhos conceituaram as duas variáveis de interesse de nossa pergunta de pesquisa, também presentes no título do trabalho – cibersegurança e estabilidade estratégica – e quais abordaram determinados blocos temáticos. O terceiro tipo é a metodologia (cor verde), que avalia se o trabalho possui resumo, se o resumo possui pergunta de pesquisa, hipótese, ou metodologia; e qual a ênfase utilizada no trabalho como um todo – se quantitativa, qualitativa, ou mista. O Quadro 5 esquematiza esta tipologia.

Quadro 5 – Esquema da planilha com tipos de variáveis divididos por cores

	tipo de variável A (bibliométrica)	**tipo de variável B** (substantiva)	**tipo de variável C** (metodologia)
título do trabalho			

Fonte: elaboração da autora (2024).

No Quadro 6, temos as variáveis usadas para tabular os trabalhos retornados pelo *Publish or Perish* os quais se encaixam nos critérios de inclusão.

Quadro 6 – Variáveis bibliométricas (dimensão formal)

Ênfase	**Variáveis**	**Descrição**	**Mensuração**
Formal (bibliométricas)	ano	Indica o ano de publicação	Nominal
	n_citac	Indica o número de citações	Nominal
	tipo_trab	Indica se o trabalho é um artigo, *grey literature*, *proceedings* (atas de conferência), ou relatório	Nominal
	idioma	Indica se o trabalho foi escrito em inglês ou português	Nominal
	revista	Nome da publicação, congresso, ou instituição em que o trabalho foi apresentado ou publicado	Nominal
	sexo_autor	Sexo do primeiro autor	*Dummy* (0 = homem; 1 = mulher)

Fonte: elaboração da autora (2024).

A primeira variável bibliométrica é o ano de publicação de trabalho. A próxima, indica o número de citações do trabalho. Em seguida, temos o tipo de trabalho, se artigo, *grey literature* (quando não é publicado por alguma revista, mas um instituto de pesquisa, por exemplo); o idioma (se em inglês ou português); revista, que cita o nome do *journal* ou conferência; e, por último, o sexo do primeiro autor – consideramos a ordem em que o seu nome aparece no começo do artigo, ou se é demarcado por uma letra, a partir do nível de contribuição (por exemplo, ‘a’ é atribuído para o primeiro autor, e ‘b’ para um coautor).

No Quadro 7, temos as variáveis substantivas, que avaliam a frequência com que determinados blocos temáticos aparecem.

Quadro 7 – Variáveis substantivas (dimensão conceitual)

Substantiva (conceitual)	cybersec	Esta variável indica se o trabalho define ou conceitua *cibersegurança*	*Dummy* (1 = sim, 0 = não)
	strat	Esta variável indica se o trabalho conceitua ou define *estabilidade estratégica*	*Dummy* (1 = sim, 0 = não)
	retaliation	Indica se o trabalho discute a relação entre um ciberataque e as chances de uma retaliação nuclear pelo país sofreu o ataque	*Dummy* (1 = sim, 0 = não)
	deterrence	O trabalho discute o impacto dos ciberataques sobre a capacidade de dissuasão nuclear	*Dummy* (1 = sim, 0 = não)
	policy	Indica se o trabalho traz recomendações, boas práticas, ou políticas para se minimizar as vulnerabilidades cibernéticas, que sejam direcionadas a coibir o comprometimento da capacidade de dissuasão, uma retaliação nuclear, ou manter a estabilidade estratégica	*Dummy* (1 = sim, 0 = não)
	modern	Indica se estabelece uma relação entre cibersegurança e modernização de sistemas NC3 (*nuclear command, control and communications*), e como isso impacta a estabilidade estratégica. Pode incluir a implementação de AI nesses sistemas como parte do processo de modernização	*Dummy* (1 = sim, 0 = não)

Fonte: elaboração da autora (2024).

Dentro das seis variáveis substantivas, possuímos duas conceituais: *cybersec* – que identifica se o trabalho aborda a definição ou conceito de cibersegurança – e *strat*, se define ou conceitua estabilidade estratégica. As outras quatro variáveis identificam a ocorrência de algumas abordagens temáticas.

O primeiro tipo de abordagem é identificada pela variável *retaliation* (1), que identifica a ocorrência da relação entre ciberataques e os riscos de uma retaliação nuclear. A partir da identificação de frequência, descrevemos, na seção de resultados, a maneira como a interação é feita pela literatura – como quão plausível seria essa retaliação, bem como as circunstâncias em que ela se desencadearia – apontando a opinião dos autores desse campo de estudos.

Deterrence (2), a segunda, identifica se o documento aborda as consequências dos ciberataques sobre a capacidade de dissuasão nuclear, e como essa disrupção ocorre; pode incluir se os sistemas nucleares permanecem fornecendo informações confiáveis para

tomadores de decisão, mesmo após sofrerem um ataque cibernético; se as armas nucleares podem ser prontamente utilizadas, quando desejável; se um *hacker* é capaz de assumir o controle das armas, e causar um lançamento por vontade própria; dentre tantos outros.

Por sua vez, a terceira variável, denominada *policy* (3), identifica as boas práticas ou recomendações para se mitigar os riscos cibernéticos que podem facilitar uma escalada nuclear – seja ela intencional ou inadvertida; por fim, (4) *modern* identifica a ocorrência da relação entre cibersegurança e a modernização dos sistemas de armas nucleares, e como a junção das duas variáveis pode impactar a estabilidade estratégica; pode incluir a adoção de Inteligência Artificial como parte dessa modernização, se ela traz vulnerabilidades cibernéticas aos sistemas NC3, ou, até mesmo, se é capaz de aprimorar a sua cibersegurança.

No Quadro 8, temos as variáveis que identificam a presença de metodologia em determinadas seções dos trabalhos de nossa amostra, bem como a ênfase adotada no trabalho como um todo.

Quadro 8 – Variáveis que representam a dimensão metodológica

Metodológica	Resumo	Indica se a publicação possui resumo (*abstract*), ou se delimita uma seção visível e demarcada de sumário ou introdução	*Dummy* (1 = sim,0 = não)
	Pergunta de pesquisa	Indica se há pergunta de pesquisa no resumo ou na primeira seção do trabalho	*Dummy* (1 = sim, a pergunta está clara, 0 = caso contrário)
	Hipótese	Indica se as hipóteses estão claras no resumo ou na introdução	*Dummy* (1 = sim, as hipóteses estão claras, 0 = caso contrário)
	Metodologia	Indica se o resumo, quando presente, ou primeira parte/seção do trabalho, apresenta os métodos utilizados	*Dummy* (1 = sim, 0 = não)
	Ênfase	Descreve se o tipo de ênfase utilizada é quantitativa, qualitativa, ou multimétodo	Nominal

Fonte: elaboração da autora (2024).

A variável ‘resumo’ indica se a publicação possui resumo (*abstract*), no caso de artigos, *proceedings*, e *grey literature*, ou se delimita uma seção visível e demarcada de sumário ou introdução, no caso de relatórios. A variável ‘pergunta de pesquisa’ indica se há, pelo menos, uma pergunta de pesquisa no resumo ou na primeira seção do trabalho. A de ‘hipótese’ indica se as hipóteses estão claras no resumo, seção de introdução, sumário, ou primeira parte do trabalho, antes da primeira seção visivelmente demarcada.

A variável ‘metodologia’ precisa estar expressa no *abstract* (se presente). Na presença de *abstract* e introdução, priorizamos a ocorrência de descrição de metodologia no *abstract*. Caso haja apenas uma seção visível e demarcada de introdução (sem *abstract*), a metodologia precisa estar descrita nele. Para os casos em que não há *abstract*, sumário, ou seção demarcada de introdução, a metodologia precisa estar explícita na primeira parte do trabalho – isto é, antes da primeira seção demarcada do documento. Por fim, a variável ‘ênfase’ identifica se o trabalho é qualitativo, quantitativo, ou multimétodo.

4.4. Google Planilhas

Criamos uma base de dados com o Google Planilhas. No documento, constam os trabalhos retornados pelo *Publish or Perish*, e os excluídos por cada etapa do processo – a partir do Protocolo PRISMA. A planilha possui mais de dez páginas, dentre as quais, os que entraram na revisão sistemática, aqueles que foram excluídos, trabalhos de base teórica (não necessariamente usados neste TCC), uma literatura complementar (a qual denominamos de “base de dados secundária”, com materiais que não atendiam aos critérios de inclusão) e, por fim, uma página dedicada ao protocolo PRISMA.

Na nota de rodapé[7], disponibilizamos o seu *link* para acesso e visualização, sem a possibilidade de terceiros, não autorizados, editarem ou comentarem. Vale mencionar que, nas células em que contêm o título de um trabalho na amostra, copiamos e colamos os trechos que nos motivaram a pontuar uma variável *dummy*, ou preencher uma variável nominal.

4.5. Leitura

Para que pudéssemos agilizar a leitura dos documentos, recorremos ao recurso ‘Ctrl + F’, utilizando palavras-chave como ‘cibersegurança’, ‘*hack*’, ‘*cyberattack*’, ‘*nuclear deterrence*’, e ‘*strategic stability*’, a fim de verificar a ocorrência de variáveis – blocos temáticos – de interesse. Incluímos variantes com hífen – como ‘*cyber-security*’ e ‘*cyber-attack*’. A partir de um julgamento subjetivo, e considerando a frequência com que essas palavras apareciam em um documento, já podíamos deduzir se o trabalho em questão respondia ou não ao nosso desenho de pesquisa.

---

7 https://docs.google.com/spreadsheets/d/18zm6Jk0i2NpbRZMEocEXGukCsWXcG3JK6ZjhwdzmwDg/edit?usp=sharing

5. RESULTADOS

Esta seção apresenta os resultados da revisão sistemática conforme as três dimensões de análise: bibliométrica, substantiva e metodológica. Há 28 artigos publicados, sete não-publicados (*grey literature*), três relatórios, e dois *proceedings* (atas de conferências).

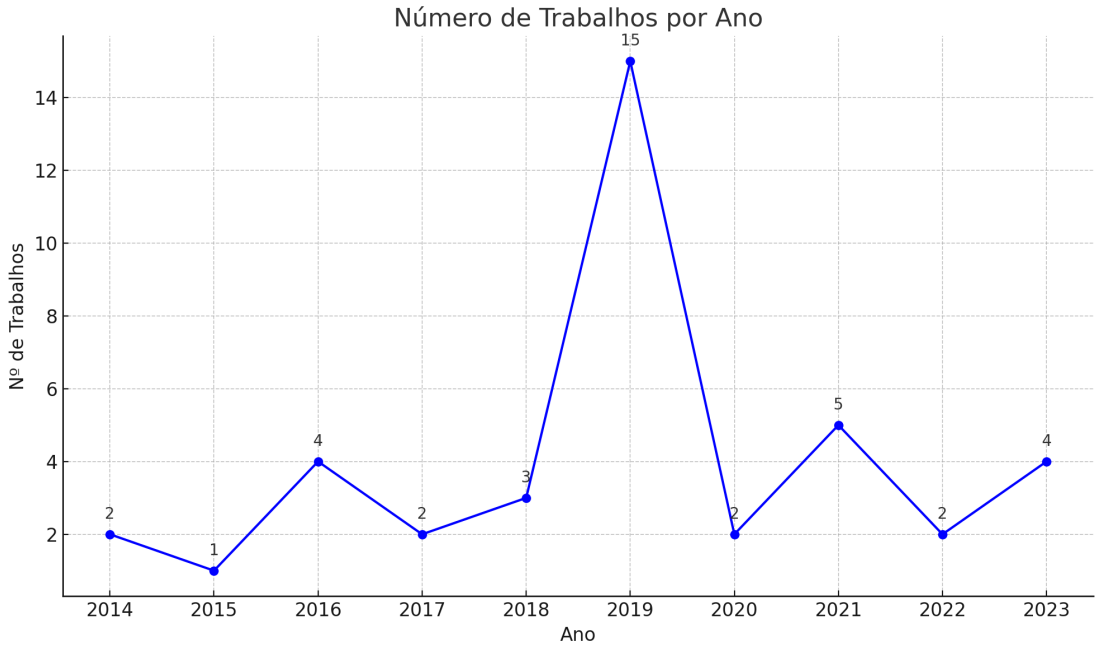
5.1. Aspecto bibliométrico

Nesta subseção, apresentamos os resultados das variáveis bibliométricas, e algumas conclusões.

5.1.1. Ano de publicação

Embora o recorte temporal tenha sido de 2010 a 2023, nossa amostra contou com trabalhos retornados apenas a partir de 2014, até 2023. O Quadro 9 mostra o número de publicações por ano.

Figura 3 – Número de trabalhos por ano de publicação



Fonte: elaboração da autora (2024), gerado pelo *ChatGPT*.

O ano com mais publicações foi 2019, com 15 títulos, e o ano com menos trabalhos foi 2015, com apenas um documento. Não está muito claro o porquê de 2019 ter retornado tantos títulos. Após realizarmos uma busca, pelo Google, com a *querie* "*cybersecurity* AND "*nuclear weapons*"", filtrando para que apareçam somente resultados de 2019, vemos que retornam

vários materiais sobre a interação entre *cyber* e nuclear, mas nada que indique uma razão em específico. Concluímos que os últimos dez anos representaram uma forte abordagem sobre o campo da cibersegurança e a sua relação com a estabilidade estratégica.

5.1.2. Citações, idioma e tipo de trabalho

O trabalho mais citado é o artigo "*Thermonuclear Cyberwar"*, de Gartzke e Lindsay (2017), com 90 citações. Nove trabalhos não possuem citações: Seis são artigos, dois são *proceedings*, e um é *grey literature*. Todos os 40 títulos de nossa amostra são em inglês, evidenciando uma forte carência de estudos em língua portuguesa sobre cibersegurança sob o contexto de dissuasão nuclear e estabilidade estratégica, e apontando para a saliência do tema no norte global. É provável que esta falta de relevância para os estudiosos e *policymakers* do Brasil seja em razão do país não possuir armas nucleares.

5.1.3. Revistas

As revistas com o maior número de aparições, em nossa revisão sistemática, foram *Survival*, *Arms Control Today*, e *Bulletin of the Atomic Scientists*, com duas aparições cada. *Survival* é uma revista de publicação bimestral sobre tópicos de política internacional e relações estratégicas. *Arms Control Today* é uma publicação mensal que provê informações e análises em propostas de controle de armas, negociações e outros tipos de acordo – inclusive sobre questões relacionadas às armas nucleares.

Por fim, o *Bulletin of the Atomic Scientists*, além de ser uma organização sem fins lucrativos da Universidade de Chicago, também publica pesquisas nos tópicos de armas nucleares e desarmamento, bem como no de tecnologias disruptivas – como as que são vistas no presente trabalho. Diante disso, vemos que todas as revistas de maior aparição, em nossa amostra de 40 trabalhos, são da área de relações internacionais; duas em especial – *Arms Control Today* e *Bulletin* – tratam, mais aprofundadamente, sobre armas nucleares.

5.1.4. Autor principal e sexo do primeiro autor

Os autores mais recorrentes foram Andrew Futter, Stephen J. Cimbala, e James Johnson – eles contaram com três trabalhos cada, todos de autoria única. Isso indica que os autores são estudiosos proeminentes no campo que estuda a interação entre cibersegurança e estabilidade estratégica. Além disso, apenas dez trabalhos – ou seja, 25% da amostra – tiveram a autoria principal de mulheres. Isso era esperado, já que o sexo feminino sofre de falta de representatividade no campo acadêmico, bem como em política e engenharia (COLET;

HARRIET, 1987 *apud* RODRIGUES, 2023; BRUSH, 1991, SONNERT; GERALD, 1996).

5.2. Aspecto substantivo

Nesta subseção, apresentamos os resultados das variáveis substantivas, que avaliam a frequência com que determinados blocos temáticos aparecem (como, por exemplo, quantos trabalhos pontuaram na variável '*retaliation*' ou '*deterrence*'). Identificar a frequência em que a variável aparece não nos diz muita coisa. Por isso, além de identificarmos a frequência, nós identificamos a maneira como a temática foi abordada dentro daquela variável, e quais foram todos os autores que trataram o bloco de uma mesma forma.

5.2.1. Variáveis 'cybersec' e 'strat'

Nenhum dos 40 artigos conceitua ou define cibersegurança, e poucos deles conceituam estabilidade estratégica. Os únicos seis trabalhos, que assim fizeram, definiram-na como "a falta de incentivos para se lançar um ataque nuclear" (KUMAR, 2023; KARASEV, 2020; ROMASHKINA, 2019; SCHNEIDER; SCHECHTER; SHAFFER, 2023), ou como "a falta de incentivo de usar armas nucleares primeiro, entre potências nucleares" (JOHNSON, 2021).

Somente Kumar (2023) distingue-a em dois tipos: a de *first-strike* (primeiro ataque), e a de *second-strike* (segundo ataque). A de *first-strike* é definida pelo autor como a falta de motivação para iniciar um ataque contra outra potência, uma vez que o poder de ambos é percebido como equivalente; a de *second-strike* é a estabilidade gerada pela capacidade de resposta de um país que iniciou o ataque.

Embora nenhum artigo defina ou conceitue cibersegurança, Sharikov (2018) menciona as *fake-news,* as quais, para o Ocidente, não seriam uma questão de cibersegurança, uma vez que os *hardware* e *softwares* estariam intactos, não importando a veracidade da informação que circula entre essas redes; no entanto, para a Rússia, um país mais ao Oriente, seria.

5.2.2. Variável 'retaliation'

Dos 40 trabalhos, 25 (62,5% da amostra) estabelecem uma relação entre ciberataques e retaliação nuclear. O que muitos têm em comum é a abordagem de cenários fictícios, ou conjunturas, das consequências de um ataque cibernético aos sistemas NC3, em quais circunstâncias ocorreria, e como ocorreria. A forma como essa interação se dá, predominantemente, é de que ataques cibernéticos, sejam eles direcionados aos sistemas NC3 sob a forma de operações cibernéticas (JOHNSON, 2021), seja direcionado a outros tipos de infraestruturas críticas, provocam incertezas para os tomadores de decisão, aumentando a

chance de um retaliação nuclear (KARASEV, 2020) de preempção, decorrente do medo de que quem atacou vencerá um conflito (SCHNEIDER; SCHECHTER; SHAFFER, 2023). Para Karasev (2020), o emprego de ciberataques cria pré-requisitos para uma retaliação nuclear.

5.2.2.1. Retaliação como cenário plausível

Alguns artigos recorrem ao *Nuclear Posture Review*, de 2018 (um documento guia de emprego e estratégia nuclear do governo estadunidense) para contextualizar a plausibilidade de um ataque nuclear como resposta a um ciberataque (SALIK; ZAHID, 2022; KLARE, 2019). Empregar um ataque cibernético "cria pré-requisitos para o uso retaliatório de armas nucleares" (KARASEV, 2020); e, conforme Klare (2019), e a sua interpretação do *Review*, se os ataques forem sendo direcionados aos sistemas NC3, os Estados Unidos justificaria o uso de armas nucleares como resposta.

5.2.2.2. Retaliação por medo de comprometer a dissuasão

Uma resposta retaliatória pode surgir do medo de que a própria capacidade de dissuasão foi, ou será comprometida por um ciberataque. Caso uma operação cibernética ofensiva seja interpretada como precursora de uma tentativa de desarmar os sistemas NC3 – impedindo a capacidade de lançar uma resposta nuclear – pode-se desencadear o uso de armas nucleares como retaliação (GOMPERT; LIBICKI, 2019; SCHNEIDER; SCHECHTER; SHAFFER, 2023). Ou seja, o receptor de uma ofensiva cibernética, por medo de possíveis ataques físicos, e da perda de seu arsenal nuclear, pode lançar as suas próprias armas nucleares de forma imediata (Klare, 2019); para Klare, este seria, provavelmente, o caminho mais perigoso para uma escalada.

5.2.2.3. Retaliação motivada pela mentalidade de "*use it or lose it*"

A expressão "*use them/it or lose them/it*" é usada em alguns dos 25 artigos (FAVARO;WILIAMS, 2023; GARTZKE; LINDSAY, 2017; DAVIS, 2019; RAUTENBACH, 2019; LINDSAY, 2019; FUTTER, 2016b), que pontuam na variável *retaliation*. A variante "*move out or lose out*" é usada por Mahmood (2014). O termo descreve a situação de que um Estado vítima pode se sentir pressionado a empregar (*use it*) as suas armas nucleares como resposta a um ciberataque para evitar mais investidas por parte do adversário que o atacou – a fim de evitar uma derrota (*lose it*) no conflito. Ou seja, a resposta de preempção seria optada caso exista o medo da derrota.

A política ou mentalidade de "*use it or lose it*" também é lida como o "uso precoce de

armas nucleares" (Davis, 2019), "aumento do risco de uso nuclear" (Favaro e Williams, 2023), "lançar as suas armas nucleares enquanto ainda pode" (Lindsay, 2019), "a pressão para agir primeiro" (FUTTER, 2016b), ou a crença de que "[é] imprudente escolher não agir e esperar se haverá um outro ataque inimigo" (MAHMOOD, 2014). Lindsay (2019) também a descreve como uma janela (*window*), ou a oportunidade que o Estado vítima tem para agir preventivamente.

5.2.2.4. A retaliação a ciberataques é uma resposta desproporcional ou problemática

Muitos autores defendem que o uso de armas nucleares como resposta a ciberataques é uma política desproporcional, problemática, ou perigosa (SHOAIB, 2018; AVIN; AMADAE, 2019; FUTTER, 2016b; MEER, 2016; HAYES; KAMPMARK, 2019). Para Avin e Amade, essa abordagem é questionável – e trazem como uma sugestão do *Nuclear Posture Review* de 2018 –, enquanto Hayes e Kampmark afirmam ser uma "séria realidade em potencial".

5.2.2.5. Falha no *deterrence* se encontra com *retaliation*

Na amostra de 40 artigos, notamos que muitos trechos podem ser interpretados como duas variáveis ao mesmo tempo – *retaliation* e *deterrence*. Ciberataques podem prejudicar a dissuasão nuclear (variável *deterrence*), quando os sistemas infectados por *malware* emitem informações falsas aos tomadores de decisões, comprometendo essa capacidade de dissuasão, e minando a estabilidade estratégica.

Ao mesmo tempo, ataques cibernéticos podem instigar uma retaliação nuclear, uma vez que os tomadores de decisão por trás dos sistemas NC3 podem interpretar informações falsas como verdadeiras, levando-os a optar por uma investida de preempção – por exemplo, ao acreditar que estão prestes a sofrer um ataque nuclear do adversário, por causa de um alarme falso provocado por um *hacking*.

Nos documentos, as duas variáveis podem ser lidas como a crença de que estão sob ataque, temer que os sistemas nucleares foram comprometidos, pressionando para agir primeiro (FUTTER, 2016b); ou "uma operação cibernética de bandeira falsa contra os sistemas NC3 que leva a uma resposta deliberada escalatória (JOHNSON, 2021, p. 6).

Ainda, é lida como "[a] incerteza tecnológica [causada por ciberataques] aumenta a chance de uso nuclear por prevenção, por medo de que os agressores vencerão o conflito" (SCHNEIDER; SCHECHTER; SHAFFER, 2023, p. 636); ou como "comprometer o sistema, enganar os computadores, ou enviar falsos sinais [...] pode provocar a Rússia ou os Estados Unidos a lançar um ataque nuclear com base em dados falsos" (SHARIKOV, 2018, p. 4).

A junção de *retaliation* e *deterrence* pode ser a percepção de que os sistemas estão comprometidos, o que aumenta a percepção do risco. Conforme Futter, "a Rússia e os Estados Unidos desejarão saber da credibilidade de suas capacidades de dissuasão nuclear, e a habilidade de que serão capazes de lançar um ataque retaliatório [...]" (FUTTER, 2015, p. 170); ou, ainda, como a possibilidade de usar meios cibernéticos para enganar a liderança, fazendo-os acreditar que estão prestes a serem alvos de uma resposta nuclear (MCKANE, 2022), criando circunstâncias em que um ataque preventivo possa parecer justificável.

Hackers podem empregar a técnica de *spoofing* (fraude), onde se cria um alarme falso de ataque nuclear, assim desencadeando um ataque retaliatório mal calculado (WILSON; FITZ, 2023; FUTTER, 2016b).

5.2.2.6. Ciberataques podem ser insuficientes para provocar uma resposta nuclear intencional

Schneider, Schechter e Shaffer (2023) trazem três hipóteses sobre operações cibernéticas e os riscos de uso de arma nuclear, decorrentes de teorias de certeza e incerteza tecnológica: (1) vulnerabilidades cibernéticas levam ao uso preemptivo de arma nuclear; (2) incertezas criam incentivos para dissuasão e restrição, diminuindo os incentivos para um Estado usar o seu nuclear arsenal, diante das incertezas que surgiriam após atacar os sistemas NC3; e (3) confiança excessiva nas próprias capacidades cibernéticas pode incentivar ciberataques contra redes nucleares, podendo gerar, também, campanhas de contra-força em outros domínios. A primeira hipótese é presente em todos os 25 trabalhos que pontuam na variável '*retaliation'*.

Somente dois trabalhos reconhecem a segunda hipótese, de que ciberataques podem ter efeito nulo sobre os incentivos a uma retaliação nuclear: o artigo de Schneider, Schechter e Shaffer (2023), e o de Gartzke e Lindsay (2017). Os autores afirmam que operações cibernéticas geram incertezas que podem criar incentivos para restrição ao invés de escalada.

Gartzke e Lindsay (2017) afirmam que a maioria das análises sobre "escalada inadvertida" – quando há a intenção de se responder com armas nucleares – foca na mentalidade de "*use ir or lose it*" criada por ciberataques aos sistemas NC3. Embora plausível, os autores consideram a possibilidade de um ciberataque encorajar a ideia – e aqui, nos esforçamos a fim de traduzir a ideia para o português – de "ponderação" ou "relutância" em lançar um ataque de preempção.

5.2.2.7. Ataques a infraestruturas críticas que não os sistemas NC3, e como se relaciona com uma retaliação nuclear

Ciberataques podem ser direcionados a infraestruturas críticas que não os sistemas NC3 – como aos sistemas de suprimento de água e eletricidade – e, ainda assim, motivarem uma resposta nuclear, conforme McKane (2022). Klare (2019), por sua vez, concorda que os ciberataques aos sistemas digitais, sejam eles nucleares ou não, podem constituir motivos o suficiente para responder com um ataque nuclear.

5.2.2.8. Motivações psicológicas ou comportamentais para uma retaliação nuclear, oriundas de uma ofensiva cibernética

25 trabalhos trazem cenários plausíveis e hipotéticos sobre a possibilidade de uma retaliação nuclear como resposta a um ciberataque, mas poucos trazem as motivações psicológicas, predisposições comportamentais, ou incentivos políticos para tal. Schneider, Schechter e Shaffer (2023) relatam a existência de trabalhos empíricos sobre o quão raramente as operações cibernéticas possuem efeitos sobre o comportamento (GOMEZ; WHYTE, 2021; KOSTYUK; WAYNE, 2020; KOSTYUK; ZHUKOV, 2019; KREPS; SCHNEIDER, 2019; VALERIANO; JENSEN; MANESS, 2018).

O aspecto cibernético da guerra híbrida (*hybrid warfare*) possui efeitos psicológicos não intencionais sobre como a dissuasão funciona (RAUTENBACH, 2019). Já Gartzke e Lindsay (2017) argumentam que lançar um míssil e vencer uma guerra nuclear torna-se sem sentido para a maioria dos *policymakers*, uma vez que milhões de pessoas morreriam.

5.2.2.9. Ciberataques podem ser orquestrados por inteligência artificial

Ciberataques aos sistemas NC3 podem ser empregados por meio de inteligência artificial (DAVIS, 2019), de forma automatizada (SHARIKOV, 2018), e podem, conforme Davis, incitar ao uso antecipado de armas nucleares. Para Sharikov, o uso de IA para atacar sistemas de comando e controle é o uso mais preocupante de todos.

5.2.3. Variável 'deterrence'

Curiosamente, 38 dos 40 artigos (95% da amostra) abordam que operações cibernéticas ofensivas podem comprometer a capacidade de dissuasão nuclear, revelando um consenso acadêmico acerca dessa possibilidade. *Hackers* seriam capazes de assumir o controle dos sistemas NC3, e lançar ataques nucleares não autorizados (SHOAIB, 2018; WILSON; FITZ, 2023). Além disso, o aspecto de *cyber warfare* oriundo do *hybrid warfare* tem efeito erosivo

sobre a dissuasão nuclear, aumentando a probabilidade de que armas nucleares sejam usadas, conforme Rautenbach (2019); por consequência, isso diminui a estabilidade estratégica.

Concluindo a partir da literatura, simplificamos que a dissuasão nuclear pode ser afetada de, pelo menos, duas formas. A primeira afeta a capacidade de utilizar armas nucleares quando desejado ou necessário – como quando *hackers* tomam o controle dos sistemas NC3, incapacitando o lançamento de mísseis. A segunda prejudica a tomada de decisões, uma vez que, após um ataque cibernético, os sistemas NC3 não emitem mais informações confiáveis, induzindo à crença de que o Estado agressor está prestes a lançar um ataque nuclear.

A segunda forma é quem mais prejudica, diretamente, a estabilidade estratégica, pois ela aumenta os incentivos para se lançar um ataque nuclear de preempção, uma vez que o Estado vítima do ciberataque se sentirá pressionado a adotar a política de "*use them or lose them*" (use ou perca). A primeira forma afeta a capacidade de dissuasão, mas não necessariamente os incentivos de uso nuclear – considerando a definição de estabilidade estratégica.

5.2.3.1 Ciberataques podem prejudicar a integridade dos sistemas, enfraquecendo a dissuasão

Para van der Meer (2016), o risco de sabotagem dos sistemas de armas nucleares é a ameaça cibernética mais óbvia à estabilidade nuclear. Alguns autores concordam sobre ameaças que podem partir do engano aos computadores, por meio de mensagens e sinais falsos (GOMPERT; LIBICKI, 2019; SHARIKOV, 2018), como falsos positivos (FUTTER, 2015; LINDSAY, 2019), onde um sensor pode identificar, erroneamente que um ataque adversário está a caminho; o Estado vítima do ataque, por sua vez, pode ser forçado a agir preventivamente, lançando o que acredita ser um segundo ataque – mas é o primeiro – a partir da mentalidade de "*use it or lose it*". Lindsay afirma que a preempção surge do medo de perder a habilidade de retaliar quando desejado.

Um ciberataque seria capaz de infiltrar os sistemas NC3, e comprometer a sua integridade (JOHNSON, 2020; MONTGOMERY; BORGHARD, 2021), por meio de dano, sabotagem, ou destruição de seus canais de comunicação (CIMBALA, 2014; ROMASHKINA, 2021; SHOAIB, 2018) e, conforme Haxhixhemajli (2021), até pelo o roubo de informações sensíveis, bloqueio de sistemas e modificação de senhas (MCKAY, 2018).

Considerando Gompert e Libicki (2019), mensagens falsas podem ser inseridas para se sobreporem às mensagens reais, a fim de persuadir os operadores dos sistemas a desconfiarem de informações verdadeiras. Ciber-atacantes podem implantar informações incorretas nos sistemas (WILSON; FITZ, 2023). Já Futter (2015) diz que falsos códigos de lançamento

podem ser enviados às armas, ou que *hackers* podem "fabricar" um ataque do adversário, gerando um falso positivo nos sistemas; ainda, Futter (2016b) afirma que comandantes podem erroneamente pensar que estão sob ataque, gerando a pressão para agirem primeiro – resultando em um ataque de preempção.

Além disso, um dos trabalhos da amostra menciona sobre os efeitos de um ciberataque a um sistema que possui inteligência artificial implantada em si; a inteligência pode gerar uma onda de falsos positivos (FITZPATRICK, 2019) e, ao mesmo tempo, ter o seu algoritmo reconfigurado para detectar esse mesmo erro, no futuro.

5.2.3.2. Operações cibernéticas podem impedir o lançamento das armas nucleares

Operações cibernéticas podem interferir nos sistemas de lançamento nuclear (GARTZKE; LINDSAY, 2017; HAYES; KAMPMARK, 2019) e, conforme Lin (2021), impedir a entrega de uma arma para o seu alvo; ele descreve os seguintes cenários: (1) um avião munido de uma bomba nuclear pode não conseguir lançar a arma no tempo apropriado; (2) ou pode nem conseguir decolar, uma vez que os seus computadores estão em constante *reboot* (reinicialização), como resultado de um *hacking*. Ou seja, os efeitos dessas ofensivas podem impedir que os sistemas funcionem conforme o desejado por não serem invulneráveis aos *hackers* (FUTTER, 2016b), que podem interferir com os meios de comunicação para impedir que as ordens de lançamento cheguem até as armas (SHOAIB, 2018).

Operações cibernéticas ofensivas podem injetar comandos falsos ou suprimir os legítimos, cegar os sensores, monitorar ou corromper a transmissão de dados, e interferir na confiabilidade do lançamento e orientação dos mísseis (GARTZKE; LINDSAY, 2017), assim comprometendo os sistemas. Haxhixhemajli (2021) afirma a possibilidade de bloquear os sistemas de armas nucleares; por bloqueio, concluímos que o lançamento também seria inviabilizado.

Vale mencionar que alguns autores concordam sobre a sabotagem ou comprometimento dos sistemas ser uma tarefa difícil, complexa (AVIN, AMADAE, 2019; SALIK; ZAHID, 2022), ou improvável de acontecer, conforme Gompert e Libicki (2019); estes afirmam que ciberataques geralmente não podem desabilitar as armas ao empregar más instruções.

5.2.3.3. A capacidade de dissuasão pode ser prejudicada por vulnerabilidades no *supply chain*

Não são muitos os artigos que exploram as vulnerabilidades cibernéticas surgidas já na cadeia de suprimento (*supply chain*) de peças para os sistemas NC3. Klare (2019) afirma ser

possível a introdução de um código malicioso nas armas nucleares, por meio da cadeia de suprimento, podendo levar ao seu comprometimento e falta de confiança na capacidade de dissuasão – o que mina a estabilidade estratégica.

Lin (2021), por sua vez, menciona que Estados podem procurar comprometer a dissuasão nuclear do adversário, implantando *malware* – ou até vulnerabilidades no *hardware* – no *supply chain* das plataformas de lançamento de armas. O autor afirma que, não existindo mais confiança na infraestrutura das armas nucleares, uma potência nuclear pode interpretar incorretamente os sinais de seus sistemas, e preferir lançar as suas armas nucleares a perdê-las para o *first-strike* de um adversário. Além disso, Unal e Lewis (2018) afirmam que muitos aspectos do desenvolvimento de armas nucleares e gerenciamento de sistemas são privatizados, nos Estados Unidos e no Reino Unido, e que o *supply chain* do setor privado pode introduzir vulnerabilidades.

5.2.3.4. Ciberataques prejudicam a tomada de decisões

Segundo Mahmood (2014), o gerenciamento de uma crise nuclear demanda boas informações e clareza de pensamento. Portanto, alguns acadêmicos compartilham a crença de que ciberataques podem perturbar a tomada de decisão (KARASEV, 2020; LINDSAY, 2019; UNAL; LEWIS, 2018), impedindo uma avaliação clara das informações transmitidas pelos sistemas, durante uma crise nuclear (MAHMOOD, 2014). Para Unal e Lewis (2018), a tomada de decisão é prejudicada em razão da incerteza gerada por atividades como manipulação de dados e *cyber spoofing* (quando um ator finge ser alguém que não é para ganhar confiança).

5.2.3.5. Ciberataques prejudicam a confiança nas informações transmitidas pelos sistemas

A literatura demonstra que ataques cibernéticos corroem a confiança nas próprias capacidades de defesa e dissuasão nuclear (LIN, 2021; HAXHIXHEMAJLI, 2021 MUSSINGTON, 2019; ROMASHKINA, 2021), uma vez que os sistemas de alerta podem estar comprometidos, os comandos necessários para lançar as armas podem estar adulterados, e mensagens falsas podem ter substituído as verdadeiras (GOMPERT; LIBICKI, 2019).

O cenário descrito no último parágrafo provoca incerteza na credibilidade da própria dissuasão nuclear (KLARE, 2019) – no caso, no status de seus sistemas NC3 e NC4ISR – *nuclear command, control, communications, computers, intelligence, surveillance, and reconnaissance* (AVIN; AMADAE, 2019) – e, conforme Klare, mina a estabilidade estratégica. Não somente a confiança é corroída, mas a própria capacidade em si.

Enquanto isso, a única abordagem no artigo de Haxhixhemajli (2021), sobre as consequências de um ataque cibernético, recai sobre o comprometimento da dissuasão nuclear, como no trecho “o efeito de ameaças cibernéticas e ciberataques pode minar a confiança na dissuasão nuclear e impactar a confiança nas capacidades das armas nucleares” (HAXHIXHEMAJLI, 2021, p. 45).

5.2.3.6. *Hackers* podem obter uso não-autorizado, e assumir o controle dos sistemas

Hackers podem assumir o controle de sistemas de comando e controle nucleares (JOHNSON, 2020; JOHNSON, 2021; MEER, 2016; WILSON; FITZ, 2023), e lançarem, por conta própria, uma arma nuclear (FUTTER, 2016a; WILSON; FITZ, 2023), por meio do uso não autorizado (WILSON; FITZ, 2023; SHOAIB, 2018), que pode se dar pela transmissão de ordens direcionadas às equipes responsáveis pelo lançamento, ou às próprias armas (FUTTER, 2015). Dentre os atores capazes de provocar ataques do tipo, estão os Estados, ou até mesmo atores não-estatais, como terroristas ou “lobos solitários” (FUTTER, 2015; 2016a).

Quanto à probabilidade disso ocorrer, alguns autores concordam que é extremamente difícil e improvável (AVIN; AMADAE; 2019; GOMPERT; LIBICKI, 2019), ou pouco provável (VELEZ-GREEN; HOROWITZ; SCHARRE, 2019). Gompert e Libicki justificam essa dificuldade porque ordens de lançamento passam por autoridades humanas, sugerindo o fator humano como possivelmente decisivo para impedir um ataque não-autorizado.

5.2.3.7. Potências nucleares e a intenção de prejudicar os sistemas NC3 do adversário

Ao que parece, apenas um artigo menciona a intencionalidade de debilitar os sistemas de comando e controle nuclear do adversário. Futter (2015) acredita ser bastante improvável que países como os Estados Unidos ou Rússia tenham planos ou a intenção de enfraquecer os sistemas um do outro.

5.2.3.8. Ciberataques a satélites e os riscos à estabilidade estratégica

Apenas um artigo trata da possibilidade dos satélites que se comunicam com os sistemas NC3 serem danificados por ofensivas cibernéticas. Egeli (2019) afirma que ciberataques a ativos espaciais podem impactar a estabilidade estratégica. Segundo o autor, ciberataques podem danificar os satélites, por meio da interrupção ou comprometimento de seus serviços; e se aproveitar de vulnerabilidades do *software* e *hardware* para obter acesso não autorizado ou injetar códigos maliciosos; *hackers* podem desde roubar dados, a assumir o seu controle.

5.2.4. Variável 'policy'

30 dos 40 trabalhos (ou seja, 75% da amostra) propuseram boas práticas de cibersegurança, a fim de minimizar os riscos cibernéticos que podem impactar, negativamente, a estabilidade estratégica, indicando que a literatura se preocupa em mitigar o problema. Alguns trechos de Avin e Amadae (2019) são úteis para sintetizarmos as principais conclusões da variável *policy*: (1) estabelecer normas que proíbam atacar sistemas NC4ISR; (2) promover normas contra o uso de inteligência artificial como arma no ciberespaço; e (3) compartilhar boas práticas de cibersegurança.

O trabalho de Futter (2016a) também é útil para sintetizar uma fração de nossos achados: (1) entender a natureza do desafio cibernético, e suas ameaças e implicações; (2) estabelecer normas ou regras para o domínio que interliga os domínios *cyber* e nuclear; e (3) buscar medidas que construam confiança, como o compartilhamento de dados e boas práticas.

Wilson e Fitz (2023) parafraseiam as *policies* trazidas pelo relatório do NTI; estas incluem o aumento de tempo no processo de tomada de decisão para ameaças aos sistemas de alarmes, estabelecimento de normas que restrinjam o uso de armas cibernéticas contra sistemas nucleares, diálogos bilaterais com a Rússia, considerar os riscos cibernéticos nos planos de modernização dos sistemas, e cooperação internacional para reduzir ameaças cibernéticas. Essas recomendações são todas descritas a seguir. Ademais, é importante que pesquisadores, a comunidade de defesa global, e tomadores de decisão dialoguem entre si (JOHNSON, 2019).

5.2.4.1. Cooperação como *policy*

A cooperação é importante para combater ameaças cibernéticas (JONHSON, 2021; KARASEV, 2020; WILSON; FITZ, 2023). Johnson (2021) sugere uma coordenação com os adversários dos aliados, para reforçar os sistemas NC3 contra ataques cibernéticos; Karasev (2020), por sua vez, aconselha uma cooperação bilateral para avaliar os problemas mais comuns para a estabilidade estratégica, como um caminho viável para superar crises, e pode se dar por meio do "desenvolvimento de recomendações e *frameworks* para reduzir ameaças cibernéticas de terceiros aos sistemas de comando, controle, comunicações, bem como defesa de mísseis".

Tal como Karasev, Johnson (2020) sugere que as grandes potências estabeleçam *frameworks*, bem como normas, regulações e transparência no desenvolvimento de capacidades militares impulsionadas por IA. Futter (2015), por sua vez, recomenda que uma grande prioridade é que Estados Unidos e Rússia trabalhem juntos para reforçar e aprimorar

os seus sistemas nucleares contra futuros ciberataques e acidentes cibernéticos.

5.2.4.2. Normas e acordos que proíbam ciberataques aos sistemas NC3 do adversário

Acordos – do tipo bilateral, entre os Estados Unidos e a Rússia – podem ser feitos para que as potências não empreguem ataques cibernéticos às forças nucleares de outro país, e aos seus sistemas de comando e controle (FUTTER, 2015). De maneira similar, Klare (2019) defende acordos, formais ou informais, também entre esses dois países – mas, incluindo a China – a fim de evitar comportamentos que gerem uma escalada nuclear acidental ou não-intencional. Pode se dar sob a forma de encontros entre oficiais dos três Estados, onde eles buscariam regras que todos possam seguir, como a proibição do emprego de *malware* nos sistemas NC3 de seus adversários – medida esta que Shoaib (2018) também sugere.

Gompert e Libicki (2019) vão ao encontro, ao sugerir que os Estados Unidos proponham entendimentos com a Rússia e China de que os sistemas NC3 não devem ser alvos de operações cibernéticas. Já Romashkina (2019) defende uma convenção que proíba o uso dano de tecnologias de informação e comunicação (ICTs) no campo das armas nucleares e padrões internacionais "de meios e métodos que previnam e eliminem conflitos cibernéticos" (p. 69), por intermédio da Organização das Nações Unidas (ONU).

Normas podem ser criadas para restringir ou proibir o emprego de armas cibernéticas contra sistemas nucleares (AVIN; AMADAE, 2019; WILSON; FITZ, 2023). Avin e Amadae defendem que essas normas são úteis para manter a dissuasão nuclear e estabilidade estratégica, que os Estados se abstenham de empregar operações cibernéticas contra os sistemas NC3 de seus adversários, e que até instituições sejam criadas a fim de proibir essas ofensivas.

No entanto, para Shoaib (2018), acordos de controle de armas, que busquem restringir o emprego de ofensivas cibernéticas contra sistemas nucleares, podem não funcionar, uma vez que estas ofensivas dependem do sigilo, o que dificulta o monitoramento e *enforcement* desses acordos. De igual modo, Gartzke e Lindsay (2017) afirmam que operações cibernéticas dependem do engano, criando obstáculos para o emprego de um acordo. Ainda, Meer (2016) concorda que, embora uma proibição internacional seja considerada, ela não é realista, devido à dificuldade de verificação e emprego de tal banimento.

5.2.4.3. Soluções técnicas de cibersegurança

Os achados mostram que acadêmicos das relações internacionais oferecem soluções técnicas de cibersegurança, as quais seriam tipicamente vistas na ciência da computação. Estas

incluem treinamento para os operadores, melhores defesa de redes, *firewalls,* e segurança física (FUTTER, 2016a; SHOAIB, 2018). Também podem incluir uma criptografia mais sofisticada, e sistemas de comunicação atualizados – incluindo cabos (FUTTER, 2015; 2016a).

Uma melhor segurança física pode consistir em *upgrades* na infraestrutura nuclear, bem como no desenvolvimento de sistemas de comunicação seguros (SHOAIB, 2018). Ao tornar os sistemas mais protegidos aos ciberataques – como por meio de arquiteturas de redes mais resilientes – Estados podem perder a confiança nas próprias capacidades ofensivas, e considerar como demasiadamente difícil e caro lançar esses ataques (SCHNEIDER; SCHECHTER; SHAFFER, 2023).

Para Avin e Amadae (2019), é importante evitar a integração entre inteligência artificial – nomeadamente *autonomy* e *machine learning* – em sistemas NC3 e NC4ISR, e separar os sistemas de qualquer rede. Johnson (2019, p. 22), por sua vez, não desaprova a integração de IA nos sistemas, ao recomendar "*hardware* seguro centrado em IA".

De forma ponderada, Gartzke e Lindsay (2017) afirmam que tecnologias antigas podem prover algum nível de proteção ao impedir o acesso de técnicas modernas de operações cibernéticas; ao mesmo tempo, essas velhas tecnologias podem ter uma segurança inadequada para se defenderem dessas técnicas.

Os acadêmicos demonstram ser fundamental manter a simplicidade dos sistemas – ou *softwares* – de comando e controle (FUTTER, 2016a; HAYES; KAMPMARK, 2019; SHOAIB, 2018). Hayes e Kampmark (2019) reproduzem a frase "a complexidade é inimiga da segurança" (p. 7). Para Lin (2021), complexidade impulsiona vulnerabilidades cibernéticas, e sistemas complexos implicam mais lugares onde falhas de segurança podem ser encontradas e exploradas por adversários. Lin (2021) conclui que complexidade gera "mais códigos [...] mais usuários [...], e mais erros humanos" (p. 114).

5.2.4.4. Modernização dos sistemas nucleares como *policy*

Um dos artigos sugeriu que os governos devem aprimorar e modernizar os seus sistemas de armas nucleares, de maneira regular (HAXHIXHEMAJLI, 2021). Curiosamente, essa não foi uma recomendação entre os trabalhos que apontaram a modernização dos sistemas NC3 como criador de novas vulnerabilidades cibernéticas – importante mencionar que eles não argumentaram contra a sua adoção. Na seção "Variável *'modern'*", explicamos melhor como a maior parte dos acadêmicos têm visto a modernização dos sistemas de comando e controle.

5.2.4.5. Migrar mísseis nucleares para que ciberataques não tenham poder de alcance

Até onde avaliamos, apenas um artigo indicou a possibilidade de migrar os mísseis nucleares para zonas livres de perigos, como os oceanos, lugar onde ciberataques não podem alcançá-los, a fim de prevenir seu uso inadvertido (MEER, 2016). Meer defende que a medida pode aumentar o tempo de resposta, principalmente para sistemas de alarmes automatizados, permitindo que os tomadores de decisão avaliem as circunstâncias cuidadosamente, antes de ordenar um lançamento.

5.2.4.6. *"Humans in-the-loop"*

Humanos devem estar envolvidos no processo de tomada de decisão, a fim de prevenir manipulações dentro do domínio cibernético (MEER, 2016). Sistemas de comando e controle sempre devem contar com um humano, para fomentar/construir confiança (MCKANE, 2022).

5.2.4.7. Considerar as novas ameaças possíveis

Muitos trabalhos sugerem a consideração das possíveis ameaças. Johnson (2019) defende a investigação do que implica a interação entre *cyber* e IA, para a segurança; Futter (2016a) aborda a interação entre *cyber* e nuclear, e defende como o ambiente nuclear deve ser gerenciado, considerando as novas ameaças; e que líderes de potências nucleares precisam discutir a natureza dessa implicação.

Por sua vez, Gartzke e Lindsay, (2017) sugerem a apreciação dos riscos de operações cibernéticas ofensivas aos sistemas NC3; Sharikov (2018) alerta para a possibilidade do uso de IA em ciberataques aos sistemas de comando e controle; por fim, Kumar (2023) defende que os tecnologistas considerem os riscos do processo de integração de IA com nuclear.

5.2.4.8. A importância do compartilhamento de informações

Compartilhar informações pode contribuir no combate às ameaças cibernéticas em potencial (HAXHIXHEMAJLI, 2021), e devem ser trocadas entre o setor público e privado (MUSSINGTON, 2019). É possível compartilhar boas ou melhores práticas em cibersegurança (AVIN; AMADAE, 2019; HAYES; KAMPMARK, 2019; SHOAIB, 2018; UNAL; LEWIS, 2018).

Considerando que parte do desenvolvimento de armas nucleares é privatizado em países como Estados Unidos e Reino Unido – o que pode introduzir vulnerabilidades na cadeia de suprimentos – é necessário que as companhias de defesa contratadas compartilhem informações sobre ciberataques com os Estados (UNAL; LEWIS, 2018).

Dentre outras boas práticas, estão a de compartilhar dados sobre ameaças cibernéticas (SHOAIB, 2018), como as de atividades de autores não-estatais que tentam manipular os sistemas pelo ciberespaço (MEER, 2016); não integrar inteligência artificial em sistemas NC4ISR (AVIN; AMADAE, 2019); e cooperação para perícia – *forensics* – cibernética (muito provavelmente para a correta atribuição de autoria de uma ofensiva *hacker*).

5.2.4.9. Como diminuir as vulnerabilidades surgidas no *supply chain*?

Salvo melhor juízo, apenas um artigo (UNAL; LEWIS, 2018) trouxe recomendações para mitigar as vulnerabilidades cibernéticas surgidas na cadeia de suprimentos de sistemas de comando e controle. Para se reduzir essas vulnerabilidades, é necessário uma abordagem de "seguro por *design*", considerando os riscos em potencial na arquitetura do sistema, *design*, fabricação, e manutenção. Unal e Lewis defendem que o treinamento de equipes que atuam em instalações nucleares, bem como medidas de segurança e conscientização, contribuem para a defesa de informações sobre o *design* de armas nucleares.

5.2.4.10. Parceria entre o setor público e o privado

Muitos autores sugerem uma parceria entre o setor público e o privado (FAVARO; WILLIAMS, 2023; JOHNSON, 2019; MUSSINGTON, 2019; UNAL; LEWIS, 2018). Johnson defende que a natureza da relação entre inteligência artificial e *cyber* exige a inclusão de especialistas em IA e cibersegurança, do setor privado. Mussington, por sua vez, defende uma comunicação aprimorada e cooperação entre governo e o setor privado para reforçar as defesas nessa área. Já Favaro e Williams sugerem a inclusão de companhias privadas no desenvolvimento de políticas sobre controle de armas e redução de riscos, bem como na discussão sobre os perigos que surgem das tecnologias emergentes – os quais podem gerar problemas de cibersegurança.

Unal e Lewis indicam uma maior coordenação entre departamentos de defesa nacional e o setor privado, a fim de assegurar que políticas de defesa estejam em sincronia com a inovação cibernética, permitindo que novas tecnologias possam ser aplicadas – presumidamente, para que não nos preocupemos com problemas de cibersegurança surgidos a partir do emprego destas.

No entanto, Sharikov (2018) parece ir na contramão, ao defender que pesquisas militares sobre inteligência artificial, bem como o seu desenvolvimento, devem permanecer sob controle total do governo, a fim impossibilitar o uso não-autorizado proveniente de um ciberataque orquestrado por IA; a sua opinião sugere que uma parceria entre setor público e

privado, para pesquisas e fornecimento de material, não é uma boa estratégia. Ainda assim, o autor defende a transparência dessas pesquisas à sociedade civil, na medida do possível, e que *policymakers* e especialistas técnicos trabalhem juntos para a prevenção de ciberataques oriundos de IA.

5.2.4.11. "*Trust building*"

Vários documentos expressam o dever de confiança mútua entre potências nucleares (FUTTER, 2016b; JOHNSON, 2019; MEER, 2016; ROMASHKINA, 2021; SHARIKOV, 2018). Aparentemente, apenas Meer se aprofunda para explicar como essa construção de confiança deveria acontecer. Segundo o autor, essas medidas devem existir entre as potências, nucleares ou não, a fim de evitar a manipulação de sistemas de armas por *hackers*. Procedimentos de emergência podem prevenir o uso inadvertido (descontrolado) após o controle sobre as armas nucleares ter sido perdido, e a transparência sobre medidas de cibersegurança deve ser adotada.

5.2.4.12. Ter informações sobre o status das forças nucleares e cibernéticas

Quanto maior for a informação sobre o *status* das próprias forças nucleares, cibernéticas, e sistemas de comando e controle, melhor (MAHMOOD, 2014). Conforme o relatório de Mussington (2019), o Congresso estadunidense criou uma medida para o Departamento de Defesa do país, requerendo uma avaliação anual do *status* de todos os segmentos dos sistemas de comando e controle nucleares dos Estados Unidos.

Por sua vez, o relatório de Hayes e Kampmark (2019) recomenda o desenvolvimento de fontes de informação imparciais e de terceiros sobre a situação das armas nucleares. A recomendação considera o novo ambiente informacional permeado pelas redes sociais, deixando subentendido que deve existir uma transparência na transmissão de informações ao público civil.

5.2.4.13. Aumentar o tempo de reação após um ciberataque

A literatura demonstra ser importante aumentar o tempo de decisão – e reação – após um ciberataque (FUTTER, 2015; GOMPERT; LIBICKI, 2019; LIN, 2021; MEER, 2016, WILSON; FITZ, 2023). Conforme supracitado, Meer defende que realocar mísseis nucleares para os oceanos – onde ciberataques não têm poder de alcance – pode aumentar o tempo de resposta, permitindo que os tomadores de decisão avaliem a real necessidade de responder com um ataque nuclear.

Por seu turno, Lin (2021) esclarece que comandantes sofrem a pressão do tempo para tomar decisões, geralmente diante de informações incompletas; se os riscos forem grandes, é sábio esperar por mais informações antes de agir. Este tempo adicional ajuda a mitigar – mas não eliminar – os riscos cibernéticos, permitindo que operadores confirmem as informações providas pelos sistemas NC3 como confiáveis, e não corrompidas por uma ofensiva cibernética inimiga.

Gompert e Libicki (2019) alegam que avanços nos sistemas NC3 podem reduzir a pressão para provocar um lançamento retaliatório, uma vez que tomadores de decisão terão mais tempo para avaliar as ameaças, e ponderar as consequências antes de decidir se vão retaliar – e de qual maneira – mantendo a estabilidade nuclear. Similarmente, Wilson e Fitz (2023) sugerem opções que aumentem o tempo de decisão para considerar as ameaças aos sistemas de alarme. Futter (2015) defende o aumento do tempo de resposta, e que algumas condições existam antes de agir.

5.2.5. Variável 'modern'

19 dos 40 trabalhos abordam sobre a interação entre cibersegurança e modernização dos sistemas de comando e controle nucleares, e como isso pode impactar a estabilidade estratégica – ou seja, quase 50% da amostra. Isso demonstra que a implementação de novas tecnologias gera preocupações sobre a integridade dos sistemas, e a sua suscetibilidade a ciberataques que podem provocar uma escalada nuclear.

5.2.5.1. A modernização causa problemas de cibersegurança

Os achados demonstram um quase completo consenso, de que a modernização dos sistemas de comando, controle e comunicações gera falhas em sua cibersegurança (CIMBALA, 2017; SCHNEIDER; SCHECHTER; SHAFFER, 2023; FUTTER, 2015, 2016b; SHARIKOV, 2018; SHOAIB, 2018; UNAL; LEWIS, 2018; WILSON; FITZ, 2023; ROMASHKINA, 2019; LIN, 2021; MONTGOMERY; BORGHARD, 2021; LINDSAY, 2019). Isso, ainda, sem mencionar outros autores que concordam sobre como a introdução de IA nos sistemas NC3 – como parte da modernização – também gera falhas cibernéticas, as quais podem impactar negativamente a estabilidade estratégica.

Schneider, Schechter e Shaffer (2023) relatam que, apesar dos acadêmicos possuírem poucas concordâncias sobre cibersegurança e estabilidade nuclear, sua grande maioria argumenta para as vulnerabilidades surgidas da interação entre sistemas NC3 e a revolução digital; essa, por sua vez, aumenta os incentivos para um first-strike, e diminui a habilidade de

controlar uma escalada nuclear quando uma guerra neste domínio estourar. Para os autores, "porque buscar a modernização digital do arsenal nuclear se os riscos cibernéticos são tão altos?" (2023, p. 634).

Futter (2016b) reconhece que, embora a modernização permita uma maior funcionalidade e gerenciamento em tempo-real, ela também torna os sistemas de armas nucleares, dos Estados Unidos, mais suscetíveis à ofensivas *hackers*, que buscam acessar e interferir com a infraestrutura nuclear. Em suas palavras, essa integração seria uma "faca de dois gumes" (FUTTER, 2016a, p. 26).

Shoaib (2018) defende que a digitalização aumenta os riscos de acidentes dentro do campo nuclear, e que sistemas complexos possuem vulnerabilidades inerentes, que podem ser exploradas ou manipuladas de várias formas por *hackers*. Unal e Lewis (2018) e Wilson e Fitz (2023), igualmente, argumentam que a digitalização aumenta a probabilidade dos sistemas de armas nucleares sofrerem ciberataques.

Sob o contexto da estabilidade estratégica, a atualização da infraestrutura nuclear – como mísseis, softwares, ou sistemas de lançamento – torna-os alvos em potencial para ataques digitais (ROMASHKINA, 2019). Ao mesmo tempo, é importante que os EUA considerem como essa dependência tecnológica pode levar a falhas na dissuasão nuclear, ou à guerra nuclear, uma vez que esses riscos são mal compreendidos (LIN, 2021).

De maneira similar, Montgomery e Borghard (2021) concordam que esses riscos cibernéticos representam riscos para a dissuasão, à medida que os EUA procuram modernizar suas infraestruturas. Até porque, a modernização pode confundir a tomada de decisão e levar a erros de cálculos numa crise nuclear (LINDSAY, 2019). Cimbala (2017), por sua vez, reconhece a posição de especialistas que essa modernização aumenta a vulnerabilidade dos sistemas NC3 à ação de *hackers*.

5.2.5.2. Introdução de Inteligência Artificial como parte da modernização

Muitos autores alertam que a introdução de IA em sistemas NC3 ou NC4ISR podem impactar negativamente a cibersegurança desses computadores (AVIN; AMADAE, 2019; HAYES; KAMPMARK, 2019; KARASEV, 2020; KUMAR, 2023). O advento do *machine learning*, por exemplo, vulnerabiliza computadores ao *hacking* – sejam eles sistemas bancários ou os reatores nucleares de uma nação (SHARIKOV, 2018).

A inteligência artificial pode ser problemática – ao expor os sistemas NC3 às novas vulnerabilidades, como informações falsas e atribuição de autoria de ciberataques – mas também promissora (HAYES; KAMPMARK, 2019). Karasev (2020) afirma que IA tem o

potencial de fortalecer ou degradar a estabilidade estratégica; usá-la para elevar o nível de consciência pode diminuir o risco de lançamento não-intencional, mas pode tornar elementos, antes previamente invulneráveis, mais suscetíveis à influência cibernética de adversários, "afetando a estabilidade estratégica de novas formas" (2020, p. 43). Karasev explica que ciberataques contra IA dificultam o processo de tomada de decisão, diminuindo o tempo que *decisionmakers* têm para decidir o que fazer.

Uma minoria reconhece os benefícios da introdução de IA nos sistemas nucleares. James Johnson (2019) afirma que *machine learning* pode, até mesmo, reforçar a cibersegurança de sistemas de comando e controle – uma opinião não-recorrente neste campo de estudos. Contudo, ele reconhece que essa interação torna computadores mais vulneráveis a ciberataques – indo ao encontro do consenso acadêmico. Dualmente, Gartzke e Lindsay (2017) argumentam que velhas tecnologias podem promover, em algum nível, proteção contra técnicas modernas de operações cibernéticas, mas também possuírem medidas de segurança inadequadas contra essas.

5.3. Aspecto metodológico

Nesta subseção, apresentamos os aspectos metodológicos, que indicam se o trabalho traz resumo e, se neste resumo (sumário, introdução, ou similar), ele possui pergunta de pesquisa, hipótese, ou metodologia. Por fim, avaliamos qual a ênfase do trabalho por completo – se quantitativa, qualitativa, ou multimétodo.

5.3.1. Variáveis 'resumo', 'pergunta de pesquisa', 'hipótese'

29 dos 40 trabalhos (72,5% da amostra) possuem *abstract*, ou uma seção de sumário e introdução visivelmente demarcadas. No entanto, apenas oito trabalhos (20%) – dentre os que possuem algum tipo de síntese introdutória – apresentam perguntas de pesquisa em seus resumos, sugerindo uma despreocupação em detectar as principais questões que podem ser de suma importância para a agenda que intersecciona os campo de cibernética e segurança internacional; e a existência majoritária de trabalhos meramente exploratórios ou primários.

Mais surpreendente ainda foi o fato de termos apenas um único trabalho com teste de hipótese – *Hacking Nuclear Stability: Wargaming Technology, Uncertainty, and Escalation*, de Schneider e coautores, 2023. Não somente uma, mas o teste de três hipóteses: (1) "incerteza tecnológica leva à preempção e escalada"; (2) "incerteza tecnológica leva à restrição"; e (3) "certeza tecnológica leva à escalada por meio de campanhas agressivas de contra-ataque" (SCHNEIDER; SCHECHTER; SHAFFER, 2023, p. 633).

5.3.2. Variáveis ‘metodologia’ e ‘ênfase’

A única metodologia detectada foi do trabalho de Schneider, Schechter e Shaffer (2023), onde utilizaram o método quasi-experimental *wargames* (jogo de guerra). Eles descrevem o desenho com duas variáveis independentes – ter uma ação cibernética (*cyber exploit*) nos sistemas NC3 do adversário, e ter uma vulnerabilidade cibernética em seu próprio sistema NC3 – e como as duas afetam uma variável dependente, que é a estabilidade estratégica. Ou seja, o trabalho explorou como as vulnerabilidades de cibersegurança, bem como ataques cibernéticos, afetam os incentivos para o uso de armas nucleares.

Para Schneider e coautores (2023), o método *wargames* sugere que a incerteza e o medo não criam incentivos imediatos para o uso preemptivo de armas nucleares. Porém, após conduzir o método *wargames* com 580 participantes. Dentre eles, pessoas com anos de experiência militar, acadêmica, na indústria privada ou em organizações não-governamentais, e com 56% dos participantes com 15 anos ou mais de experiência.

O artigo conclui que as incertezas cibernéticas provocadas por um ciberataque podem, na verdade, corroborar a segunda hipótese deles – de que isso gera incentivos para a restrição. Por fim, todos os 40 trabalhos da amostra possuem uma ênfase qualitativa, indicando que o campo de estudos não é familiarizado com métodos quantitativos.

6. CONCLUSÃO

A maioria dos trabalhos não traz perguntas de pesquisa, metodologia, ou a hipótese que pretende corroborar – além de serem, exclusivamente, de ênfase qualitativa. Esse achado vai ao encontro do artigo de Albuquerque, Mesquita e Lira-Brito, de 2022, corroborando a "obscuridade metodológica" – que vai além do continente sul-americano, e se estende ao norte global. Supomos que por ser um tema relativamente novo entre acadêmicos internacionalistas, a maioria das pesquisas são de caráter meramente exploratório, e uma minoria são metodologicamente rigorosos.

O único trabalho com metodologia expressa foi o *Hacking Nuclear Stability*, de Schneider, Schechter e Shaffer (2023). O artigo apresenta o método quasi-experimental denominado de *wargames*, simulando uma tomada de decisão sob o cenário de vulnerabilidades cibernéticas que atingia os sistemas NC3 próprios e do adversário, e como a confiança excessiva pode, supostamente, impulsionar um ataque nuclear de preempção. Ao fim do trabalho, os autores concluíram que, na verdade, um ciberataque pode incentivar a um comportamento restritivo.

Excluímos 13 trabalhos após a leitura completa por três razões: (1) houve apenas menção às tecnologias emergentes ou disruptivas, e seus impactos sobre a estabilidade estratégica, sem considerar aspectos ou problemas de cibersegurança oriundos de sua adoção; (2) o termo 'estabilidade estratégica' não foi tratado como "a falta de incentivos para lançar um ataque nuclear"; e (3) porque eram *pre-prints* e já havíamos codificado as versões finais.

100% da amostra é em inglês, indicando que o tema não é explorado por acadêmicos brasileiros, provavelmente em razão do Brasil não possuir armas nucleares. Ao que parece, grande parte dos estrangeiros que estudam sobre cibersegurança e a sua relação com estabilidade estratégica ou dissuasão nuclear são do norte global. Isto entra em concordância com o fato de que, praticamente, apenas países do hemisfério norte possuem armas nucleares, sendo assim, portanto, coerente que autores do norte do globo se preocupem em refletir sobre a cibersegurança destes artefatos bélicos.

A modernização de sistemas nucleares, embora nem sempre mostrada como algo que melhora a cibersegurança dos sistemas em si, pode ajudar na avaliação de ameaças cibernéticas e das consequências antes de decidir se e como irá retaliar (GOMPERT; LIBICKI, 2019). Além disso, muitas vulnerabilidades cibernéticas podem surgir já na cadeia de suprimentos de peças e softwares para sistemas NC3.

É necessário que os setores públicos e privados firmem parcerias, como o compartilhamento de melhores práticas em cibersegurança. É sábio que potências nucleares

estabeleçam acordos a fim de coibir o emprego de operações cibernéticas nos sistemas de comando e controle nucleares do adversário, assim evitando uma escalada nuclear, seja ela deliberada ou não-intencional. É importante melhorar os *firewalls*, e prezar pela simplificação dos *softwares* dos sistemas nucleares, uma vez que sistemas complexos aumentam as vulnerabilidades cibernéticas e, por consequência, a superfície para ciberataques.

A literatura que relaciona cibersegurança com estabilidade nuclear é relativamente extensa, apontando à relevância do tema, e à urgência de se discutir ainda mais a respeito. Os vários artigos publicados – ou de literatura cinzenta – relatórios, e outros tipos de documentos governamentais e de *think-tanks,* preocupados com as ameaças cibernéticas aos sistemas de armas nucleares, indicam que a temática está longe de ser uma discussão trivial.

6.1. Limitações

O trabalho possui algumas limitações, e a primeira é referente à sua condução. Revisões sistemáticas, formalmente, requerem pelo menos dois pesquisadores para fazer a codificação e correção do que foi codificado e analisado; e costumam levar muito mais tempo – de seis meses a um ano e meio. Com muito esforço, e sob um tempo corrido e limitado, conseguimos este feito em apenas quatro meses, o que pode ter resultado em inconsistências e vieses indesejáveis, como a exclusão de artigos que deveriam ter sido selecionados, inclusão dos que deveriam ter sido excluídos, codificação errônea, entre outros. Sabemos que um dos propósitos de uma revisão sistemática é limitar os vieses de seleção, mas considerando que somos apenas um pesquisador, a probabilidade desse viés ser maior que o desejado é alta.

A segunda limitação é o fato de não termos tido tempo de checar, manualmente, se ainda restavam resultados duplicados em nossa planilha, antes de realizarmos a seleção dos trabalhos com base em seus títulos. Ao utilizarmos a ferramenta de remoção automática do próprio Google Planilhas, nenhuma duplicata foi identificada, mas percebemos que haviam trabalhos com títulos idênticos – mudando apenas questões pontuais, como o ano de publicação, indicando que há versões finais e *preprints* de um mesmo trabalho. Dito isso, é necessário que haja, posteriormente, um trabalho de remoção manual.

Nós reconhecemos que a leitura de muitos trabalhos foi prejudicada pelo tempo curto. Em muitos documentos, realizamos uma leitura dinâmica, e utilizamos o comando de busca "Ctrl + F", por palavras-chave desejadas, como cibersegurança, ciberataque, *hack*, dissuasão nuclear e estabilidade estratégica. Ao identificarmos a ausência de algumas dessas palavras, já supomos, de imediato, que o artigo por completo não relaciona as nossas variáveis de interesse. Para fins de transparência e replicabilidade, inserimos as razões (dentro das células

do Google Planilhas) pelas quais esses artigos foram excluídos. Muitas dessas razões se originam do uso do recurso de busca de palavras, e a interpretação subjetiva e pessoal que pressupõe a ausência de blocos temáticos de interesse.

Também reconhecemos que a aplicabilidade de uma fração de nossos achados pode ser irrelevante para a política de segurança nacional brasileira, uma vez que o Brasil não possui armas nucleares, e pesquisas nesse campo são somente para fins pacíficos, conforme Lei nº 7.781, de 27 de junho de 1989[8]. De qualquer forma, uma outra fração – em específico, a de boas práticas de segurança da informação – é aplicável para a segurança cibernética de infraestruturas críticas que o país já possui – como as de geração elétrica a partir de usinas nucleares.

A princípio, a nossa intenção era de ter criado uma variável bibliométrica denominada de "região global", a fim de somar à variável "idioma". Por região global, isso nos permitiria concluir qual o país mais proeminente nos estudos que estudam a interação entre a cibersegurança e a estabilidade estratégica. No entanto, identificar o país no qual o trabalho foi produzido demandaria muito mais tempo – recurso que não tínhamos. Recorremos, somente, ao idioma do trabalho e ao nome do autor. Além disso, vale mencionar que a interpretação de uma palavra-chave ser simples ou composta é subjetiva.

A próxima limitação refere-se a um possível viés conceitual na seção "glossário", onde alguns dos conceitos trazidos são de fontes da área de ciência da computação e cibersegurança – como empresas de tecnologia – ao invés de definições trazidas por acadêmicos das relações internacionais e de estudos estratégicos, devido ao tempo reduzido para explorar uma literatura acadêmica de fato. Propomos que, em futuros trabalhos, tragam-se os mesmos conceitos, mas definidos de um ponto de vista internacionalista, ao invés de técnico e computacional, a fim de constatar as disparidades teóricas entre estudiosos de campos distintos.

Continuando, como nenhum dos trabalhos de nossa amostra definiu cibersegurança, a ausência de uma definição de cibersegurança oriunda de acadêmicos das Relações Internacionais nos impossibilita de avaliar a proximidade conceitual para definições oriundas de estudiosos da computação.

Utilizamos somente o *Google Scholar* como biblioteca de dados, devido ao tempo escasso para buscarmos trabalhos em outras bases. Além disso, não sabemos qual a proporção dos trabalhos de nossa amostra que são *peer-reviewed* (revisado por pares). De toda forma, esta limitação foi minimizada com a criação das variáveis de metodologia, o que permite

[8] Art. 1, inciso IV, alínea a.

termos uma certa dimensão da rigorosidade metodológica dos documentos.

Muitos trabalhos da amostra abordam somente a maneira como a dissuasão nuclear pode ser comprometida através de ciberataques, sem interligar, diretamente ou explicitamente, às consequências para a estabilidade estratégica. De uma escolha subjetiva, e a partir das pesquisas primárias teóricas, assumimos que esse comprometimento da dissuasão nuclear, oriunda de ataques cibernéticos, necessariamente impacta o equilíbrio nuclear – ainda que de forma não-explicitamente expressa.

O fato das variáveis *deterrence* e *retaliation* estarem tão interligadas – com trechos podendo ser interpretados como as duas variáveis ao mesmo tempo – pode indicar uma má formulação metodológica. Problemas do tipo são esperados, uma vez que é a primeira revisão sistemática feita pela autora. Porém, é importante reconhecer que os conceitos de dissuasão nuclear e estabilidade estratégica são bem interconectados – conforme Klare (2019), se a capacidade de dissuasão é prejudicada, a estabilidade estratégica também é. Esta pode ser uma explicação parcial do porquê as duas variáveis estarem muito entrelaçadas.

Existe a probabilidade de alguns trabalhos terem sido repetidos – isto é, podemos ter incluído a versão final e os *preprints* de forma não-intencional. Além disso, o que podemos ter classificado como revistas de publicação, podem ser, na verdade, matérias de jornal derivadas de artigos. Suspeitamos que seja o caso para o *Russia in Global Affairs* e *Arms Control Today*. Portanto, é necessário que seja revisto a classificação dos trabalhos retornados, ou seja, se são realmente artigos publicados, ou outra categoria de publicação. Novamente, o tempo curto foi um dificultador, não nos permitindo fazer uma dupla-checagem da tabulação.

Estabelecemos quatro possíveis razões para a possibilidade de alguns trabalhos retornados do PoP não estarem inclusos em nossa amostra da revisão sistemática, nem na base secundária ou de excluídos, ainda que seus títulos atendessem aos critérios de inclusão: (1) o artigo estava indisponível, (2) ou não foi catalogado por desatenção.

Continuando, (3) a página *web* aberta no navegador, a partir do duplo clique no resultado do PoP, não carregou, e não mostrou o nome do trabalho em questão; por termos aberto várias abas de uma só vez, e termos ter que lidar com os títulos de outros trabalhos, não pudemos realizar uma nova pesquisa por meio do buscador do Google, com o título do trabalho em questão, pois não sabíamos qual era o nome do artigo; por fim, (4) o autor do texto pediu para que o trabalho, normalmente um *draft* (esboço) não fosse citado sem a sua permissão; como não contatamos os autores que fizeram esse pedido, para que tivéssemos permissão, não citamos o seu artigo.

Apesar das buscas terem sido feitas em janeiro de 2024, o recorte temporal da revisão

sistemática foi, somente, até 2023. Isso porque, em dezembro de 2023, havíamos realizado as buscas pelo *Publish or Perish* que deram origem a base de dados atual – com 40 trabalhos. Logicamente, a busca só foi possível até o ano em questão. No entanto, um problema no *laptop* pessoal nos fez perder os registros das buscas de dezembro, antes que pudéssemos salvá-los. Para realizar uma nova pesquisa, da forma mais acurada e fidedigna possível, reproduzimos as mesmas buscas, em janeiro de 2024, a fim de obter os mesmos retornos – agora, salvos no OSF, e com todos os filtros e palavras-chave usadas em dezembro – e manter a transparência e reprodutibilidade dos achados.

6.2. Futura agenda de pesquisa

Para futuras pesquisas, sugerimos que mais estudos primários sejam feitos na área, e que uma inédita revisão sistemática seja feita sobre AI, ao invés de cibersegurança, também sob o contexto da estabilidade nuclear, assim como o presente trabalho. Isso porque o tema de Inteligência Artificial é frequentemente abordado em trabalhos sobre cibersegurança sob o contexto de dissuasão nuclear e estabilidade estratégica. Desta forma, mediante esta agenda de pesquisa sugerida, podemos, sistematicamente, expandir a relação entre tecnologias emergentes – dentre as quais, Inteligência Artificial, como *Machine Learning* e *Autonomy* – e os seus impactos sobre a estabilidade estratégica.

Ademais, identificando o método quasi-experimental como a única metodologia presente em toda a amostra da revisão sistemática, propomos que mais trabalhos primários reproduzam o mesmo método, com amostras diferentes – graduandos em ciência política ou relações internacionais, por exemplo, ao invés de especialistas consolidados da área – a fim de verificarmos a ocorrência de resultados – se semelhantes ou distintos.

7. REFERÊNCIAS

ALBUQUERQUE, R. B. MESQUITA, R. BRITO, R. V. L. **Obscuridade metodológica: um mapeamento da formação em métodos na pós-graduação em Relações Internacionais e áreas afins no Brasi**l. Revista Brasileira de Ciência Política, nº 39, p. 1-25, 2022.

AVIN, S. AMADAE, S.M. **Autonomy and Machine Learning as Risk Factors at the Interface of Nuclear Weapons, Computers and People**. The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: EuroAtlantic Perspectives. SIPRI, p. 105-118, 2019.

BRASIL. **Lei nº 7.781, de 27 de junho de 1989**. Diário Oficial da União, Brasília, DF, 27 de junho de 1989. Disponível em: https://legis.senado.leg.br/norma/549657/publicacao/15680896. Acesso em 01 de mar. 2024.

BRUSH, Stephen G. **Women in Science and Engineering**. American Scientist, v. 79, n. 5, p. 404–19, 1991. Disponível em: http://www.jstor.org/stable/29774475 .

CARNEGIE COUNCIL FOR ETHICS IN INTERNATIONAL AFFAIRS. **Nuclear deterrence**. Carnegie Council, 2024. Disponível em: https://www.carnegiecouncil.org/explore-engage/key-terms/nuclear-deterrence. Acesso em 26 de fev. 2024.

CIMBALA, S. J. **Nuclear deterrence and cyber warfare: coexistence or competition?**. Defense & Security Analysis, 33:3, p. 193-208, 2017.

CIMBALA, S. J. **Nuclear Deterrence in Cyber-ia: Challenges and Controversies**. Air & Space Power Journal, Fall, 2016.

CIMBALA, S. J. **Cyber War and Deterrence Stability: Post-START Nuclear Arms Control**. Comparative Strategy, v. 33, p. 279-286, 25 jul., 2014.

COOPER, H. **Research Synthesis and Meta-Analysis: A Step-by-Step Approach**. Applied Social Research Methods Series, Fifth Edition, v. 2, 2017.

DACOMBE, R. Systematic Reviews in Political Science: **What can the approach contribute to political research?**. King's College London, 2017.

DAVIS, Z. **Artificial Intelligence on the Battlefield: Implication for Deterrence and Surprise**. PRISM, 2019.

FELDMAN, K. A. **Using the Work of Others: Some Observations on Reviewing and Integrating**. American Sociological Association, v. 44, n. 1, p. 86-102, Winter, 1971.

FINK, A. **Conducting Research Literature Reviews: From the Internet to Paper, 2nd edition**. London: Sage, 2005.

KASTELIC, A. **International Cyber Operations: National Doctrines and Capabilities**. United Nations Institute for Disarmament Research, 2021.

HANSON, F.; UREN, T. **Policy Brief: Australia's Offensive Cyber Capability**, 2018.

HERBERT, A. J. **Information Battleground**. Air Force Magazine, v. 88, n. 2, dec., 2005.

KUMAR, K. **Technology and Talk: Exploring Escalation Risks as an Outcome of AI and Nuclear Integration**. California Legal Studies Journal, p. 46-58, 2023.

EGELI, S. **Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability**. Journal for Peace and Nuclear Disarmament, 2019.

FAVARO, M.; WILLIAMS, H. **False Sense of Supremacy: Emerging Technologies, the War in Ukraine, and the Risk of Nuclear Escalation**. Journal for Peace and Nuclear Disarmament, 2023

FITZPATRICK, M. **Artificial Intelligence and Nuclear Command and Control**. Survival, 2019.

FUTTER, A. **Hacking the Bomb: Cyber Threats and Nuclear Weapons**. Washington, DC: Georgetown University Press, 2018. 216 p.

FUTTER, A. **Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security, and Strategy.** Royal United Services Institute for Defence and Security Studies, July, 2016a.

FUTTER, A. **The dangers of using cyberattacks to counter nuclear threats.** Arms Control Today, 2016b.

FUTTER, A. **War Games Redux? Cyberthreats, US-Russian strategic stability, and new challenges for nuclear security and arms control**. European Security, v. 25, n. 2, p. 163-180, 2015.

GARTZKE, E.; LINDSAY, J. R. **Thermonuclear Cyberwar**. Journal of Cybersecurity, 2017.

GLOBAL ZERO COMMISSION ON NUCLEAR RISK REDUCTION. **De-Alerting and Stabilizing the World's Nuclear Force Postures**. Global Zero Commission on Nuclear Risk Reduction, Set. 2015.

GOMEZ, M. A.; WHYTE, C. **Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats**. International Studies Quarterly, 65 (4):1137–50, 2021.
GOMPERT, D. C.; LIBICKI, M. **Cyber War and Nuclear Peace**. Survival, 2019.

HAXHIXHEMAJLI, A. **The necessity to protect nuclear weapons from cyberattacks**. New Technologies, Future Conflicts, and Arms Controls, Center for Security Analyses and Prevention, Prague, 2021.

HAYES, P.; KAMPMARK, B. **NC3 Systems and Strategic Stability: A Global Overview**. Technology for Global Security, May 5, 2019

JOHNSON, J. **Deterrence in the age of artificial intelligence & autonomy: a paradigm shift in nuclear deterrence theory and practice?**. Defense & Security Analysis, 2021.

JOHNSON, J. **Artificial Intelligence in Nuclear Warfare: A Perfect Storm of Instability?**. The Washington Quarterly, 2020.

JOHNSON, J. **The AI-cyber nexus: implications for military escalation, deterrence, and strategic stability.** Journal of Cyber Policy, 2019.

KARASEV, P. A. **Cyber Factors of Strategic Stability: How the Advance of AI Can Change the Global Balance of Power**. Russia in Global Affairs, 2020.

KLARE, M. T. **Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation**. Arms Control Today, 2019.

KOSTYUK, N.; WAYNE, C. **The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public**. Journal of Global Security Studies, 6 (2), 2020.

KOSTYUK, N.; ZHUKOV, Y. M. **Invisible Digital Front: Can Cyber-Attacks Shape Battlefield Events**?. Journal of Conflict Resolution 63 (2):317–47, 2019.

KREPS, S.; SCHNEIDER, J. **Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics**. Journal of Cybersecurity 5 (1), 2019.

LINDSAY, J. R. **Cyber Operations and Nuclear Weapons**. Technology for Global Security, June 20, 2019.

LIN, H. **Cyber Risks Across the U.S. Nuclear Enterprise**. Texas National Security Review, 2021.

MAHMOOD, M. **Strategic Stability and Cyber Warfare: Challenges and Implications**. CISS Insight Quarterly News & Views, 2014.

MCKANE, T. **New Technologies and Nuclear Deterrence**. Arms Control and Europe, Contributions to International Relations, 2022.

MEER, S. **Cyber Warfare and Nuclear Weapons: Game-changing Consequences?**. Netherlands Institute of International Relations, 2016.

MONTGOMERY, M.; BORGHARD, E. **Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence**. Joint Force Quarterly, 2021.

MUSSINGTON, D. **Strategic Stability, Cyber Operations and International Security**. Centre for International Governance Innovation, 2019.

NUCLEAR THREAT INITIATIVE. **2018 Annual Report**. Nuclear Threat Initiative, 2018.

ROMASHKINA, N. P. **Strategic Issues of Application of Information and Communication Technologies in the Military and Political Sphere**. XI International Scientific and Technical Conference on Secure Information Technologies, 2021.

ROMASHKINA, N. P. **New Technologies: Challenges to International Security and Stability**. International Security Center, Primakov National Research Institute of World

Economy and International Relations, 2019.

SALIK, H.; ZAHID, R. I. **From Cold to Code War: Dissecting Security Strategies for the Cyberspace Strategic Environment and Identifying Cyber Risks to the Nuclear Strategic Environment**. Cyberpolitik Journal, 2022.

TRENIN, D. **Russian views of US nuclear modernization**. Bulletin of the Atomic Scientists, 75:1, p. 14-18, 2019.

PAPAIOANNOU, Diana; SUTTON, Anthea; BOOTH, Andrew. **Systematic approaches to a successful literature review**. Systematic approaches to a successful literature review, p. 1-336, 2016.

RAUTENBACH, P. **The Subtle Knife: A Discussion on Hybrid Warfare and the Deterioration of Nuclear Deterrence**. The Journal of Intelligence, Conflict, and Warfare, v.2, n. 1, 2019.

RODRIGUES, R. G. M. **Criptomoedas e a economia política: Uma revisão sistemática da literatura heterodoxa**. 2023. 51 f. Trabalho de Conclusão de Curso (Bacharelado em Ciência Política) – Universidade Federal de Pernambuco, Recife, 2023.

SCHNEIDER, J.; SCHECHTER, B.; SHAFFER, R. **Hacking Nuclear Stability: Wargaming Technology, Uncertainty, and Escalation**. International Organization, 2023.

SHAH, S. S. H. **The Perils of AI for Nuclear Deterrence**. CISS Insight Journal, v. 7, n. 2, 2019.

SHARIKOV, P. Artificial Intelligence, Cyberattack, and Nuclear Weapons. Bulletin of the Atomic Scientists, 22 oct., 2018.

SHOAIB, M. **The Cyber-Nuclear Nexus and Threats to Strategic Stability**. Journal of Strategic Affairs, 2018.

SHOAIB, M. **Conceptualising Cyber-Security: Warfare and Deterrence in Cyberspace**, sem ano.

SONNERT, Gerhard; HOLTON, Gerald. **Career Patterns of Women and Men in the Sciences**. American Scientist, v. 84, n. 1, p. 63–71, 1996. Disponível em: http://www.jstor.org/stable/29775599 .

TIMOTHY, T. **Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?** The Journal of Slavic Military Studies, 27(1), p. 101-130, 2014.

UNAL, B.; LEWIS, P. **Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences**. Chatham House, 2018

VALERIANO, B. MANESS, R. C. **International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain**. The Oxford Handbook of International Political Theory. Disponível em: https://academic.oup.com/edited-volume/28084/chapter-abstract/212149124?redirectedFrom=fulltext. Acesso em 26 de fev. 2024.

VALERIANO, B.; JENSEN, B. M.; MANESS, R. C. **Cyber Strategy: The Evolving Character of Power and Coercion**. Oxford University Press, 2018.

VELEZ-GREEN, A. HOROWITZ, M. C. SCHARRE, P. **A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence**. Cornell University, 2019.

WILSON, R.; FITZ, A. **Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues**. 18th International Conference on Cyber Warfare and Security, 2023.

YETLEY *et al*. **Options for basing Dietary Reference Intakes (DRIs) on chronic disease endpoints: report from a joint US-/Canadian-sponsored working group**. American Journal of Clinical Nutrition, 2016.