ISSN 1809-1628
REVISTA MULTIDISCIPLINAR
HUMANIDADES E TECNOLOGIAS (FINOM)
FACULDADE DO NOROESTE DE MINAS

A fronteira final: guerra cibernética e o futuro da segurança internacional para 2050

The final frontier: cyber warfare and the future of international security to 2050

Caroline Silva Ribeiro[1]
Giovanna Carla Nogueira Moreira[2]
Jéssica Regina Guerra de Souza[3]
Lívia Prado Sadoyama[4]

Resumo: A guerra cibernética e a segurança internacional são tópicos interconectados que têm ganhado relevância à medida que a tecnologia da informação desempenha um papel fundamental nas relações internacionais e na segurança global. Dessa forma, a técnica cenários prospectivos auxilia os atores envolvidos a se prepararem para mudanças potenciais orientando ações presentes a futuros possíveis. O objetivo do estudo deste cenário, portanto, é fornecer uma revisão das possíveis ameaças no ciberespaço, assim como seus impactos na segurança internacional, consequências políticas e diplomáticas, proteção de dados e privacidade usando, para isso, a metodologia desenvolvida por Michel Godet. Como consequência, os quatro cenários obtidos narram dois possíveis cursos de ação: o da cooperação e o da anarquia, os quais possuem diferentes efeitos analisados neste trabalho.

Palavras-chave: Guerra Cibernética, Segurança Internacional, Cenários Prospectivos, Método Godet.

[1] Graduanda em Relações Internacionais pela Universidade Federal de Uberlândia (UFU). E-mail: caroline.ribeiro1@ufu.br

[2] Graduanda em Relações Internacionais pela Universidade Federal de Uberlândia (UFU). E-mail: giovannac.nogueira@ufu.br

[3] Graduanda em Relações Internacionais pela Universidade Federal de Uberlândia (UFU). E-mail: jessica.guerra@ufu.br

[4] Graduanda em Relações Internacionais pela Universidade Federal de Uberlândia (UFU). E-mail: livia.sadoyama@ufu.br

Recebido em 20/12/2023
Aprovado em 24/01/2024

Sistema de Avaliação: ***Double Blind Review***

OPEN ACCESS

Abstract: Cyber warfare and international security are interconnected details that have gained relevance as information technology plays a fundamental role in international relations and global security. In this way, the prospective scenarios technique helps the actors involved to prepare for potential changes by guiding present actions towards possible futures. The objective of studying this scenario, therefore, is to provide a review of possible threats in cyberspace, as well as their impacts on international security, political and diplomatic consequences, data protection and privacy using, for this, a methodology developed by Michel Godet. As a consequence, the four scenarios obtained narrate two possible courses of action: that of cooperation and that of anarchy, which have different effects developed in this work.

Keywords: Cyber War, International Security, Prospective Scenarios, Godet Method.

1. INTRODUÇÃO

A guerra cibernética pode ser conceituada como um termo que se refere a um conflito entre países ou organizações usando a tecnologia como principal arma de combate. Na maioria das vezes, os principais objetivos são obter informações confidenciais, prejudicar sistemas ou interromper serviços essenciais, tudo isso utilizando o ciberespaço (BUGHUNT, 2023). À medida que a digitalização se expande globalmente, organizações, sejam elas governamentais ou do setor privado, estão se tornando cada vez mais relevantes nas tecnologias. Nesse contexto, a guerra cibernética emerge como uma forma contemporânea de conflito que emprega recursos tecnológicos para atingir alvos militares, políticos ou econômicos. Ademais, a história da segurança cibernética é uma jornada que se estende desde os primeiros dias da computação até o mundo altamente conectado e digital de hoje (BUGHUNT, 2023).

Nesse sentido, o desenvolvimento dos primeiros sistemas de computadores no período entre 1960-1980 marcou o início da revolução tecnológica da informação. As preocupações iniciais com a segurança de dados confidenciais resultaram na implementação de medidas de segurança básicas. Paralelamente, surgiram os primeiros hackers e vírus de computador, como é o caso do *Creeper*, primeiro vírus de computador desenvolvido em 1971 pelo americano Bob Thomas, que era pesquisador de segurança da BBN Technologies (PLAZA, 2022).

Durante a década de 1990, a internet se tornou acessível ao público em geral, promovendo uma explosão de conectividade global. Nesse cenário, as ameaças cibernéticas começaram a surgir com mais frequência e o vírus "ILOVEYOU" (2000) foi um exemplo notável, onde teve origem nas Filipinas, e espalhou-se via e-mail. O *worm* danificava o computador do usuário e mandava uma cópia de si mesmo para todos os seus contatos no Outlook. Ao executar o arquivo, que tratava-se de um *script* em *Visual Basic* disfarçado de uma

carta de amor vinda de um conhecido, o programa sobrescreve mídias no computador do usuário, tais como arquivos do pacote Microsoft Office, arquivos de áudio, imagens, entre outros (STRICKLAND, 2012).

Nos anos 2000, houve um aumento na complexidade das ameaças cibernéticas. Os ataques de negação de serviço em larga escala chamaram a atenção para a vulnerabilidade da infraestrutura digital. Além disso, tornaram-se frequentes os ataques de espionagem patrocinados por Estados, como o caso *Titan Rain*, termo usado pelo governo dos Estados Unidos para descrever uma série de ataques cibernéticos coordenados que ocorreram em 2003. Esses ataques supostamente tiveram origem no sul da China, mas devido ao uso de várias técnicas de ocultação, não foi possível determinar com precisão a localização exata dos computadores envolvidos ou a identidade dos perpetradores. Acredita-se que esses ataques estivessem direcionados especificamente ao governo dos Estados Unidos e fossem parte de uma estratégia de ameaça persistente avançada (APT), revelaram o crescente envolvimento governamental na ciberespionagem. Concomitantemente, a disseminação do *malware* Stuxnet em 2010 marcou a sofisticação das ameaças virtuais, visto que a Stuxnet é um *worm* de computador projetado e implantado para atacar instalações nucleares iranianas, tornando-se assim a primeira arma cibernética do mundo que impactou uma infraestrutura física. O Stuxnet atacou centrífugas nucleares iranianas, danificando e destruindo recursos militares críticos e causando grandes interrupções no programa nuclear do país (BUXTON, 2022).

Já durante a década de 2010, testemunhamos um aumento notável nos ataques de alto perfil. Isso incluiu o impacto global de ataques de *ransomware*, que é um tipo de *malware* de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate para restabelecer o acesso a estes arquivos, como o WannaCry e NotPetya, que afetaram empresas e instituições em todo o mundo. Ainda, as ameaças cibernéticas patrocinadas por Estados se tornaram mais comuns, com destaque para o envolvimento da Rússia nas eleições dos Estados Unidos em 2016, onde um relatório que concluiu que o governo russo interferiu nas eleições de 2020 com um impulso de desinformação que buscava manchar a campanha do presidente Joe Biden e apoiar Trump. O relatório do Escritório do Diretor de Inteligência Nacional descobriu que a Rússia usou supostos representantes ligados à inteligência russa para pressionar por afirmações mentirosas sobre Biden (CNN BRASIL, 2021). Conflitos cibernéticos começaram a se mesclar com conflitos militares convencionais, como os envolvendo a Rússia na Ucrânia e a China no Mar do Sul da China.

Na década atual, a cibersegurança tornou-se uma prioridade global, com um aumento na cooperação entre nações e organizações internacionais. As ameaças cibernéticas estão se tornando mais sofisticadas, com um foco crescente na infraestrutura crítica, militares e sistemas de defesa (ALCASSA E PAPPERT, 2023). A capacidade de guerra cibernética é agora reconhecida como parte integrante da estratégia militar, levando a investimentos em capacidades tanto ofensivas quanto defensivas, sendo as capacidades ofensivas envolvendo a capacidade de atacar e explorar vulnerabilidades em sistemas de computador, redes e infraestrutura de um inimigo e as defensivas referindo-se a medidas que protegem os próprios sistemas e redes contra ataques cibernéticos (O GLOBO, 2023). Isso permite que as nações alcancem objetivos de maneira mais eficaz e, em muitos casos, com menor custo humano, protegendo os interesses nacionais e alcançando objetivos estratégicos em um ambiente digital em constante expansão.

À medida que avançamos, é esperado que a guerra cibernética continue a evoluir e representar uma ameaça substancial para a segurança internacional. Portanto, a cibersegurança se tornará uma prioridade crescente, com países, organizações e indivíduos enfrentando o desafio de proteger seus sistemas e dados em um ambiente digital em constante evolução. A cooperação internacional será fundamental para enfrentar essas ameaças e estabelecer normas de comportamento responsável no ciberespaço (CISO ADVISOR, 2022a).

Assim, ao estudar os aspectos relacionados à guerra cibernética, torna-se clara a necessidade de uma revisão das possíveis ameaças no ciberespaço, assim como seus impactos na segurança internacional, consequências políticas e diplomáticas, proteção de dados e privacidade.

2. DESENVOLVIMENTO

2.1. A PROSPECTIVA ESTRATÉGICA

Um cenário futuro é elaborado a partir da reflexão sobre ocorrências passadas e tendências presentes, podendo evidenciar, de acordo com o sistema em questão analisado, situações mais favoráveis, favoráveis, desfavoráveis e catastróficas (VILLELA e MAIA, 2020; GODET, 1993), assim como orientar os atores envolvidos na preparação de potenciais mudanças. Com isso, é possível criar diferentes visões do futuro, estas desejáveis ou não, para guiar a formulação de estratégias e planos de ação dos atores em jogo.

Para isso, a técnica desenvolvida por Michel Godet usa da análise das condições atuais do sistema mediante a denominação das chamadas "sementes do futuro", assim como a delimitação dos principais atores e das variáveis-chaves para construir representações dos futuros possíveis, bem como as sequências de acontecimentos a que eles conduzem. Usa-se da investigação das tendências influentes sobre o sistema para identificar os mecanismos e agentes que, mediante diferentes possibilidades de atuação, podem contribuir ou atrapalhar a realização de diversos objetivos. A prospecção de cenários, portanto, infere o cruzamento de diferentes rotas diante de um horizonte temporal estabelecido (GODET, 1993).

Com isso, este trabalho se estrutura conforme o método de Godet. Ou seja, é dividido em três etapas, sendo a primeira compondo a investigação através da apresentação das sementes do futuro responsáveis por indicar possíveis tendências a serem observadas nos cenários criados. São sementes do futuro: tendências de peso, as quais consistem em movimentos de fácil previsão dos atores ou de uma variável dentro do cenário; fatos ou elementos pré determinados compostos por eventos já conhecidos e certos, cuja solução ou controle pelo sistema ainda não se efetivou; fatos portadores de futuro, sendo estes sinais ínfimos, por sua dimensão presente, existentes no ambiente, mas imensos por suas consequências e potencialidades; incertezas críticas que, de certo modo, são fatos portadores de futuro considerados mais importantes e com grau de incerteza maior para a questão principal; surpresas inevitáveis que são forças previsíveis, pois têm suas raízes em forças que já estão em operação no momento, mas não se sabe quando irão se configurar nem podemos conhecer previamente suas consequências e como nos afetarão; coringas, os quais referem-se às grandes surpresas, difíceis de serem antecipadas ou entendidas, diferente das surpresas inevitáveis que são de fácil previsão e cuja probabilidade de ocorrência é pequena, mas possui grande impacto (MARCIAL, 2008).

Após essa determinação segue-se para a denominação das variáveis, as quais – após análise estrutural por meio da criação de um quadro matricial qualitativo, assim como de um gráfico dispersivo – servirão para encontrar as variáveis-chave, as quais, de fato, interferem no sistema e são o resultado da investigação. Em seguida, passa-se para a segunda etapa, a qual consiste na análise do jogo de atores, cujos indivíduos e entidades que possuem capacidade de ação frente a guerra cibernética sejam evidenciados e seus objetivos e estratégias determinados. Para isso seguem-se sete fases de definição e análise, porém, neste trabalho, apenas estão presentes cinco delas: (1) Construção do quadro de Estratégias dos Atores; (2) Avaliação das relações de força entre os atores; (3) Identificação dos desafios estratégicos e dos objetivos

associados do sistema; (4) Posicionamento dos atores em função dos objetivos e identificação das convergências e divergências; (5) Hierarquização das prioridades no que tange aos objetivos de cada ator. A prospecção de cenários é a última etapa deste trabalho e também compõe os resultados e discussão da análise realizada na etapa anterior. Aqui, abordam-se os efeitos positivos e negativos da guerra cibernética diante da segurança internacional até 2050 compondo, assim, os seguintes cenários: mais favorável, favorável, desfavorável e, por fim, catastrófico (GODET e DURRANCE, 2011).

2.1.1. 1ª ETAPA: ENCONTRANDO AS SEMENTES DO FUTURO E VARIÁVEIS-CHAVE

A segurança internacional compõe uma das principais preocupações das nações desde os primórdios da formação do Estado de Direito, sendo pauta de diversas teorias da literatura de Relações Internacionais. Para muitos estudiosos, a agenda de segurança está atrelada à noção de poder e paz, podendo uma ser favorecida em relação a outra – como o poder para os defensores do Realismo e a paz para os teóricos do Idealismo (RUDZIT, 2005) –, porém a Revolução Digital inovou a forma com que os Estados e demais entidades a enxergam, uma vez que exige um certo nível de cooperação e inteligência para ser efetiva. Com tudo conectado, a privacidade e a proteção de informações são a prioridade, em especial com o desenvolvimento das ameaças digitais. Assim, a cibersegurança enraizou-se como pauta crucial dentro das discussões sobre segurança de cada país.

Internacionalmente, no entanto, pode-se afirmar que uma guerra é travada no ciberespaço tanto dos países contra hackers e demais programas quanto entre nações, visto que, em muitos casos, conflitos tradicionais usam do ciberespaço para causar dano à infraestrutura crítica de seus inimigos, tal como ocorreu no conflito entre Rússia e Ucrânia (FONSECA, 2023). Diante disso, é possível elencar algumas sementes do futuro:

Quadro 1 – Sementes do futuro

Tendências de peso	• Avanço tecnológico • Securitização dos crimes digitais • Debates sobre a privacidade no ciberespaço • Corrupção e furto de dados • Globalização
Fatos ou elementos predeterminados	• Aumento da desinformação e manipulação de dados • Aumento do cibercrime • Desigualdade tecnológica entre os países • Substituição do capital humano em conflitos
Fatos portadores de futuro	• Desenvolvimento de Inteligências Artificiais • Cooperação entre os Estados para o combate ao cibercrime • Ciberataques no setor privado • Protestos por parte da população • Investimento em segurança cibernética pela União Europeia • Formação de novos grupos de hackers
Incertezas críticas	• Uso do ciberespaço como arma estratégica por militares • Contratação de hackers por países • Ataques a órgãos governamentais de defesa dos Estados • Ataques ao sistema financeiro de um Estado • Promoção de legislações internacionais para a proteção do ciberespaço
Surpresas inevitáveis	• Ataques cibernéticos no conflito entre Rússia e Ucrânia • Uso de Inteligências Artificiais em conflitos • Guerra comercial entre China e Estados Unidos
Coringas	• Guerra cibernética generalizada • Uso de hackers para ataque nuclear

Fonte: Elaboração própria.

Com isso, é possível notar a crescente relevância do tema para a segurança internacional, visto que diversos acontecimentos da atualidade são capazes de instigar uma melhora ou piora na cibersegurança global. O avanço tecnológico (X1) observado na revolução digital é um claro exemplo disto, uma vez que o mesmo ganha destaque por sua atuação crucial no desenvolvimento da humanidade, não apenas no âmbito da tecnologia cibernética. Seu surgimento se deu na época da Segunda Guerra Mundial com o aprimoramento do maquinário existente no período. Posteriormente, a tecnologia cibernética passou por refinamentos e, graças aos avanços tecnológicos, a área se desenvolveu atuando na automotiva, informática e prospera para os tempos atuais com tecnologias como a internet (CLARO, 2009).

De forma semelhante, a globalização (X2) também se destaca por ser um dos processos em que a humanidade foi capaz de se desenvolver em diversas áreas e âmbitos diferentes. Portanto, no que tange a temática discutida quanto ao meio cibernético, foi o processo de globalização que permitiu a ciência atuar com mais força e impactar em cenários como o desenvolvimento tecnológico, permitindo que indivíduos tivessem um maior contato com diferentes tipos de tecnologia. A possibilidade de se conectar de diferentes formas com diversas pessoas ao redor do mundo abriu caminhos para que a tecnologia se desenvolvesse cada vez mais. Contudo, apesar dos benefícios que o mundo cibernético apresentou, também surgem preocupações, como a crimes cometidos nesse meio, a falta de regularização e jurisdição para atuar num ambiente que transcende o espaço físico, entre outros diversos casos (LOPES, 2018).

Em contrapartida, como exposto, graças aos avanços tecnológicos e o maior acesso da humanidade a tais ferramentas, não houveram apenas benefícios, mas também malefícios. Tendo em mente uma tecnologia como a internet e as redes sociais, o ambiente que se compõe nesse meio é, em sua maioria, um ambiente que é deficiente de um maior controle e regularização de informações. Dessa forma, as redes sociais são um exemplo de um meio de comunicação que, ao democratizar o acesso para as pessoas, também possibilitou ações que geram a manipulação de dados – e ao depender da intenção da informação – e consequentemente, geram uma maior desinformação (SANTOS, 2023). Portanto, com o desenvolvimento de novas tecnologias a cada década, tendo como exemplo a IA, a manipulação de dados se torna cada vez mais refinada e ocorre um aumento da desinformação (X3) (IAMASSITA, ARAÚJO, 2023).

Já o estímulo da ajuda estatal e das despesas militares, bem como do investimento privado, fará com que o desenvolvimento de novas tecnologias como a IA, o aprendizado de máquina, a robótica, o *big data* e as redes influencie amplamente os processos de produção, porém, segundo estudo realizado pelo corpo técnico do FMI em 2020, também contribuirá para o aumento da distância entre os países ricos e pobres ao transferir mais investimentos para economias avançadas onde a automação já está estabelecida (ALONSO, KOTHARI, REHMAN, 2020). Nesse sentido, o Relatório de Riscos Globais 2023 destaca a tendência à desigualdade tecnológica no futuro (X4), assim como a permanência – e agravamento em alguns casos – dos riscos de cibersegurança. Assim, o acesso a essas novas tecnologias para os países que as possam pagar, poderá solucionar parcialmente uma série de crises emergentes, desde a resposta a novas ameaças à saúde e à crise na capacidade dos cuidados de saúde, até ao aumento da segurança alimentar e da mitigação climática. Contudo, aos países sem essa

capacidade, o risco a ataques que colocam em xeque a soberania digital individual e o direito à privacidade se tornará uma realidade frequente. Além disso, a desinformação e a alta rotatividade de empregos são previsões que se acentuarão com o aumento desta desigualdade (WORLD ECONOMIC FORUM, 2023).

Por outro lado, o uso de tecnologias em conflitos (X5) é concomitantemente comum, porém, no que diz respeito à Inteligência Artificial, seu uso em conflitos costuma se manter no âmbito da análise de dados, tendo em vista que a maioria das IAs atuam via satélites e possuem um contato mais forte com meios tecnológicos como as redes sociais. Dessa forma, a análise de dados realizada pelas IAs possibilita um monitoramento de ações feitas por pessoas utilizando meios digitais, além de proporcionar o compartilhamento de dados entre Estados e a criação de novas estratégias para serem utilizadas em conflitos (DUTRA, 2023).

Ademais, uma vez que a segurança cibernética concentra-se na formação de uma infraestrutura para defender computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados de ataques maliciosos, a cooperação entre os Estados (X6) se mostra necessária para o bom funcionamento do sistema repressivo formado através de leis, acordos e normas internacionais de combate ao cibercrime. Ainda, os crimes cibernéticos causam ameaças particulares ao campo das finanças, escolas, serviços, governos, entre outros, e são vistos por alguns atores como crimes contra os direitos fundamentais da sociedade global, afetando a liberdade de expressão e a privacidade no ciberespaço. Com isso, debates internacionais como a Convenção de Budapeste – ou Convenção sobre o Crime Cibernético –, aberta para assinatura em 2001 e ratificada por 64 países, são modos de fomentar a cooperação neste sentido, trazendo luz aos males do cibercrime (ARAUJO, 2022).

Contudo, ataques cibernéticos podem constituir ataques de guerra, visto que esses se configuram como aplicação da força para produzir efeitos violentos, que não necessariamente são letais, como por exemplo ataques ao setor privado (STONE, 2013). Em ataques aos setores privados (X7), os hackers encontram falhas nos sistemas informáticos das empresas, os bloqueiam e exigem uma quantia em dinheiro para reiniciá-los. Nesse tipo de ataque, apesar de não letal, prejudica a produção de uma empresa, que se vê obrigada a interromper seus processos para que a violação não se estenda, além de influenciar o mundo físico apontando lacunas à Segurança e à Defesa dos países (G. VAZ, 2022).

Além disso, a chamada revolução dos assuntos militares (RAM) dá luz ao entendimento do ciberespaço como o quinto domínio a ser dominado pela via militar (X8). Neste sentido, a informação passa a ser o ativo estratégico central de modo que proteger a capacidade de coletar,

processar e disseminar um fluxo ininterrupto de informações são as principais metas. Para isso, no entanto, é necessário o domínio de três áreas: física, informacional e cognitiva. A primeira diz respeito aos elementos de uma força militar que devem estar ligados à realização segura e transparente da conectividade e interoperabilidade; a segunda corresponde à capacidade de pessoas e plataformas acessarem, compartilharem e protegerem os dados de forma a manter a superioridade informacional sobre o adversário; por fim, a última área indica que os militares devem ser capazes de usar essa informação comum para desenvolver a consciência de seu ambiente e compartilhá-la com outros participantes da rede. Desta forma, a compreensão da guerra pelas forças armadas com a inserção do quinto domínio à equação torna o uso do ciberespaço como uma arma estratégica uma relevante força da máquina de guerra das principais potências, uma vez que o controle da informação indica uma nova noção de superioridade bélica (TEIXEIRA JÚNIOR, LOPES, FREITAS, 2017).

Da mesma forma, conflitos e ataques cibernéticos fazem parte da trajetória da guerra "virtual" que ocorre silenciosamente entre diversos países, em sua maioria potências. Dessa forma, a contratação de hackers por países (X9) é decorrente de conflitos cibernéticos que se destaca por ganhar uma ressignificação nas últimas décadas do século XXI (TIDY, 2023). Devido ao aumento considerável de ataques cibernéticos, diversos países buscaram por novas táticas para melhorar a segurança de seus sistemas. Com o refinamento dos ataques se teve uma procura por *ethical hackers*, também conhecidos como "hackers do bem", capazes de criar um sistema de segurança mais potente (ALVES, 2023).

No entanto, a guerra comercial entre China e Estados Unidos (X10) também é relevante para a discussão. Seu início se deu em 2018 quando Donald Trump foi eleito presidente dos Estados Unidos e, assim como prometeu em sua campanha eleitoral, determinou uma taxação de 45% dos produtos chineses sob a bandeira do *America First*. Como retaliação, o governo chinês impôs tarifas de US$60 bilhões sobre os produtos americanos (dentre eles a soja, produtos químicos, automóveis e outros produtos). O embate comercial influenciou a economia chinesa não só no sentido comercial, mas também no aumento no foco interno do país com a formulação do programa *Made in China 2025*, o qual visa modernizar as indústrias nacionais e diminuir a dependência de países estrangeiros, contribuindo para o financiamento da criação de novas tecnologias e culminando no aparecimento da *Huawei* e da tecnologia do 5G. No entanto, as sanções estadunidenses a *Huawei* acarretaram no atraso da Revolução 4.0 no cenário internacional, uma vez que a gigante chinesa é impedida pelos norte-americanos de se inserir em novos mercados e a tecnologia 5G, cuja relevância se deve a melhoria significativa nas

formas de comunicação dos países, é impedida de vigorar no ciberespaço internacional, impedindo otimizações no controle de dados (NASCIMENTO *et al*, 2022).

Concomitantemente, como supracitado, o conflito entre Rússia e Ucrânia usa do ciberespaço para realizar ataques (X11), tornando a investigação do conflito uma variável importante para o contexto estudado. Nesse sentido, Hunter (2014) classifica a guerra entre Rússia e Ucrânia como uma guerra híbrida, isto é

> campanhas sofisticadas que combinam, em baixo nível, ações convencionais e operações especiais; mais ações virtuais e espaciais ofensivas; e operações psicológicas que usam as mídias sociais e tradicionais para influenciar a percepção de populares e a opinião pública internacional. (*apud* SOUZA *et al*, 2020, p. 2)

De acordo com o International IT (2022a), logo antes da invasão terrestre pela Rússia em fevereiro de 2022, a Ucrânia sofreu ataques de *Distributed Denial-of-Service* (DDoS) em dois bancos estatais, no Ministério da Defesa e nas Forças Armadas. Com a invasão, os ataques foram intensificados, em especial, em infraestruturas críticas da Ucrânia, além das instituições. A reação ucraniana foi o recrutamento de voluntários para formar um "Exército de TI", o qual visava promover ataques às instituições e serviços russos (INTERNATIONAL IT, 2022b; FONSECA, 2023).

Ademais, o envolvimento de atores não estatais levou a hacktivistas e cibercriminosos a se posicionarem e defenderem um dos lados do conflito. O grupo *Anonymous* declarou-se contra a Rússia e efetivou ataques DDoS a sites corporativos, estatais e de notícias, o que afetou mais de 90 bancos de dados de telecomunicações, organizações do setor governamental e do varejo, além de vazar milhares de documentos. O mesmo pode ser dito do grupo GhostSec, o qual declarou ter feito ataques DDoS a sites militares russos. Já os grupos pró-Rússia como o grupo de *ransomware* Conti e grupos de crimes cibernéticos *CoomingProject* manifestaram proteção ao governo russo. A gangue hacktivista *Killnet*, por exemplo, costuma promover ataques DDoS a infraestruturas críticas dos membros da OTAN e apoiadores da Ucrânia (FONSECA, 2023; MALLICK, 2022).

Por outro lado, ao analisar a cooperação em prol ao combate ao cibercrime, a União Europeia (UE) é um dos principais atores envolvidos neste processo, uma vez que a cibersegurança é uma das prioridades políticas e institucionais do bloco desde 1990. Suas ações giram em torno de políticas de privacidade para proteger governos, economias e cidadãos. Assim, o bloco investe incisivamente no tópico (X12) como observado em debates ocorridos em 2023 acerca da criação da Lei de Solidariedade Cibernética que visa melhorar a segurança

cibernética e fazer com que os países do bloco cooperem em caso de ataque. Esse projeto surgiu em março de 2022, após a invasão da Ucrânia pela Rússia e os ataques cibernéticos advindos do conflito e possui um investimento de € 1,1 bilhão, contemplando tanto a esfera pública quanto privada (CRYPTOID, 2023).

Nesse sentido, é fato afirmar que uma preocupação não só da UE como de diversos países e agentes está na ameaça de criação de novos vírus (X13). Os vírus de computador – reconhecidos pela maioria populacional do mundo como vandalismo cibernético – com o passar dos anos evoluíram e hoje são considerados crimes virtuais. Em 2014, cientistas da Universidade de Liverpool criaram um vírus que poderia ser transferido via redes *wi-fi* abertas e depois de conectar- se a um ponto, se espalhava por outras redes atacando roteadores e coletando informações de seus usuários. Esse vírus cria um alerta sobre a criação de novos vírus de computador, visto que esse tipo poderia atacar sistemas de *data link* e contaminar toda uma rede inviabilizando a troca de informações (NETO, 2017).

Da mesma forma, o uso de *softwares* e outras técnicas invasivas com a intenção de adquirir informações confidenciais e danificar instalações civis e militares já é reconhecida mundialmente como um dos muitos tipos de ciberataques realizados até mesmo por países. No entanto, suspeita-se que Israel e Estados Unidos desenvolveram em suas agências de segurança, *malwares* que teriam o propósito de atacar as centrífugas de enriquecimento de urânio do Irã, além de espionar outros países do Oriente Médio (X14) (NETO, 2017), o que pode prejudicar a cooperação internacional sobre a cibersegurança.

Outra preocupação está nos ataques promovidos por hackers a petroquímicas e até mesmo usinas nucleares (X15), dado que os mesmos poderiam causar a explosão de um reator. Um exemplo deste fato está que, desde o início da invasão russa em território ucraniano em 2022, o grupo de hackers russos *Cold River* reorganizaram seus ataques contra os aliados da Ucrânia, atacando a Polônia e a Letônia, além de três laboratórios de pesquisa nuclear nos Estados Unidos (DEUTSCHE WELLE, 2023).

Ainda, como já mencionado, a disputa entre China e Estados Unidos pelo domínio da tecnologia ganha novos capítulos a cada dia (X16). Em uma resposta aos aliados dos norte-americanos na Ásia, que restringiram a venda de chips de memória chineses para Pequim, a China iniciou uma investigação de cibersegurança na *Micron Tecnology*, uma das maiores fabricantes de tecnologia dos Estados Unidos (HE, 2023).

Como consequência, os ataques cibernéticos aumentaram gradativamente. Somente em 2022, por exemplo, foram mais de 31,5 bilhões de tentativas de ataques a empresas. Isso

evidencia a necessidade da contratação de profissionais formados em cibersegurança (X17) tanto para prevenir ataques quanto para restaurar o sistema caso algo dano seja infringido (FUNDAÇÃO VANZOLINI, 2023). O reconhecimento deste fato fez com que o Ministério da Ciência, Tecnologia e Inovação (MCTI) lançasse o programa “Hackers do bem” com o objetivo de suprir a demanda de profissionais na área de cibersegurança (SECURITY REPORT, 2023).

Ademais, também é fato que, como a infraestrutura crítica de um país abarca tanto sistemas digitais quanto físicos que fornecem serviços essenciais à população, um ataque às mesmas significa um grande impacto na segurança, economia, política, energia, saúde e outros setores importantes de um país. A partir de 2010, a ideia de utilizar de *malwares* como “arma” em tensões geopolíticas (X18) tornou-se palpável, em especial em 2022 quando *malwares* foram usados arma para gerar desestabilização no conflito entre a Rússia e a Ucrânia (MENDOZA, 2022).

Em contrapartida, debates acerca da regulamentação do ciberespaço ganham espaço na atualidade, dado que o mesmo é definido como um mundo virtual, ou seja, um mundo completamente artificial e imaterial existente em um local indefinido e em outra realidade. Muitos, por o visualizarem como um domínio anárquico, creem ser impossível regulamentá-lo, porém Lawrence Lessig, professor de "*cyber laws" da Harvard Law School*, defende a possibilidade de se criar um código do ciberespaço que assim como as leis fixaria os valores do espaço virtual (X19). Esse código pode tornar certas condutas obrigatórias ou até mesmo proibi-las, por fim os legisladores reais podem regular o próprio código (KAMINSKI, 2001).

Por fim, a última tendência relevante observada diz respeito ao uso do metaverso para a segurança cibernética (X20), uma vez que a Organização Internacional de Polícia Criminal (Interpol) lançou o primeiro metaverso planejado para combater crimes cibernéticos**.** O projeto foi pensado em vista dos criminosos que se aproveitam do espaço virtual para realizar atos ilegais. O espaço se chama Interpol Metaverso e é um ambiente virtual no qual os policiais podem interagir e trocar informações, além de poderem fazer cursos de policiamento (CISO ADVISOR, 2022b).

Desta forma, os fatores elencados anteriormente podem ser compreendidos como variáveis do sistema, visto que estão, incisivamente, relacionados ao contexto da guerra cibernética e, consequentemente, da segurança internacional. Como afirma o Godet em sua metodologia, para a identificação das variáveis-chave, é preciso realizar uma matriz de análise estrutural (Quadro 2), na qual classifica-se de 0 a 1 a capacidade de influência de cada variável

uma para com a outra. Após isso, soma-se cada nota para se obter a quantidade de influência de cada variável e de dependência.

Quadro 2 – Matriz de análise estrutural

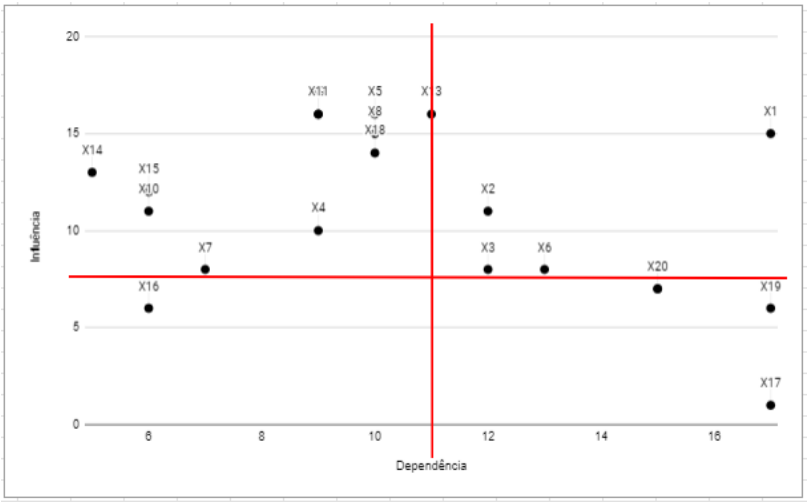
	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	X11	X12	X13	X14	X15	X16	X17	X18	X19	X20	I
X1	0	1	1	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1	1	1	15
X2	1	0	1	1	0	1	0	0	1	1	1	0	0	0	0	1	1	0	1	1	11
X3	0	0	0	1	0	1	1	0	0	1	1	1	0	0	0	0	1	0	1	0	8
X4	0	0	1	0	1	0	0	1	0	1	1	1	0	0	0	1	0	1	1	1	10
X5	1	0	1	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	16
X6	1	1	0	0	1	0	0	1	0	0	0	1	0	0	0	0	1	0	1	1	8
X7	1	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	1	1	8
X8	1	0	1	0	1	1	0	0	1	0	1	1	1	1	1	1	1	1	1	1	15
X9	1	1	1	0	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	16
X10	1	1	1	1	0	0	1	0	1	0	0	1	1	0	0	1	1	0	1	0	11
X11	1	1	1	1	1	1	1	1	1	0	0	1	1	0	1	0	1	1	1	1	16
X12	1	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	1	1	7
X13	1	1	1	0	1	1	1	1	1	0	1	1	0	1	1	0	1	1	1	1	16
X14	1	1	1	1	1	1	0	1	1	0	0	0	1	0	0	0	1	1	1	1	13
X15	1	1	0	0	1	1	0	1	1	0	0	1	1	0	0	0	1	1	1	1	12
X16	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	6
X17	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
X18	1	0	0	1	1	1	1	1	1	0	1	1	1	0	1	0	1	0	1	1	14
X19	1	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	1	6
X20	1	1	0	1	0	1	0	0	0	0	0	1	0	0	0	0	1	0	1	0	7
D	17	12	12	9	10	13	7	10	9	6	9	15	11	5	6	6	17	10	17	15	–

Fonte: Elaboração própria.

Obtidas as relações de influência e dependência das variáveis, encontra-se o Ponto Médio de Influência (PMi) e o Ponto Médio de Dependência (PMd) a fim de encontrar-se, mediante uso de um gráfico de dispersão, as variáveis-chave. As mesmas são definidas observando-se a posição das variáveis em cada quadrante, sendo o primeiro quadrante composto por variáveis de entrada, as quais são muito influentes e pouco dependentes; o segundo quadrante formado por variáveis de ligação que são muito influentes e muito dependentes; o terceiro por variáveis excluídas cuja influência e dependência são mínimas para o sistemas; e o quarto quadrante formado por variáveis de resultado que são pouco influentes e muito dependentes (GODET e DURRANCE, 2011).

Como resultado desta matriz, portanto, tem-se que o PMi equivale a 8,5 enquanto o PMd é igual a 11, permitindo concluir que as variáveis-chave são: X1, X2, X3, X4, X5, X6,X7, X8, X9, X10, X11, X12, X13, X14, X15, X17, X18, X19 e X20.

Gráfico 1 – Gráfico de dispersão das variáveis



Fonte: Elaboração própria.

2.1.2. 2ª ETAPA: O JOGO DOS ATORES

Com isso, passamos para a análise do jogo estratégico de atores, o qual visa fornecer a um determinado ator formas de apoio à decisão para a implementação da sua política de alianças e de conflitos, condicionando a evolução do sistema (GODET, 1993). A apresentação dos agentes responsáveis pelo comando das variáveis chaves é um fator essencial para compreender seus objetivos, problemas e meios de ação no sistema, assim como para compor o quadro de Estratégias dos Atores (Quadro 3). Desta maneira, os Estados Nacionais (A1) destacam-se como o primeiro ator relevante para este trabalho. Os mesmos são entidades políticas soberanas que exercem autoridade sobre um território geográfico específico e sua população (AMORIM, 2022) e desempenham um papel fundamental na cibersegurança, exercendo influência em várias frentes. Eles estabelecem legislação e regulamentações para orientar a segurança cibernética, abrangendo áreas como proteção de dados, cibersegurança e combate ao cibercrime, tornando-se um dos primeiros atores relevantes para a análise.

A segurança cibernética também é uma parte crítica da defesa nacional, com investimentos significativos em medidas de proteção contra ameaças cibernéticas que visam infraestruturas críticas, redes de comunicação e sistemas militares. Agências de inteligência cibernética são mantidas para coletar informações sobre ameaças cibernéticas e conduzir operações de ciberespionagem. Além disso, Estados nacionais participam de esforços internacionais para estabelecer normas e acordos no ciberespaço, incluindo a regulação de cibersegurança global e acordos de não proliferação de armas cibernéticas. Alguns Estados também exercem poder estatal no ciberespaço, conduzindo operações cibernéticas ofensivas

para proteger seus interesses ou responder a ameaças percebidas. Outro ponto, é o fato dos Estados nacionais terem um papel na aplicação da lei e no combate ao cibercrime, colaborando com agências policiais e internacionais para investigar e processar criminosos cibernéticos (AGÊNCIA CÂMARA NOTÍCIAS, 2011).

Em suma, a influência dos Estados nacionais na cibersegurança é abrangente e fundamental. Eles são atores-chave na promoção da cibersegurança em suas jurisdições e no cenário global, protegendo interesses nacionais e promovendo um ambiente seguro na internet. A cibersegurança é um desafio complexo e global, no qual os Estados desempenham um papel central na proteção contra ameaças cibernéticas e na promoção da resiliência cibernética (AGÊNCIA CÂMARA NOTÍCIAS, 2011).

Já os grupos cibernéticos estatais (A2), também conhecidos como atores cibernéticos estatais, são equipes de especialistas em cibersegurança que operam sob o comando e o financiamento de um governo ou agência governamental (HSC, 2023). Esses grupos são geralmente responsáveis por conduzir operações cibernéticas em nome do Estado para alcançar objetivos específicos, que podem incluir vigilância, coleta de informações, ciberespionagem, sabotagem, defesa cibernética e outras atividades relacionadas à segurança nacional.

Outra ação que os grupos cibernéticos estatais realizam são operações ofensivas, eles também trabalham na proteção das redes de computadores do governo contra ataques cibernéticos. Ademais, desenvolvem estratégias e tecnologias de segurança para impedir ou mitigar ameaças. Em algumas situações, esses grupos podem ser encarregados de conduzir ataques cibernéticos ofensivos, como operações de ciberataque ou guerra cibernética em resposta a ameaças percebidas ou para alcançar objetivos estratégicos (TIDY, 2023).

É importante notar que a atuação de grupos cibernéticos estatais também é uma área de grande controvérsia, uma vez que a atribuição de ataques cibernéticos a governos nem sempre é clara e pode levar a tensões internacionais (TIDY, 2023). Além disso, o uso de ferramentas cibernéticas em conflitos políticos e militares têm implicações significativas em termos de ética e direito internacional. Dessa forma, os grupos cibernéticos estatais desempenham um papel crucial na segurança e na política internacionais, pois moldam o cenário cibernético global e têm um impacto direto na proteção das infraestruturas críticas e na coleta de informações sensíveis.

Os grupos cibernéticos não estatais (A3), também conhecidos como atores cibernéticos não estatais, são organizações ou indivíduos que operam no ciberespaço, mas não têm afiliação

ou respaldo governamental. Eles podem incluir hackers independentes, grupos de hacktivistas, organizações criminosas cibernéticas e grupos de ciberativistas (TECNOBLOG, 2022).

Primeiramente, o hacktivismo é uma forma de ativismo online, em que esses grupos utilizam suas habilidades técnicas para promover causas políticas ou sociais. Isso pode envolver a divulgação de informações confidenciais, ataques de negação de serviço (DDoS) contra alvos relacionados à causa e a exposição de práticas corporativas questionáveis (MANAGEENGINE BLOG, 2023). Eles desempenham um papel fundamental na ampliação do debate público sobre questões importantes.

Além disso, alguns grupos cibernéticos não estatais concentram-se em questões de segurança cibernética e defesa. Eles podem identificar vulnerabilidades em sistemas e redes e divulgá-las ou, em alguns casos, ajudar a corrigi-las. Isso contribui para o aumento da conscientização sobre a importância da segurança cibernética e para a melhoria da segurança global na internet. Por outro lado, alguns desses grupos têm motivações criminosas, envolvendo-se em atividades ilegais, como o roubo de dados pessoais, fraudes financeiras e ataques de ransomware (TECNOBLOG, 2022). Isso resulta em prejuízos financeiros significativos para empresas e indivíduos, destacando a necessidade de combater o cibercrime.

No entanto, é importante notar que a atuação de grupos cibernéticos não estatais também pode ser controversa e levantar preocupações de legalidade e ética. Algumas de suas atividades podem ser ilegais e prejudiciais, como ataques cibernéticos indiscriminados ou ações de cibercrime. A complexidade desses grupos reside no fato de que eles podem operar em uma zona cinzenta, trata-se de uma zona de contornos mal definidos (LEVI, 2004) onde os limites entre atividades legítimas, como pesquisa em segurança cibernética, e atividades ilegais, como ataques cibernéticos, não são sempre claros. Portanto, o impacto dos grupos cibernéticos não estatais depende da natureza de suas ações e das motivações por trás delas. Suas atividades moldam o debate e os desafios enfrentados no ciberespaço contemporâneo.

Em contrapartida, as empresas privadas de segurança cibernética (A4) são organizações especializadas em fornecer serviços, produtos e soluções destinados a proteger sistemas de computadores, redes e dados de ameaças cibernéticas. Elas desempenham um papel crucial na defesa contra uma ampla gama de ameaças cibernéticas, elas desenvolvem soluções e implementam medidas de segurança para proteger sistemas e dados, garantindo a continuidade das operações de empresas e instituições (TPS, 2023). Além de estarem na vanguarda da inovação em tecnologia de segurança cibernética, onde constantemente desenvolvem novas

soluções e estratégias para lidar com ameaças em constante evolução. Isso contribui para a melhoria contínua da cibersegurança em todos os setores.

Quando ocorrem violações de segurança cibernética, as empresas privadas de segurança cibernética desempenham um papel crucial na resposta a incidentes. Elas ajudam a identificar a causa da violação, mitigar os danos e restaurar a integridade dos sistemas afetados. Outro impacto a ser levantado é que as empresas privadas de segurança cibernética desempenham um papel na construção da resiliência cibernética. Isso envolve a implementação de medidas de segurança proativas para reduzir a probabilidade e o impacto de incidentes cibernéticos (AWS, 2024).

Dessa forma, as empresas privadas de segurança cibernética são peças fundamentais para garantir a segurança e a estabilidade no mundo digital em constante evolução. Seu papel na defesa contra ameaças cibernéticas, na promoção da inovação em segurança e na educação sobre cibersegurança é essencial para a proteção de ativos digitais e a manutenção da confiança no ambiente online (TIVIT, 2024).

As Organizações Internacionais (OIs) (A5) são coalizões de países que se unem para enfrentar questões globais, promover a paz e resolver problemas que ultrapassam fronteiras nacionais (DUFFIELD, 2007). No contexto da segurança cibernética, essas organizações desempenham um papel essencial, uma vez que as ameaças cibernéticas não reconhecem fronteiras. Elas impactam a segurança cibernética de diversas maneiras, incluindo o desenvolvimento de normas e diretrizes internacionais para a segurança cibernética, a promoção da cooperação entre países para enfrentar ameaças cibernéticas, a mediação de conflitos cibernéticos entre nações e a oferta de assistência técnica a países em desenvolvimento para fortalecer suas defesas cibernéticas (MAPA MUNDI, 2023).

Por outro lado, Organizações Não Governamentais (ONGs) (A5), independentes de governos, desempenham um papel importante na promoção da segurança cibernética por meio de atividades como advocacia, conscientização pública, pesquisa, educação e defesa dos direitos digitais. Elas advogam por políticas públicas que melhorem a segurança cibernética, promovem a conscientização sobre boas práticas cibernéticas e defendem a privacidade e a liberdade na internet. Algumas ONGs também oferecem assistência a vítimas de cibercrimes e contribuem para a segurança online (PORTAL BRASILEIRO DA CIBERSEGURANÇA, 2024).

Tanto organizações internacionais quanto ONGs complementam os esforços dos governos na busca de um ambiente cibernético mais seguro e na mitigação dos riscos

cibernéticos. Sua influência e impacto são fundamentais para lidar com as complexas ameaças cibernéticas que afetam a sociedade globalmente. A colaboração entre governos, organizações internacionais e ONGs é essencial para enfrentar de maneira eficaz essas ameaças e promover a segurança cibernética em todo o mundo.

Já hackers são indivíduos (A6) que têm habilidades técnicas em computação e redes para acessar sistemas de computadores, redes, software e dispositivos eletrônicos de maneira não autorizada ou para encontrar vulnerabilidades e falhas de segurança nesses sistemas (MICHAELIS, 2024).

As ameaças associadas aos hackers incluem: roubo de dados, visto que, eles podem acessar informações confidenciais, como informações pessoais, números de cartão de crédito, segredos comerciais e dados governamentais; ataques de Ransomware, onde eles podem criptografar sistemas e exigir resgates em troca da chave de descriptografia, causando interrupções graves nos negócios e prejuízos financeiros; espionagem cibernética, esses hackers podem coletar informações sensíveis, como segredos comerciais, planos de governo e informações militares, em operações de ciberespionagem; ataques de negativa de Serviço (DoS) e Distribuídos (DDoS), tais hackers podem sobrecarregar servidores e redes com tráfego malicioso, tornando os serviços inacessíveis, o que pode prejudicar empresas e instituições (TUDO CELULAR, 2022)

A ameaça dos hackers é real e constante, e as organizações e indivíduos devem adotar medidas robustas de segurança cibernética para proteger seus sistemas e dados. Isso inclui a implementação de firewalls, software antivírus, autenticação de dois fatores, monitoramento de rede e educação em segurança cibernética para funcionários (CEDROTECH, 2023). Além disso, é importante manter sistemas e software atualizados para corrigir vulnerabilidades conhecidas que os hackers poderiam explorar.

A infraestrutura crítica (A7), por fim, refere-se a sistemas, instalações, ativos e redes essenciais para o funcionamento de uma sociedade, economia e governo. Essas infraestruturas desempenham um papel fundamental na manutenção da estabilidade e do funcionamento adequado de uma nação. São consideradas críticas porque sua interrupção, destruição ou comprometimento significativo pode ter sérias consequências para a segurança nacional, a economia e o bem-estar público (IBM,2023).

A infraestrutura crítica pode abranger uma variedade de setores, incluindo: energia (redes de eletricidade, produção de petróleo e gás, refinarias, usinas nucleares e fontes de energia renovável); transportes (rodovias, ferrovias, aeroportos, portos e sistemas de trânsito);

comunicações (redes de telecomunicações, internet, satélites e sistemas de rádio e televisão); água (abastecimento de água potável, tratamento de águas residuais e sistemas de distribuição); saúde (hospitais, clínicas, instalações de pesquisa médica e farmacêutica); segurança pública (polícia, bombeiros, serviços de emergência e sistemas de segurança); financeiro (sistemas financeiros, como bancos e bolsas de valores) (IBM, 2023).

A importância da infraestrutura crítica reside no fato de que ela sustenta a vida cotidiana e a funcionalidade da sociedade. Qualquer interrupção significativa ou ataque a essas infraestruturas pode resultar em consequências graves, como perda de vidas, desestabilização econômica e caos social (O TEMPO, 2022) . Portanto, proteger e fortalecer a infraestrutura crítica é uma prioridade para a segurança nacional e a resiliência da nação.

Isto posto, a definição dos atores do sistema permite a criação do quadro de Estratégias dos Atores (Quadro 3) no qual analisa-se os objetivos e meios de ação de cada ator para com os demais.

Quadro 3 – Estratégias dos Atores

Ação de atores sobre atores	A1 (Estados Nacionais)	A2 (Grupos Cibernéticos Estatais)	A3 (Grupos Cibernéticos Não Estatais)	A4 (Empresas de Segurança Cibernética)	A5 (OI e ONG)	A6 (Indivíduos)	A7 (Infraestrutura Crítica)
A1 (Estados Nacionais)	X	Investir e legalizar os grupos cibernéticos estatais.	Criação de leis direcionadas ao combate desses grupos.	Incentivo para o desenvolvimento de soluções para segurança.	Fomento da colaboração.	Criação de leis direcionadas ao combate desses grupos.	Proteger e fortalecer.
A2 (Grupos Cibernéticos Estatais)	Defender os interesses nacionais e aprimorar o sistema de segurança.	X	Bloquear os ataques contra os sistemas.	Cooperar.	Cooperar.	Aprimorar o sistema de segurança.	Aprimorar o sistema de segurança.
A3 (Grupos Cibernéticos Não Estatais)	Ataques direcionados à inteligência nacional.	Aprimorar táticas de hackeamento.	X	Buscar formas de enfraquecer o sistema.	Realizar boicotes.	Recrutamento.	Aprimorar táticas de hackeamento e ataques direcionados.
A4 (Empresas de Segurança Cibernética)	Negociar softwares de segurança.	Cooperar.	Capacitação dos colaboradores contra possíveis invasões.	X	Negociar softwares de segurança.	Capacitação dos colaboradores contra possíveis invasões.	Venda de softwares de segurança.
A5 (OI e ONG)	Busca por financiamento de sistemas de segurança.	Cooperar.	Devem buscar se defender dos ataques para que suas informações não sejam comprometidas.	Parceria para maior proteção contra os hackers.	X	Devem buscar se defender dos ataques para que suas informações não sejam comprometidas.	Conscientizar sobre a importância da defesa dos sistemas.
A6 (Indivíduos)	Buscar informações confidenciais.	Enfraquecer os sistemas.	Cooperar.	Hackear para chantagear.	Realizar boicotes.	X	Enfraquecer os sistemas de segurança.
A7 (Infraestrutura Crítica)	Buscar apoio para melhorias.	Cooperar.	Devem buscar se defender dos ataques para que suas informações não sejam comprometidas.	Compra de softwares de segurança.	Cooperar a fim de minimizar as falhas do sistema.	Devem buscar se defender dos ataques para que suas informações não sejam comprometidas.	X

Fonte: Elaboração própria.

Além disso, realiza-se uma nova matriz estrutural (Quadro 4), classificando a capacidade de influência e dependência dos atores com as variáveis-chave do sistema com notas

de 0 a 1, sendo 0 nenhum pouco influente ou dependente e 1 influente ou dependente. Ao fim, somam-se as notas de cada linha para se obter o quão influente é cada ator, assim como a soma das colunas revela o quão dependente cada variável pode ser. Assim, após analisar os resultados, podemos afirmar que os atores mais influentes são A1, A2 e A6, enquanto as variáveis mais dependentes são X5, X8 e X18.

Quadro 4 – Relação de influência entre atores e variáveis-chave

	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	X11	X12	X13	X14	X15	X17	X18	X19	X20	I
A1	1	0	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	16
A2	0	0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	15
A3	0	0	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	13
A4	1	1	1	1	1	0	1	0	0	0	0	0	1	1	1	1	1	0	1	12
A5	0	1	0	0	0	1	0	0	0	1	1	0	0	0	0	0	1	1	1	7
A6	1	1	1	0	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	17
A7	1	0	0	1	1	0	0	1	0	0	1	0	0	0	0	0	1	0	0	6
D	4	3	5	4	6	5	3	6	4	5	5	2	4	5	5	5	7	4	4	

Fonte: Elaboração própria.

Com essa análise, a fase um da análise do jogo dos atores é finalizada, permitindo o início da segunda fase, na qual avalia-se a relação de forças entre os atores. Deste modo, baseando-se na avaliação dos objetivos, problemas e meios de ação, torna-se possível construir uma uma matriz de influência direta (MID) entre os atores do cenário. Nesse sentido, distribui-se quatro níveis de valores fundamentados a partir dos seguintes critérios: em um nível 0 o ator tem pouca ou quase nenhuma influência sobre outro ator; no nível 1 o ator possui influência fraca sobre outro ator, colocando em causa de maneira limitada os processos operatórios de gestão de outro ator; no nível 2 o ator possui influência média sobre outro ator, de maneira a colocar em causa a realização dos projetos de outro ator; por último, no nível 3 o ator possui influência forte sobre o outro ator, de modo a colocar em causa o cumprimento das missões ou a existência de outro ator. Essa categorização em níveis facilita uma análise mais aprofundada das interações entre os diferentes agentes do cenário, proporcionando uma compreensão mais clara do impacto e das dinâmicas presentes entre eles.

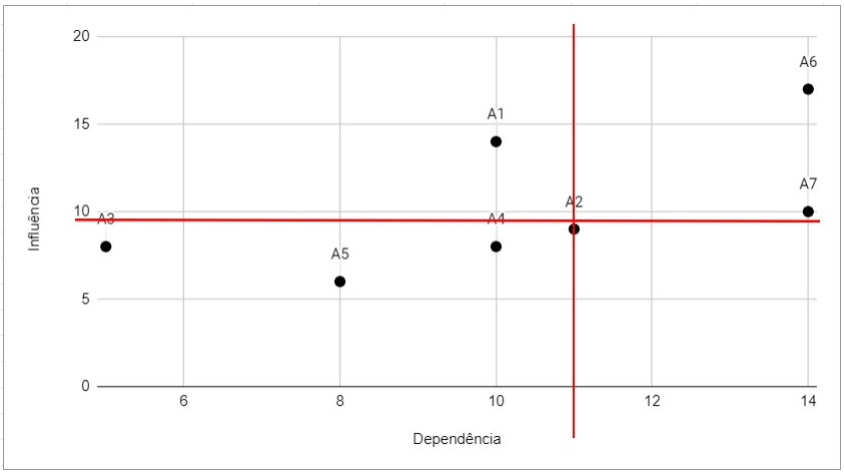
Quadro 5 – Matriz de influência direta entre os atores: Atores X Atores

	A1	A2	A3	A4	A5	A6	A7	I
A1	0	3	1	1	3	3	3	14
A2	2	0	0	1	1	2	3	9
A3	0	1	0	2	1	2	2	8
A4	1	1	1	0	0	2	3	8
A5	2	0	0	1	0	3	0	6
A6	2	3	3	3	3	0	3	17
A7	3	3	0	2	0	2	0	10
D	10	11	5	10	8	14	14	–

Fonte: Elaboração própria.

Assim, com os resultados obtidos de influência e dependência dos atores entre si, encontra-se o Ponto Médio de Influência (PMi) e o Ponto Médio de Dependência (PMd) a fim de distinguir-se, mediante uso de um gráfico de dispersão, os atores dominantes, dominados, de ligação e autônomos. Da mesma forma que a definição das variáveis-chave, esta classificação se dá por meio da localização dos atores em cada quadrante. No primeiro quadrante estão os atores dominantes; no segundo os atores de ligação; no terceiro os autônomos; e no quarto os atores dominados (GODET e DURRANCE, 2011). Assim, tem-se que o PMi equivale a 11,5 enquanto o PMd é igual a 9,5, permitindo concluir que apenas o A1 é um ator dominante, o A2 um ator dominado, os atores A3, A4 e A5 são autônomos e os atores A6 e A7 são de ligação.

Gráfico 2 – Gráfico de dispersão dos atores



Fonte: Elaboração própria.

Assim inicia-se a fase 3, ou de identificação dos desafios estratégicos e dos objetivos associados do sistema. O Quadro 6 contém os referidos desafios e objetivos.

Quadro 6 – Desafios Estratégicos e Objetivos Associados do sistema

Desafios Estratégicos	Objetivos Associados
Cooperação	1) Criação de leis mais restritivas
	2) Compartilhamento de tecnologias para segurança
Desenvolvimento de tecnologias	3) Desenvolvimento em P&D de novas tecnologias
	4) Aprimoramento do sistema de segurança

Fonte: Elaboração própria.

E, com isso, partimos para a fase 4 na qual há o posicionamento dos atores em função dos objetivos e identificação das convergências e divergências. Esta fase consiste na percepção das relações entre os atores e os objetivos (Quadro 7) e dos atores entre si (Quadro 8). Nesse sentido, a primeira matriz demonstra se os atores são favoráveis (+1), indiferentes (0) ou desfavoráveis (-1) a cada objetivo, enquanto a segunda avalia as convergências e divergências entre os atores do sistema.

	O1	O2	O3	O4
A1	+1	+1	+1	+1
A2	0	0	0	+1
A3	-1	-1	0	-1
A4	0	0	+1	+1
A5	+1	+1	+1	+1
A6	-1	-1	-1	-1
A7	+1	+1	+1	+1

Quadro 7 – Matriz de Convergências e Divergências (Atores X Objetivos)

Fonte: Elaboração própria.

Quadro 8 – Matriz de Convergências e Divergências (Atores X Atores)

		A1	A2	A3	A4	A5	A6	A7

A1	**Convergência** **Divergência**	–	1 0	0 3	2 0	4 0	0 4	4 0
A2	**Convergência** **Divergência**	1 0	–	0 1	1 0	1 0	0 1	1 0
A3	**Convergência** **Divergência**	0 3	0 1	–	0 1	0 3	3 0	0 3
A4	**Convergência** **Divergência**	2 0	1 0	0 1	–	2 0	0 2	2 0
A5	**Convergência** **Divergência**	4 0	1 0	0 3	2 0	–	0 4	4 0
A6	**Convergência** **Divergência**	0 4	0 1	3 0	0 2	0 4	–	0 4
A7	**Convergência** **Divergência**	4 0	1 0	0 3	2 0	4 0	0 4	–

Fonte: Elaboração própria.

Por fim, a última fase de análise se inicia, cuja hierarquização das prioridades no que tange aos objetivos de cada ator é feita. Nela, uma tabela estabelece a hierarquia dos objetivos para cada ator, evidenciando a intensidade de seu posicionamento a partir de critérios separados em 5 níveis. Em um nível 0 o objetivo é pouco consequente para o ator; no nível 1 o objetivo favorece de modo limitado, no tempo e no espaço, o processo de operação; no nível 2 o objetivo é indispensável para o sucesso de seus projetos; no nível 3 o objetivo é indispensável para o sucesso de suas missões; (depende completamente para atuar no sistema), já no nível 4 o

HUMANIDADES & TECNOLOGIA (FINOM) - ISSN: 1809-1628. vol. 46- jan./mar.2024
Doi 10.5281/zenodo.10565391

objetivo é indispensável para sua própria existência. Com este conhecimento, a prospectiva de cenários torna-se possível, tendo todos os elementos necessários para traçar os caminhos futuros do sistema.

Quadro 9 – Atores X Objetivos

	O1	O2	O3	O4
A1	2	1	2	4
A2	1	1	1	3
A3	0	0	1	0
A4	1	1	3	4
A5	1	2	2	2
A6	0	0	1	0
A7	2	1	3	4

Fonte: Elaboração própria.

2.1.3. 3ª ETAPA

2.1.3.1. CENÁRIO MAIS FAVORÁVEL

Entre todos os cenários, o mais favorável se dá pelo fim da ameaça cibernética no âmbito internacional, especialmente com o fim de conflitos cibernéticos e plena cooperação entre os Estados em busca da segurança. As culturas como a de utilização de hackers para espionagem e outros métodos como cibercrimes, que incentivam tais conflitos entre os Estados, devem ser colocados em evidência, questionados e solucionados.

O evidenciamento de tais adversidades é promovido por ações como a reunião dos Estados Nacionais, em conferências ou encontros que busquem se aprofundar nas discussões e estimular resoluções, a partir da exposição dos ataques que os próprios possam estar sofrendo e dessa forma os outros agentes consigam contribuir para a resolução do problema, através do desenvolvimento de planos de ação contra esses conflitos. Tendo como exemplo a União Europeia, que se distingue como forte ator capaz de tomar a iniciativa de melhorar a segurança cibernética no mundo, através de seus investimentos, outros países se incentivam e buscam trabalhar em conjunto para aprimorar o sistema de segurança e assim conseguir enfraquecer conflitos cibernéticos.

Dessa forma, é possível se criar um sistema e uma rede de apoio forte o suficiente para se treinar profissionais capacitados o bastante para a cultivação de uma nova cultura de segurança cibernética, que busquem seguir a visão de cooperação não somente entre os Estados Nacionais como também entre as ONGs, os atores cibernéticos e os países, a fim de sanar e evitar ao máximo os incentivos aos conflitos que envolvem ciberataques. A criação de uma estrutura sustentável é ideal para que a cooperação entre esses atores seja efetiva e assim, possibilite o aprofundamento de tais resoluções até que por fim, se acabe com a guerra cibernética e atinja o verdadeiro estado de segurança, no qual haverá a cooperação plena entre os agentes e o devido cumprimento dos planos de ação desenvolvidos.

Em síntese, a erradicação da ameaça cibernética no cenário internacional é um imperativo que exige a união e ação coordenada de Estados, organizações e profissionais da área. Ao expor e questionar as culturas que fomentam conflitos cibernéticos, evidenciamos a necessidade de soluções globais. A visão de cooperação entre Estados, ONGs e atores cibernéticos é fundamental para prevenir incentivos aos conflitos. A construção de uma estrutura sustentável permite aprofundar resoluções e, eventualmente, alcançar um estado de segurança plena, marcado pela cooperação efetiva entre todos os envolvidos e a implementação bem-sucedida dos planos de ação desenvolvidos conjuntamente.

2.1.3.2. CENÁRIO FAVORÁVEL

Numa perspectiva favorável, novas leis restritivas seriam desenvolvidas pelos Estados nacionais contra os hackers, os quais seriam identificados e responsabilizados de maneira adequada pelos crimes que cometem contra os outros atores (CRYPTOID,2023). Através de uma cooperação internacional entre os Estados, é possível o compartilhamento de tecnologias para segurança entre os agentes a fim de manterem os sistemas de segurança atualizados para conseguirem bloquear, e até mesmo prever, os boicotes e ataques realizados por hackers ou grupos cibernéticos não estatais, podendo assim controlar esses grupos (CISO ADVISOR, 2022a). Ademais, ocorrerá entre as empresas de segurança cibernética e os Estados nacionais a negociação de *softwares* e hackers do bem, os quais em conjunto protegem os sistemas e os dados tanto das infraestruturas críticas do país, quanto das empresas que as contratam (ALVES,2023).

Além disso, através de um acordo multilateral, possível pelo fortalecimento das relações entre os Estados nacionais, os agentes poderão financiar o desenvolvimento em P&D de novas tecnologias que serão usadas posteriormente para o fortalecimento e proteção da infraestrutura crítica, de modo a garantir que os ataques não interfiram na segurança da sociedade como um todo, bem como o compartilhamento das mesmas tecnologias com as OIs e ONGs que contribuem para a promoção da segurança cibernética de diversas formas, como, por exemplo, a assistência a vítimas de cibercrimes, e assim podem retribuir mantendo a sociedade informada e assistida (PORTAL BRASILEIRO DA CIBERSEGURANÇA, 2024).

Ainda nesse sentido haverá a continuidade no projeto de criação de um metaverso, no qual as entidades responsáveis pela segurança da população mundial, como por exemplo as Organizações Internacionais como a Interpol, consigam se comunicar e se auxiliarem mutuamente em operações contra grupos cibernéticos não estatais e outros indivíduos (CISO ADVISOR, 2022b).

Dessa forma, a desigualdade tecnológica seria ínfima e traria poucas consequências num cenário mundial, visto que todos os atores - Estados nacionais, OIs e ONGs e grupos cibernéticos estatais - estariam em constante comunicação e cooperação por diversas vias, facilitando a assistência recíproca e controlando de maneira efetiva os ataques sofridos e o surgimento de novas organizações criminosas e grupos cibernéticos não estatais, bem como o desenvolvimento de novos vírus.

2.1.3.3. CENÁRIO DESFAVORÁVEL

Em um contexto desfavorável, as nações poderiam enfrentar desafios substanciais. A possível fragmentação da cooperação internacional resultaria em desordem global, privando o cenário de normas e regulamentações cibernéticas coesas. Isso abriria espaço para zonas de ciberanarquia, limitando a influência dos Estados na segurança global. Além disso, a espionagem cibernética entre nações poderia atingir níveis alarmantes, dando origem a conflitos cibernéticos recorrentes e prejudicando a estabilidade internacional (INSTITUTO HUMANITAS UNISINOS, 2022). A falta de confiança mútua propiciaria ações de grupos cibernéticos estatais, desencadeando confrontos e elevando o risco de escalada para conflitos reais.

A ameaça representada pela proliferação descontrolada de armas cibernéticas é iminente. A ausência de regulamentação eficaz permitiria o desenvolvimento agressivo dessas ferramentas, aumentando o perigo de escalada para conflitos reais e gerando uma corrida armamentista digital com implicações sérias para a segurança global. A falta de clareza na atribuição de ataques cibernéticos poderia aumentar as tensões internacionais, com ações ofensivas mal interpretadas por outros Estados, potencialmente desencadeando crises internacionais e conflitos digitais com consequências tangíveis (VELANDIA, 2017).

Ataques de ransomware em larga escala teriam o potencial de paralisar setores críticos, resultando em interrupções generalizadas e danos significativos (JÚNIOR, 2013). A falta de coordenação entre tais setores críticos poderia levar a falhas na resposta a incidentes, exacerbando os impactos econômicos e sociais, além de desconfiança generalizada na segurança digital. Assim, hackers, hacktivistas e organizações criminosas independentes tornar-se-iam mais agressivos e difíceis de serem contidos, representando uma ameaça constante à segurança digital de organizações e indivíduos (TECNOBLOG, 2022). A falta de investimento em programas educacionais eficazes permitiria que hackers continuassem explorando a falta de conscientização, aumentando o sucesso de ataques simples, mas eficazes.

A estagnação na inovação em segurança cibernética, combinada com a persistência de ameaças, poderia resultar em lacunas crescentes na proteção digital. Dessa forma, empresas de segurança cibernética enfrentariam desafios consideráveis, com ataques sofisticados contornando suas defesas e erodindo a confiança pública em sua eficácia. Mostrando-se necessário um investimento significativo em pesquisa e desenvolvimento em segurança cibernética, com o objetivo de implementar tecnologias avançadas, como inteligência artificial

e aprendizado de máquina, para detecção e prevenção automatizadas de ameaças seriam uma estratégia proativa para fortalecer as defesas cibernéticas (MARTINS, 2023)

Esse cenário desfavorável destaca a necessidade urgente de abordagens proativas, cooperação internacional eficaz e investimentos contínuos em segurança cibernética para mitigar os riscos associados ao ciberespaço ao longo das próximas décadas.

2.1.3.4. CENÁRIO CATASTRÓFICO

O aumento do cibercrime faz com que a cooperação internacional seja criticamente abalada devido a divergências por parte dos Estados nacionais quanto aos métodos de ação (ARAUJO, 2022). O financiamento conjunto praticado pelos mesmos para o desenvolvimento de mecanismos de defesa aos sistemas de defesa também mostra-se ineficaz para deter o avanço de hackers e novos vírus; da mesma forma que legislações criadas por Organizações Internacionais não bastam para garantir a completa proteção de grupos cibernéticos estatais e infraestruturas críticas, uma vez que hackers encontram rapidamente formas de burlar as normas criadas (CRYPTOID, 2023). Com isso, as relações internacionais são enfraquecidas, de modo a prevalecer a desconfiança entre as nações.

Ademais, o pensamento de dominância do quinto domínio – isto é, o ciberespaço – por militares é fortalecido, fazendo com que novas tecnologias e armas cibernéticas surjam e sejam usadas em conjunto de conflitos tradicionais, enfraquecendo Estados incapazes de revidar à altura (TEIXEIRA JÚNIOR, LOPES, FREITAS, 2017). Empresas privadas são contratadas pelas grandes potências para desenvolver *softwares* eficazes para enfraquecer sistemas de defesa, contrariando o escopo de serviços observado nestas companhias até então. Com isso, o preço a ser pago por essas tecnologias cresce, mantendo seu acesso restrito às grandes nações e potencializando uma corrida armamentista digital.

Nesse sentido, passa a reinar a desigualdade tecnológica, com um grupo seleto de Estados detendo o poder e acesso a tecnologias capazes de defender e atacar *softwares*. Além disso, aos países fora do eixo de controle digital, há a ruptura de suas soberanias digitais, assim como ao direito à privacidade, aumento da desinformação e alta rotatividade de empregos (WORLD ECONOMIC FORUM, 2023).

No entanto, pode-se alegar que o estopim da guerra cibernética generalizada se dá a partir do uso do metaverso para a realização de ataques digitais, contrariando mais uma vez o

que é defendido em Organizações Internacionais voltadas para a segurança. O mesmo é agravado pela contratação de hackers para auxiliar nestes ataques, uma vez que esses grupos marginais aprimoraram suas habilidades ao ponto de se tornarem, praticamente, imbatíveis. Ademais, a evolução da Inteligência Artificial (IA) é outro fator agravante ao conflito, uma vez que, para as situações cujas habilidades dos indivíduos é insuficiente, ela possui a capacidade de agir (CISO ADVISOR, 2022b; TIDY, 2023).

Contudo, alguns hackers, como aqueles pertencentes a grupos hacktivistas, resistem ao ataque desproporcional a Estados tecnologicamente inferiores, porém, mesmo assim, o impacto que causam ao atacarem grandes potências repercute diretamente nos países mais pobres (TEIXEIRA JÚNIOR, LOPES, FREITAS, 2017; ALVES, 2023), contribuindo para o escalonamento das tensões internacionais e para a indignação da sociedade internacional, que tenta se manifestar por meio de ONGs.

Por fim, o contexto de desconfiança internacional é tamanha que os métodos pacíficos de resolução de conflito mostram-se ineficientes. Assim, as tensões são escalonadas a ponto de se iniciar uma guerra nuclear através do uso de hackers, os quais, em conjunto de IAs, conseguirão destruir cidades inteiras a pedido de Estados nacionais.

3. CONSIDERAÇÕES FINAIS

Tendo em vista os cenários obtidos, as possíveis ameaças no ciberespaço, assim como seus impactos na segurança internacional, consequências políticas e diplomáticas, proteção de dados e privacidade puderam ser revisadas neste trabalho. Seus efeitos possuem duas rotas a serem seguidas: a cooperação internacional e a anarquia. A primeira visa proteger a população global e demais atores envolvidos dos impactos negativos de falhas na cibersegurança, promovendo ações legais, investimentos na proteção de dados e atuações conjuntas de Estados nacionais, grupos estatais e não estatais, OIs, ONGs e empresas privadas. Enquanto a segunda promove a insegurança e desigualdade entre os atores, em especial por meio da utilização do ciberespaço como máquina de guerra.

O futuro da guerra cibernética apresenta tendências positivas que permitem o alcance de cenários mais favoráveis e favoráveis, porém, caso as tentativas de combate conjuntas aos crimes no ciberespaço falhem, as realidades narradas nos cenários desfavorável e catastrófico possuem alta probabilidade de ocorrerem e, como apontado nos referidos cenários, possuem

potencialidade de causar mudanças irreversíveis no Sistema Internacional, como a ruptura de alianças e o escalonamento das tensões político-diplomáticas entre nações.

Logo, a fim de evitar estes cenários negativos, os Estados nacionais devem buscar fortalecer as relações entre si de modo a, conjuntamente, construir uma rede de segurança entre os agentes inseridos no ciberespaço que visa proteger informações – em especial às vinculadas a infraestruturas críticas – e, gradativamente, erradicar os crimes cibernéticos, com a ajuda de hacktivistas, empresas privadas, OIs e ONGs.

Sendo assim, até 2050 a segurança internacional a nível do ciberespaço tem potencialidade para fortalecer-se e torna-se um importante mecanismo de cooperação entre os Estados, no entanto, na mesma medida, possui potencialidade para ser a ferramenta responsável por desencadear novas guerras cibernéticas que se desenvolverão a ponto de alcançar novos patamares de destruição. Portanto, cabe aos atores em jogo analisarem as tendências e variáveis aqui apresentadas e traçar estratégias para alcançar os cenários mais convenientes para seus objetivos.

REFERÊNCIAS

ALONSO, Cristian; KOTHARI, Siddharth; REHMAN, Sidra. Como a inteligência artificial pode aumentar a distância entre as nações ricas e pobres. **IMFBlog**, Washington D.C, 3 dez. 2020. Disponível em: https://www.imf.org/pt/Blogs/Articles/2020/12/02/blog-how-artificial-intelligence-could-widen-the-gap-between-rich-and-poor-nations. Acesso em: 20 out. 2023.

ALVES, Martha. Com alta de ataques cibernéticos, mercado financeiro disputa contratação de hackers (mas do bem). **InfoMoney**, 2023. Disponível em: https://www.infomoney.com.br/carreira/com-alta-de-ataques-ciberneticos-mercado-financeiro-disputa-por-contratacao-de-hackers-mas-do-bem/. Acesso em: 21 de out. de 2023.

AMORIM, João. Capítulo 1. Soberania, Território, Povo e Nacionalidade. In: AMORIM, João. Direito dos estrangeiros no Brasil. São Paulo (SP): Editora Revista dos Tribunais. 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/capitulo-1-soberania-territorio-povo-e-nacionalidade-parte-geral-direito-dos-estrangeiros-no-brasil/1481212173 Acesso em: 12 de jan. 2024

ARAUJO, Clayton Vinicius Pegoraro. Os aspectos gerais dos tratados internacionais e a Convenção de Budapeste sobre Crimes Cibernéticos. **Revista da Faculdade de Direito da Universidade Federal de Uberlândia**, Uberlândia, v. 50, n. 1, pp. 145-165, jan-jun. 2022. Disponível em:

https://seer.ufu.br/index.php/revistafadir/article/download/65259/35246/303434. Acesso em: 20 out. 2023.

Ameaça de Guerra Cibernética: um desafio global em destaque. ALCASSA E PAPPERT. 2023. Disponível em: https://alcassapappert.adv.br/ameaca-de-guerra-cibernetica-um-desafio-global-em-destaque/ Acesso em: 15 de jan. 2024

Ataque hacker: veja quais são as cinco ameaças mais comuns do momento. **Tudo Celular**. 2022. Disponível em: https://www.tudocelular.com/seguranca/noticias/n193788/ataque-hacker-cinco-ameacas-mais-comuns.html Acesso em: 12 de jan. 2024

Blog BugHunt. O que é guerra cibernética? **Blog BugHunt.** Disponível em: https://blog.bughunt.com.br/o-que-e-guerra-cibernetica/. Acesso em: 17 de out de 2023.

BUXTON, Oliver. **Avast**. C Stuxnet: o primeiro ciberataque com consequências reais. Disponível em: https://www.avast.com/pt-br/c-stuxnet. Acesso em: 20 de out de 2023.

Ciberanarquia, a guerra digital silenciosa (e ainda sem regras). **Instituto Humanitas Unisinos**. 2022. Disponível em: https://www.ihu.unisinos.br/categorias/618186-ciberanarquia-a-guerra-digital-silenciosa-e-ainda-sem-regras Acesso em: 15 de jan. 2024

CINTRA, Rodrigo. Cibersegurança: um problema global, uma solução global. **Mapa Mundi**. 2023. Disponível em: https://mapamundi.org.br/2023/ciberseguranca-um-problema-global-uma-solucao-global/ Acesso em: 10 de jan. 2024

CISO ADVISOR. **Cooperação internacional é crucial para combate ao cibercrime**. CISO Advisor. 2022a Disponível em: https://www.cisoadvisor.com.br/cooperacao-internacional-e-crucial-para-combate-ao-cibercrime/ Acesso em:12 de jan. 2024

CISO ADVISOR. **Interpol entra no metaverso para combater crime cibernético** | CISO Advisor. 25 out. 2022b. Disponível em: https://www.cisoadvisor.com.br/interpol-entra-no-metaverso-para-combater-crime-cibernetico/. Acesso em: 24 out. 2023.

CLARO, Fernanda Del. O avanço tecnológico no mundo econômico. FAE Centro Universitário. Vitrine da Conjuntura, Curitiba, v.2, n.8, outubro 2009.

CNN Brasil. Inteligência dos EUA indica nova interferência da Rússia nas eleições de 2022. Disponível em: https://www.cnnbrasil.com.br/internacional/inteligencia-dos-eua-indicam-nova-interferencia-da-russia-nas-eleicoes-de-2022/#:~:text=A%20comunidade%20de%20inteligência%20no,Joe%20Biden%20e%20apoiar%20Trump. Acesso em: 22 de out de 2023.

CRYPTOID. Europa lança Lei de Solidariedade Cibernética. **Insania**, [S. L], 26 abr. 2023. Disponível em: https://cryptoid.com.br/identidade-digital-destaques/europa-lanca-lei-de-solidariedade-cibernetica/. Acesso em 19 out. 2023.

DEUTSCHE WELLE. **Hackers russos atacaram laboratórios nucleares dos EUA**. 7 jan. 2023. Disponível em: https://www.dw.com/pt-br/hackers-russos-atacaram-laboratorios-nucleares-dos-eua/a-64314276. Acesso em: 24 out. 2023.

DUFFIELD, John. What Are International Institutions?, International Studies Review, Volume 9, Issue 1, March 2007, Pages 1–22. Disponível em: https://doi.org/10.1111/j.1468-2486.2007.00643.x Acesso em: 10 de jan. 2024

DUTRA, Laura Távora. A inteligência artificial nas relações internacionais: conflitos, paz e possibilidades. Orientador: João Gabriel Burmann. 2023. TCC (Graduação) - Curso de Relações Internacionais, Uniritter. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/35063. Acesso em: 22 de out. de 2023.

Espionagem cibernética: A ameaça silenciosa. **Blog Zerum**. 2023. Disponível em: https://www.zerum.com/pt/cybersecurity/espionagem-cibernetica-a-ameaca-silenciosa/ Acesso em: 13 de jan. 2024

FONSECA, Leila Oliveira da. A guerra cibernética e o conflito Rússia versus Ucrânia. **Revista Relações Exteriores**, [S. L], 24 fev. 2023. Disponível em: https://relacoesexteriores.com.br/a-guerra-cibernetica-e-o-conflito-russia-versus-ucrania/. Acesso em: 18 out. 2023.

FUNDAÇÃO VANZOLINI. **Cibersegurança profissional: formação especializada**. 17 jul. 2023. Disponível em: https://vanzolini.org.br/blog/educacao/ciberseguranca-profissional/. Acesso em: 24 out. 2023.

GODET, Michel. De la anticipación a lá acción. Barcelona: Marcombo, 1993, p. 107-127.

GODET, Michel; DURRANCE, Philippe. A prospectiva estratégica: Para as empresas e os territórios. DUNOD; UNESCO; Fondation Prospective et Innovation, 2011, p. 48-92.

Guerra cibernética e seus impactos na sociedade. **HSC** . 2023. Disponível em: https://hsclabs.com/pt-br/guerra-cibernetica-e-seus-impactos-na-sociedade/ Acesso em: 12 de jan. 2024

HACKER. In: Michaelis. Editora Melhoramentos Ltda. 2024. Disponível em:https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=hacker Acesso em: 10 de jan. 2024

Hacktivism: The intersection of cybersecurity and social activism. **ManageEngine Blog**. 2023. Disponível em: https://blogs.manageengine.com/corporate/general/2023/11/21/hacktivism-the-intersection-of-cybersecurity-and-social-activism.html Acesso em: 12 de jan. 2024

HAGE, Lara. Saiba como os crimes na internet são tratados em outros países. **Agência Câmara Notícias**. 2011. Disponível em: https://www.camara.leg.br/noticias/217913-saiba-como-os-crimes-na-internet-sao-tratados-em-outros-paises/%5D Acesso em: 15 de jan. 2024

HE, Laura. **China investiga fabricante de chips dos EUA por riscos de segurança cibernética** | CNN Brasil. 3 abr. 2023. Disponível em: https://www.cnnbrasil.com.br/economia/china-investiga-fabricante-de-chips-dos-eua-por-riscos-de-seguranca-cibernetica/. Acesso em: 24 out. 2023.

IAMASSITA, Paula Natsumi Vasconcelos & ARAÚJO, João Marcos Ferreira. Inteligência Artificial e Desinformação, um novo fenômeno. UNICEF, 2023. Disponível em: https://www.unicef.org/brazil/blog/inteligencia-artificial-e-desinformacao. Acesso em: 22 de out. de 2023.

Infraestruturas críticas. **O Tempo.** 2022. Disponível em: https://www.otempo.com.br/opiniao/rodrigo-bustamante/infraestruturas-criticas-1.2757029 Acesso em: 10 de jan. 2024

INTERNATIONAL IT. Guerra Cibernética: Governo e bancos da Ucrânia são atingidos por ataques DDoS. 28 set. 2022. **International IT**, [S. L], 2022a. Disponível em: https://www.internationalit.com/post/guerra-cibern%C3%A9tica-governo-e-bancos-da-ucr%C3%A2nia-s%C3%A3o-atingidos-por-ataques-ddos. Acesso em: 18 out. 2023.

INTERNATIONAL IT. Principais violações de dados e ataques cibernéticos de 2022. 05 jul. 2022. **International IT**, [S. L], 2022b. Disponível em: https://www.internationalit.com/post/principais-viola%C3%A7%C3%B5es-de-dados-e-ataques-cibern%C3%A9ticos-de-2022. Acesso em: 18 out. 2023.

JUNIOR, Samuel Cezar da Cruz Junior. Tecnologias e riscos: armas cibernéticas. Instituto de pesquisa econômica aplicada IPEA. Brasília, julho de 2013. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/5813/1/NT_n11_Tecnologias-riscos_Diset_2013-jul.pdf Acesso em:15 de jan. 2024

KAMINSKI, Omar. **O código é Lei: a arquitetura na Internet dita as regras**. 5 nov. 2001. Disponível em: https://www.conjur.com.br/2001-nov-05/codigo_ciberespaco_regula_espaco_fisico. Acesso em: 24 out. 2023.

KOVACS, Leandro. O que é um hacker? **Tecnoblog**. 2022 Disponível em: https://tecnoblog.net/responde/o-que-e-um-hacker/ Acesso em: 8 de jan. 2024

LEVI, P. Os afogados e os sobreviventes. São Paulo: Paz e terra, 2004.

LOPES, Jéssica Rodrigues. Mecanismos de cooperação internacional de repressão e combate dos crimes cibernéticos. egov.ufsc.br, [S.L], 19 outubro 2018. Disponível em: https://egov.ufsc.br/portal/en/conteudo/mecanismos-de-coopera%C3%A7%C3%A3o-internacional-de-repress%C3%A3o-e-combate-dos-crimes-cibern%C3%A9ticos. Acesso em: 22 de out. de 2023.

MALLICK, P. K. Decoding Russia's 'Missing' Cyberwar Amid War in Ukraine. New Delhi: **Vivekananda International Foundation**, 2022. Disponível em: https://www.vifindia.org/sites/default/files/Decoding-Russia-s-Missing-Cyberwar-Amid-War-in-Ukraine.pdf. Acesso em: 18 out. 2023.

MARCIAL, Elaine; GRUMBACH, Raul. Cenários prospectivos: como construir um futuro melhor. 5.ed, Rio de Janeiro: 2008.

MARTINS, Fernanda. Crescimento alarmante de ataques de ransomware: Uma ameaça persistente no mundo digital. **ITSHOW**. 2023. Disponível em: https://itshow.com.br/crescimento-alarmante-de-ataques-de-ransomware-uma-ameaca-persistente-no-mundo-digital/ Acesso em: 15 de jan. 2024

NASCIMENTO, G. S. D. *et al*. **OS IMPACTOS DA GUERRA COMERCIAL ENTRE EUA E CHINA (2018- 2020) SOB A ÓTICA DA SEGURANÇA CIBERNÉTICA E DA GOVERNANÇA DE DADOS.** Orientadora: Clarissa Nascimento Forner. 2022. TCC (Graduação) - Curso de Relações Internacionais, Universidade São Judas Tadeu, São Paulo, 2022. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/31019/1/TRABALHO%20DE%20CONCLUS%c3%83O%20DE%20CURSO.pdf. Acesso em: 19 out. 2023.

NETO, Ricardo Borges Gama. Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interação. **Política Hoje**, v. 26, n. 1, 2017. Acesso em: 24 out. 2023.

O que é infraestrutura crítica? **IBM.** Disponível em:https://www.ibm.com/br-pt/topics/critical-infrastructure Acesso em: 15 de jan. 2024

O que é segurança cibernética? **AWS**. Disponível em: https://aws.amazon.com/pt/what-is/cybersecurity/#:~:text=Esses%20especialistas%20avaliam%20os%20riscos,e%20outros%20dispositivos%20conectados%20existentes. Acesso em: 10 de jna. 2024

PLAZA, William R. Qual foi o primeiro vírus de computador?. **Hardware.com.br**, [S. L], 24 maio. 2022. Disponível em: https://www.hardware.com.br/artigos/qual-primeiro-virus-de-computador/. Acesso em: 22 out. 2023.

PORTAL BRASILEIRO DA CIBERSEGURANÇA. **Instituto Igarapé**. 2021. Disponível em: https://ciberseguranca.igarape.org.br/sobre/ Acesso em: 15 de jan. 2024

RIBEIRO, Gustavo. Cibersegurança: 8 dicas essenciais de segurança cibernética para empresas. **Cedro**. 2023 Disponível em: https://www.cedrotech.com/blog/ciberseguranca-8-dicas-essenciais-de-seguranca-cibernetica-para-empresas/#:~:text=Mantenha%20seus%20sistemas%20atualizados,contra%20vulnerabilidades%20detectadas%20pela%20marca. Acesso em: 15 de jan. 2024

RUDZIT, Gunther. O debate teórico em segurança internacional: mudanças frente ao terrorismo?. Civitas: revista de Ciências Sociais, [S. l.], v. 5, n. 2, p. 297–323, 2006. Disponível em: https://revistaseletronicas.pucrs.br/ojs/index.php/civitas/article/view/5. Acesso em: 10 jan. 2024.

SANTOS, Walmir Coelho da Costa. O impacto da desinformação digital na provisão de serviços ecossistêmicos essenciais à qualidade de vida. Revista da Defensoria Pública RS. Porto Alegre, ano 14, v. 2, n. 33, p. 1-21, 2023.

SECURITY REPORT. **Governo lança programa de formação de profissionais em Cibersegurança** | Security Report. 23 maio 2023. Disponível em: https://www.securityreport.com.br/governo-lanca-programa-de-formacao-de-profissionais-em-ciberseguranca/. Acesso em: 24 out. 2023.

STRICKLAND, Jonathan. **UOL Educação**. Os piores vírus de computador. Arquivado em: 14 dez. 2011. Disponível em: https://web.archive.org/web/20111214031456/http://informatica.hsw.uol.com.br/piores-virus-computador2.htm. Acesso em: 22 de out. de 2023

SOUZA, Deywisson Ronaldo Oliveira de; CASALUNGA, Fernando Henrique; PINHEIRO, Alane Costa; BARBOSA, Augusto Ferreira Nascimento; MARINHO, Caroliny dos Santos; GUEDES, Matheus Guerra. GUERRA HÍBRIDA E CIBERCONFLITOS: UMA ANÁLISE DAS FERRAMENTAS CIBERNÉTICAS NOS CASOS DA SÍRIA E CONFLITO RÚSSIA-UCRÂNIA. **Revista Eletrônica da Estácio Recife**, [S. L], v. 5, n. 3, 2020. Disponível em: https://reer.emnuvens.com.br/reer/article/view/346. Acesso em: 18 out. 2023.

SUGUIHARA, Guilherme. As 19 Principais Empresas De Cibersegurança Conhecidas Em 2023. **TPS Cyber Security**. 2023. Disponível em: https://tps.com.br/as-19-principais-empresas-de-ciberseguranca-conhecidas-em-2023/#O_que_e_uma_empresa_de_Ciberseguranca Acesso em: 12 de jan. 2024

TEIXEIRA JÚNIOR, A. W. M.; LOPES, G. V.; FREITAS, M. T. D. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. **Carta Internacional**, [S. L], v. 12, n. 3, p. 30–53, 2017. Disponível em: https://www.cartainternacional.abri.org.br/Carta/article/view/620. Acesso em: 18 out. 2023.

TIDY, Joe. Hackers: a guerra de versões sobre países que promovem mais ataques cibernéticos. **BBC News Brasil**, 2023. Disponível em: https://www.bbc.com/portuguese/articles/cjl9jglk1kro. Acesso em: 22 de out. de 2023.

VELANDIA, Karenina. Quais são as sofisticadas armas cibernéticas da guerra do século 21? **BBC News Brasil**, 2017. Disponível em: https://www.bbc.com/portuguese/internacional-39149203 Acesso em: 15 de jan. 2024

VILLELA, L. E. ; MAIA, Sergio Wright. **A Análise Prospectiva visa avaliar futuros possíveis, prováveis e desejáveis.** Professor Cordella. Disponível em: https://www.profcordella.com.br/unisanta/textos/tgs41_analise_prospectiva_cenarios_conceitos.html#:~:text=A%20Análise%20Prospectiva%20visa%20avaliar,futuros%20possíveis%2C%20prováveis%20e%20desejáveis. Acesso em: 18 de outubro de 2023.

WORLD ECONOMIC FORUM. **Global Risks Report** 2023. Geneva, 11 jan. 2023. Disponível em: https://www.weforum.org/reports/global-risks-report-2023/. Acesso em: 20 out. 2023.