GEOPOLÍTICA CIBERNÉTICA: COMO AS AMEAÇAS PERSISTENTES AVANÇADAS REDEFINEM O PODERIO CIBERNÉTICO DAS NAÇÕES

CYBER GEOPOLITICS: HOW ADVANCED PERSISTENT THREATS REDEFINE THE CYBER POWER OF NATIONS

Bruno Cantelli

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

bruno.cantelli@fatec.sp.gov.br

Marcus Vinicius Lahr Giraldi

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

marcus.lahr@fatec.sp.gov.br

Resumo

Este artigo examina o papel das ameaças persistentes avançadas na geopolítica cibernética, destacando seu uso estratégico para espionagem, sabotagem e desestabilização entre nações. O objetivo é identificar e compreender os impactos dessas ameaças na geopolítica global, especialmente quanto à estabilidade e ao poder no ciberespaço. A metodologia adotada foi uma pesquisa bibliográfica com fontes confiáveis que apontam o crescente uso das ameaças persistentes avançadas em estratégias geopolíticas, transformando o ciberespaço em um domínio competitivo. Conclui-se que, apesar dos riscos à segurança digital, essas ameaças também impulsionam inovações em cibersegurança e favorecem alianças estratégicas, sendo a resposta coordenada crucial para fortalecer a resiliência cibernética e a estabilidade global.

Palavras-chave: geopolítica cibernética, ameaça persistente avançada, ciberespaço.

Abstract

This article examines the role of advanced persistent threats in cyber geopolitics, highlighting their strategic use for espionage, sabotage, and destabilization among nations. The main objective is to identify and understand the impacts of these threats on global geopolitics, particularly regarding stability and power in cyberspace. The methodology adopted was a bibliographic review of reliable sources indicating the growing use of advanced persistent threats in geopolitical strategies, transforming cyberspace into a competitive domain. The study concludes that, despite the risks to digital security, these threats also drive cybersecurity innovations and foster strategic alliances, with coordinated responses being crucial to strengthening cyber resilience and global stability.

Keywords*: cyber geopolitics, advanced persistent threats, cyberspace*.

1. Introdução

Na era digital, o poderio cibernético emergiu como um dos pilares centrais da geopolítica global, redefinindo as estratégias de segurança e defesa das nações. As ameaças persistentes avançadas se destacam nesse cenário como vetores sofisticados de ataque cibernético, direcionados e frequentemente patrocinados por Estados-nação. Essas ameaças têm a capacidade de penetrar redes altamente seguras, mantendo-se latentes por longos períodos, o que permite a coleta contínua de informações sensíveis, sabotagem de infraestruturas críticas e a manipulação de dados estratégicos.

O impacto das ameaças persistentes avançadas na geopolítica não pode ser subestimado, pois elas oferecem aos países atacantes uma ferramenta silenciosa e eficaz para exercer influência, sem a necessidade de confrontos militares tradicionais. Nações com capacidades cibernéticas avançadas utilizam essas ameaças como parte de suas estratégias de poder, visando tanto a dissuasão quanto a projeção de força em um ambiente global interconectado.

Sendo assim, o objetivo geral desse trabalho é identificar e promover a compreensão dos impactos das ameaças persistentes avançadas na geopolítica cibernética global. Para atingir tal objetivo, os autores adotaram os seguintes objetivos específicos:

- Introduzir a geopolítica cibernética, mostrando sua importância no cenário internacional, explorando como o ciberespaço se tornou um campo estratégico para a manutenção e disputa de poder entre os estados-nações.
- Analisar o uso das ameaças persistentes avançadas como ferramentas geopolíticas, abordando como o uso para fins de espionagem, sabotagem e desestabilização de outros Estados, com o intuito de ampliar a influência e o poder das nações que o utilizam.
- Examinar o impacto dessas ameaças no contexto da geopolítica cibernética, discutindo como essas ameaças modificam o equilíbrio de poder, influenciam as políticas de defesa cibernética e apoiam a criação de alianças estratégicas e novas regulamentações internacionais.

A justificativa deste estudo consiste em que o ciberespaço se tornou um campo estratégico essencial nas relações de poder entre as nações, sendo fundamental compreender como as ameaças persistentes avançadas estão redefinindo o cenário de segurança cibernética global. Estas ameaças, altamente sofisticadas e persistentes, não apenas comprometem a segurança dos dados e infraestruturas críticas, mas também influenciam diretamente a soberania nacional e o equilíbrio geopolítico. Assim, este estudo busca incentivar o desenvolvimento de políticas e estratégias que aprimorem a defesa cibernética e promovam a cooperação internacional, garantindo a proteção dos ativos nacionais e contribuindo para a estabilidade no cenário global.

2. Referencial Teórico

Seguindo a introdução, observa-se que uma fundamentação teórica é primordial para entender a importância da geopolítica cibernética no cenário internacional, destacando o papel do ciberespaço como um campo estratégico para a manutenção e disputa de poder entre os Estados-nações. A discussão teórica abordará como o uso de ameaças persistentes avançadas se tornou uma ferramenta geopolítica relevante, permitindo que países realizem espionagem, sabotagem e ações de desestabilização contra outros Estados, com o objetivo de ampliar sua influência e consolidar seu poder no cenário global.

Além disso, será objeto de discussão o impacto dessas ameaças no equilíbrio de poder entre as nações, incluindo a forma como as ameaças influenciam as políticas de defesa cibernética e incentivam a criação de alianças estratégicas, além de fomentar novas regulamentações internacionais para fortalecer a segurança e a estabilidade no ciberespaço. Esses aspectos serão aprofundados nas próximas seções deste artigo, com base nos objetivos estabelecidos para uma análise completa do fenômeno.

2.1 Introdução à geopolítica cibernética

A geopolítica estuda as relações de poder entre países e seus territórios, analisando conflitos, alianças diplomáticas e estratégias políticas, econômicas e culturais. Ela busca entender as motivações por trás de ações internacionais e o impacto dessas interações no cenário global, considerando, por exemplo, o papel de organizações supranacionais e blocos econômicos (Cnn, 2023).

Como afirma Fernandes (2020), a geopolítica se concentra nos relacionamentos dos Estados sob o ponto de vista geográfico e político, especialmente nas disputas e conflitos decorrentes desses aspectos. Com o advento do ciberespaço, as nações têm uma nova dimensão para se preocupar: este terreno imaginário que, embora sustentado por uma estrutura física, ultrapassa as fronteiras geográficas e é considerado um cenário global.

Em suma, podemos dizer que a geopolítica cibernética adiciona o ciberespaço como mais um domínio a ser debatido, requerido ou conquistado. Como cita Cátedra (2024), o ciberespaço se tornou crítico para as nações, pois através dele os Estados podem impactar significativamente as relações internacionais, segurança nacional e a economia mundial. Cabe lembrar ainda das guerras cibernéticas, que podem utilizar-se de ataques a infraestruturas críticas de outros países, como redes de energia, sistemas militares, de saúde pública ou financeiros para espionagem e/ou destruição de dados.

No âmbito das guerras cibernéticas, os grupos de ameaças persistentes avançadas têm um papel decisivo, porém também oculto: Muitas vezes patrocinados por um Estado, esses grupos são utilizados como ferramenta estratégica para espionagem e sabotagem digital. Diferentes

nações desenvolvem suas capacidades de ciberataque para obter vantagem competitiva em diversas áreas, como militar, econômica e política.

2.2 Ameaças persistentes avançadas como ferramentas geopolíticas

Os ataques persistentes avançados representam uma das ameaças mais críticas no cenário da cibersegurança moderna. Eles combinam técnicas de infiltração contínuas e sofisticadas com o objetivo de comprometer sistemas de alto valor e manter presença dentro das redes, sem serem detectados, por longos períodos. A principal diferença entre ameaças persistentes avançadas e ataques convencionais é que os invasores não estão interessados em ganhos rápidos, mas em acesso prolongado para coletar informações sensíveis, geralmente em nome de estados-nação ou grupos bem financiados. (Kaspersky,2024).

Ainda de acordo com a Kaspersky (2024), as ameaças persistentes avançadas podem ser vistas como operações coordenadas, muitas vezes envolvendo várias fases, como reconhecimento, infiltração inicial, elevação de privilégios, movimento lateral dentro da rede, coleta e exfiltração de dados. Essa abordagem estruturada significa que as defesas tradicionais, como antivírus e *firewalls*, podem falhar em detectar e bloquear as ameaças, uma vez que elas são projetadas para escapar de ferramentas de segurança convencionais, utilizando técnicas como exploração de vulnerabilidades *zero-day*, *backdoors* e comunicações disfarçadas.

Para a Fortinet (2024), uma ameaça persistente avançada é um tipo de ataque cibernético que se mantém ativo e furtivo, utilizando técnicas sofisticadas de invasão para ganhar acesso a um sistema e permanecer nele por um período prolongado. Os responsáveis por esses ataques são geralmente cibercriminosos organizados, como o grupo iraniano APT34 ou a entidade russa APT28. Embora esses invasores possam surgir de várias partes do mundo, alguns dos mais conhecidos são originários do Irã, de regiões do Oriente Médio e da Coreia do Norte.

Complementando, a Crowdstrike (2023), afirma que a execução de um ataque necessita de uma sofisticação e personalização de mais alto nível, em que são empregados maior tempo e demais recursos no levantamento de informações sobre o alvo, de modo que o ataque surta o maior efeito possível. Normalmente, esses levantamentos são realizados por membros

experientes que formam uma equipe contratada especialmente para o desenvolvimento e execução da ação.

Trazendo para o âmbito da política, Buchanan(2020), compara as capacidades cibernéticas das nações, com seus grupos de ameaças persistentes avançadas oficiais (ou não), com a capacidade nuclear das mesmas, pois a simples ciência de que as capacidades cibernéticas existem já os colocam em vantagem, visto que o uso de ambas as capacidades (nuclear ou cibernética) causam impactos potencialmente enormes, devido ao alto número de alvos afetados e força demonstrada.

2.3 Identificação e mapeamento global das ameaças persistentes avançadas

A identificação de um grupo de ameaça persistente avançada normalmente se refere, segundo Poireault (2023), a um grupo de personagens que se utilizam de táticas, técnicas e procedimentos sofisticados que são subsidiados e/ou atuando sob a bandeira de uma nação. O objetivo das táticas, técnicas e procedimentos são ataques cibernéticos indetectáveis, concebidos para o roubo de dados confidenciais, a espionagem cibernética e/ou a sabotagem de sistemas de infraestrutura crítica por um longo espaço de tempo (Lindemulder; Forrest, 2024). Apenas a título de exemplificação, temos um caso notório de sabotagem de infraestrutura crítica, o vírus Stuxnet, criado especialmente para alterar o código dos controladores lógicos programáveis, conhecidos como CLP, de centrífugas de enriquecimento nuclear do Irã, com objetivo alcançado de danificar e destruir recursos militares e causar grandes interrupções no programa nuclear do país (Buxton, 2022).

Buscando ainda a identificação de uma ameaça persistente avançada, Maloney(2024) define como um ataque cibernético furtivo no qual uma pessoa ou grupo obtém acesso não autorizado a uma rede privada e ali permanece sem ser detectado por um período extenso.

Analisando a tabela 1, podemos verificar a quantidade de grupos de ameaças persistentes avançadas que são conhecidos como 490 grupos enquanto cerca de 1500 supostos grupos não foram identificados. Podemos avaliar também uma alta quantidade de operações dado ao tempo de execução de uma operação ser bem mais longo que um ataque normal já que um dos objetivos da operação é a manutenção de acesso por um período prolongado.

Tabela 1 - Resumo de grupos de ameaças persistentes

Data de atualização do banco de dados	24 de outubro de 2024
Total de grupos de ameaças	490
Total de supostos grupos	1506
Total de operações	2786
Setores vítimas exclusivos	42

Fonte: Elaborado e traduzido pelos autores (2024) com base em ETDA (2024)

A concentração de grupos de ameaça persistente avançada na China, Irã e Rússia revela um cenário alarmante para a segurança cibernética global. Esses países não apenas lideram em número de grupos de ameaças persistentes, conforme mostrado na tabela 2, mas também estão implementando atividades cibernéticas inovadoras e dinâmicas, que visam expandir sua influência e capacidade ofensiva no ciberespaço, citado pelo relatório referente ao primeiro trimestre de 2024 da Cyfirma(2024).

Tabela 2 - Grupos de ameaças persistentes avançadas por país

Posição	País de origem	Quantidade
1	China	164
2	Rússia	51
3	Irã	43
4	Coréia do Norte	13
5	Estados Unidos da América	8
6	Paquistão	7
7	Índia	6
8	Líbano	4
	Turquia	4
10	Vietnã	3

Fonte: Elaborado e traduzido pelos autores (2024) com base em ETDA (2024)

Corroborando com o objetivo da análise do presente artigo, temos o disposto na tabela 3 mostrando que a grande quantidade dos ataques dos grupos de ameaças persistente avançadas tem como alvo os setores governamentais, de defesa e financeiro. Tais setores podem influenciar positivamente ou negativamente qualquer relação internacional entre Estados, dado que as informações contidas nesses setores são de extremo sigilo e sensibilidade.

Tabela 3 - Quantidade de ataques por setor

Posição	Setor vítima	Quantidade
1	Governamental	199
2	Defesa	115
3	Financeiro	105
4	Telecomunicações	87
5	Energia	86
6	Educação	77
7	Mídia	72
8	Saúde	57
	Manufaturas	57
10	Tecnologia da Informação	39

Fonte: Elaborado e traduzido pelos autores (2024) com base em ETDA (2024)

2.4 Impacto das ameaças persistentes avançadas na geopolítica internacional

Para conseguirmos mensurar o impacto das ameaças persistentes avançadas na geopolítica internacional devemos nos aprofundar em cada um dos objetivos que elas propõem alcançar. Buchanan (2020) e Buzatu (2022) apontam alguns objetivos principais:

- Espionagem;
- Sabotagem;
- Interferência externa em processos políticos;
- Ataques a sistemas de informação.

2.4.1 Espionagem

Para a Agência Brasileira de Inteligência (ABIN) (2020), a espionagem é a ação realizada por um agente adverso que procura a obtenção, de maneira oculta, de informações sensíveis, críticas ou sigilosas de governos e instituições nacionais para benefícios de outros Estados, organizações ou grupos de interesses. O acesso indevido a conhecimentos sensíveis como domínios de novas tecnologias ou decisões tomadas em relações internacionais são exemplos de interesses da espionagem.

Dentro da espionagem, Buchanan (2020), cita 5 vertentes da espionagem, que podem ser elencadas como:

- Exploração da vantagem do "campo doméstico": A atuação de agências de inteligência na parceria com empresas que detém ou trafegam dados de Estados-alvo em território nacional, recebendo de forma oculta essas informações para tomada de decisões;
- Quebra de criptografia: Agências ou grupos de Estados recorrem a empresas de equipamentos que tenham segurança criptográfica para que elas "quebrem" a criptografia para que possam ser acessadas informações relevantes para o Estado;
- Implantação de *backdoors:* Equipamentos de comunicação já são concebidos com algum subterfúgio que permite o acesso sem que o proprietário perceba, podendo fazer a exfiltração de dados sensíveis e/ou sigilosos;
- Espionagem estratégica: Utilizando-se de ataques direcionados a funcionários do alvo, de modo que se obtenha acesso a rede e consiga coletar documentos estratégicos, como segredos comerciais, patentes e projetos de desenvolvimento;
- Contra inteligência: Para a Agência Brasileira de Inteligência (ABIN) (2021), a contra inteligência previne, detecta, obstrui e neutraliza qualquer ameaça que ponha em risco área e/ou assuntos de interesse da sociedade e do Estado.

2.4.2 Sabotagem

Sabotagem é o ato de infiltração nas estruturas do alvo com intuito de interromper ou prejudicar totalmente o correto funcionamento de infraestruturas, serviços e sistemas essenciais, tais como sistemas de defesa, radares, telecomunicações militares, entre outros, desmobilizando o inimigo antes mesmo de qualquer reação que ele possa ser capaz (Augusténé, 2023).

Analisando o descritivo da Agência Brasileira de Inteligência (ABIN) (2023), na política nacional de inteligência, para a sabotagem, podemos concluir que se trata de uma ação deliberada que visa destruir, danificar ou comprometer dados, equipamentos, materiais e cadeias produtivas, impactando principalmente a infraestrutura crítica do país. O objetivo dessas ações é interromper o funcionamento de serviços essenciais, prejudicando a capacidade do Estado em atender às necessidades básicas da população.

2.4.3 Interferência externa em processos políticos

A interferência externa em processos políticos nacionais é uma prática cada vez mais presente, envolvendo atores que buscam influenciar decisões governamentais para atender a interesses que nem sempre coincidem com os da população local. De acordo com a Agência Brasileira de Inteligência (ABIN, 2023), trata-se de uma atuação deliberada realizada por governos, grupos de interesse ou entidades, sejam elas pessoas físicas ou jurídicas, com o objetivo de influenciar o rumo político do país, favorecendo interesses estrangeiros em detrimento dos interesses nacionais. Essa manipulação pode se manifestar de diversas formas, como através de campanhas de desinformação, financiamento de movimentos políticos, lobby em setores estratégicos e até ciberataques direcionados a instituições democráticas. O impacto dessas ações coloca em risco a soberania nacional, desestabiliza o processo democrático e afeta a confiança da população nas instituições políticas, demandando, assim, uma vigilância constante e medidas eficazes de proteção.

2.4.4 Ataques a sistemas de informação

Utilizando-se de operações chamadas de operações de informação, compostas de estratégias e táticas para influenciar a percepção e o comportamento da população do Estado-alvo, valendo-se de manipulação em plataformas digitais. Disseminando informações verdadeiras, falsas ou manipuladas, influenciam a opinião pública, desestabilizam sociedades e promovem agendas políticas específicas. Tais operações podem, potencialmente, alterar a dinâmica geopolítica ao influenciar eleições, fomentar conflitos internos e criar tensões entre nações. (ETUDO *et al*, 2023).

2.5 Respostas e políticas internacionais

Atribuir responsabilidade por ataques cibernéticos, tanto aos executores quanto aos mandantes, é crucial para a dissuasão. Contudo, a atribuição entre estados é um desafio complexo. O Direito Internacional exige que Estados avisem antes de atacar e respondam por atores não estatais sob seu controle, mas essas normas são frequentemente ignoradas no ciberespaço. A identificação precisa dos responsáveis, em meio a operações de bandeira falsa e atores dispersos, está além das capacidades da maioria dos países. Nesse cenário, estabelecer uma base legal clara para futuras regulamentações é um passo fundamental. (Assumpção, 2020).

A grande parte das políticas internacionais se utilizam da criação de agências internacionais de cibersegurança, tais como:

- ENISA (Agência da União Europeia para a Cibersegurança): Atuando na união européia, a agência tem como diretrizes capacitar as comunidades, a cooperação operacional, o reforça das capacidades, entre outras atribuições;
- EUROPOL (*European Union Agency for Law Enforcement Cooperation*): Agência de aplicação da lei da união européia, a Europol lida com crimes que exigem uma abordagem internacional e cooperação entre vários países, dentro e fora da união européia.

- CCDCOE (Centro de Excelência em Defesa Cibernética Cooperativa da OTAN): A missão do CCDCOE é “apoiar nossos países-membros e a OTAN com expertise interdisciplinar única no campo de pesquisa, treinamento e exercícios de defesa cibernética, abrangendo as áreas de foco de tecnologia, estratégia, operações e direito” (CCDCOE,2024).

Outra importante iniciativa de diversos centros, grupos e nações são os exercícios de cibersegurança e simulações de ataques que, de acordo com a Fundação Getúlio Vargas e o Comando de Defesa Cibernética (2024), “são atividades simuladas que podem ser realizadas em âmbito nacional, setorial ou das organizações para testar e/ou aprimorar a prontidão, as capacidades de resposta e a resiliência das medidas contra potenciais ameaças e ataques cibernéticos. ”

O exercício se segurança cibernética promovido pela CCDCOE, chamado Locked Shields, “permite que especialistas em segurança cibernética aprimorem suas habilidades na defesa de sistemas nacionais de TI e infraestrutura crítica sob ataques em tempo real. O foco está em cenários realistas, tecnologias de ponta e simulação de toda a complexidade de um incidente cibernético massivo, incluindo tomada de decisão estratégica, aspectos legais e de comunicação”.(CCDCOE,2024). Na edição de 2022, por exemplo, foi dado um cenário de um país fictício sofrendo severos ataques cibernéticos coordenados com “graves interrupções na operação de redes governamentais e militares, comunicações, sistemas de purificação de água e rede elétrica e, eventualmente, levaram a distúrbios e protestos públicos”.

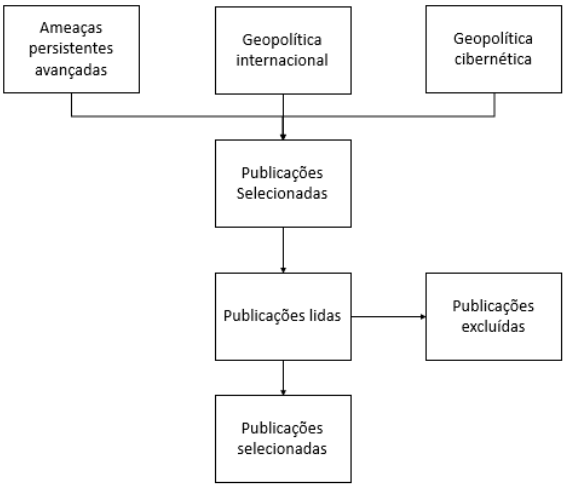
O exército brasileiro também coordena o maior exercício cibernético do hemisfério sul, chamado Guardião Cibernético. “Essas simulações permitirão que Forças Armadas, órgãos parceiros e representantes de infraestruturas críticas, como água, energia e comunicações, trabalhem em conjunto para desenvolver soluções estratégicas e avaliar a capacidade de defesa contra ataques simulados, impedindo, assim, sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade”.(Exército Brasileiro, 2024).

3 Materiais e Métodos

Neste estudo, adotou-se a metodologia exploratória com uma abordagem quantitativa. Foram realizadas leituras de materiais acadêmicos relacionados à geopolítica cibernética e ao impacto das ameaças persistentes avançadas no cenário global. As fontes de pesquisa incluíram artigos acadêmicos, revistas científicas disponíveis online, relatórios de empresas de segurança cibernética, livros e publicações de instituições governamentais, com foco nos principais fatores que influenciam o poderio cibernético das nações e como as ameaças persistentes avançadas impactam a geopolítica cibernética.

Para compilar e comparar os dados, foram consideradas apenas fontes publicadas que atendiam aos critérios de seleção relacionados à relevância e atualidade no contexto das ameaças persistentes avançadas e sua influência na geopolítica cibernética. Publicações foram excluídas com base em títulos e resumos que não atendiam ao escopo do estudo, bem como por falta de relevância. As fontes selecionadas foram analisadas em detalhe, possibilitando uma compreensão abrangente dos principais fatores que sustentam a relação entre poder cibernético e geopolítica internacional. A Figura 1 apresenta o fluxograma do processo de seleção das publicações utilizadas.

Figura 1 - Fluxograma do processo de seleção das publicações selecionadas



Fonte: Elaborada pelos autores (2024)

4 Resultados e Discussões

As ameaças persistentes avançadas continuarão a evoluir, impulsionadas pelo avanço tecnológico e pela crescente sofisticação das capacidades cibernéticas dos Estados. À medida que essas ameaças se tornam mais complexas e integradas a estratégias geopolíticas, espera-se que o ciberespaço se torne um campo de batalha ainda mais contestado, onde nações competem por superioridade tecnológica e informacional. A evolução das ameaças persistentes avançadas aponta para um futuro onde ataques cibernéticos não apenas se tornarão mais frequentes, mas também mais difíceis de detectar e mitigar, representando uma ameaça crescente para a estabilidade global.

Nesse cenário, os desafios são imensos. A proteção de infraestruturas críticas, a manutenção da soberania digital e a preservação da confiança pública nas instituições tornam-se questões centrais para os Estados. As ameaças persistentes avançadas colocam à prova as capacidades de defesa cibernética, exigindo uma cooperação internacional mais estreita, o desenvolvimento contínuo de tecnologias de segurança e a implementação de políticas eficazes de resposta a incidentes cibernéticos.

No entanto, as ameaças persistentes avançadas também apresentam oportunidades para o fortalecimento da resiliência cibernética global. A necessidade de enfrentar essas ameaças pode catalisar inovações em segurança digital, promover alianças estratégicas entre nações e fomentar uma cultura global de cibersegurança mais robusta. Ao reconhecer e responder aos desafios impostos pelas ameaças persistentes avançadas, as nações têm a oportunidade de redefinir o equilíbrio de poder no ciberespaço, moldando o futuro da geopolítica digital de maneira que privilegie a segurança e a estabilidade global.

5 Considerações Finais

O presente artigo revela a crescente complexidade das ameaças persistentes avançadas, que fazem parte cada vez mais das estratégias geopolíticas. Com a evolução dessas ameaças, o ciberespaço se torna um domínio disputado, exigindo das nações o desenvolvimento robusto das capacidades de defesa e promovam uma colaboração internacional eficaz. A proteção das

infraestruturas críticas e manutenção da soberania digital são desafios centrais que devem ser enfrentados para garantir a estabilidade global.

Porém, esse enfrentamento oferece significativas oportunidades. As necessidades de respostas aos ataques cibernéticos impulsionam constante aprimoramento da segurança digital e fomenta alianças estratégicas entre os países. Assim, ao enfrentar os desafios impostos pelas ameaças persistentes avançadas, as nações podem redefinir o equilíbrio de poder no ciberespaço, promovendo uma cultura global de cibersegurança que privilegie a resiliência e a estabilidade no futuro da geopolítica digital.

Referências

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Espionagem**. Disponível em: https://www.gov.br/abin/pt-br/assuntos/fontes-de-ameacas/espionagem. Acesso em 28 de outubro de 2024.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Política nacional de inteligência.** Disponivel em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/politica-nacional-de-inteligencia-1/politica-nacional-de-inteligencia. Acesso em 12 de novembro de 2024.

ASSUMPÇÃO, C. **The problem of cyber attribution between states**. Disponível em: https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/. Acesso em 17 de outubro de 2024.

AUGUSTÉNÉ, A. **O que é guerra cibernética e cyberwarfare?**. Disponível em: https://nordvpn.com/pt-br/blog/guerra-cibernetica-o-que-e/. Acesso em 28 de outubro de 2024.

BUCHANAN, B. **The hacker and the state: cyber attackes and the new normal of geopolitics**. Cambridge, Massachusetts : Harvard University Press, 2020.

BUXTON, O. **O que é stuxnet?.** Disponível em: https://www.avast.com/pt-br/c-stuxnet. Acesso em 28 de outubro de 2024.

BUZATU, A. **Advanced persistente threats groups increasingly destabilize Peace and security in cyberspace.** Cambridge University Press. 2022. Disponível em: https://www.cambridge.org/core/books/cyber-peace/advanced-persistent-threat-groups-increasingly-destabilize-peace-and-security-in-cyberspace/62DDC1ED4F22A03F64F307DE1CEA3371. Acesso em 30 de outubro de 2024.

CÁTEDRA. **Geopolítica: O estudo das relações de poder entre nações**. Disponível em: https://idcatedra.com.br/2024/08/geopolitica-o-estudo-das-relacoes-de-poder-entre-nacoes/. Acesso em 24 de setembro de 2024.

CNN. **Geopolítica: conheça a origem, história e importância para o Brasil e o mundo**. Disponível em: https://www.cnnbrasil.com.br/politica/geopolitica/. Acesso em 10 de setembro de 2024.

COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. **About us**. Disponível em: https://ccdcoe.org/about-us/. Acesso em 29 de outubro de 2024.

CYFIRMA. **Apt quarterly highlights q1 2024**. Disponível em: https://www.cyfirma.com/research/apt-quarterly-highlights-q1-2024/. Acesso em 28 de outubro de 2024.

ENISA. **European union agency for cybersecurity**. Disponível em: https://www.enisa.europa.eu/. Acesso em 28 de outubro de 2024.

ETDA. **Threat group cards: a threat actor encyclopedia**. Disponível em: https://apt.etda.or.th/cgi-bin/aptstats.cgi. Acesso em 28 de outubro de 2024.

ETUDO, U. WHYTE, C. YOON, V. YARAGHI, N. **From Russia with fear: fear appeals and the patterns of cyber-enabled influence operations**. Journal of Cybersecurity, Volume 9, Issue 1, 2023. Disponivel em: https://academic.oup.com/cybersecurity/article/9/1/tyad016/7250062. Acesso em 30 de outubro de 2024.

EUROPOL. **European union law enforcement agency**. Disponível em: https://www.europol.europa.eu/about-europol/our-thinking. Acesso em 28 de outubro de 2024.

EXERCITO BRASILEIRO. **Exército coordena o maior exercício cibernético do hemisfério sul.** Disponível em: https://www.eb.mil.br/web/noticias/w/exercito-coordena-maior-exercicio-cibernetico-do-hemisferio-sul. Acesso em 29 de outubro de 2024.

FERNANDES, J. P. T. **Nem novo, nem livre: o ciberespaço é a geopolítica mundial**. Disponível em: https://www.publico.pt/2020/11/29/opiniao/noticia/novo-livre-ciberespaco-geopolitica-mundial-1941031. Acesso em 24 de setembro de 2024.

FORREST, A. LINDEMULDER, G. **What are advanced persistente threats?.** Disponível em: https://www.ibm.com/topics/advanced-persistent-threats. Acesso em 28 de outubro de 2024.

FORTINET. **Ameaça persistente avançada (APT)**. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/advanced-persistent-threat. Acesso em 01 de outubro de 2024.

FUNDAÇÃO GETULIO VARGAS. COMANDO DE DEFESA CIBERNETICA. **Manual de orientação sobre exercícios de cibersegurança**. Disponível em: https://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/manual_de_orientacao_sobre_exercicios_de_ciberseguranca_fgv.pdf. Acesso em 29 de outubro de 2024.

HUSKAJ, G. **Digital geopolitics: a review of the current state**. Disponível em: https://papers.academic-conferences.org/index.php/iccws/article/view/955. Acesso em 10 de setembro de 2024.

KASPERSKY. **O que é uma ameaça persistente avançada (APT)?.** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/advanced-persistent-threats. Acesso em 01 de outubro de 2024.

LENAERTS-BERGMANS, B. **Advanced persistente threat (APT)**. Disponível em: https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/. Acesso em 01 de outubro de 2024.

MALONEY, S. **What is an advanced persistente threat (apt)?**. Disponível em: https://www.cybereason.com/blog/advanced-persistent-threat-apt. Acesso em 28 de outubro de 2024.

POIREAULT, K. **What´s in a name? Understanding threat actor naming conventions**. Disponível em: https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/understanding-threat-actor-naming-conventions.html. Acesso em 17 de outubro de 2024.