UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS V
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS
CURSO DE RELAÇÕES INTERNACIONAIS

ELAYNE FRANCINNE CORDEIRO VILELA

Os impactos do uso militarizado do serviço privado Starlink-Space X, as consequências do acesso à informação no caso russo-ucraniano

JOÃO PESSOA
2024

ELAYNE FRANCINNE CORDEIRO VILELA

Os impactos do uso militarizado do serviço privado Starlink-Space X, as consequências do acesso à informação no caso russo-ucraniano

Trabalho de Conclusão de Curso apresentado ao Departamento de Relações Internacionais da Universidade Estadual da Paraíba (UEPB), como requisito parcial à obtenção do título de Bacharela em Relações Internacionais.

Área de concentração: Mídia e Opinião Pública, Segurança Internacional, Governança Global.

Orientador: Prof. Dr. Fábio Rodrigo Ferreira Nobre

JOÃO PESSOA
2024

V699i Vilela, Elayne Francinne Cordeiro.
Os impactos do uso militarizado do serviço privado Starlink-Space X, as consequências do acesso à informação no caso Russo-Ucraniano [manuscrito] / Elayne Francinne Cordeiro Vilela. - 2024.
49 p. : il. colorido.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2024.
"Orientação : Prof. Dr. Fábio Rodrigo Ferreira Nobre, Coordenação do Curso de Relações Internacionais - CCBSA. "

1. Ciberespaço. 2. Starlink-SpaceX. 3. Privatização militar.
4. Segurança e Soberania dos Estados. I. Título

21. ed. CDD 327.17

Elaborada por Maria I. de A. S. C. Marcelino - CRB - 15/473 BSC5/UEPB

ELAYNE FRANCINNE CORDEIRO VILELA

Os impactos do uso militarizado do serviço privado Starlink-Space X, as consequências do acesso à informação no caso russo-ucraniano

Trabalho de Conclusão de Curso apresentado ao Curso de Relações Internacionais da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de bacharel em Relações Internacionais.

Aprovado em: 27/06/2024..

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br
FABIO RODRIGO FERREIRA NOBRE
Data: 27/06/2024 10:25:16-0300
Verifique em https://validar.iti.gov.br

Fábio Rodrigo Ferreira Nobre
(Orientador) Universidade Estadual da Paraíba (UEPB)

Documento assinado digitalmente
gov.br
CRISTINA CARVALHO PACHECO
Data: 27/06/2024 14:51:51-0300
Verifique em https://validar.iti.gov.br

Cristina Carvalho Pacheco
Universidade Estadual da Paraíba (UEPB)

Documento assinado digitalmente
gov.br
GILLS VILAR LOPES
Data: 27/06/2024 14:02:27-0300
Verifique em https://validar.iti.gov.br

Gills Vilar Lopes
Universidade da Força Aérea (UNIFA)

Aos meus pais, pela compreensão, dedicação, esforço e amor. A toda minha família, amigos e professores, pelo carinho, suporte e apoio ao longo dos anos, DEDICO.

AGRADECIMENTOS

À Deus pela saúde e pela oportunidade de ter ingressado e concluído uma formação de nível superior em uma universidade pública.

Ao meu professor orientador Dr. Fábio Rodrigo Ferreira Nobre por toda a sua dedicação, apoio e conselhos ao longo da orientação.

Ao professor Filipe, coordenador do curso de Relações Internacionais, por seu empenho e atenção sempre que necessário.

A toda minha família, pela compreensão da minha ausência e mudança de estado. Mas em especial aos meus pais Marcos e Sandra, aos meus irmãos Larissa e Victor, aos meus avós paternos Raquel e Joaquim (que o Senhor o tenha em Sua graça), ao meu avós maternos Maria do Carmo e Fernando, ao meus primo Edmilson e ao meu tio Adriano pelas orientações e aconselhamentos durante o período de formação.

As minhas amigas Sophia, Laura e Joana, por permanecerem ao meu lado, durante esses anos, me incentivando e alegrando.

Aos professores do Curso de Relações Internacionais da UEPB, em especial, Cristina Pacheco, Anna Beatriz, Caio Cesmark, Matheus Figueiredo, Lucila Vilhena, Giuliana Vieira, Silvia Nogueira e Raquel Melo que contribuíram ao longo dos anos, por meio das disciplinas e debates, para o desenvolvimento desta pesquisa.

Aos meus amigos de curso, em especial Ana Luiza Guimarães, Paloma Reina, Vitor Tiriba, Sophia Gonçalves e Pedro Nunes, por toda a paciência, ajuda e consideração nos desafios que encontrei durante todo meu desenvolvimento profissional e construção dessa pesquisa e formação do curso.

"A Terra é o berço da humanidade, mas não se pode permanecer no berço para sempre."
(Konstantin Tsiolkovsky)

RESUMO

O presente trabalho tem como proposta analisar o uso irrestrito das informações contidas no ciberespaço por empresas privadas como a *Starlink*. Pois ao serem processadas e utilizadas como instrumento militar, podem pôr em risco a soberania dos Estados. Metodologicamente, ao colocar em perspectiva o uso da tecnologia no caso do conflito russo-ucraniano, percebe-se o lugar de fragilidade em que os exércitos militares se encontram, ao depender de serviços privados, visto que as demandas de mercado podem confundir-se com a necessidade de manutenção da segurança de um Estado, principalmente diante de um combate. Destarte, a pesquisa buscou responder o seguinte questionamento: qual o impacto do acesso indiscriminado à informação capitalizado por sistemas como a *Starlink-SpaceX* na segurança e soberania dos Estados? A hipótese é de que sistemas de satélites privados, como a *Starlink*, oferecem riscos à soberania estatal, por se tratarem de mecanismos pertencentes a grupos com interesses privados e com acesso a informações estratégicas de forma indiscriminada. Os resultados do caso estudado apontam para a consequente imprevisibilidade trazida pelo envolvimento de uma empresa privada diante de um conflito internacional, pois, ao considerar a soberania de um Estado, sua capacidade de atuação é limitada diante da dependência da esfera política-militar a tais sistemas. Conclui-se que as forças divergentes e dinâmicas do campo econômico-comercial (mercado) a qual uma empresa privada (*Starlink*) atende não obedecem exatamente a normativas político-estatais de um país e podem interferir diretamente na segurança dos Estados.

Palavras-chave: Ciberespaço; *Starlink-SpaceX*; Privatização militar; Segurança e Soberania dos Estados.

ABSTRACT

This paper aims to analyze the unrestricted use of information in cyberspace by private companies like Starlink. When processed and used as a military tool, such information can jeopardize the sovereignty of states. Methodologically, by placing the use of technology in the context of the Russo-Ukrainian conflict into perspective, one can see the vulnerability of military forces relying on privatized services. Market demands can confuse the necessity of maintaining state security, especially during combat. Thus, this research aimed to answer the following question: What is the impact of indiscriminate access to information capitalized by systems like Starlink-SpaceX on the security and sovereignty of states? The hypothesis is that private satellite systems, like Starlink, pose risks to state sovereignty because they are mechanisms owned by groups with private interests and have indiscriminate access to strategic information. The results of the case study point to the consequent unpredictability brought about by the involvement of a private company in an international conflict. Considering a state's sovereignty, its capacity for action is limited by the political-military sphere's dependence on such systems. Additionally, the divergent and dynamic forces of the economic-commercial field (market), to which a private company (Starlink) caters, do not exactly follow the political-state norms of a country and can directly interfere with state security.

Keywords: Cyberspace; Starlink-SpaceX; Military Privatization; State Security and Sovereignty.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A necessidade de conectar-se através do globo terrestre tornou-se uma fatídica realidade. Atualmente, com o desenvolvimento da tecnologia de comunicação via satélite, fez-se possível a conexão via internet em áreas remotas difíceis de serem alcançadas através de fibra óptica ou sinal telefónico. Um fruto desta conjuntura, é o serviço *Starlink*, desenvolvido pela empresa privada *SpaceX,* que fornece globalmente internet de alta velocidade através da interação entre uma rede de satélites em baixa órbita terrestre e uma antena digital facilmente instalável. Ademais, à medida que esse projeto garante o serviço de internet a lugares de difícil cobertura, a capacidade das informações acessadas por ele tem alcance de vigilância tridimensional. Sendo assim, a *Starlink* faz parte de um sistema de informações que está em constante expansão e atualização e pode conectar tudo ao mesmo tempo em tempo real. (Cowhig, 2022)

No caso do conflito russo-ucraniano (2022 - presente momento), estudado no presente trabalho, além das inúmeras capacidades de atuação na esfera cívico-comercial, o *Starlink* ocupa um papel importante na esfera estratégico-militar. Como é evidenciado no envolvimento direto da tecnologia na guerra, ao fornecer *kits* de antenas digitais com o serviço disponível. Com isso, foi facilitada a operação de comando e controle (C2) de veículos aéreos não tripulados de vigilância e reconhecimento no campo de batalha do exército ucraniano no início do conflito (Vilar-Lopes e Manhães, 2022). No entanto, meses depois, o uso da mesma tecnologia começa a sofrer ameaças de redução pela própria empresa, ao alegar discordância entre as intenções da política empresarial da *Starlink*-*SpaceX* e a sua aplicação e uso na guerra. Bem como, é identificada, meses depois do então comunicado, a presença das mesmas antenas *Starlink* em territórios ocupados pelo exército inimigo, instaladas para prover serviço de acesso à informação.

Diante dessa conjuntura, torna-se evidente a importância do entendimento do uso do ciberespaço e as informações contidas nele. Principalmente porque, em contexto de instabilidades como a guerra, a capacidade de ação de um Estado pode tornar-se dependente de interesses privados e essa interação impacta diretamente o ambiente internacional. Portanto, diante dessas variáveis de poder entre atores não estatais no meio do ciberespaço, Vilar-Lopes (2016) pontua que a necessidade de ajustar-se individual e coletivamente a inovações sociais e tecnológicas do século XXI fica explícita para a Segurança nas Relações

Internacionais. Sendo assim, a pesquisa buscou responder a seguinte pergunta: qual o impacto do acesso à informação capitalizado por sistemas como a *Starlink-Space X*? A hipótese é de que sistemas de satélites privados, como a *Starlink*, influenciam diretamente na capacidade de ação de um Estado, por terem desenvolvido uma tecnologia de relevância estratégica. Conclusivamente nota-se que com o auxílio do serviço *Starlink* fornecido ao exército ucraniano, as tecnologias de informação da Rússia não foram capazes de limitar a Ucrânia a ter uma resposta pária diante do conflito.

A temática foi escolhida devido à participação cada vez maior das tecnologias digitais nas esferas cívico, militar, governamental e internacional de forma transformadora. Dessa forma, como objetivo, o trabalho dissertará em resposta ao crescente desenvolvimento da constelação de satélites da *SpaceX*, assim como propõe-se a analisar os impactos dos interesses comerciais em cenários como o exposto. Para o desenvolvimento deste trabalho foi realizado um estudo de caso e a abordagem escolhida foi a qualitativa explicativa, pois, ao analisar o conflito russo-ucraniano e registrar os fatos, foi possível dissertar a interpretação acerca destes. Para tanto, os procedimentos técnicos adotados possuem caráter bibliográfico, uma vez que foram utilizadas diversas fontes de pesquisa como livros, artigos e monografias, mas também documental, pela contemplação de relatórios oficiais dos governos e das entidades envolvidas no conflito.

Para alcançar o objetivo proposto, o trabalho está dividido em considerações iniciais, finais e três capítulos principais. Inicialmente é trazido um panorama geral do que se pretende discutir no trabalho assim como, as divisões metodológicas. No primeiro capítulo será explicado conceitualmente o poder no ciberespaço e suas subdivisões, para entender como essa concepção se manifesta através desse ambiente, assim como separa as esferas entre público e privado, ao demarcar a distinção entre Segurança e Defesa Cibernéticas. No segundo, apresenta-se um breve histórico da guerra entre Rússia e Ucrânia, o início da crise, com as manifestações do *Euromaidan* e a consequente anexação da Crimeia, em 2014, seguida por um aumento de hostilidades sociopolíticas que levaram ao início da chamada Operação Militar Especial, realizada pela Rússia, em fevereiro de 2022. Por último, no terceiro capítulo, o trabalho contextualiza o histórico da *Starlink-Space X* desde a sua criação e desenvolvimento, até sua atuação em campo de batalha. Propõe-se, então, analisar o envolvimento do uso da tecnologia no conflito através da sua constelação de satélites, seus usuários e suas finalidades.

2 A REALIDADE NO CIBERESPAÇO

2.1 Do ciberespaço como domínio da guerra

O espaço cibernético possui diversas definições – algumas mais abrangentes do que outras –, que contribuem para a existência de um amplo espectro de abordagens e compreensões (Kuehl, 2009). Algumas interpretações o concebem em um contexto mais teórico, visualizando-o como um novo campo de interação que atravessa e conecta as telecomunicações em uma vasta rede global. Outras abordagens consideram os elementos físicos e adaptáveis das diversas conexões e dispositivos interconectados do ciberespaço (Medeiros, Carvalho e Goldoni, 2019). No presente trabalho, ao analisar o papel da *Starlink* no conflito russo-ucraniano, a intenção é utilizar-se das definições estabelecidas naquela perspectiva para versar sobre acontecimentos da segunda.

Ao compreenderem o ciberespaço de maneira mais ampla, Lobato e Kenkel (2015, p. 24-25) o definem como "a rede de informações mundialmente interconectada e a infraestrutura de comunicações que engloba a Internet, redes de telecomunicações, sistemas de computadores e as informações contidas neles". No entanto, para entender o ciberespaço como novo ambiente de domínio para o exercício das relações de poder, é importante oferecer uma definição mais específica, alinhando-o com suas vulnerabilidades e consequências. Segundo Clarke e Knake (2012, p. 63), "o ciberespaço é composto por todas as redes de computadores no mundo e por tudo que elas conectam e controlam".

Já Libicki (2009), por exemplo, interpreta o espaço cibernético como um meio menos tangível que os tradicionais domínios de terra, ar e mar, e destaca a desterritorialidade do espaço cibernético. Para o autor, o espaço cibernético é composto por camadas interconectadas, as quais abordam componentes eletrônicos físicos, suas conexões, comandos e controles e seus métodos de armazenamento informacional. Portanto, essencialmente, por não possuir fronteiras, espaço aéreo e muito menos águas nacionais, o ciberespaço surge como um ambiente alternativo e paralelo aos domínios tradicionais (Hildebrandt, 2013). No conflito então analisado, o ambiente digital é utilizado como aparelho militar para obtenção de informações precisas e estratégicas fundamentais para disputa de poder, assim como se faz presente no uso diário das redes sociais entre civis como peça importante para o

desenvolvimento da Guerra Híbrida. Tal conceito é explicado por autores como James N. Mattis e Frank G. Hoffmann (2005, p. 57) que discute como os conflitos futuros envolvem uma mistura de guerra regular e irregular. Eles destacam: “A guerra híbrida envolve não apenas o uso de forças armadas, mas também ataques cibernéticos, propaganda e outras formas de guerra psicológica.”

Diante dessa capilaridade pertencente ao ciberespaço, diversos atores tomadores de decisão aproveitam-se dele e o transformam em um ambiente de recorrente disputa de poder, ameaçando a segurança e a soberania dos Estados como conceitos tradicionais, arraigados a noções tradicionais do que são fronteiras ou jurisdições de um país. Desde que foi popularizado o termo “ciberespaço” pelo escritor estadunidense-canadense Gibson (2014) no início dos anos 1980, na obra *Neuromancer,* essa palavra “[...] tornou-se, inclusive, sinônimo de *world wide web*”, isto é, a ideia de ciberespaço como ‘uma espécie de realidade virtual que reina sobre toda a humanidade’” (Gibson *apud* Vilar-Lopes, 2016, p. 34). E tendo em vista que, para operar no ciberespaço, basta uma conexão com a internet, essa difusão de poder inerente ao meio digital proporciona um domínio operacional para atores particulares em paralelo às forças estatais (Nye, 2012).

Diante disso, ao ser compreendido como um ambiente que emerge da interligação de fluxos de informação, o ciberespaço converge diversas redes e infraestruturas essenciais à sociedade contemporânea. E é com essa nova dinâmica de poder, que o meio digital encontra espaço para originar diferentes ameaças capazes de influenciar, modificar e explorar os fluxos de informação nesse domínio. Como reafirma Lipson (1967, p. 33), “[o] poder se manifesta de vários modos, desde a presença despercebida, o respeito e [a] obediência normal até [mesmo] o temor e o terror”. No caso do conflito, o poder é expresso na prática estratégica do uso do meio digital na tática militar.

Nota-se, portanto, que o impacto da projeção de forças e interesses nesse novo espaço operacional engendra desafios antes desconhecidos aos domínios tradicionais. Ao versar sobre tais acontecimentos cibernéticos, o apoio em conceitos fundamentais do subcampo internacionalista de Ciber RI é fundamental. Tal ideia aborda aspectos das relações internacionais moldados ou influenciados a partir desse ambiente digital. De acordo com Vilar-Lopes (2016, p. 43), autor responsável pela sistematização desse subcampo, “Ciber RI encoraja estudos sobre o impacto das relações internacionais no ciberespaço”. Tal área de estudo concentra-se em analisar como as atividades cibernéticas afetam as dinâmicas tradicionais de poder, segurança e cooperação entre atores internacionais, assim como,

investiga a forma como os Estados utilizam o ciberespaço para alcançar seus objetivos políticos, econômicos e estratégicos, bem como os desafios que enfrentam em termos de proteção de infraestruturas críticas, privacidade de dados e defesa contra ameaças cibernéticas.

2.2 Poder no ciberespaço

O poder, sob a bruma do ciberespaço, se desenvolve de variadas formas. Seja pela multiplicidade de atores, seja pela facilidade do acesso e aquisição de equipamentos, essas capacidades permitem relativo distanciamento entre Estados militarmente mais fortes, Estados fragilizados, organizações e/ou indivíduos não estatais (Medeiros, Carvalho e Goldoni, 2019). Segundo Vilar-Lopes (2016, p. 94), "o ciberespaço configura-se não apenas como um locus social para a interação de indivíduos, mas também para a atuação estratégica de Estados. Isso porque, ele [o ciberespaço] se torna, um espaço para, dentre outros, a projeção de poder" (Vilar-Lopes, 2016).

No caso russo-ucraniano, o ambiente do ciberespaço é categoricamente instrumentalizado através da *Starlink* para projeção de poder e predomínio da demonstração de força. De acordo com Manhães e Vilar-Lopes (2022, p. 27), "o apoio que os satélites dão às operações militares nos dias de hoje [atuam] como verdadeiros multiplicadores de força (*force multiplier*), ou ainda, como aprimoradores de força (*force enhancement*)". Isso porque a integração entre satélites e operações militares viabiliza, entre outros: comunicações globais; informações para serviços meteorológicos, de inteligência, vigilância e reconhecimento; dados para posicionamento, navegação e cronometragem; e sistemas de alerta precoce (*early warning system)* (Manhãs; Vilar-Lopes, 2022 *apud* Dolman, 2018; Harding, 2013; Hays, 2009). Como destaca Vilar-Lopes (2016, p. 94 *apud* Wight, 2002), "não é por mero acaso que Martin Wight, um dos expoentes da chamada Escola Inglesa de RI, constitui as relações internacionais em termos de política do poder".

Sendo assim, ao envolver-se diretamente no conflito, a *Space X* desempenha papel fundamental na manutenção da força com o poder do domínio da informação de forma decisiva diante de uma das instituições efetivas da sociedade internacional, de acordo com Bull[1]. Para Valente (2007, p. 15-16), "[...]os Estados não devem estar perdendo a oportunidade de usar esses novos tempos de informação num trabalho de conquista,

[1] De acordo com Bull (2002, p. 04), as verdadeiras instituições efetivas que moldam a sociedade internacional são o equilíbrio do poder, o Direito Internacional, a diplomacia, o papel das grandes potências e a guerra.

manutenção ou ampliação de poder". Diante dessa lógica, materializa-se a máxima de que não existe vácuo de poder nas relações internacionais, muito menos no ciberespaço (Vilar-Lopes, 2016), especialmente quando "o poder se desenvolve a partir das relações sociais, objeto de investigação das ciências sociais" (Megale, 1990, p. 53).

Nota-se, portanto, a necessidade de analisar as ações dos governantes dos Estados de forma racional e amoral na política internacional, ao direcionar suas escolhas políticas na busca pela manutenção, aumento ou demonstração de poder, como afirma Morgenthau (2003). Ou ainda, observar essa demonstração de poder por meios diplomáticos ou de projeção de força e/ou capacidades, nos dizeres de Clausewitz (2005). De uma forma ou de outra, identificam-se, por fim, duas vias de exercício do poder no ciberespaço, tanto o *soft* quanto o *hard power* (Nye, 2012).

2.2.1 Software Power

> Os acontecimentos a que se chamam de sociais "[...]são quase invariavelmente aqueles que, do mesmo modo, designamos como 'intencionais' ou revestidos de uma intenção, de uma finalidade" (Vilar-Lopes, 2016, p. 94 *apud* Rudner, 1969, p.
> 126).

É importante aqui mencionar que, quando qualquer tipo de influência cibernética é operado sem que haja intenções claras de tal feito, não se configura o que Vilar-Lopes (2016, *passim*) cunha de *Software Power*. No entanto, quando o contrário é verdadeiro, este sim enseja intenções, mais precisamente, intenções políticas (Vilar-Lopes, 2016), assim como "[...] o uso de *software* por um *cracker* representa o poder do *software*; já o seu uso por um Estado contra outro, representa o *Software Power*" (Vilar-Lopes, 2016, p. 98).

Como exemplo, tem-se o caso Julian Assange, jornalista, ativista e fundador do *WikiLeaks*, organização sem fins lucrativos que se dedica a divulgar informações confidenciais e secretas de governos e corporações por todo o mundo (Bessa, 2014). Ou mesmo o caso do *Stuxnet*, que, segundo Zetter (2014), causou, em 2010, grandes estragos ao programa nuclear iraniano, visto que tal *malware* foi projetado por potências estrangeiras desconhecidas, para controlar e inutilizar as centrífugas Siemens de enriquecimento de urânio daquele país (Portela, 2016, p. 94). O uso do *Starlink* em cenários de guerra, a preocupação é de como essa rede pode ser facilmente utilizada para ataques com *malwares*.

O que se espera provar com tais exemplos é que "aquilo que se inicia no ciberespaço tem consequências fora dele [...]" (Vilar-lopes, 2016, p. 95). E é, ao definir *Software Power*

como “a capacidade político-estratégica de que dispõem Estados para intervir na política internacional ou externa de outro Estado via utilização de *software*”, que Vilar-Lopes (2016, p. 98) justifica a razão pela qual o *Software Power* se insere nos estudos de RI, uma vez que esse poder é capaz de projetar força sem preocupações clássicas do tempo-espaço, sem o condicionamento da territorialidade, mas permeado pelo constrangimento da anarquia internacional do ciberespaço. Segundo Lipson (1967, p. 33), “[...] as armas e os equipamentos podem mudar, mas os princípios da estratégia permanecem constantes”. Sendo assim, mudam-se também as roupagens técnicas de ataque e danos, mas o compromisso e a intenção de instaurar vulnerabilidade e destruição permanecem as mesmas. Como Nye Jr (2011b, p. 114) apregoa, não é a primeira vez na história que mudanças paradigmáticas na tecnologia da informação ocorrem no seio das sociedades.

2.2.2 Software Warfare e Cyber Power ou Poder Cibernético

Nessa seção, atestam-se a conceitualização e a diferenciação entre o *Software Warfare* e o *Cyber Power* ou poder cibernético dos estudos concentrados em Ciber RI, aqui supracitados. O primeiro refere-se a um dos três modelos criados por Bellamy (2001), o qual versa sobre Guerra Centrada em Redes (GCR), ao conjecturar o uso do ciberespaço em guerras hodiernas. Nesse sentido, *Software Warfare* ou “guerra de *softwares*” constitui:

> [...]um combate travado no campo de fluxo de dados computacionais, através de manipulação de códigos-fonte, acesso à dependência de softwares via Internet, com o objetivo de atingir as capacidades inimigas, neutralizando-as e, assim, alcançando uma supremacia no combate físico. (PERON, 2016, p. 122).

Como bem pontua Vilar-Lopes (2016), o conceito de *Software Warfare* limita-se mais a aspectos específicos, com ênfase central na Internet e atrelado a combates físicos. Nesse sentido, vislumbra-se o *Software Warfare* mais em estratégias de Defesa do que em políticas de Defesa. Já o *Cyber Power* é definido por Nye Jr (2011b, p. 123 *apud* Vilar-Lopes, 2016, p. 102) como sendo o:

> [...]conjunto de recursos relacionados à criação, controle e comunicação da informação eletrônica e computacional – infraestrutura, redes, softwares e habilidades humanas, incluindo não apenas a Internet de computadores em rede, mas também Intranets, tecnologias móveis e comunicações espaciais.

Aproxima-se, assim, mais do sentido de “potência” timbrado por Kant (2008) e Rousseau (2003) enquanto projeção de poder de sentido mais polissêmico no ambiente das RI

(Vilar-Lopes, 2016, p. 102). Portanto, *Cyber Power*, ao mesmo tempo que é constituidor de uma nova e diferente forma de poder, é também "uma nova revolução da informação [que] está mudando a natureza do poder e aumentado sua difusão" (Vilar-Lopes, p. 103 *apud* Nye Jr, 2011b, p. 114).

2.2.3 Hardware Power

O conceito de *Hardware Power* é literariamente mais difuso no campo dos estudos de Ciber RI. No entanto, de acordo com Vilar-Lopes (2016, p. 102), um arcabouço teórico de cunho neoliberal institucionalista dentro das RI afirma que a projeção e obtenção de poder acontecem por duas vias: "a de forma bruta, mediante o uso de mecanismos militares e econômicos de *Hard Power*; e a de forma branda, pelo *Soft Power* da diplomacia, da influência cultural e de outros meios não brutos." A agenda política internacional do governo dos EUA, por exemplo, é uma nítida identificação da projeção desse poder de forma bruta na prática. Visto que suas capacidades cibernéticas foram capazes de criar o *Stuxnet,* conhecido na literatura especializada, como a primeira arma cibernética projetada para as guerras do século XXI (Langner, 2011). Outra prova disso, é a justificativa das prioridades do orçamento militar do país, cujo Departamento de Defesa apregoa:

> Nossa capacidade de projetar poder é um componente-chave de nossa orientação estratégica. Protegemos importantes capacidades, tais como o novo bombardeiro, a atualização da bomba de pequeno diâmetro, os porta-aviões, a modernização dos nossos soldados e as capacidades cibernéticas. Nós também protegemos capacidades que nos permitam projetar poder em ambientes negados. (Vilar-Lopes, 2016, p. 104 *apud* Departamento de Defesa dos Estados Unidos da América, 2014, p. 9).

Essa lógica se transcreve, por exemplo, nos ataques envolvendo o *malware Black Energy* na Ucrânia, em 2015. Nesse evento, *hackers* conseguiram comprometer sistemas de distribuição de energia elétrica no oeste da Ucrânia, causando cortes de energia que afetaram cerca de 225 mil pessoas, as deixando vulneráveis, de acordo com relatório da CISA (2024). Com isso, o Estado oponente foi capaz de operar, de forma tática, um ataque cibernético motivado por intenções políticas. Confirma-se, dessa forma, o eficaz potencial do ciberespaço como um domínio estratégico para ações militares[2] e de Inteligência de Estado[3]. Ora, se uma das finalidades do Estado é prover segurança, ele necessita de meios para tal.

[2] De acordo com Proença Jr e Diniz (1998, p. 50), "[a]s ações militares são, como deveria ser óbvio, a razão de ser da existência de forças armadas". Duarte (2012, p. 35) as chama de "estado das práticas".
[3] Hipótese testada e não refutada, qualitativa e quantitativamente, em Lopes (2013).

2.3 Segurança Cibernética ou Defesa Cibernética

Ao versar sobre acontecimentos cibernéticos, é necessário apoiar-se em conceitualizações tradicionais dos Estudos de Segurança Internacional (ESI), como Segurança e Defesa, os meios pelos quais o Estado se instrumentaliza para exercer a mesma função - garantir a segurança - dependendo do âmbito ao qual se adereça. No âmbito interno, chama-se Segurança Pública; no externo, Defesa Nacional. No primeiro caso, os órgãos de investigação referem-se às medidas e práticas adotadas para proteger sistemas, redes e dados contra ataques cibernéticos, violações de privacidade, roubo de informações e outras ameaças digitais. No caso da Defesa Nacional, as Forças Armadas são invocadas a utilizar um tipo especial de poder, o militar, que, segundo Vilar-Lopes (2016, p. 96), "[...]é o braço armado do [poder] político, utilizado, sobretudo, quando a Diplomacia não encontra resultados por meio de seus tratados, acordos e encontros". Ele complementa ainda, através de outros autores, que:

> Segurança e proteção compõem, portanto, lados de uma mesma moeda: para serem alcançadas, é imprescindível que se faça o uso da força, ou, na melhor das hipóteses, sua dissuasão, i.e., a capacidade concreta e intencional de projetar poder, para inibir tentativas de uma outra potência agressora ir de encontro aos interesses de um Estado (Vilar-Lopes, 2016, p. 96 *apud* Covarrubias, 1999, p. 5; Proença Jr; Diniz, 1998, p. 26).

Portanto, mesmo que haja uma interseção entre as esferas de Segurança e Defesa, suas diferenciações são fundamentalmente importantes para o entendimento do conflito a ser analisado.

2.3.1 Defesa

Para o realismo clássico das Relações Internacionais, que entende o Estado como ator central das interações internacionais, a legitimidade do uso da força através do monopólio do poder estatal é a forma garantidora da segurança e da defesa. Mas, no caso do ciberespaço, essa exclusividade da Defesa estatal para garantia da segurança é dificultada pela pluralidade de atores que exercem algum tipo de influência no meio digital. Segundo Nye (2010):

> "no mundo virtual, os atores são diversos, às vezes anônimos, a distância física é irrelevante, e uma 'única ofensa virtual quase não tem custo algum". Como a internet foi projetada para facilidade de uso em vez de segurança, a

> ofensa atualmente tem vantagem sobre a defesa"[4] (Nye, 2010, p. 5 *apud* Johnson e Pettit, 2010, p. 17)

Ou seja, as características do ciberespaço reduzem as diferenças entre os atores e provoca uma difusão de poder que tipifica a política global do século XXI (Nye Jr, 2010, p. 19). Em contextos de conflito internacional como no caso russo-ucraniano, a Defesa Cibernética é analisada através de documentos como o Manual Tallinn, que foi desenvolvido como resultado de um projeto de pesquisa liderado pelo Centro de Excelência da Organização Tratado Atlântico Norte (OTAN) para Ciberdefesa em Tallinn, na Estônia, de 2009-2013 (Schmitt, 2013, p. 01). Esse documento tem o intuito de compreender melhor a aplicabilidade do direito em operações cibernéticas mais complexas e funciona, portanto, como um trabalho adicional ao direito internacional já existente. Já que questões legais relacionadas a qualquer tipo de uso da força em conflitos armados, independentemente do tipo de arma utilizada, devem também obedecer às normas já estabelecidas na Corte Internacional de Justiça (Schimitt, 2013, p. 03).

Entende-se, portanto, que, ao tratar-se de Defesa no ciberespaço em contexto de guerra, atores tradicionais como o Estado são menos prováveis de dominar tal ambiente, devido à característica plural do meio digital. Parafraseando Nye Jr (2010, p. 5), "A ambiguidade é onipresente e reforça a habitual névoa da guerra. Redundância, resiliência e rápida reconstituição tornam-se componentes cruciais da defesa". E, por isso, com a evidente expansão e distribuição do poder no meio digital, revela-se a importância das redes como uma dimensão crucial do poder na contemporaneidade.

2.4 Soberania no Ciberespaço

Ao analisar o ciberespaço através da sua característica desterritorializante, entende-se o porquê do conceito de soberania, como lógica tradicional de definição e interpretação de território, ser questionada, visto que:

> A desterritorialidade do ciberespaço se faz presente a partir do momento que sua lógica reticular, na forma de fluxos interconectados, permeia o território de diferentes Estados; ou quando os dispositivos que servem de nós na rede do ciberespaço são controlados e/ou explorados por outros Estados. (Medeiros; Carvalho; Goldoni, 2019, p. 48).

[4] Texto original: *"In the virtual world, actors are diverse, sometimes anonymous, physical distance is immaterial, and a 'single virtual offense is almost cost free.'" Because the internet was designed for ease of use rather than security, the offense currently has the advantage over the defense."* (Johnson e Pettit, 2010, p. 17 *apud* Nye, 2010, p. 5 - tradução da autora)

Ou seja, a permeabilidade das fronteiras no ambiente digital questiona as bases nas quais o conceito de território é fundamentado. Como, por exemplo, foi o caso do vírus conhecido como *Not Petya*, espalhado na Ucrânia, no ano de 2017, e rapidamente disseminado para além das fronteiras territoriais ucranianas, responsável por causar destruição global em larga escala (Greenberg, 2019). Sendo assim, a urgência da adaptação à desterritorialidade no mundo virtual advém da preocupação no controle e monitoramento de dados, pois encontra-se na guerra cibernética um ponto em comum no emprego de instrumentos de altíssima tecnologia para atividades que importam à tomadas de decisão e manutenção da segurança de um Estado soberano (Medeiros; Carvalho; Goldoni, 2019).

Ao afirmar que "o ciberespaço tem recentemente emergido como uma preocupação de segurança estratégica"[5], Mazanec (2015, p. 219) prevê as complicações que esse ambiente gera para a máxima weberiana no uso legítimo da força física/violência estatal em um dado território, pois, essencialmente, o espaço cibernético surge como um espaço alternativo e paralelo aos domínios tradicionais de terra, ar e mar; porém, o ciberespaço não possui fronteiras, espaço aéreo e nem águas nacionais (Medeiros; Carvalho; Goldoni, 2019, p. 47 *apud* Hildebrandt, 2013, p. 47). Exatamente por isso, o ciberespaço é dotado de valor estratégico para os Estados, e, ao proporcionar um domínio operacional para atores particulares em paralelo com forças estatais, difunde o poder e cria um novo ambiente do qual emanam ameaças não necessariamente estatais (Medeiros; Carvalho; Goldoni, 2019 *apud* Nye Jr, 2012).

Conclui-se, portanto, a urgente necessidade de adaptação política e socioterritorial à nova era digital, pois, como Lipson (1967, p. 33) apregoa:

> [...]haverá sempre problemas idênticos de moral, treinamento, disciplina[...], bem como o de aplicar o devido grau de força no lugar certo e no momento preciso. [...] o que hoje tende cada vez mais a impressionar é a permanente necessidade de nos ajustarmos, individual e coletivamente, às invenções da tecnologia, à inovação social[...].

Diante do conflito a ser analisado em seguida, tal narrativa é diretamente aplicada a um contexto de guerra tecnológica e novos cenários socioculturais.

[5] Texto original: "*The cyberspace domain is defined in numerous ways and has only recently emerged as a strategic security concern"* (Mazanec, 2015, p. 219 - tradução da autora)

3 GUERRA RÚSSIA-UCRÂNIA

O conflito russo-ucaniano não começou no dia 24 de fevereiro de 2022, o histórico apresentado a seguir relata passos e desdobramentos considerados relevantes para entender a guerra eslava aqui exposta. Laços históricos, sociais, econômicos e políticos são levados em conta, a fim de assimilar o conflito separatista. Sendo assim, faz-se necessário, inicialmente, entender como o movimento do *Euromaidan* foi o estopim responsável pela anexação da Crimeia, em 2014, e como esse acontecimento gera impacto no tabuleiro internacional entre Rússia e Ucrânia em 2022.

3.1 Euromaidan

As fortes manifestações que aconteceram na Ucrânia, em 2013, logo após a suspensão das negociações para o Acordo de Associação com a União Europeia (UE) pela Ucrânia, são intituladas de *Euromaidan.*[6] Horas depois da declaração de pausa nas conservas com a UE feita pelo gabinete ucraniano, no dia 21 de novembro de 2013, centenas de ucranianos se reuniram na Praça da Independência (*Maidan*), em Kiev, para protestar (House of Commons, 2023). O país, que enfrentava uma forte crise econômica e social desde 2009, era então liderado pelo presidente Viktor Yanukovych, o qual entendeu que a adesão à União Europeia não resolveria os problemas econômicos ucranianos e ainda dificultaria a estreita relação com a Rússia, cujo país Yanukovych mantinha fortes relações (Duffield; Donini, 2014).

A escala violenta dos protestos antigoverno, entre o final de 2013 e o início de 2014, registrou dúzias de mortes e centenas de protestantes feridos (House of Commons, 2023). Diante da crise, o parlamento ucraniano decidiu, então, depor o presidente Yanukovych e chamar novas eleições até o final do mesmo ano. Assim sendo, Petro Poroshenko assumiu a presidência em junho de 2014. No entanto, o vazio de poder que marcou os meses de manifestação do *Euromaidan*, trouxe consequências significativas e permanentes para a Ucrânia. Diante desse cenário de instabilidade, ao leste do país, a escalada para o conflito armado começou na região da Criméia, onde exércitos militares iniciaram operações de ocupação, que mais tarde levariam a sua anexação (House of Commons, 2023).

[6] "O protesto foi batizado de 'Euromaidan', unindo o nome do local com a inclinação pró-europeia dos seus participantes. Tal denominação, contudo, não é precisa, uma vez que o elo principal entre a massa heterogênea de manifestantes não era a orientação externa do país, mas o rechaço ao regime" (FORTES, 2017, p. 77-78).

3.2 Anexação da Crimeia (2014)

A anexação da Crimeia, em 2014, pelo governo russo, faz parte de uma estratégia geopolítica histórica empregada pela Rússia devido à importância socioeconômica dessa região. A região interessa aos russos por duas razões: diversidade sociocultural e posição geoestratégica. Sua população era composta por 60% de russos e 25% de ucranianos[7] na época da sua anexação em 1954, e sua localização permite acesso e controle do Mar Negro e dos Estreitos de Bósforo e Dardanelos. Militarmente, a Crimeia também acolhe na cidade de Sevastopol, uma importante base naval, a qual a Federação Russa possui acordo de pertencimento, através do Tratado Russo-Ucraniano de Amizade de 1997, origem da posse da Frota do Mar Negro para Rússia (Bandeira, 2016).

Mas é diante do ciberespaço que a Rússia desenvolve sua influência, ao utilizar-se da Guerra Híbrida como meio de mudança da percepção do próprio povo russo em ataques cibernéticos. Com isso, o objetivo de prejudicar infraestruturalmente a capacidade do inimigo de agir eficazmente, é atingido através de *fake news* como parte das operações psicológicas de desinformação diante do conflito (Nakashima, 2017). Nesse contexto, a tática híbrida é desenvolvida, ao combinar o emprego das ações informacionais com a atuação das forças militares em campo. Sendo assim, em fevereiro de 2014, a Rússia finalmente utilizou-se de suas forças convencionais, ao bloquear os portos ucranianos para alcançar, no dia seguinte, a base naval de Sevastopol e a região de Yalta (Bouwmeester, 2021).

Enquanto isso, no meio digital, através do discurso “de operações de treinamento” nas proximidades da Crimeia, a Rússia conseguiu enviar soldados convencionais como meio de fortificação das regiões e como forma de dissuadir Kiev de realizar uma contraofensiva. No entanto, uma estratégia híbrida emprega não apenas elementos operacionais cibernéticos ou militares, mas também utiliza fatores psicológicos como forma de desestabilização (Nakashima, 2017). Consequentemente, o apoio dado pela Rússia às regiões do leste levou à criação das Milícias Populares nas regiões de Donbass e Luhansk (Gardner, 2015). Portanto, diante do sucesso de suas operações híbridas, em março de 2014, Moscou "levantou a bandeira" em defesa de seu direito de proteger[8] os russos étnicos que viviam fora da Rússia. Esse fato levou à votação de um referendo em 6 de março de 2014, visando o retorno da Crimeia ao controle russo (Galeotti, 2019).

[7] Senso referente ao ano de 1991 (NATO, 1997)
[8] Doutrina presente no governo de Yeltsin e que foi trazida à tona durante o conflito de 2014.

3.3 Aumento das hostilidades

A intensificação da hostilidade entre as forças russas e ucranianas foi ainda maior, após a assinatura do acordo comercial com a UE e a tentativa de trégua com os insurgentes de Donbass, em 27 de junho de 2014. Mas vale destacar que, até então, as operações russas eram caracterizadas por sua plausível negação. Isso porque as ações de fortalecimento das bases navais e as atividades próximas ao território ucraniano foram declaradas pela Rússia como exercícios de treinamento (Bouwmeester, 2021). Além do que, em paralelo às operações táticas, o reconhecimento do poder de projeção e delineamento, possibilitado por uma estratégia irregular híbrida, fica explicitado no uso de Empresas Militares e de Segurança Privadas (PMSCs)[9], como a E.N.O.T Corp, que administraram recursos midiáticos e organizaram campanhas de desinformação (USASOC, 2016).

O propósito de citação da Tecnologia da Informação utilizada através do ciberespaço nesse contexto conflituoso é para reforçar que o emprego de atividades digitais alinhadas a práticas militares em cenário de guerra não é novidade entre ambos os países citados. Como afirma o relatório ISW em 2015 acerca da atuação informacional da Rússia nessa fase inicial do conflito contra a Ucrânia:

> Tornou-se claro, no entanto, que a Rússia está ativamente utilizando suas técnicas de guerra informacional em apoio a um esforço de guerra híbrida para alcançar seus objetivos atuais, a saber, a federalização da Ucrânia ou a concessão por parte de Kyiv de um status legal especial às regiões controladas pelos separatistas no leste da Ucrânia. (ISW, 2015, p. 9)[10]

> No nível tático, a guerra informacional permite que a Rússia obtenha surpresa quanto ao momento ou à maneira de um ataque. Dessa forma, a Rússia ganha tempo e eficiência contra as forças terrestres inimigas. Como, oficialmente, a guerra na Ucrânia não foi declarada, e os separatistas conduzem operações de alta intensidade em curtos períodos que limitam o tempo de resposta dos Estados Unidos antes que a situação volte ao silêncio, o inimigo geralmente é pego de surpresa e/ou apresentado a uma imagem errônea ou incompleta da situação. (ISW, 2015, p. 17)[11]

[9] As Empresas Militares e de Segurança Privadas (PMSCs, do inglês Private Military and Security Companies) são entidades privadas que fornecem serviços de segurança e defesa militar (Singer, 2003)

[10] Texto original: *"It has become clear, however, that Russia is actively using its information warfare techniques in support of a hybrid-warfare effort to achieve its current objectives, namely the federalization of Ukraine or Kyiv's concession of special legal status to the separatist-controlled regions of eastern Ukraine."* (ISW, 2015, p. 9 - tradução da autora)

[11] Texto original: "*On the tactical level, information warfare allows Russia to achieve surprise in the time or manner of an attack. Russia thereby gains time and efficiency against the enemy's ground forces. Since, officially, the war in Ukraine is not declared, and the separatists conduct high-intensity operations in short bursts that*

Ambas passagem deixam explícita a maneira pela qual a Rússia, por exemplo, delega relevância ao uso do ciberespaço como prática tática e estratégica militar. Em seguida, o cenário se desenvolve na primavera do ano de 2014, quando forças militares russas seguem com seu apoio às repúblicas separatistas pró-Rússia presentes nas regiões de Donbass, Donetsk e Luhansk. E, para tal, diversas emboscadas e ataques foram realizados contra soldados ucranianos (Kosiuk, 2020). Foi o caso do ataque à aeronave IL-76 da Força Aérea da Ucrânia, na região de Luhansk, em junho de 2014, causando a morte de 40 paraquedistas ucranianos.[12] Tal operação teve como foco principal a eliminação do fornecimento de apoio à região sul de Luhansk, além de visar a expulsão da infantaria ucraniana da área (Foley; Kaunert, 2022).

É diante desse contexto que o governo da Ucrânia e os rebeldes pró-Rússia assinam um cessar-fogo em Minsk (referido como o Primeiro Acordo de Minsk) para encerrar quase cinco meses de combates. No entanto, o cessar-fogo entra em colapso em questão de dias. Em seguida, o conflito avança para o dia 24 de janeiro de 2015 quando uma série de ataques com foguetes deixa 30 pessoas mortas e muitas outras feridas na cidade de Mariupol, no leste da Ucrânia (House of Commons, 2023). Com esse evento, o início de 2015 foi marcado por simultâneas tentativas de acordos e ofensivas militares, ao mesmo tempo, pois, mesmo com a assinatura do acordo de Minsk II em 11 de fevereiro de 2015, às tropas de Kiev seguem avançando para a região de Debaltseve, de modo a tentar recuperar os territórios, até então, perdidos para as forças russas (Bandeira, 2016).

Nos anos seguintes, as ofensivas registradas entre o período de 2013-2015 às ações políticas da Ucrânia começam a ser ainda mais direcionadas a reaproximação com a União Europeia e a OTAN. Como ficou explícito ao ser firmado o Pacote de Assistência Abrangente[13], em julho de 2016, entre a Ucrânia e a OTAN. Assim como aconteceu em junho de 2018, ao ser votada, no Parlamento Ucraniano, a restauração da adesão à OTAN como objetivo estratégico da política externa do país[14]. Esse fator contribuiu para que, em setembro

limit the amount of time that the United States has to respond before the situation goes quiet, the enemy is usually taken by surprise and/or presented with an erroneous or incomplete image of the situation." (ISW, 2015, p. 17, tradução nossa).

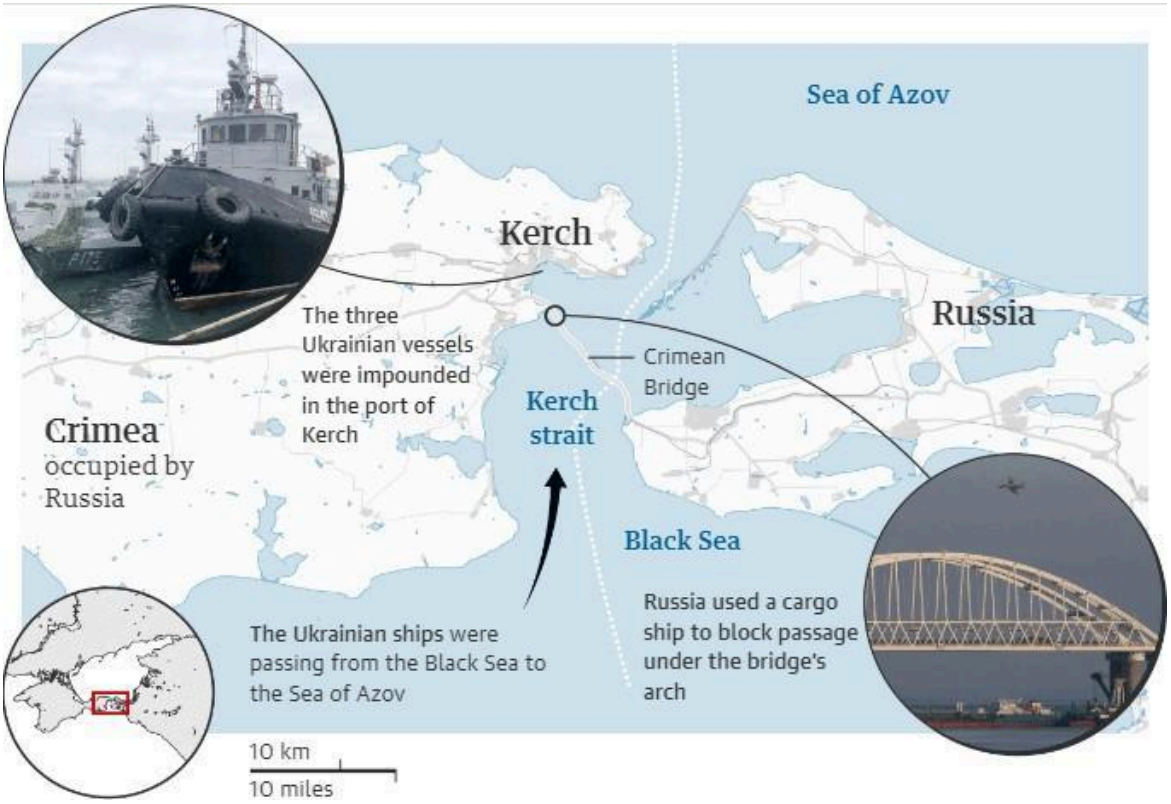
[12] MARTEN, Kimberly. Russia's use of semi-state security forces: the case of the Wagner Group. Post Soviet Affairs, mar, 2019.

[13] NATO. *NATO's Comprehensive Assistance Package for Ukraine*. 2016. Disponível em: https://www.nato.int/cps/en/natohq/topics_136027.htm. Acesso em: 17 de Junho de 2024.

[14] NATO PARLIAMENTARY ASSEMBLY. *Ukraine's Path to NATO: Legislative and Strategic Steps*. 2018. Disponível em: https://www.nato-pa.int/document/ukraines-path-nato-legislative-and-strategic-steps. Acesso em: 17 de Jun. de 2024.

do mesmo ano, entrasse em vigor o acordo de associação da Ucrânia com a União Europeia[15]. Enquanto isso, as investidas russas seguiram, com a inauguração de uma ponte de 12 milhas entre o continente russo e a Crimeia, reforçando o controle da Rússia sobre a península anexada (MacFarquhar, 2018)[16], como é observado na Figura 1 a seguir.

Figura 1: Ponte entre a Rússia e a península da Crimeia



Fonte: The Guardian, 2018[17]

No entanto, é no ano de 2019, que a emenda à Constituição da Ucrânia estabelece a adesão à OTAN como uma política estratégica de segurança externa e a eleição avassaladora do então presidente Volodymyr Zelensky ocorre (House of Commons, 2023, p. 24). Ao lado oriental, no final do mesmo ano, os laços com a Rússia dão sinal de estreitamento com a

[15] EUROPEAN COMMISSION. *EU-Ukraine Association Agreement: Strengthening the Partnership*. Brussels, 2018. Disponível em: https://europa.eu/rapid/press-release_IP-18-5808_en.htm. Acesso em: 17 de Jun. de 2024.
[16] Disponível em: https://www.nytimes.com/2018/05/15/world/europe/russia-crimea-bridge.html. Acesso em: 17 de Jun. de 2024.
[17] Disponível em: https://www.theguardian.com/world/2018/nov/27/russia-to-charge-ukrainian-sailors-as-kerch-crisis-deepens.

primeira troca de prisioneiros capturados, desde a anexação da Crimeia em 2014.[18] No entanto, as relações com a OTAN seguem a escalonar: por volta de junho e setembro de 2020, o presidente Zelensky aprova a nova Estratégia de Segurança Nacional da Ucrânia[19], com o objetivo de aderir à OTAN.

Diante desse cenário, é em abril de 2021 que a Rússia anuncia novos exercícios militares aumentando as tensões com a Ucrânia e as preocupações sobre o risco de novos combates. Por volta do final do mesmo mês, o ministro da Defesa da Ucrânia declara que 110.000 tropas russas estão se agrupando na fronteira em 56 grupos táticos do tamanho de batalhões (House of Commons, 2023, p. 26). A partir de então, entre o final do ano de 2021 e o início do ano de 2022 as hostilidades escalonam consecutivamente, principalmente após a rejeição pelos EUA e aliados à exigência russa de garantias da OTAN de que a Ucrânia e a Geórgia nunca se juntariam à aliança militar (Pifer, 2021). Mesmo perante as tentativas de acordo entre aliados do Ocidente e a Rússia para diminuição das animosidades, a preparação e a presença militar seguem crescendo. Até que em 24 de fevereiro de 2022, a Rússia lança uma invasão em grande escala na Ucrânia.[20]

3.4 Início da Operação Militar Especial

No então evento categorizado pelo *Institute for the Study of War* (ISW, 2022) de "segunda fase das operações militares", a Rússia invade o restante do território ucraniano e utiliza-se do aparato estatal para caracterizar tal acontecimento como uma "operação militar especial" (Foreign Affairs Institute, 2022). Apesar disso, mesmo diante das alertas de agências de inteligência ocidentais dos EUA[21], do Reino Unido[22] e da Estônia[23], dentro do

[18] THE GUARDIAN. Ukraine and Russia Conduct Prisoner Swap in Bid to Ease Tensions. *The Guardian*, 29 de dezembro de 2018. Disponível em: https://www.theguardian.com/world/2018/dec/29/ukraine-russia-conduct-prisoner-swap. Acesso em: 17 jun. de 2024.
[19] NATO PARLIAMENTARY ASSEMBLY. *Ukraine's New National Security Strategy: Aligning with NATO*. 2020. Disponível em: https://www.nato-pa.int/document/ukraines-new-national-security-strategy-aligning-nato. Acesso em: 17 jun. 2024.
[20] THE NEW YORK TIMES. Russia Invades Ukraine in Largest European Attack Since WWII. *The New York Times*, 24 de fevereiro de 2022. Disponível em: https://www.nytimes.com/2022/02/24/world/europe/russia-ukraine-invasion.html. Acesso em: 17 jun. 2024.
[21] Harris, S. and Sonne, P., 'Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns', Washington Post, 3 December 2021, https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b 11ec-8769-2f4ecdf7a2ad_story.html.
[22] Sabbagh, D., 'US and UK intelligence warnings vindicated by Russian invasion', The Guardian, 24 February 2022, https://www.theguardian.com/us-news/2022/feb/24/us-uk-intelligence-russian-invasionukraine.
[23] Välisluureamet/Estonian Foreign Intelligence Service (ed.), International Security and Estonia 2022, 1/2022, Tartu, https://www.valisluureamet.ee/doc/raport/2022-en.pdf.

período de dezembro de 2021 a fevereiro de 2022, de que uma invasão russa era tanto provável como iminente, Putin continua a negar qualquer planejamento de invasão ou continuação de conflito. E, nesse jogo político entre discurso diplomático e estratégia militar, Putin tenta novamente empregar sua tática híbrida sobre a Ucrânia. Quando a Rússia invade o território ucraniano, anexa a Crimeia, e separatistas apoiados pela Rússia no leste da Ucrânia conseguem controlar uma parte significativa da região sudeste de Donbass, na Ucrânia, em 2014, e a demonstração das capacidades militares e de guerra cibernética da Rússia ficam consolidadas (Pisciotta, 2020).

Consecutivamente, após a vitória decisiva das forças políticas pró-Ocidente durante os protestos do *Euromaidan*, em 2014, juntamente com a tentativa subsequente da Ucrânia de se aproximar da União Europeia e a situação geopolítica daquele período, levaram os oficiais russos a intensificar sua agressão e revisionismo contra a Ucrânia, acreditando estar defendendo seus interesses nacionais legítimos (Aleprete, 2017). É diante desse contexto que, em 22 de fevereiro, o Conselho da Federação da Rússia autoriza o uso de força militar no exterior[24] e a Ucrânia é atacada por múltiplas frentes a partir da Rússia, da Bielorrússia e dos territórios ocupados na Ucrânia (Foreign Affairs Institute, 2022).

Inicialmente, os planos estratégicos russos de capturar a capital ucraniana, Kiev, em três dias, e colapsar a eventual resistência do exército ucraniano para obter total controle estratégico do país por volta de maio foram frustrados. Meses depois, nenhum desses planos tinha se consolidado, a Ucrânia seguiu resistindo. Enquanto isso, as frentes ao norte e ao leste de Kiev eram abandonadas em meio a tentativas do exército russo de reagrupar-se para direcionar sua ofensiva às regiões orientais, sul da Ucrânia e ao norte da Crimeia, ao longo da zona costeira do Mar Negro (Foreign Affairs Institute, 2022). Em abril, as tentativas russas de reajustar-se a constantes derrotas continuam e a nova ofensiva russa é lançada com um novo objetivo estratégico, a "liberação completa" das províncias de Donetsk e Luhansk (Institute for the Study of War, 2022), como pode ser observado na Figura 2.

[24] Hodge, N., 'Russia's Federation Council gives consent to Putin on use of armed forces abroad, Russian agencies report', CNN, 22 February 2022, https://edition.cnn.com/europe/live-news/ukraine-russia-news-0222-22/h_59a413ce984eda5954ce5b9c4655bcc5.

Figura 2: Reajuste da ofensiva russa no território ucraniano em 30 de abril de 2022

Fonte: Institute for the Study of War (ISW), 2022[25]

Nesse contexto de fracasso operacional e tático do exército russo, a resposta de Putin veio através da mesma propaganda política histórica da Rússia, aos moldes da Segunda Guerra Mundial. Em 9 de maio, ele reafirma publicamente que a OTAN já planejara uma invasão à Crimeia usando a Ucrânia como um ator *proxy*:

[25] Disponível em: https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-april-30. Acesso em: 22 jun. 2024.

> Os países da OTAN não quiseram nos ouvir. Eles tinham planos diferentes, e nós vimos isso. Eles estavam planejando uma invasão em nossas terras históricas, incluindo a Crimeia. [...] A Rússia deu uma resposta preventiva à agressão; foi uma decisão forçada, oportuna e a única decisão correta.[26] (Putin, 2022 *apud* The Guardian, 2022).

Ademais, o conflito continua entre vitórias ucranianas, como a da Batalha de Kharkiv, e reagrupamentos militares russos em direção ao leste, com a Rússia solidificando ganhos territoriais ao longo de maio e junho[27]. Nessa fase inicial do conflito, a presença russa é fortificada nas áreas costeiras do sul da Ucrânia e majoritariamente nas províncias de Donetsk e Luhansk, assim como em Kherson e Mariupol, como se observa na Figura 3.

Figura 3 – Território da Ucrânia em 23 de junho de 2022

[26] Texto original: *"NATO countries did not want to listen to us. They had different plans, and we saw it. They were planning an invasion into our historic lands, including Crimea. […] Russia gave a preemptive rebuff to aggression; it was a forced, timely, and only right decision"*. Roth, A., 'Putin ties Ukraine invasion to second world war in Victory Day speech', The Guardian, 9 May 2022. Disponível em: 17 jun. 2024 https://www.theguardian.com/world/2022/may/09/putin-ties-ukraine-invasion-second-world-warvictory-day-speech-russia. Acesso em: 18 jun. 2024.

[27] Hird, K., Barros, G. and Clark, M., 'Russian offensive campaign assessment', Institute for the Study of War, 15 June 2022, https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessmentjune-6.

Fonte: Ministério da Defesa do Reino Unido, 2022[28]

Quanto à resposta diplomática, países como os Estados Unidos e o bloco da União Europeia impuseram seguidas sanções à economia russa, em uma série de pacotes.[29] Nesse mesmo sentido de contramedidas externas, países historicamente neutros decidiram incorporar-se na aliança militar após os fatídicos acontecimentos, em junho de 2022, como foi o caso da Finlândia.[30] Já em relação ao nível estratégico, a Rússia subestimou gravemente a coesão e a determinação dos países ocidentais, resultando em uma espécie de "profecia autorrealizável na expansão da OTAN" (Foreign Affairs Institute, 2022, p. 14-15), visto que, após a invasão, os EUA, a OTAN e membros individuais da aliança ocidental têm fornecido extensa ajuda militar, incluindo *drones*, sistemas antitanque e antiaéreos, e inteligência militar em tempo real.[31] De acordo com o Instituto de Relações Exteriores da Grécia, de 2014 até o início da invasão em 2022, os Estados Unidos concederam mais de $6,4 bilhões em apoio de segurança, fornecendo treinamento e equipamento para auxiliar a Ucrânia na defesa de sua integridade territorial, na proteção de suas fronteiras e no aprimoramento da cooperação com a OTAN. Conclui-se, portanto, que inicialmente, mesmo ao descartar uma intervenção militar direta no conflito, os membros da OTAN se comprometeram a fornecer ajuda essencial de inteligência militar avançada à Ucrânia, com armas pesadas e sistemas de longo alcance.[32] E o fizeram de maneira sistemática e contínua. É diante desse contexto que a Starlink se apresenta como uma componente estratégica.

---

[28] MINISTRY OF DEFENCE (UK). Country Policy and Information Note: Security Situation, Ukraine, June 2022. Disponível em: https://www.gov.uk/government/publications/ukraine-country-policy-and-information-notes/country-policy-and-i nformation-note-security-situation-ukraine-june-2022-accessible. Acesso em: 17 jun. 2024.

[29] Atlamazoglou, S., 'Putin's Next Problem: Russia Is Getting Hit with Tougher Sanctions',19fortyfive, 22 April 2022. Disponível em: https://www.19fortyfive.com/2022/04/putins-next-problem-russia-is-getting-hit-with-tougher-sanctions/. Acesso em: 17 jun. 2024.

[30] Office of the President of the Republic of Finland/Prime Minister's Office, 'Joint statement by the President of the Republic and Prime Minister of Finland on Finland's NATO membership', Press Release 30/2022. Disponível em: https://www.presidentti.fi/en/press-release/joint-statement-by-the-president-of-the-republic-andprime-minister-of-finland-on-finlands-nato-membership/; Milne, R., 'Finland's president and prime minister back NATO membership', Financial Times, 12 may 2022. Disponível em: https://www.ft.com/content/4783d924-9a22-4e6ca59b-b10496b8d755. Acesso em: 17 jun. 2024.

[31] Barnes, J.E., 'Cooper, H. and Schmitt, E., 'U.S. Intelligence Is Helping Ukraine Kill Russian Generals, Officials Say', The New York Times, 4 May 2022. Disponível em: https://www.nytimes.com/2022/05/04/us/politics/russia-generalskilled-ukraine.html. Acesso em 17 jun. 2024.

[32] 'Bill Signed: S. 3522', The White House, 9 May 2022. Disponível em: https://www.whitehouse.gov/briefingroom/legislation/2022/05/09/bill-signed-s-3522/.

4 STARLINK

4.1 Histórico da *Starlink-SpaceX*

A SpaceX, ou Space Exploration Technologies Corp., é uma empresa americana de transporte e fabricação aeroespacial, fundada em 2002 pelo empresário sul-africano Elon Musk, com o objetivo de reduzir os custos da exploração espacial e tornar possível a colonização de Marte (Vance, 2015). A trajetória da SpaceX começa distante dos fins militares mas com grande potencial tecnológico. O desenvolvimento do foguete *Falcon 1*, foi o primeiro projeto próspero, o mesmo realizou seu primeiro voo em 2006, e após várias tentativas falhadas, alcançou órbita em 2008, registrando, assim, a marca de primeiro foguete a combustível líquido desenvolvido por uma empresa privada a alcançar o espaço (Berger, 2021).

Com esse sucesso inicial, a *SpaceX* foi impulsionada a desenvolver o *Falcon 9*, um foguete maior e mais poderoso, agora com o objetivo de ser reutilizável para reduzir custos. Em 2010, tal projeto teve seu voo inaugural bem-sucedido e marcou, assim, um grande avanço na capacidade de lançamento da empresa (Berger, 2021) e de toda a logística para lançamento de foguetes, desde então. A partir disso, os projetos e desenvolvimentos das tecnologias criadas pela *SpaceX* tiveram grande avanço e apreço estadunidense. Os feitos históricos da empresa no mundo aeroespacial foram inúmeros, projetos ambiciosos como o *Falcon Heavy*[33], a missão *Demo-2*[34] e o desenvolvimento do *Starship*[35], são resultado da combinação de inovação tecnológica, ousadia empresarial e marcos históricos liderados pela *SpaceX* na nova era da exploração espacial conhecida como New Space[36].

É nesse cenário que a *Starlink* se desenvolve. Anunciada publicamente pela Space X em 2015, a *Starlink* começa o desenvolvimento dos seus satélites oficialmente neste ano e três anos depois, em 2018, os dois primeiros satélites de teste para validação da tecnologia são lançados.[37] Em 2019, a empresa lançou seu primeiro grande lote, composto por 60 satélites

[33]NASA. 5 years ago: First flight of the Falcon Heavy rocket. Disponível em: https://www.nasa.gov/history/5-years-ago-first-flight-of-the-falcon-heavy-rocket/. Acesso em: 18 jun. 2024. [34]NASA. SpaceX Demo-2 mission launches into history. Disponível em: https://www.nasa.gov/image-article/spacex-demo-2-mission-launches-into-history/. Acesso em: 18 jun. 2024. [35] SPACEX. Starship. Disponível em: https://www.spacex.com/vehicles/starship/. Acesso em: 18 jun. 2024. [36] Definido por Deganit Paikowsky (2017) como a mudança no ecossistema das atividades espaciais globais,
onde há um aumento significativo da participação do setor privado, contrastando com o domínio histórico dos estados nacionais. Este novo paradigma é caracterizado por inovação acelerada, menor custo de acesso ao espaço e uma variedade maior de atores envolvidos, incluindo startups e empresas privadas que trazem novas oportunidades e desafios para o setor espacial (Paikowsky, 2017).
[37] SPACE. Microsat 2. Disponível em: https://space.skyrocket.de/doc_sdat/microsat-2.htm. Acesso em: 18 jun. 2024.

operacionais[38] e expandiu, nos anos seguintes, seu impacto no meio digital com os primeiros testes de serviço através da constelação, como foi o caso do Projeto Beta nos EUA e Canadá (O'Callaghan, 2020)[39]. Em janeiro de 2021, o número de satélites em órbita já passava de 1.000, enquanto o serviço era disponibilizado para mais países, incluindo Reino Unido, Alemanha e Nova Zelândia.[40] Até o início de 2023, meses após o conflito russo-ucraniano, o alcance e a velocidade da internet de alta frequência da *Starlink* já chegava a ser disponibilizado para aviões comerciais e em áreas de difícil acesso com planos T-Mobile.[41] No Brasil, atualmente, é possível acessar a internet por meio do *Starlink* na região amazônica e na área alagada em Porto Alegre. É importante ser resgatado aqui a característica desterritorializante desse serviço no ciberespaço o qual, mais uma vez, permeia entre fronteiras e ultrapassa a conceitualização arraigada em padrões tradicionais obsoletos que urge adaptações política e sócio-territorial, as quais Lipsom chama atenção com sua narrativa em 1967.

No entanto, as conquistas da empresa são possíveis também por conta de uma série de permissões adquiridas pela mesma ao navegar por regulamentações internacionais de atuação e domínio. Junto ao Departamento de Patentes do governo dos Estados Unidos, em agosto de 2017, a Starlink conseguiu expandir sua atuação. Apesar de, originalmente, propor que o serviço satelital fosse apenas provedor de internet, com essa nova expansão foram incluídas atividades de comunicação e transmissão via satélite, imagens e sensores remotos, assim como outros serviços complementares para registros e atuações militares responsáveis por garantir grande domínio sobre o potencial para obter informações estratégicas. (Cowhig, 2022)

Além disso, o exército estadunidense desempenhou papel crucial no desenvolvimento do projeto Starlink, seja ao patrocinar a Space X para expansão de possibilidades de uso do programa em diferentes cenários desde o início do seu lançamento, seja na participação direta

[38] KUPERMAN, Rachel. SpaceX launches 60 Starlink satellites, aiming to build a global internet network. CNN, 29 jan. 2020. Disponível em: https://www.cnn.com/2020/01/29/tech/spacex-starlink-satellite-internet-launch-scn/index.html. Acesso em: 18 jun. 2024.

[39]Disponível em: https://www.forbes.com/sites/jonathanocallaghan/2020/10/27/spacex-reveals-monthly-cost-of-starlink-internet-in-its-better-than-nothing-betabut-is-it-too-expensive/. Acesso em: 18 jun. 2024.

[40] KELION, Leo. Elon Musk's Starlink broadband beats UK download targets. BBC, 13 jan. 2021. Disponível em: https://www.bbc.co.uk/news/technology-55625071. Acesso em: 18 jun. 2024.

[41] STARLINK. Business Aviation. Starlink, 2024. Disponível em: https://www.starlink.com/pt/business/aviation. Acesso em: 18 jun. 2024 e T-MOBILE. T-Mobile takes coverage above and beyond with SpaceX. T-Mobile Newsroom,25 ago. 2022. Disponível em: https://www.t-mobile.com/news/un-carrier/t-mobile-takes-coverage-above-and-beyond-with-spacex. Acesso em: 18 jun. 2024.

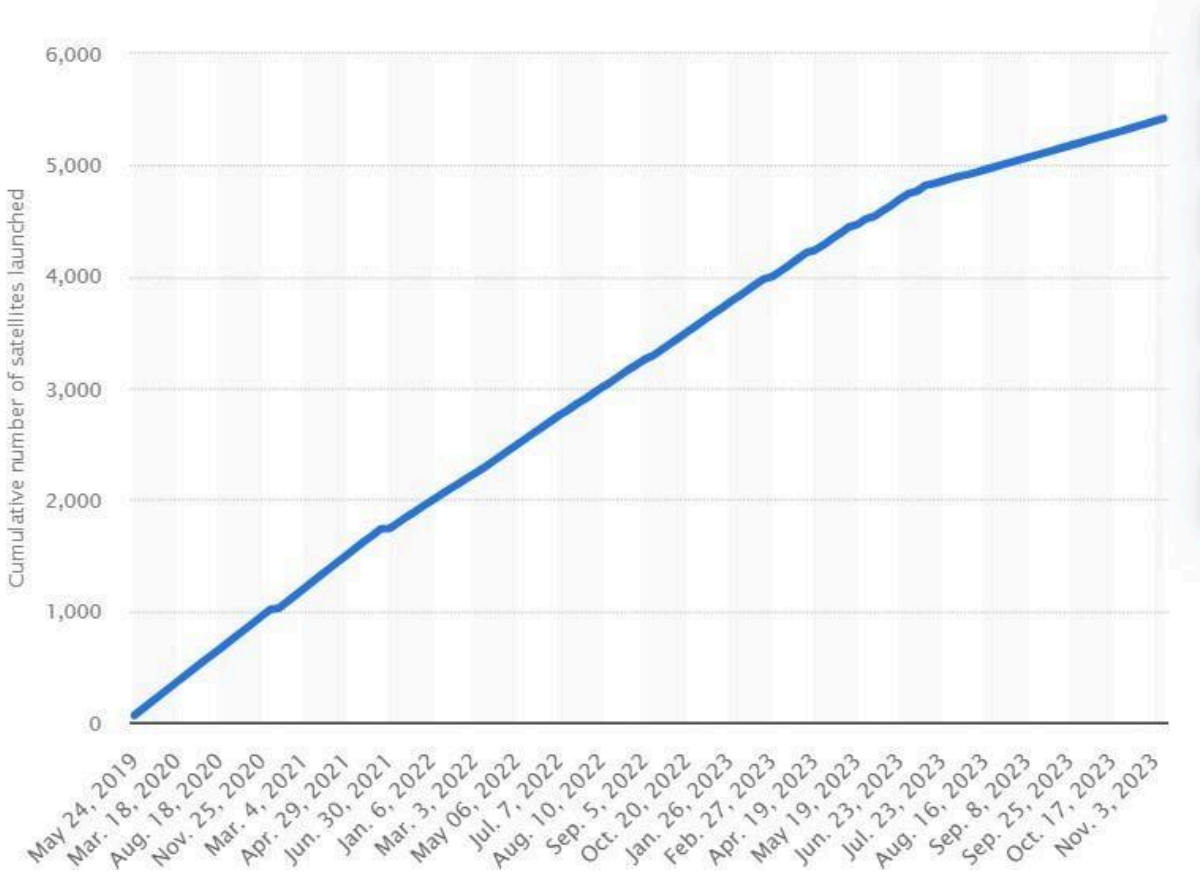
durante recorrentes verificações de testes e construção de *networking*, incentivando a Starlink a desenvolver capacidades para além dos usos civis (Cowhig, 2022). Diante desse cenário, outras empresas como Amazon (com seu Projeto Kuiper) e OneWeb, também estão desenvolvendo suas próprias constelações de satélites para competir no mercado de internet através do espaço.

4.2 Da constelação de satélites *Starlink*

A constelação de satélites da Starlink garante/entrega um serviço de acesso à internet banda larga que atua no mercado internacional desde outubro de 2020 (Cowhig, 2022). Desde sua proposta inicial, em 2015 até junho de 2024, a empresa reuniu mais de 4.300 veículos lançados no espaço, com o intuito contínuo de criação e aprimoramento desse sistema *on-line* de conexão, que envolve frequentes lançamentos e adição de novos equipamentos.[42] Conforme pode ser observado na Figura 4, essa constelação, segundo Cowhig (2022), é a rede de internet mais significativa, garantidora da maior cobertura global e responsável pelo maior número de satélites lançados em órbita atualmente. Desde 2019 até 2023 o crescimento nos lançamentos de veículos espaciais tem garantido à empresa filiada a Space X uma qualidade avançada em tecnologia da informação. Entre os anos de 2022 e 2023, período em que nota-se uma expansão contínua do serviço, é também quando as antenas são disponibilizadas para uso nos terminais de guerra e a elevada taxa de satélites em órbita torna-se urgente.

[42] STARLINK. SECOND GENERATION STARLINK SATELLITES. Disponível em: https://www.starlink.com/pt/updates. Acesso em: 18 jun. 2024. e STARLINK MAP. Starlink Map. Disponível em: https://www.starlinkmap.org/. Acesso em: 18 jun. 2024.

Figura 4- Número cumulativo de satélites lançados pela Starlink-SpaceX (maio 2019 a nov. 2023)



Fonte: Site Statista, 2023

No entanto, a *Starlink* não está sozinha no ciberespaço. De acordo com Burton, Papa e Wong (2022):

> Em maio de 2022, mais de 5.4000 satélites, de diversas origens encontram-se ativos em órbita, com um crescimento exponencial projetado pela indústria privada nos próximos anos. Esse ambiente cada vez mais "congestionado, disputado e competitivo" criou uma miríade de iniciativas internacionais, nacionais e privadas ao redor do mundo, dedicadas a promover e proteger seus interesses no espaço. Esse crescimento também aumentou significativamente a dependência global de dados, produtos e serviços espaciais, uma realidade que atores adversários estão ávidos para explorar. (Burton, Papa e Wong, 2022, p. 2).

Nota-se, portanto, que a intenção de aprimoramento de constelações de satélites não é uma prática desconhecida; pelo contrário, é incentivada também pelo âmbito governamental, para fins estratégicos de segurança entre os Estados. Um exemplo disso é a atuação

diplomática e política intergovernamental da OTAN, a qual declara que seus princípios e postulados-chave de Política Espacial Global estão alinhados para garantir o "livre acesso" ao espaço para "fins pacíficos", conforme estabelecido pelo Tratado do Espaço Exterior de 1967[43] e outras leis internacionais. Isso porque a organização considera a interoperabilidade sob as dimensões técnica, processual, humana e informacional fundamental para defender seus objetivos de "capacidade dos Aliados de atuarem juntos de maneira coerente, eficaz e eficiente para alcançar objetivos táticos, operacionais e estratégicos"[44]. No caso do conflito russo-ucraniano (2022), a *Starlink,* por exemplo, atua de forma direta como variável não-estatal constante (Manhães; Vilar-Lopes, 2022).

4.3 Uso do *Starlink* no Conflito

No caso da Guerra russo-ucraniana (2022), a *Starlink* desempenha um papel crucial ao oferecer serviços de comunicação de internet via satélite à Ucrânia logo após a sua invasão, visto que o país enfrentou interrupções significativas na sua infraestrutura. Poucos dias após o início do conflito, Mykhailo Fedorov, Ministro da Transformação Digital da Ucrânia, entrou em contato com Elon Musk pelo Twitter, solicitando que os serviços Starlink fossem fornecidos ao país para garantir uma comunicação estável para os civis e o governo, durante o conflito.[45] Dentro de 12 horas após o apelo de Fedorov, Musk respondeu na plataforma de mídia social dizendo que: "O serviço Starlink está agora ativo na Ucrânia". O pedido de Fedorov ocorreu em meio a apagões generalizados de internet no país, então a resposta eficiente provou ser vantajosa – levou apenas algumas horas para a SpaceX ativar o serviço e apenas dois dias para que novos terminais fossem enviados para a Ucrânia, aumentando e ampliando a conectividade na região (Belfer Center for Science and International Affairs, 2023). O espaço cibernético é, então, utilizado pela Ucrânia através do Starlink como componente estratégico de poder.

[43] NAÇÕES UNIDAS. Tratado sobre os Princípios que Regem as Atividades dos Estados na Exploração e Uso do Espaço Exterior, Incluindo a Lua e Outros Corpos Celestes. 1967. Disponível em: https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf. Acesso em: 18 jun. 2024.
[44] "Interoperability: Connecting Forces," NATO (website), updated February 22, 2022. Disponível em: https://www.nato.int/. Acesso em: 17 jun. 2024.
[45] Disponível em: https://x.com/FedorovMykhailo/status/1497543633293266944.

4.3.1 Usuários

Desde o início do conflito, em fevereiro de 2022 e o começo de junho do mesmo ano, mais de 15 mil kits do serviço *Starlink* foram disponibilizados para a Ucrânia com o intuito de manter a melhoria das capacidades de comando, controle, computadores, comunicações, inteligência, vigilância e reconhecimento (*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance - C4ISR*) (Manhães; Vilar-Lopes, 2022, p. 27) Isso porque, com a Starlink, é possível obter informações de localizações extremamente precisas e confiáveis para guiar dispositivos de inteligência militares, provendo serviço de rastreamento completo de vigilância com alcances terrestres, aéreos e marítimos (Cowhig, 2022).

No entanto, o uso do serviço ultrapassa a esfera estratégica, visto que desde a sua ativação, a *Starlink* tem sido usada tanto por civis quanto por militares. Em maio de 2022, mais de 150.000 ucranianos estavam usando o *Starlink* diariamente[46](Sheetz, 2022). Diante disso, o ministro da Transformação Digital da Ucrânia declarou publicamente que o Starlink "é um suporte crucial para a infraestrutura da Ucrânia e para a restauração dos territórios destruídos". Com a rápida integração da tecnologia na infraestrutura de comunicações do país, o exército de Kiev pode aplicá-la de forma criativa no campo de batalha, no controle de veículos aéreos não tripulados de vigilância, reconhecimento e combate (*drones*)[47] (The Economist, 2022).

4.3.2 Finalidades

Conforme o conflito no leste europeu avança, o envolvimento da SpaceX tornou-se mais complexo. Pois, para além dos objetivos militares e propósitos pacíficos pretendidos pela empresa, os interesses comerciais vieram à tona. No início de 2023, a SpaceX anunciou que limitaria o uso do Starlink para operações militares ofensivas pela Ucrânia, destacando as considerações éticas da tecnologia comercial na guerra (Belfer Center for Science and International Affairs, 2023). Com essa decisão, ficou explícito o equilíbrio que a SpaceX

[46] SHEETZ, Michael. About 150,000 People in Ukraine Are Using SpaceX's Starlink Internet Service Daily, Government Official Says. CNBC, 2 maio de 2022. Disponível em: https://www.cnbc.com/2022/05/02/ukraine-official-150000-using-spacexs-starlink-daily.html. Acesso em: 18 de jun. 2024.

[47] THE ECONOMIST. Ukrainian cities are suffering internet blackouts. The Economist Newspaper, 26 fev. 2022. Disponível em: https://www.economist.com/graphic-detail/2022/02/26/ukrainian-cities-are-suffering-internet-blackouts. Acesso em: 18 jun. 2024.

precisava manter entre fornecer apoio à Ucrânia e cumprir seus compromissos de mercado de "uso pacífico da tecnologia".

No início, a SpaceX ofereceu o serviço Starlink à Ucrânia com um custo reduzido, em um gesto aparentemente altruísta de Elon Musk. No entanto, em setembro de 2022, cerca de seis meses após a implantação do Starlink na Ucrânia, a empresa informou ao Pentágono que não poderia mais arcar com os custos[48] (Marquardt, 2022). Nesse mesmo comunicado, a SpaceX solicitou que o Departamento de Defesa dos EUA assumisse o financiamento do uso do Starlink pelo governo e pelas forças armadas ucranianas, o que, segundo a empresa, custaria mais de US$ 120 milhões apenas para o restante de 2022.[49] Manter a operação por mais 12 meses custaria quase US$ 400 milhões. Contudo, a SpaceX não estava arcando com a maior parte dos custos até então. De acordo com os dados fornecidos pela própria empresa, cerca de 85% dos terminais e 30% da conectividade de internet disponibilizados até aquele momento foram pagos pelos Estados Unidos (incluindo a USAID), Polônia e outros grupos.[50] A SpaceX, no entanto, queria que o governo dos EUA assumisse uma parte maior dessas despesas.

Embora os detalhes sobre um acordo entre os EUA e a SpaceX não tenham sido divulgados publicamente, o Starlink continua operando na Ucrânia. Cinco meses depois, em fevereiro de 2023, a SpaceX fez outra mudança significativa no uso do Starlink na guerra. Durante a Conferência de Transporte Espacial Comercial da Administração Federal de Aviação em Washington, DC, a empresa anunciou que limitaria o uso do Starlink pela Ucrânia para fins militares ofensivos[51] (FAA Commercial Space Transportation Conference, 2023). Gwynne Shotwell, presidente e diretora de operações da SpaceX, afirmou que a intenção da empresa "nunca foi permitir que [o exército ucraniano] usasse o Starlink para fins ofensivos"[52] (C4ISRNET, 2023). Ainda assim, permitiram o uso ofensivo da tecnologia por quase um ano sem objeções. Repentinamente, no aniversário de um ano da guerra, mudaram sua posição (Belfer Center for Science and International Affairs, 2023). Ainda não está claro como essa

[48] MARQUARDT, Alex. Exclusive: Musk's SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick up the Tab. CNN, 14 out. 2022. Disponível em: https://www.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html. Acesso em: 18 jun. 2024.
[49] *Ibid.*
[50] *Ibid.*
[51] FAA COMMERCIAL SPACE TRANSPORTATION CONFERENCE. SpaceRef. Disponível em: https://spaceref.com/event/faa-commercial-space-transportation-conference/. Acesso em: 18 jun. 2024.
[52] C4ISRNET. SpaceX's Shotwell says Ukraine 'weaponized' Starlink network. 8 fev. 2023. Disponível em: https://www.c4isrnet.com/battlefield-tech/space/2023/02/08/spacexs-shotwell-says-ukraine-weaponized-starlink-network/. Acesso em: 18 jun. 2024.

decisão afetará a performance das forças armadas ucranianas, mas é provável que traga consequências significativas.

É diante desse contexto que, em meados de fevereiro de 2024, surgem relatos e alegações de que terminais Starlink teriam sido encontrados em territórios controlados pela Rússia[53] (REUTERS, 2024). Embora a SpaceX e Elon Musk tenham negado o fornecimento da tecnologia para o país supracitado em resposta à carta endereçada pelo Congresso Nacional dos EUA[54] (Comitê de Supervisão dos Democratas, 2024). De acordo com autoridades de inteligência ucranianas, como Andriy Yusov, os "casos de uso dos dispositivos pelos ocupantes russos foram registrados. Isso está começando a assumir um caráter sistêmico"[55], sugerindo que as forças russas haviam adquirido e ativado ilegalmente terminais *Starlink* em certas áreas ocupadas pela Rússia no leste da Ucrânia. Diante disso, Elon Musk continua a negar, via rede social X, a existência de negócios com o governo russo e afirma a não atividade do serviço da Starlink em territórios controlados pela Rússia.[56] Fica explícito, portanto, como as variáveis comerciais podem impactar cenários políticos quando ambas se confundem/misturam. Pois sem o auxílio da Starlink a Ucrânia muito provavelmente não teria a mesma capacidade de resposta ao exército russo, quando o mesmo precisou também aderir a mesma tecnologia para adequar-se e seguir com o conflito.

No entanto, o que chama atenção no caso russo-ucraniano é como ambos os países se utilizam do meio digital pelo qual os objetivos de controle e vigilância são alcançados para fins militares. O *hardware power* adquire aqui novas roupagens e as diferenças entre ator privado *(Starlink)* e atores estatais (Rússia e Ucrânia) provoca uma difusão de poder típica do século XXI. O ponto principal consiste no impacto decisivo da atuação da *Starlink* na garantia das intenções políticas-estatais da Ucrânia e eventualmente da Rússia também.

[53]REUTERS. Russia using thousands of SpaceX Starlink terminals in Ukraine, WSJ says. 15 fev. 2024. Disponível em: https://www.reuters.com/world/europe/russia-using-thousands-spacex-starlink-terminals-ukraine-wsj-says-2024 - 02-15/. Acesso em: 14 jun. 2024.

[54]COMITÊ DE SUPERVISÃO DOS DEMOCRATAS. Ranking Member Raskin and Subcommittee Ranking Member Garcia launch investigation into Trump administration's secret scheme to transfer sensitive nuclear technology to Saudi Arabia. Disponível em: https://oversightdemocrats.house.gov/news/press-releases/ranking-member-raskin-and-subcommittee-ranking-member-garcia-launch. Acesso em: 18 jun. 2024.

[55] THE GUARDIAN. Ukraine accuses Russia forces of using Elon Musk's Starlink. 12 fev. 2024. Disponível em: https://www.theguardian.com/world/2024/feb/12/ukraine-accuses-russia-forces-using-elon-musk-starlink. Acesso em: 18 jun. 2024.

[56] https://x.com/elonmusk/status/1756758674087825879.

Considerações Finais

No entanto, o que chama atenção no caso russo-ucraniano é como ambos os países se utilizam do meio digital pelo qual os objetivos de controle e vigilância são alcançados para fins militares. O *hardware power* adquire aqui novas roupagens e o envolvimento entre ator privado *(Starlink)* e atores estatais (Rússia e Ucrânia) provoca uma difusão de poder típica do século XXI. O ponto principal analisado foi o impacto decisivo da atuação da *Starlink* na manutenção das atividades militares e políticas-estatais da Ucrânia, assim como, eventualmente, da Rússia também. Pois o uso estratégico do serviço no início da guerra foi garantia fundamental para a longínqua resistência ucraniana. Resgatando um expoente da escola inglesa, Wight (), esse é mais um momento em que as relações internacionais constituem-se em termo de política do poder, pois, em um movimento de reajuste ao conflito, a exércitos russos utilizam-se da nova tecnologia para ampliação de poder. E, até mesmo antes da Operação Militar Especial, a Rússia opera no ciberespaço ao empregar a Guerra Híbrida, confirmando, assim, o que Lipson (1967) apregoa sobre a aplicação de força "[...]no lugar e momento preciso pela existência permanente da necessidade de nos ajustarmos, individual e coletivamente, às invenções da tecnologia, à inovação social" (Lipson, 1967, p. 33).

Nota-se, portanto, que a guerra de *softwares* como intitula Vilar-Lopes (2016), tem impacto significativo no conflito, tanto na esfera militar quanto na civil, influenciando também as dimensões política, econômica e social (Ricque, 2022b). O *cyberpower, também* sistematizado por Vilar-Lopes, afirma-se, então, como componente fundamentalmente estratégica para a defesa de um país.

Documentos internacionais como o Manual Tallinn, no entanto, oferecem uma perspectiva mais nítida e aproximada de como o sistema internacional deve se adequar às novas tendências da era digital, porque, diante da esfera político-militar, a tomada de decisão impacta diretamente na segurança dos Estados e consequentemente, na sua capacidade de ação e nos limites da sua prospecção nacional.

Mas, de acordo com a análise do caso do envolvimento do *Starlink* no conflito russo ucraniano, a capacidade de alterar profundamente a cadeia de comunicação e do sistema informacional de conexão de tudo ao mesmo tempo em tempo real enriquece, energiza e revitaliza o mercado e o mundo digital. No entanto, o desempenho desse serviço em diferentes cenários concerne a segurança e a proteção dos Estados. A urgência do estudo e da análise sobre o acesso à informação no ciberespaço faz-se necessária, visto que, à medida que inovações no setor tecnológico militar avançam cada vez mais, poucas respostas sobre os

impactos do uso do ciberespaço ou as consequências no mundo real fora dele, ficam nítidas a ao fenômeno majoritariamente privado da exploração digital. Ademais, a participação de atores não-estatais com objetivos divergentes e variantes em conflitos internacionais e em guerras entre Estados é constante e interfere nos rumos de um conflito.

De acordo com Burton, Thompson, Papa e Wong (2022), "esse ambiente cada vez mais 'congestionado, contestado e competitivo' criou uma miríade de iniciativas internacionais, nacionais e de empresas privadas ao redor do mundo dedicadas a promover e proteger seus interesses no espaço.[57] Assim como esse crescimento também aumenta significativamente a dependência global de dados, produtos e serviços espaciais, em uma realidade que atores adversários estão ávidos para explorar.[58] No entanto, a miríade de iniciativas espaciais explora lacunas na governança espacial estabelecida e causa um aumento do medo de colisões entre satélites e da ameaça de atividades malignas.[59], pois, claramente, a atividade global no espaço exige normas de comportamento globalmente reconhecidas que contribuam ativamente para a segurança dos satélites de cada ator, ao mesmo tempo em que garantem a sustentabilidade a longo prazo do domínio espacial[60] (Burton;Papa; Wong, 2022, p. 36).

Sendo assim, convém destacar também o fato de que as inúmeras concessões e facilidades adquiridas através do sistema de domínio de patentes pelo governo dos EUA garantiu a expansão da atuação da empresa em questão. Em outras palavras, sem a interação do governo de uma nação soberana em financiar parte, senão todos, os custos para a manutenção do serviço, a SpaceX, especialmente Elon Musk, não conseguiria se posicionar como um herói de guerra. Ao mesmo tempo em que demonstrou poder e valor para seus produtos tecnológicos, evitou custos pesados e contínuos, gerando receita para uma de suas principais empresas. É então, dessa forma que o programa *Starlink* tem capacidade de instrumentalizar-se do ambiente aeroespacial e informacional para adequá-lo ao seu favor e

[57] UN General Assembly, First Committee, Outer Space Increasingly 'Congested, Contested and Competitive,' First Committee Told as Speakers Urge Legally Binding Document to Prevent Its Militarization, GA/DIS/3487 (October 25, 2013), (statement of Jeffrey L. Eberhardt). Disponível em: https://www.un.org/. Acesso em: 16 jun. 2024.

[58] Jonathan Beale, "Space, the Unseen Frontier in the War in Ukraine," BBC, October 6, 2022. Disponível em: https://www.bbc.com/; and Ashish Dangwal, "Sabotaging Starlink, Russia Is Using EW Complex 'Tirada' to Disrupt SpaceX Satellites Connecting Ukraine – Media," EurAsian Times, October 9, 2022. Disponível em: https://eurasiantimes .com/. Acesso em: 16 jun. 2024.

[59] Rajeswari Pillai Rajagpalan, "It Is Time for Space Governance Talks," Diplomat, May 21, 2020. Disponível em: https://thediplomat.com/. Acesso em: 14 jun. 2024

[60] Citação direta do autor: O pensamento convencional sobre como deter um inimigo de atacar em terra, por mar ou pelo ar não se aplica realmente ao espaço. Novas doutrinas e normas para o espaço precisam ser estabelecidas, principalmente por diplomatas (Burton; Papa; Wong, 2022, p.2).

realizar a missão que lhes é dada pelo seu cliente/comprador, seja ele quem for, bem como age de forma independente e imprevisível, sem o compromisso de atender ou obedecer às normativas, demandas e exigências político-estatais de um país soberano, o qual deve ser responsável pela manutenção da sua própria segurança.

REFERÊNCIAS

Aleprete, Jr., M.E., ‘Minimizing Loss: Explaining Russian Policy: Choices during the Ukrainian Crisis’, Soviet and Post-Soviet Review 44 (2017): 53-75.

BANDEIRA, Luiz Alberto Moniz. A desordem mundial: o espectro da total dominação: guerras por procuração, terror, caos e catástrofes humanitárias. Rio de Janeiro: Civilização Brasileira, 2016.

BERGER, Eric. Liftoff: Elon Musk and the Desperate Early Days That Launched SpaceX. Nova Iorque: William Morrow, 2021.

BESSA, Jorge. O escândalo da espionagem no Brasil: o caso Snowden. Brasília: Thesaurus, 2014.

Belfer Center for Science and International Affairs. Starlink and the Russia-Ukraine War: The Case of Commercial Technology and Public Purpose. Disponível em: https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-te c hnology-and-public-purpose. Acesso em: 18 de Junho de 2024.

BELLAMY, Christopher. What is information warfare?. In: MATTHEWS, Ron; TREDDENICK, John. Managing the Revolution in Military Affairs. Nova York: Palgrave, 2001. p. 56-75.

BOUWMEESTER, A.J.H. The art of Deception revisited (part 2): the unexpected annexation of Crimea in 2014. Militaire Spectator, Out., 2021. Disponível em: https://militairespectator.nl/artikelen/art-deception-revisited-part-2-unexpected-annexationcri mea-2014. Acesso em: 16 de Junho de 2024.

BULL, Hedley. A sociedade anárquica: um estudo da ordem na política mundial. Tradução de: Sergio Bath. Brasília: Editora UnB; IPRI; São Paulo: Imprensa Oficial de São Paulo, 2002. (Clássicos IPRI, 5).

BURTON, John; THOMPSON, Domenic; PAPA, Alessandro; WONG, Arthur. International Space Strategy: International Space Collaboration and Security - A NATO Perspective.
ÆTHER: A Journal of Strategic Airpower & Spacepower, 2022.

CENTRO DE EXCELÊNCIA DE DEFESA CIBERNÉTICA DA OTAN (CCDCOE). Tallinn Manual. Disponível em: https://ccdcoe.org/research/tallinn-manual/. Acesso em: 18 Junho 2024.

CLAUSEWITZ, Carl von. Da guerra. São Paulo: Tahyu, 2005.

CLARKE, Richard A.; KNAKE, Robert K. Cyber war: the next threat to national security and what to do about it. 2. ed. New York: HarperCollins, 2012.

COMITÊ DE SUPERVISÃO DOS DEMOCRATAS. Ranking Member Raskin and Subcommittee Ranking Member Garcia launch investigation into Trump administration's secret scheme to transfer sensitive nuclear technology to Saudi Arabia. Disponível em: https://oversightdemocrats.house.gov/news/press-releases/ranking-member-raskin-and-subcommittee-ranking-member-garcia-launch. Acesso em: 18 Junho 2024.

COWHIG, D. PRC Defense: Starlink Countermeasures. David Cowhig's Translation Blog, de 25 de maio de 2022. Disponível em: https://gaodawei.wordpress.com/2022/05/25/prc-defensestarlink-countermeasures. Acesso em: 20 abril 2023.

CISA - CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. *IR-ALERT-H-16-056-01: Malware Targeting Industrial Control Systems (ICS)*. Disponível em: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. Acesso em: 16 de junho de 2024.

DUARTE, Érico. Conduta da guerra na era digital e suas implicações para o Brasil: uma análise de conceitos, políticas e práticas de defesa. Brasília: IPEA, 2012.

DUFFIELD, Mark; DONINI, Antonio. Global Governance and the New Wars - The Merging of Development Security. New York: Zed Book, 2014.

FOLEY, Emmet; KAUNERT, Christian. Russian Private Military and Ukraine: Hybrid Surrogate Warfare and Russian State Policy by Other Means. Central European Journal of International and Security Studies, vol. 16, 2022, pp. 172-192.

FORTES, Denis Matoszko. A Federação Russa e a Crise Ucraniana de 2013-2014: entre o jogo das potências e as disputas históricas no ⁝exterior próximo⁝. 2017. 94 f. Dissertação (Mestrado) - Curso de Relações Internacionais, Instituto de Filosofia e Ciências Humanas, Universidade Estadual de Campinas, Campinas, 2017. Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/330639/1/Fortes_DenisMatoszko_M.pdf .

FREEDMAN, Lawrence. Ukraine and the Art of Strategy. Oxford University Press: Inglaterra, 2019.

GALEOTTI, Mark. Armies of Russia's War in Ukraine. Osprey Publishing: Oxford, 2019.

GARDNER, John. The Conflict in Ukraine: From Civil Strife to Proxy War. Cambridge: Cambridge University Press, 2015.

GIBSON, William. Neuromancer. Tradução de: Fábio Fernandes. São Paulo: Aleph, 2014. Edição especial de 30 anos.

GREENBERG, Andy. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Doubleday, 2019.

HILDEBRANDT, Mireille. Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace. University of Toronto Law Journal, [S.l.], v. 63, n. 2, p. 196-224, 2013.

HOUSE OF COMMONS LIBRARY, Conflict in Ukraine: A timeline (2014 - eve of 2022 invasion). London: House Of Commons Library, 2023. Disponível em: https://commonslibrary.parliament.uk/research-briefings/cbp-9476/. Acesso em: 16 de junho de 2024.

Institute for the Study of War (ed.), 'Ukraine invasion update 24', 22 April 2022 Disponível em: https://www.understandingwar.org/backgrounder/ukraine-invasion-update-24. Acesso em: 16 de junho de 2024.

KOSIUK, Alona. The invisible hand of Russia. The Kootneet, nov.,2020. Disponível em: https://thekootneeti.in/2020/11/26/the-invisible-hand-of-russia/. Acesso em: 17 de Junho de 2024.

KOTOULAS, Ioannis E.; PUSZTAI, Wolfgang. Geopolitics of the War in Ukraine. Report No. 4. June 2022. Foreign Affairs Institute. Athens: University of Athens, 2022.

KUEHL, Daniel T. From cyberspace to cyberpower: defining the problem. Washington, DC: National Defense University, 2009.

LANGNER, Ralph. Stuxnet: dissecting a cyberwarfare weapon. Journal of Computer Virology and Hacking Techniques, v. 7, n. 1, p. 41-52, mar. 2011.

LIBICKI, Martin C. Cyberdeterrence and cyberwar. Santa Monica, CA: Rand Corporation, 2009.
LIPSON, Leslie. Os grandes problemas da Ciência Política. Rio de Janeiro: Zahar, 1967.
LOBATO, Luisa Cruz; KENKEL, Kai Michael. Discourses of cyberspace securitization in
Brazil and in the United States. Revista Brasileira de Política Internacional, Brasília, v. 58, n. 2, p. 23-43, 2015.

VILAR-LOPES, Gills. **Relações Internacionais Cibernéticas (CiberRI)**: uma defesa acadêmica à luz dos Estudos de Segurança Internacional. Tese (Doutorado em Ciência Política) – Universidade Federal de Pernambuco, Recife, 2016.

MACFARQUHAR, Neil for THE NEW YORK TIMES. Russia Opens Bridge to Crimea, Cementing Control. *The New York Times*, 15 de maio de 2018. Disponível em: https://www.nytimes.com/2018/05/15/world/europe/russia-crimea-bridge.html. Acesso em: 17 jun. 2024.

MANHÃES, A.; VILAR-LOPES, G. Programa Starlink na Guerra Russo-Ucraniana. Revista da UNIFA, Rio de Janeiro, v. 35, n. 2, 2022. DOI: 10.22480/revuinfa.%y.v35.500. Disponível em: https://revistaeletronica.fab.mil.br/index.php/reunifa/article/view/500. Acesso em: 5 julho 2023.

MEDICOS, B. P., Carvalho, A. C., & Goldoni, L. R. F. (2019). Uma análise sobre o processo de securitização do ciberespaço. Coleção Meira Mattos. https://doi.org/10.22491/CMM.A003

MEGALE, Januário F. Expressões latinas usadas nos clássicos de ciências sociais e em textos acadêmicos. In:_. Introdução às ciências sociais. 2. ed. São Paulo: Atlas, 1990. p. 200-208.

MORGENTHAU, Hans J. A política entre as nações: a luta pelo poder e pela paz. Tradução de: Oswaldo Biato. Brasília: Editora UnB; IPRI; São Paulo: Imprensa Oficial do Estado, 2003. (Clássicos IPRI).

NAKASHIMA, Ellen. How a Secretive U.S. Agency Discovered the Truth About Russia's Role in the NotPetya Cyberattack. The Washington Post, 12 de dezembro de 2017. Disponível em: https://www.washingtonpost.com/world/national-security/how-a-secretive-us-agency-discover ed-the-truth-about-russias-role-in-the-notpetya-cyberattack/2017/12/12/f95a0eac-db63-11e7-a841-2066faf731ef_story.html. Acesso em: 17 de junho de 2024.

NYE, Joseph S. O futuro do poder. São Paulo: Benvirá, 2012._____. The future of power. New York: Public Affairs, 2011b. cap. 5.

O'CALLAGHAN, Jonathan. SpaceX reveals monthly cost of Starlink internet in its 'Better Than Nothing' beta—but is it too expensive? Forbes, 27 out. 2020. Disponível em: https://www.forbes.com/sites/jonathanocallaghan/2020/10/27/spacex-reveals-monthly-cost-of -starlink-internet-in-its-better-than-nothing-betabut-is-it-too-expensive/. Acesso em: 18 jun. 2024.

PERON, Alcides E. dos Reis. Guerra virtual e eliminação da fricção? O uso da cibernética em operações de contrainsurgência pelos EUA. In: OLIVEIRA, Marcos A. Guedes de; GAMA NETO, Ricardo B.; VILAR LOPES, Gills (Org.). Relações Internacionais Cibernéticas (CiberRI): oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: Ed. UFPE, 2016. p. 109-132. (Defesa & Fronteiras Virtuais, 3).

PERVEZ, F. Blackwater: Can't Stop, Won't Stop. Foreign Policy In Focus, 2010. Disponível em: https://ips-dc.org/blackwater_cant_stop_wont_stop/. Acesso em: 25 de Julho de 2023.

PIFER, S., 'Russia's draft agreements with NATO and the United States: Intended for rejection?', Brookings, 21 December 2021. Disponível em: https://www.brookings.edu/blog/order-from-chaos/2021/12/21/russias-draftagreements-with-n ato-and-the-united-states-intended-for-rejection/. Acesso em: 17 de junho de 2024.

Pisciotta, B., 'Russian revisionism in the Putin era: An overview of post-communist military interventions in Georgia, Ukraine, and Syria', Italian Political Science Review 50:1 (2020), 87-106.

PORTELA, Lucas S. Agenda de pesquisa sobre o espaço cibernético nas Relações Internacionais. Revista Brasileira de Estudos de Defesa, v. 3, n. 1, p. 91-113, jan./jun. 2016. Disponível em: http://seer.ufrgs.br/index.php/rbed/article/view/62071. Acesso em: 16 de junho de 2024.

PROENÇA JR, Domício; DINIZ, Eugenio. Política de Defesa no Brasil: uma análise crítica. Brasília: Humanidade; Editora UnB, 1998.

RICQUE, E. Elon Musk porte secours à l'Ukraine par le biais de Starlink. Tom's Guide, de 27 fev. 2022a. Disponível em: https://www.tomsguide.fr/elon-musk-porte-secours-a-lukraine-par-le-biaisde-starlink. Acesso em: 17 de Junho de 2024.

SCHMITT, Michael N. (Ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO
Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press, 2013.

SHEETZ, Michael. "About 150,000 People in Ukraine Are Using SpaceX's Starlink Internet Service Daily, Government Official Says." CNBC. CNBC, May 2, 2022. Disponível em: https://www.cnbc.com/2022/05/02/ukraine-official-150000-using-spacexs-starlink-daily.html . Acesso em: 18 Junho 2024.

SINGER, P.W. Corporate Warriors: The Rise of the Privatized Military Industry. Cornell University Press, 2003.

STATISTA. Number of Starlink satellites launched from May 2019 to November 2023. Disponível em: https://www.statista.com/statistics/1224164/starlink-satellite-launches/. Acesso em: 18 Junho 2024.

TEDESCHI, P.; SCIANCALEPORE, S.; PIETRO, R. Satellite-Based Communications Security: A Survey of Threats, Solutions, and Research Challenges.
THE GUARDIAN. Ukraine accuses Russia forces of using Elon Musk's Starlink. 12 fev. 2024. Disponível em: https://www.theguardian.com/world/2024/feb/12/ukraine-accuses-russia-forces-using-elon-m usk-starlink. Acesso em: 18 de Junho de 2024.

VALENTE, Leonardo. Política externa na era da informação: o novo jogo do poder, as novas diplomacias e a mídia como instrumentos de Estado nas relações internacionais. Rio de
Janeiro: Revan; UFF, 2007.

VANCE, Ashlee. Elon Musk: Tesla, SpaceX, and the quest for a fantastic future. Nova York: HarperCollins, 2015.

ZETTER, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown, 2014.