UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO DE CIÊNCIAS ECONÔMICAS

DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS

Caio Felipe Carvalho Murata

O Novo Paradigma de Ciber-Securitização da Ucrânia: Um Estudo sobre os Desafios Cibernéticos Atuais

Florianópolis

2022

Caio Felipe Carvalho Murata

O Novo Paradigma de Ciber-Securitização da Ucrânia: Um Estudo sobre os Desafios Cibernéticos Atuais

Trabalho de Conclusão do Curso de Graduação em Relações Internacionais do Centro Socioeconômico da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Relações Internacionais.
Orientadora: Prof.ª Dra. Graciela de Conti Pagliari

Florianópolis

2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Murata, Caio Felipe Carvalho Murata
O Novo Paradigma de Ciber-Securitização da Ucrânia : Um Estudo sobre os Desafios Cibernéticos Atuais / Caio Felipe Carvalho Murata Murata ; orientador, Graciela de Conti Pagliari, 2022.
92 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Sócio Econômico, Graduação em Relações Internacionais, Florianópolis, 2022.

Inclui referências.

1. Relações Internacionais. 2. Cibersegurança. 3. Relações Internacionais. 4. Ucrânia. 5. Resposta-Estratégica. I. de Conti Pagliari, Graciela. II. Universidade Federal de Santa Catarina. Graduação em Relações Internacionais. III. Título.

Caio Felipe Carvalho Murata

Ciber-Securitização na Ucrânia: O Novo Paradigma de Segurança - Um Estudo sobre os Desafios Atuais

Florianópolis, XX de novembro de 2022.

O presente Trabalho de Conclusão de Curso foi avaliado e aprovado pela banca examinadora composta pelos seguintes membros:

_____

Prof. Dra. Danielle Jacon Ayres, Dr.

Universidade Federal de Santa Catarina

_____

Prof. Dra. Jessica Maria Grassi

Universidade Federal de Santa Catarina

Certifico que esta é a versão **original e fina**l do Trabalho de Conclusão de Curso que foi julgado adequado para obtenção do título de Bacharel em Relações Internacionais por mim e pelos demais membros da banca examinadora

Documento assinado digitalmente
Graciela de Conti Pagliari
Data: 17/12/2022 07:51:30-0300
CPF: ***.263.070-**
Verifique as assinaturas em https://v.ufsc.br

_____

Prof. Dra. Graciela de Conti Pagliari, Dr.

Orientadora

Florianópolis, 2022

RESUMO

O campo cibernético tem ganhado cada vez mais destaque no espaço político internacional, sendo usado nos últimos anos como complemento tático às operações bélicas. Esse fenômeno foi registrado amplamente durante a ocupação russa da Crimeia no ano de 2014. Desde então, no entanto, a legislação securitária ucraniana passou por diversas readequações. Esta monografia tem como objetivo analisar as mudanças ocorridas a nível de segurança cibernética na Ucrânia, e como o país tem lidado com os desafios cibernéticos recentes. Inicialmente, buscou-se definir alguns dos entendimentos mais comuns do campo cibernético, para depois destacar o histórico geopolítico com a vizinha Rússia, e a importância da OTAN e da UE no processo de formulação das novas diretrizes cibernéticas do país. O trabalho tem um caráter metodológico exploratório, dada a revisão dos documentos de cibersegurança ucranianos e de sua respectiva capacidade de defesa. Conclui-se que, apesar da crescente relevância do campo cibernético como ferramenta estratégica nas operações bélicas, o seu uso ainda é muito limitado, e pode-se atribuir grande parte do insucesso das operações russas às mudanças e atualizações sofridas no seio da ciberdefesa ucraniana.

Palavras-chave: Ciberdefesa, Ameaças Cibernéticas, Ucrânia.

ABSTRACT

The cyber field has gained increasing prominence in the international political space, being used in recent years as a tactical complement to war operations. This phenomenon was widely recorded during the Russian occupation of Crimea in 2014. Since then, however, Ukrainian security legislation has undergone several readjustments. This bachelor thesis aims to analyze the changes that have taken place in terms of cybersecurity in Ukraine, and how the country has dealt with recent cyber challenges. Initially, an effort was made to define some of the most common understandings in the cyber field, to then highlight the geopolitical history with neighboring Russia, and the importance of NATO and the EU in the process of formulating the country's new cyber guidelines. The work has an exploratory methodological character, given the review of Ukrainian cybersecurity documents and their respective defense capabilities. It is concluded that, despite the growing relevance of the cyber field as a strategic tool in war operations, its use is still very limited, and a large part of the failure of Russian operations can be attributed to the changes and updates suffered within the Ukrainian cyber defense field.

Keywords: Cyberdefense, Cyber Threats, Ukraine.

LISTA DE FIGURAS

LISTA DE QUADROS (TABELAS)

LISTA DE ABREVIATURAS E SIGLAS

ANP - Programas Nacionais Anuais

CAIP - Centro de Proteção de Informações de Antivírus

CEC - Comissão Eleitoral Central

CERT - Equipe de Resposta a Emergências de Computadores

CNDS - Conselho Nacional de Segurança e Defesa da Ucrânia

CSIRT1 - Equipe de Resposta a Incidentes de Segurança Informática

CWIX - Coalition Warrior Interoperability Exercise

DDoS - Ataque de negação de serviço

DEEP - Programa de Aprimoramento da Educação em Defesa

EUAM - Missão Consultiva da UE na Ucrânia

ISIS - Estado Islâmico

NIS - Diretiva de Segurança da Informação de Rede da UE

NUC - Comissão OTAN-Ucrânia

OTAN - Organização do Tratado do Atlântico Norte

SPS - Programa de Cooperação Científica para a Paz e Segurança

SSSCIP - Serviço Estadual de Comunicações e Informações Especiais

SSU - Setor de Segurança e Defesa da Ucrânia

TAIEX - Instrumento de Assistência Técnica e Intercâmbio de Informações da Comissão Europeia

UE - União Europeia

SUMÁRIO

1 INTRODUÇÃO

O campo cibernético é um elemento relativamente novo dentro das discussões das Relações Internacionais. E ainda falta consenso quanto ao alcance e efetividade das operações cibernéticas. No entanto, é indiscutível que este domínio de operações tem-se politizado cada vez mais, e que tem servido de importante meio para a realização da política no mundo moderno. A Ucrânia não tem escapado desta lógica, e tem buscado atualizar suas políticas cibernéticas, para fazer frente à realidade geopolítica enfrentada pelo país.

Com a eclosão do conflito entre a Rússia e a Ucrânia, à ocasião da invasão da Crimeia, elevou-se a tensão cibernética entre os dois países a um nível jamais visto - aumentando as ameaças e os impactos em outras áreas. Esta guerra, portanto, tem reforçado a importância deste campo não só na Ucrânia, mas também em diversos países. Portanto, estudar o histórico de evolução do campo cibernético ucraniano é de extrema importância para entendermos os possíveis impactos dos conflitos cibernéticos atuais e futuros.

Este estudo tem como objetivo central analisar, dentro do contexto de segurança nacional na Ucrânia, a postura ucraniana frente à segurança cibernética, através da análise de documentos oficiais que estabelecem relações supranacionais, e também através da análise das capacidades de segurança cibernética atuais. Para tal, faz-se importante uma análise prévia do contexto recentes de escalada de tensão com a Rússia e as novas ameaças sofridas pelo país, bem como a influência direta da OTAN e UE na formulação de novas políticas.

A pergunta a ser feita inicialmente é se de fato o contexto geopolítico no qual se insere a Ucrânia tem servido como propulsor do processo de ciber-securitização do país nos últimos anos. Buscar-se-á também verificar se as agressões e ameaças externas, sobretudo russas, têm servido como propulsoras dos esforços em construir uma estrutura de segurança cibernética mais eficiente.

Primeiramente, será necessário elucidar em que consistem tais ameaças e por que a Rússia tem desempenhado um papel central no processo de evolução deste campo nas políticas estratégicas do país. A problemática a ser abordada aqui se centra em responder

quais são as estratégias adotadas pela Ucrânia. Posteriormente, buscar-se-á explorar se tais políticas securitárias têm atendido às expectativas dos setores de segurança.

Este trabalho divide-se em três capítulos. O primeiro explorará possíveis definições dentro do campo cibernético, que servirão como guia semântico posteriormente. Também busca-se mostrar o posicionamento histórico da Rússia frente à Ucrânia, destacando o pequeno protagonismo (até o momento) das operações cibernéticas, frente, por exemplo, aos esforços cinéticos. Este capítulo também abordará os diferentes desafios à soberania estatal resultantes de um protagonismo crescente do campo cibernético na política.

O capítulo seguinte se dedica a analisar a evolução do jovem campo cibernético ucraniano e de que maneira o país tem tomado proveito das relações com a OTAN e com a UE para desenvolver esforços securitários técnicos conjuntos e para atualizar suas políticas regulatórias no campo cibernético aos moldes dos principais atores destas instituições.

Por fim, o capítulo final procurou expor as ameaças cibernéticas atuais e quais têm sido as respostas estratégicas adotadas pelo país. Para tal fim, foi importante identificar os principais atores dentro deste campo estratégico e as respectivas legislações cibernéticas atuais que os respaldam.

A metodologia aplicada neste projeto de pesquisa tem um caráter exploratório e uma abordagem hipotético-dedutiva, dada a revisão extensiva das ferramentas de defesa cibernéticas ucranianas. Em essência, este trabalho buscou fazer uma análise qualitativa de como a Ucrânia tem abordado e reagido às ameaças e ataques cibernéticos recentes.

2 O UNIVERSO CIBERNÉTICO: PONDERAÇÕES SOBRE O CASO UCRANIANO

O presente capítulo tem como objetivo explorar definições presentes no meio cibernético, que posteriormente serão aplicadas ao caso ucraniano. A análise destas definições aporta uma base sintática que permite uma análise mais detalhada da evolução do campo cibernético na Ucrânia.

O capítulo se divide em 4 subseções, começando pela busca de uma possível definição para o meio cibernético. Em seguida, buscou-se analisar a configuração atual dos conflitos cibernéticos, dos novos desafios e das agendas de segurança, incluindo a crise na ideia clássica de soberania, e por fim, abordou-se o papel do cibernético na guerra moderna, neste caso analisando-se especificamente o caso da Ucrânia.

2.1 DEFININDO O MEIO "CIBERNÉTICO" NO CONTEXTO DAS RELAÇÕES INTERNACIONAIS

O século XXI vem sendo marcado pela consolidação e afirmação do campo cibernético como um importante espaço de ação. O termo "cibernético", por sua vez, pode-se aplicar a diversos contextos dentro das relações internacionais. Em essência, refere-se ao mundo digital, regulado por meio dos hardware e software. Ou seja, assume um caráter dual, entre a sua parte material e imaterial. Contudo, há divergências quanto à aplicação do termo. Por isso, é importante explorá-las para se chegar a uma definição aplicável ao momento atual e que sirva de base para explorar possíveis soluções.

Alguns autores o definem como um novo domínio das Relações Internacionais - ou seja, como sendo o quinto domínio estratégico (KUEHL, 2009; SHELDON, 2011 apud. MEDEIROS; GOLDONI, 2020). Em 2010, The Economist declarou que "a guerra entrou no quinto domínio: o ciberespaço". Em 2011, o Departamento de Defesa dos EUA incorporou oficialmente o novo domínio em seu planejamento nas áreas de segurança, doutrina, recursos e operações. A OTAN, por sua vez, reconheceu o ciberespaço como um domínio operacional

em 2016 (SEEBECK, 2019). A análise dos documentos de diferentes agências nacionais de defesa e instituições de segurança de diferentes países são importantes para melhor entender o tema, porque estão na vanguarda das atualizações semânticas pelas quais passa o campo cibernético.

No campo acadêmico, não são poucos os esforços no sentido de tentar definir o campo cibernético, ou "ciberespaço". Ventre (2013) o enxerga como um domínio que perpassa os demais, dado o seu caráter configurativo dual - é composto de uma camada física de dispositivos tecnológicos, intitulada "hardware", e uma camada imaterial, que neste caso é o universo digital, "software", manipulada pelos usuários da rede e por suas ações cognitivas, chamado aqui de "peopleware". É na camada cognitiva dos usuários que o ciberespaço se socializa, perdendo seu caráter puramente mecânico, e podendo assumir o papel de moldador de relações de poder (MEDEIROS; GOLDONI, 2020).

A fins de análise, considerar-se-á o termo "ciberespaço" como locus em que as atividades cibernéticas acontecem. Medeiros (2020) aponta que esse conceito passou a ser essencial ao entendimento de parte das problemáticas exploradas pelas agendas nacionais de segurança. De acordo com o Dicionário de Termos Militares e Associados:

> Consiste em uma rede interdependente de infraestruturas de tecnologia da informação e dados, incluindo a Internet, redes de telecomunicações, sistemas de computadores, processadores e controladores incorporados (DOD, s.d., apud. MEDEIROS; GOLDONI, 2020, p. 34, tradução própria).

Alguns autores bastante conhecidos no campo das Relações Internacionais também tentam definir este novo campo de atuação. A definição de ciberespaço de Nye (2011) explorada por Valeriano e Maness (2018) é útil para a análise política que posteriormente será explorada:

> O domínio cibernético inclui a Internet de todos os computadores em rede, mas também intranets, tecnologias celulares, cabos de fibra óptica e comunicações espaciais. O ciberespaço tem uma camada de infraestrutura física que segue as leis econômicas dos recursos rivais e as leis políticas de justificação e controle soberano. (NYE apud. VALERIANO & MANESS, 2018, p. 261, tradução própria).

É fundamental pontuar também que se trata de um domínio moldado pela experiência dos usuários - intitulados de 'peopleware' por Ventre (2013) - e pelos avanços tecnológicos. Portanto, é válido dizer que o ciberespaço está em constante mudança, e revisões esporádicas da definição que se lhe outorga são extremamente necessárias (VENTRE, 2013, apud. MEDEIROS; GOLDONI, 2020). Kuhn (2018) também defende que "o desenvolvimento

social e tecnológico pressupõe desafios constantes à manutenção ou derrocada dos paradigmas existentes, chegando a um ponto em que a ciência em seu status quo não consegue mais explicar certas transformações sociais e tecnológicas, exigindo o desenvolvimento de novos paradigmas científicos" (apud. MEDEIROS; GOLDONI, 2020, p. 32, tradução própria).

Por se tratar de um espaço de exercício de poder, é impossível dissociá-lo da política e, portanto, do Estado. É importante destacar aqui a diferença entre os termos "ciberespaço" e "poder cibernético". O primeiro se refere ao domínio através do qual as operações cibernéticas se processam. O poder cibernético, por sua vez, faz alusão à soma dos efeitos estratégicos gerados pelas operações cibernéticas que fazem parte do ciberespaço. Tais efeitos podem ser sentidos não só a nível cibernético, mas também nos demais domínios, sejam eles "terra, mar, ar ou espacial" (SHELDON apud. MEDEIROS; GOLDONI, 2020).

Também é certo que os diversos centros de segurança de diferentes países têm servido como importantes expoentes no processo de consolidação de uma definição mais ampla - como é o caso de potências cibernéticas, como EUA e Rússia, que progressivamente vêm buscando alocar este novo campo de atuação dentro de suas agendas de segurança, passando a enxergá-lo como essencial à manutenção da estabilidade e da segurança internas. Termos como "guerra de informação" ou "terrorismo cibernético" também têm sido moedas comum em documentos de políticas, projetos de defesa e doutrinas de segurança do início do século XXI, bem como a crescente ênfase na segurança informacional e nas ameaças cibernéticas (ERIKSSON; GIACOMELO, 2016).

Os principais estados também se aproveitam do poder cibernético para aprimorar as capacidades em outras áreas, e costumam usá-lo como uma ferramenta importante para alcançar este fim. Estados como Rússia, China e Estados Unidos, são o que se pode chamar de "pesos-pesados do campo cibernético". Como pontuado por Nye, são os estados que continuam tendo vantagens em termos de exercício de poder dentro deste campo, isto porque são detentores de grande parte dos elementos da camada material, ou física, do ciberespaço (infraestruturas, que incluem satélites, equipamentos, cabos submarinos, servidores, entre outros), o que por sua vez contribui para que continuem a manter um relativo monopólio da violência, neste caso, digital (NYE, 2011, apud. VALERIANO; MANESS, 2018).

Embora outros atores ou grupos como o Estado Islâmico (ISIS) ou Anonymous sejam capazes de alavancar capacidades cibernéticas, continuam tendo uma capacidade limitada de

demonstrar poder (LINDSAY, 2013, apud. VALERIANO; MANESS, 2018). No entanto, atores secundários começam a emergir e ameaçam estreitar a lacuna de capacidade de exercício de poder na camada virtual - vemos cada vez mais a emergência de outros atores, como é caso de estados mais vulneráveis (o caso da Estônia é destacável), dissidentes, separatistas, terroristas, ativistas, alguns militares, e no caso da Ucrânia, a atuação de hacktivistas (MEDEIROS; GOLDONI , 2020).

Devido a sua onipresença e aos baixos custos de empregabilidade do ciberespaço, foi possível diminuir a lacuna de capacidades entre esses diferentes atores e os entes estatais. Nye (2012) refere-se a esse fenômeno como “difusão de poder, representada por um grande número de atores envolvidos e pela relativa redução dos diferenciais de poder entre eles” o autor acrescenta:

> Devido à diminuição dos custos de acesso e operação no ciberespaço, o domínio cibernético passou a ser considerado um locus de relações de poder onde múltiplos atores podem perseguir seus próprios interesses, especialmente devido à assimetria do ciberespaço, em que quanto mais sofisticada é uma infraestrutura estatal, mais vulnerável a ataques cibernéticos (NYE, 2012, apud. MEDEIROS: GOLDONI, 2018, p. 42, tradução própria).

Apesar das facilidades e da difusão oferecidas pelo ciberespaço, ainda não há um consenso sobre a sua real efetividade. Principalmente porque o advento da internet trouxe consigo altas expectativas quanto ao universo cibernético, levando alguns teóricos a conclusões precipitadas acerca da sua aplicabilidade bélica. Maschmeyer (2021) aponta que nos anos 1990 - década em que se populariza o chamado World Wide Web - alguns autores já teorizavam sobre o possível domínio da informação como recurso bélico. Porém, hoje questiona-se até que ponto o domínio informacional propiciado pelas redes informáticas é eficiente em combate.

2.2 DEFININDO OS CONFLITOS E AMEAÇAS CIBERNÉTICOS

Os ataques cibernéticos e a guerra cibernética são muitas vezes colocados como fenômenos independentes e distintos das dinâmicas clássicas que definem um conflito, circunscrito apenas à esfera imaterial. No entanto, analisando-se a postura de diferentes teóricos sobre o assunto, parece que tal simplificação é imprecisa e que esses ataques não podem ser dissociados dos contextos políticos em que se inserem - isso porque os governantes

cada vez mais demonstram usar o domínio cibernético como um instrumento de política, servindo como complemento às forças cinéticas e como ferramenta coercitiva em tempos de conflito (WEEDON, 2015).

No caso da Ucrânia, tentativas de classificar as ameaças cibernéticas dividem opiniões sobre se o que está acontecendo dentro e ao redor do país pode ou deve ser chamado de guerra cibernética. Como argumenta Jan Stinissen (2015), as operações cibernéticas atuais não atendem a uma definição legal estrita de estado de guerra. Mas, ao mesmo tempo, de acordo com outras análises, as operações na Ucrânia sem dúvida constituem guerra cibernética. O conflito:

> (...) atende ao padrão geralmente aceito pelas seguintes razões: o componente de guerra cibernética é explícito, o que significa que os perpetradores fazem pouco esforço para esconder suas identidades e lealdades. Os dois países estão em conflito aberto, hostil e declarado um com o outro. Ambos os lados declararam objetivos militares e políticos (GILES, 2015, p. 23, tradução própria).

No entanto, termos usados com frequência como “ciberguerra” e “cyberattack”, não são aplicados de maneira consensual pelos autores que exploram o tema. O termo “ciberguerra”, por exemplo, deve ser usado corretamente, como aponta Rid (2013), isto porque “guerra” como termo implica a presença de violência e letalidade para alcançar fins políticos. Guerra sem violência e morte não é guerra (VALERIANO & MANESS, 2018). Segundo Rid ,

> ‘A guerra é um ato de força que compele o nosso inimigo a exercer nossa vontade’. Portanto, a guerra em essência é violenta, sendo potencialmente ou efetivamente letal - pelo menos para um dos lados. (CLAUSEWITZ, 1980, apud. RID, 2013 p. 1, tradução própria).

Apesar disso, para alguns dos autores abordados, como Lewis (2010), Rid (2013), Gartzke (2013), Valeriano e Maness (2014), Weedon (2015) e Maschmeyer (2021), é improvável que venha a ocorrer uma guerra cibernética que resulte em letalidade, principalmente devido aos cálculos estratégicos envolvidos e à resistência geral à dinâmica de escalada no ciberespaço (VALERIANO & MANESS, 2016).

Rid (2013), por exemplo, destaca que a guerra deve envolver três aspectos específicos: motivação política, instrumentalização no caráter, e potencial letalidade. De maneira mais genérica, considera os termos força, violência e letalidade, quando abordando a guerra, e

sustenta uma relação causal: força implica violência, que por sua vez implica letalidade (RID, 2013). Porém, há autores que rebatem, e afirmam que a guerra não exige nenhuma conexão causal necessária entre o que são realmente três fenômenos distintos: toda guerra envolve força, mas força não implica necessariamente violência – particularmente se se considera que a violência implica letalidade (STONE, 2013, destaque nosso). Ou seja, permitir que os atos de guerra sempre envolvam força e violência não é permitir que eles devam envolver necessariamente letalidade (ou dano). Tanto que o termo "dano" implica que a violência pode ser dirigida também a objetos, não sendo, portanto, necessariamente letal (STONE, 2013).

Além de Stone, autores como Lewis (2010) corroboram a ideia de que conflitos cibernéticos, na maioria das vezes, não envolvem necessariamente violência - apesar de poder envolver. Stone (2013) destaca, no entanto, que a evolução constante da tecnologia

> (...) constitui um meio de ação através do qual a aplicação de pequenas quantidades de força se traduz em grandes quantidades de violência. Com base nisso, os ataques cibernéticos representam um meio particularmente eficiente de traduzir a força em violência: bastam alguns toques de tecla para desencadear uma sequência de eventos potencialmente muito violentos (STONE, 2013, p. 107, tradução própria).

Apesar desta capacidade em potencial, o papel que o ciberespaço tem desempenhado na guerra ainda é limitado e centra-se, sobretudo, na sabotagem, subversão e coleta de inteligência. O seu caráter subversivo e recolector, neste caso de dados, não é, necessariamente, violento - e embora a sabotagem possa sê-lo, a violência geralmente se concentra em equipamentos físicos, não em pessoas (RID, 2013).

Na maioria dos casos, os ataques cibernéticos não exigem necessariamente um ato de violência para obrigar nosso oponente a cumprir nossa vontade. A violência por meios cibernéticos é de fato possível, mas esse não é o único ou principal uso dos ataques cibernéticos. Seus efeitos são mais frequentemente intangíveis e informativos, e destinam-se sobretudo à manipulação da intersubjetividade. De fato, dar ênfase ao possível efeito cinético dos cyberattacks pode obscurecer outros pontos importantes, complicando os esforços para que se desenvolvam normas mais condizentes com este tipo de conflitos (LEWIS, 2015).

Além da dificuldade em enquadrar a natureza dos efeitos resultantes dos cyberattacks, também há um esforço na tentativa de conferir-lhes um caráter mais conciso e universal, ao que se soma o debate se tais atos devem ser considerados efetivamente como guerra - ou se podem ser mais bem entendidos como criminalidade, espionagem, sabotagem. Essas

discussões são obstaculizadas pela dificuldade de definir o que se constitui como guerra. E, segundo Stone, os meios de guerra, sejam eles interpretados como força ou violência, ainda permanecem como temas sub-explorados pelos teóricos estratégicos (STONE, 2013).

O autor também aponta que a distinção de Rid (2013) entre guerra e sabotagem baseia-se apenas em questões de segmentação: “guerra envolve matar pessoas, sabotagem envolve quebrar coisas; a guerra envolve letalidade, a sabotagem não”. Neste ponto, a letalidade sai de cena, e portanto, o status dos ataques cibernéticos não pode ser julgado com base nisso. Nesse contexto, a violência deve ser considerada um produto da força e não uma característica definidora da guerra (STONE, 2013).

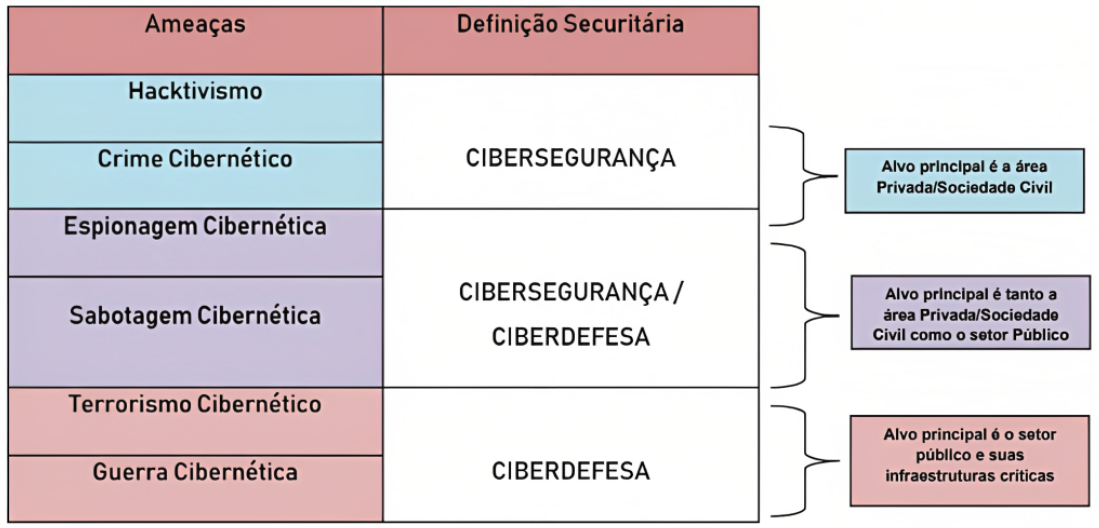
Porém, argumenta que uma redefinição nestes moldes exigiria redefinir todo o clássico entendimento liberal de guerra como sendo atos de sabotagem – porque preocupa-se mais em infligir danos físicos a objetos e infraestruturas, como uma alternativa a matar pessoas. Em conclusão, a guerra cibernética é possível no sentido de que os ataques cibernéticos podem constituir atos de guerra, que por sua vez envolvem a aplicação da força para produzir efeitos violentos. Esses efeitos não precisam ter caráter letal: eles podem infligir dano a infraestruturas, em vez de matar pessoas, e ainda se enquadram na rubrica de guerra (STONE, 2013).

Rid (2013), por sua vez, argumenta que o termo sabotagem - “tentativa deliberada de enfraquecer ou destruir um sistema econômico ou militar, em que as coisas (objetos, infraestruturas) são os alvos principais, não os humanos” - pode enquadrar-se bem neste caso. O autor argumenta que historicamente os atos de guerra estiveram vinculados a posteriores atribuições - o que não ocorre em grande parte dos ataques cibernéticos.

Alguns autores, no entanto, preferem usar o termo “conflito cibernético” para descrever a forma da malícia cibernética usada nas interações de relações internacionais, que seriam definidos como “o uso de tecnologias computacionais”, especialmente para propósitos malévolos e destrutivos visando impactar ou modificar interações diplomáticas ou militares (VALERIANO; MANESS, 2015, p. 87). Esta definição é mais abrangente, e engloba todas as interações entre os diferentes atores, incluindo ataques menos maléficos, como campanhas de disrupção, sabotagem e espionagem, típicas em interações cibernéticas, até a guerra cibernética direta – se alguma vez acontecer (VALERIANO; MANESS, 2015).

Buscando categorizar os diferentes tipos de ameaças cibernéticas, Pinto, Freitas e Pagliari (2018) propõem a divisão entre as noções de ciberdefesa (ligada às questões da sociedade) e cibersegurança (ligada às questões do estado e de sua soberania). Podemos identificar através desta análise os diferentes tipos de ameaças cibernéticas, e a sua definição securitária correspondente.

Figura 1 - Ameaças Cibernéticas e Suas Definições Securitárias



Fonte: Pinto; Freitas; Pagliari, 2018

Há um extenso histórico de ataques cibernéticos recentes atingindo diversas agências governamentais, instituições militares, serviços civis de emergência, e outros setores estratégicos em termos de infraestrutura, sobretudo fabricantes de base industrial de defesa, serviços de tecnologia da informação e empresas de energia diretamente relevantes para a capacidade militar da Ucrânia (CATTLER & BLACK, 2022). Além disso, os ataques perpetrados contra a sociedade civil e contra entidades do setor privado, como veremos mais adiante, sustentam esta análise. A ciberdefesa entra como importante ferramenta de manutenção da ordem, ao assegurar, em maior ou menor medida, a integridade dos setores públicos estratégicos e suas infraestruturas críticas.

Até o momento, no entanto, o debate acadêmico internacional tem-se atentado principalmente em analisar se os alvos afetados atingem os objetivos políticos almejados. E até aqui, as guerras cibernéticas de grande escala permanecem hipotéticas, e não há, realmente, uma comprovação do grau de eficácia dos esforços de combate das operações cibernéticas (MASCHMEYER, 2021).

Maschmeyer (2021) sugere que a alta taxa de insucesso das ações subversivas em conseguir resultados práticos é fruto de um "trilema subversivo", uma ideia cunhada pelo autor que ajuda a entender o porquê da eficiência e da utilidade estratégica serem tão comprometidas pela configuração das operações subversivas. Para o autor as operações de sabotagem cibernéticas encaram o mesmo trilema - por sua configuração essencialmente subversiva. O autor propõe que, para se alcançar um nível de sigilo operacional (essencial no caso das operações cibernéticas), os atores cibernéticos enfrentam quatro desafios principais:

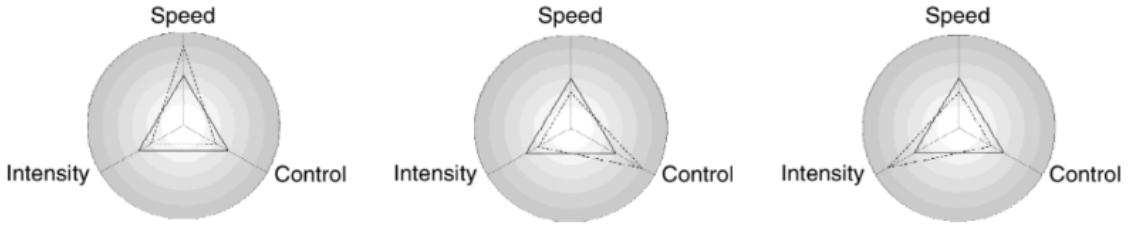
1) Identificar vulnerabilidades em um sistema projetado por outros,
2) Explorá-las sem serem detectados;
3) Estabelecer acesso e controle sobre o sistema sem detecção;
4) E por fim, manter o dito controle para produzir efeitos por meio desse sistema que atinjam os resultados desejados.

(MASCHMEYER, 2021)

Esses quatro obstáculos afetam a eficiência operacional das operações cibernéticas em três áreas distintas específicas: velocidade operacional, intensidade dos efeitos e controle. A ideia principal do autor é a de que essas três variáveis restritivas estão negativamente correlacionadas - produzindo um trilema subversivo.

No diagrama proposto por Maschmeyer (2021), o triângulo pontilhado mostra como o aumento de uma dessas três variáveis tende a diminuir as outras, tendo-se em conta um determinado estado em que todas estão equilibradas, representadas pelo triângulo sólido no centro das esferas.

Figura 2 - O Trilema Subversivo



Fonte: Maschmeyer (2021)

O autor argumenta que

> Aumentar a velocidade operacional significa menos tempo para reconhecimento e desenvolvimento, o que aumenta o risco de cometer erros e de que os alvos descubram a subversão, o que diminui o controle. O aumento da intensidade exige que os atores expandam o escopo ou a escala de acesso aos sistemas, o que aumenta os riscos de descoberta. A redução dos riscos de descoberta para uma determinada intensidade de efeitos tende a aumentar o tempo de desenvolvimento, o que reduz a velocidade. Além disso, aumentar o controle geralmente reduz a velocidade porque os hackers precisam de mais tempo para reconhecimento e desenvolvimento, além de esforços extras para evitar danos colaterais, limitando a escala dos efeitos e, portanto, da intensidade (MASCHMEYER, 2021, p 65, tradução própria).

As diferentes permutações desse trilema produzem as seguintes hipóteses: “o aumento da velocidade tende a diminuir a intensidade e o controle (H1); o aumento da intensidade tende a diminuir a velocidade e o controle (H2); aumentar o controle tende a diminuir a intensidade e a velocidade (H3); e aumentar duas variáveis tende a diminuir duplamente a variável restante (H4)” (MASCHMEYER, p. 66, 2021, tradução própria). A exposição de tais hipóteses de limitações operacionais - o intitulado “trilema subversivo” - é importante para que posteriormente entendamos por que as operações cibernéticas subversivas operadas na Ucrânia, mesmo que complexas e de alto alcance, não têm sido capazes de se traduzir em eficiência operacional russa, e tampouco têm sido capazes de cumprir a promessa de ser ao mesmo tempo um instrumento de baixo risco e baixo custo, mas altamente eficaz, para conduzir sabotagem, interferência política e perturbação econômica.

2.3 A GUERRA MODERNA E A ONIPRESENÇA RUSSA: DEFININDO O PAPEL DO CAMPO CIBERNÉTICO NA UCRÂNIA

Com o colapso da União Soviética, há pouco mais de 3 décadas, a Ucrânia procurou construir vínculos mais estreitos com o Ocidente, o que incluiu a busca contínua de laços institucionais com entidades como a OTAN e UE - com a qual a Ucrânia viria a estabelecer parcerias distintas. Seu interesse em se tornar membro da OTAN continuou a crescer desde 2014, e o país continua enxergando a aproximação com a OTAN, com o Ocidente e com a UE, como um meio de proteger a soberania do jovem país e manter a integridade territorial frente à ameaça russa (PIFER, 2020).

Durante esses 31 anos, as trocas de regime da Ucrânia foram acompanhadas por mudanças na orientação da política externa do país, bem como mudanças na sua posição estratégica e geopolítica, posicionando-se ora entre o Ocidente e ora entre o Oriente, de acordo com seus interesses. Para Pridham (2014), Moscou nunca deixou de esforçar-se por construir uma espécie de soft power russo em diferentes níveis dentro da Ucrânia, incluindo "negócios, influências socioculturais, mídias e redes sociais, e redes da Igreja Ortodoxa – enquanto infiltrava seu serviço secreto em estruturas estatais – com o objetivo de tornar a Ucrânia um aliado sob o regime de Yanukovich (2010-2014)[1]" (PRIDHAM, 2014, p.57, tradução própria).

No entanto, a crise em torno da Ucrânia, que já perdura por anos, faz parte de um confronto mais amplo entre a Rússia e o Ocidente, que envolve um forte fator subjetivo, e que persiste em diferentes graus de intensidade desde a queda da URSS - apesar dos períodos em que o Ocidente como um todo se recusou a reconhecer que qualquer conflito de interesse estratégico com a Rússia existia. Após um período em que esse confronto permaneceu relativamente adormecido, o conflito na Ucrânia resulta da culminação de duas tendências importantes na visão russa de si e do mundo, de acordo com a própria doutrina militar russa: primeiro, uma percepção maior e mais urgente de ameaça, real ou imaginária, à própria segurança russa; e segundo, o reconhecimento de que o país recuperou força suficiente (militar ou não) para se afirmar no cenário internacional (SINOVETS, 2015).

Desde sua desvinculação da URSS, a Ucrânia passou por diversas trocas de regimes internos e por um esforço em adequar suas políticas com as da UE. No entanto, a falta de consolidação de elementos democráticos no país o afastou de uma aproximação mais contundente com o bloco econômico. Os protestos de Maidan no final de 2013, no entanto,

[1] Nota do autor.

abriram um canal para um novo redirecionamento sistêmico em direção à democratização aos moldes da União Europeia e uma aproximação com as entidades ocidentais supracitadas.

Isso ficou claro quando, em junho de 2014, elegeu-se à Presidência do país Petro Oleksiyovych Poroshenko, que viria a ser conhecido como o presidente responsável pela finalização do Acordo de Associação da Ucrânia à União Europeia, que marcaria o início de uma nova etapa em suas relações, sinalizando um claro gesto de apoio da UE a esse país em seu conflito com a Rússia, após a anexação da Crimeia (PRIDHAM, 2014). O posicionamento ucraniano continua a ser mantido pelo atual presidente do país, Volodymyr Zelensky, que em fevereiro de 2022, mesmo com a atual invasão russa, oficialmente assinou e remeteu uma carta de associação como membro da UE, reforçando o Acordo de Associação (NORMAN, 2022) e a predisposição do país em fazer parte da zona de influência ocidental.

Como resposta, os líderes da UE deram alguns grandes passos para impor sanções à Rússia e apoiar a Ucrânia no atual conflito – incluindo assistência militar sem precedentes – mas a adesão à UE é um pedido que o bloco dificilmente aceitará nos próximos anos. Apesar da predisposição dos líderes da União Europeia, Norman (2022) destaca que a incorporação costuma levar anos, especialmente considerando o fato de que há membros relutantes, como é o caso da França.

Pridham (2014) argumenta que a Rússia viu nas "revoluções coloridas" uma "ameaça sistêmica" à ideologia do "eurasianismo", que ressalta a Rússia como uma potência conservadora em oposição aos valores liberais ocidentais. Embora a ideia de que a Rússia enfrenta uma constante ameaça existencial não seja perceptível e compartilhada fora da Rússia, ela tem origens múltiplas e respaldo teórico em autores russos. Em essência, Maschmeyer (2021) argumenta que há um consenso de que a Rússia persegue dois objetivos estratégicos complementares que são centrais à diplomacia do país:

> Primeiro, prevenir e reverter o realinhamento da Ucrânia em relação à União Europeia e ao Ocidente, bem como manter a Ucrânia dentro de sua esfera de influência. Assim, estudiosos russos destacam a prioridade da Rússia em "parar o governo pró-Ocidental de Kyiv", e explicam que "a Rússia vê os antigos estados da URSS como arcos de segurança na Europa Oriental". Declarações públicas da liderança da Rússia alertam a Ucrânia contra a "inevitável catástrofe financeira" que resultaria da integração da UE, e o presidente Vladimir Putin enfatizou repetidamente a história compartilhada da Ucrânia e da Rússia e sua "mesmice" como "um só povo" (MASCHMEYER, 2021, p. 69, tradução própria).

Algumas destas ideias são permanentes e persistentes, como por exemplo, a ideia de que, frente à vulnerabilidade das fronteiras da Rússia, o país deveria exercer controle

geopolítico muito além delas para efetivamente protegê-las. Giles (2015) destaca que este foi um dos impulsionadores dos ultimatos soviéticos aos estados bálticos e à Finlândia, que eventualmente levaram a sua invasão em 1939.

Putin teria dito já em 1991 que “a Rússia voluntariamente e conscientemente fez concessões absolutamente históricas ao abrir mão de seu próprio território” (GILES, 2015, p. 22, tradução própria). Depoimentos mais recentes do líder da Rússia reforçam a manutenção desse posicionamento, o discurso segue sendo o de que a queda da União Soviética representou a "desintegração da Rússia histórica". O presidente afirma que "a Ucrânia nunca teve tradições estáveis de um estado genuíno", e que russos e ucranianos são um só povo, negando à Ucrânia, portanto, o direito a seguir estruturando um projeto de identidade cultural autônomo, e vendo o estado independente de hoje como parte de um "projeto anti-Rússia" e como um entrave para o real exercício da sua influência nas ex-repúblicas soviéticas (RÚSSIA, 2022).

Em relação ao alargamento da OTAN, portanto, o posicionamento russo continua sendo o de vê-lo como uma ameaça. Independentemente da intenção da OTAN, esta representa uma ameaça simplesmente por “aproximar-se das fronteiras da Rússia” (GILES, 2015). É cabível afirmar, portanto, que o Kremlin resistirá ativamente a qualquer movimento de adesão de um estado pós-soviético, mesmo que, de acordo com o direito internacional, isso seja uma questão que apenas a OTAN e o país aspirante possam decidir (PIFER, 2020).

No caso da evolução do campo cibernético ucraniano, é impossível dissociá-la da histórica influência russa e da evolução tecnológica pela qual passou o país. A conectividade com a Internet existe no país desde 1990, momento em que se inicia o confronto dissimulado entre os dois países, que se estenderia até os dias atuais - Pagliusi (2022) refere-se ao fenômeno como “guerra fria cibernética” russo-ucraniana, fazendo alusão ao período de tensão entre EUA e Rússia, em que a competição tecnológica era um fator central e incrementos de um lado geralmente eram compensados por esforços de adequação tecnológica do outro (PAGLIUSI, 2022).

A Ucrânia herdou grande parte desta infraestrutura soviética de comunicações e há um fator agravante que é o de a Rússia ter penetrado intrinsecamente nas redes de comunicação do país, facilitando um acesso vantajoso aos canais de comunicações, que provavelmente fornecerá um valor considerável para as táticas e o planejamento russos futuros (LEWIS, 2015).

Maschmeyer (2021) argumenta que, embora a Rússia não tenha sido capaz de atingir os seus objetivos estratégicos complementares expostos acima pelo autor, seus esforços bélicos mudaram o equilíbrio de poder em favor do país com a anexação da Crimeia e com o controle parcial da região do Donbass. Porém, não há nenhuma comprovação de que a "guerra híbrida" esteja de fato dando protagonismo às operações cibernéticas.

Embora a Rússia seja uma das nações mais habilidosas quando se trata de suas capacidades cibernéticas, não foi visto uso extensivo de ataques reais contra a Ucrânia, isto porque o cibernético como poder coercitivo provou-se de utilidade limitada nas investidas contra a Ucrânia - pelo menos até o momento. Tais ataques não foram capazes de interromper o comando e controle ucranianos, negando o acesso à informação, tampouco tiveram qualquer efeito militar de escala considerável (LEWIS, 2015). Maschmeyer (2021) também destaca que as operações cibernéticas foram irrelevantes, inclusive no caso das ações militares no Donbass e na Crimeia, e sustenta que tampouco há evidências que quaisquer operações cibernéticas atribuídas à Rússia contribuíram para a operação de mudança de regime da península.

Ao menos até a invasão russa de princípios de 2022, incidentes cibernéticos que produzissem ferimentos ou morte a pessoas e a destruição ou dano à propriedade, ou então que produzissem efeitos intangíveis de tal alcance e intensidade, com resultados nocivos em termos de escala e gravidade, não foram registrados - nem a infraestrutura crítica, nem as armas ucranianas foram danificadas ou interrompidas. Não vimos nada comparável, por exemplo, aos ataques cibernéticos realizados contra a Estônia em 2007 ou a Geórgia em 2008. No geral, o uso de recursos cibernéticos ofensivos para efeito cinético foi mínimo, com apenas alguns incidentes conhecidos (LIBICKI, 2015). Maschmeyer (2021) destaca que essa ausência é surpreendente dada a relevância das operações cibernéticas dentro da doutrina russa de "guerra de informação". Outro importante ponto destacado pelo autor é o fato da Rússia parecer ter implementado as operações cibernéticas como parte de uma campanha subversiva maior visando a Ucrânia como um todo (MASCHMEYER, 2021).

A Rússia tem usado suas capacidades cibernéticas principalmente para coerção política, formação de opinião e coleta de inteligência, e essas operações cibernéticas ficam abaixo do limite estabelecido no Artigo V do Tratado do Atlântico Norte - pelo menos até o momento (LEWIS, 2015). De fato, alguns autores como Maschmeyer (2021) e Wirtz (2015) destacam as operações cibernéticas do russas como apenas uma parte de uma estratégia maior de subversão focada em moldar a opinião pública e o discurso oficial vigente na Ucrânia.

A ausência de ataques mais contundentes, no entanto, não demonstra que a Rússia não tenha capacidade cibernética. Pelo contrário, o país tem sido um expoente quando se trata de experimentação envolvendo o campo cibernético, e tem buscado formas de produzir benefícios políticos e militares advindo destas operações. No entanto, a configuração geopolítica e as relações de aliança da região têm uma influência poderosa na restrição do uso da força, incluindo os ataques cibernéticos. De momento, suas ações cibernéticas parecem refletir uma decisão cautelosa, de não envolver toda a gama de capacidades cibernéticas (LEWIS, 2015).

Também é verdade que, no futuro, é possível que se saiba que de fato houve ataques mais contundentes de autoria russa, mas que, em seu momento, não sofreram nenhum tipo de atribuição, dada a própria configuração do ciberespaço (LIBICKI, 2015). Ou que então foram efetivamente neutralizados pelo sistema de defesa cibernético ucraniano. Um caso que vale ressaltar, que é explorado por Libicki (2015) em seu artigo, é o incidente que ficou conhecido como Stuxnet, em que "a planta de centrífugas do Irã em Natanz foi infectada por seis meses, com centrífugas falhando em taxas inesperadas antes que os engenheiros iranianos entendessem o porquê". Segundo o autor, os ataques cibernéticos bem-sucedidos são justamente aqueles não-atribuíveis, percebidos muitas vezes como falha de gerenciamento. No caso dos sistemas militares, versões confiáveis de ataques cibernéticos bem-sucedidos podem surgir anos depois, quando as pessoas estiverem mais livres para falar sobre o que aconteceu em tempos de guerra (LIBICKI, 2015, p. 51, tradução própria).

A Federação Russa tem um histórico extenso de espionagem cibernética, sabotagem e hacks que lhe são atribuídos. O caso da Crimeia é destacável, dado que o país usou diferentes estratégias para comprometer a infraestrutura física das linhas de comunicação da península, quando da sua invasão, momento de intensa atividade de hacktivistas patrióticos de ambos os lados, que realizaram ataques cibernéticos, ainda que pequenos, um contra o outro (LIBICKI, 2015).

A maioria destes ataques vêm na forma de incidentes de negação de serviço distribuído (DDoS) contra sites com alvo político ou econômico - ambos os lados realizaram ataques de negação de serviço distribuído (DDoS). Libicki (2015) cita, por exemplo, o incidente perpetrado pela Rússia contra o parlamento da Ucrânia, e uma campanha, que acabou sem sucesso, para desvirtuar os processos de votação na ex-nação soviética. Durante

as eleições, os hackers tiveram uma participação ativa, frequentemente mirando os sites dos partidos políticos, de entidades governamentais e de figuras públicas (LIBICKI, 2015).

Segundo artigo publicado na Hyderabad Central University, os ataques Dos e DDos consistem em:

> (...) ataques lançados para tornar os recursos de redes e sistemas indisponíveis para os usuários legítimos, para que ninguém mais possa acessá-los. Os hackers podem criar uma situação em que as organizações param. Os principais alvos desses ataques são servidores web, gateways, computadores pessoais, etc.(...) Os invasores usam um único computador ou vários computadores para iniciar esses ataques. O uso de vários computadores para realizar o ataque é conhecido como ataque DDoS. Os diferentes sistemas são primeiro comprometidos pelo uso de cavalos de Tróia, *worms*, etc. e, em seguida, usados pelos invasores. Essas máquinas comprometidas são nomeadas como zumbis enquanto a máquina controladora é intitulada mestre. Essa relação mestre-zumbi funciona um pouco semelhante à arquitetura cliente-servidor. Pode ser muito difícil detectar os ataques DDoS porque os zumbis podem estar localizados em todo o mundo. Como resultado, eles não podem ser diferenciados do tráfego legítimo (TRIPATHI, 2013, p.1, tradução própria).

Com a manutenção da "guerra fria cibernética russo-ucraniana", e com a recente eclosão da guerra na Ucrânia, resultando na invasão e parcial ocupação de parte do território ucraniano, a maioria dos países pró-Ocidente da antiga cortina de ferro, mais notadamente os países do norte, vêm adotando medidas claramente pró-OTAN, no sentido de repensar a relação atual com a organização. Para Limnéll (2015), estes países já vem se preparando para uma possível guerra híbrida com a Rússia há algum tempo, que, segundo o autor, combinaria pressão econômica operações convencionais e não convencionais, táticas regulares e irregulares, guerra de informação e guerra cibernética, e ataques físicos limitados, que serviriam para gerar insegurança na opinião pública (LIMNÉLL, 2015).

Em artigo sobre a Guerra híbrida e impactos cibernéticos na infraestrutura de energia ucraniana, Malyarchuk, Danyk e Briggs (2019) definem o conceito de guerra híbrida levando em consideração o caso ucraniano

> Em conflitos híbridos de qualquer intensidade, as ações de combate (operações) são um elemento de outras ações (não contundentes) mutuamente coordenadas segundo um único plano, principalmente econômico, político, diplomático, informacional, psicológico, cibernético, cognitivo, entre outros. Isso dá origem a processos internos e externos desestabilizadores no Estado que são objeto de agressão, como agitação e descontentamento da população, migração e atos de desobediência civil. As guerras híbridas não são declaradas e, portanto, não podem ser completadas no sentido clássico do fim das guerras e conflitos militares. Trata-se de uma espécie de guerra permanente de intensidade variável em diversos setores, com efeitos em cascata e manifestações sinérgicas destrutivas, em que toda a população do país e a comunidade internacional estão, de certa forma, conscientes ou inconscientemente envolvidas. O impacto é sentido em todas as esferas da vida, em todos os setores da sociedade e em todo o estado (MALYARCHUK et al., 2019, p. 1-2).

Fica claro quando falamos de “guerra híbrida” o caráter complementar do campo cibernético nos conflitos bélicos, que assume mais um papel de instrumento, que de meio para se fazer a guerra. No contexto da chamada guerra híbrida, ameaças russas têm sido recentemente notificadas na Ucrânia, mas também em outros países do Norte, como a Finlândia, incluindo ataques cibernéticos e boicotes comerciais (KAGUBARE; MITCHELL, 2022).

Como mencionado, entender o papel geopolítico russo na Ucrânia é essencial para compreender a evolução do campo cibernético ucraniano como política de estado, assim como ocorre com outros países da região, que têm agendas de segurança intensamente influenciadas pelas relações geopolíticas com a vizinha Rússia (LIMNÉLL, 2015). Apesar dos dois países terem se engajado em um conflito militar moderno e “quente”, ainda pouco se fala sobre cyberwar. Past (2015) nos revela que embora nenhum dos dois países neguem a importância do ciberespaço como ferramenta de guerra, até o momento nenhum deles declarou o ciberespaço como parte central ou integral do conflito.

2.4 NOVOS DESAFIOS À SOBERANIA ESTATAL: A REDEFINIÇÃO DA NOÇÃO CLÁSSICA DE FRONTEIRA

Para autores como Fernandes (2012), com o avanço tecnológico e com a disseminação da internet e da sua aceitação no meio social, o controle soberano do Estado sobre suas fronteiras passou a sofrer ameaças e a ser paulatinamente desconstruído (FERNANDES, 2012). Os atores do mundo digital assumem um caráter de “sistemas autônomos” que, na grande maioria dos casos, não se deixam disciplinar pelo controle dos Estados (PINTO; FREITAS; PAGLIARI, 2018). Quando se discute o ciberespaço, percebe-se a centralidade das redes como mantenedoras dessa estrutura, para Coelho (2013) a rede é concebida como uma matriz técnica, referindo-se à existência de um sistema denso, complexo e interligado de infraestruturas técnicas que viabilizam as novas possibilidades de organização territorial das sociedades e se apresenta como locomotiva da transformação social (apud. MEDEIROS et al., 2018).

Trata-se, portanto, de um espaço de poder, em que os elementos físicos e virtuais atuam através das infovias, que representam o canal de expressão social de diferentes atores.

Destaca-se aqui o caráter de “experimentação” do universo cibernético. Ou seja, as respostas estratégicas aos problemas enfrentados, envolvendo alguns destes atores cibernéticos, vão sendo moldadas a partir do surgimento de novos fenômenos na realidade social, em lugar de ser parte de um processo de extensa análise prévia. Esse fenômeno é reforçado pela própria natureza do ciberespaço, que tem como base a Internet, que opera respaldada pelas redes e viabiliza a manutenção de um canal universal e aberto, podendo ser ampliada através de mais infraestrutura de redes, cabeamentos e satélites (MEDEIROS et al., 2018).

A co-dependência das redes às estruturas físicas, que inclui dispositivos tecnológicos operados nos tradicionais domínios das RI, mostra que o ciberespaço permeia cada vez mais o mundo material, o que resulta, segundo Hildebrandt (2014), em um espaço “alternativo, parcialmente imaterial, sem fronteiras, espaço aéreo e/ou águas nacionais” (HILDEBRANDT, 2014. apud. MEDEIROS et al., 2018, p. 38, tradução própria). Parte da noção clássica de Estado inclui a ideia de soberania e de territorialização, cabendo às fronteiras delimitar o território como zona de uso legítimo da força pelo Estado Nacional, ou seja, de poder. Segundo Haesbaert (2004), a territorialização

> desdobra-se ao longo de um continuum que vai da dominação político-econômica mais concreta e funcional à apropriação mais subjetiva e/ou cultural-simbólica de uma área, ou zona, demarcada por limites fronteiriços, profundamente associada ao exercício do poder, em virtude de suas limitações fronteiriças (HAESBAERT apud. MEDEIROS et al., 2018, p. 38, tradução própria).

Tratando-se do Estado Nacional Moderno, portanto, a noção do espaço físico, neste caso de “território”, é indissociável, bem como a ideia da legitimidade do controle sobre seus recursos, riquezas e população, que nos leva à noção de soberania (PINTO; FREITAS; PAGLIARI, 2018). A territorialização, que é uma parte central da existência do ente estatal, corresponde a uma “tentativa de um indivíduo ou grupo de alcançar, influenciar ou controlar pessoas, fenômenos e relações, delimitando e afirmando o controle sobre uma área geográfica” - a delimitação fronteiriça resultante deste processo cerceará uma zona de poder, convertendo-a em território (HAESBAERT apud. MEDEIROS et al., 2018, p. 38, tradução própria).

Os atores que atuam no ciberespaço são capazes de territorializá-lo, ao fazer uso dos seus atributos para alcançar seus interesses, convertendo-o em objeto e meio das relações de poder (MEDEIROS et al., 2018). No caso da Ucrânia, os ataques cibernéticos demonstram uma forma de exercício de poder, ao serem operados por diversos atores cibernéticos, que podem produzir efeitos estratégicos ou militares que incluem a manipulação de software,

dados, conhecimento e opinião, sobretudo a fim de produzir efeitos políticos ou psicológicos na população.

A crise na definição das fronteiras, portanto, pressupõe um desafio ao exercício efetivo da soberania, que é um conceito intimamente ligado à ideia de “espaço delimitado, identidade coletiva e uso da força”. Quando se trata de questões populacionais, definições dos interesses nacionais e legitimação do uso da força, a soberania joga um papel importante, por estar diretamente ligada a um espaço de controle estatal - uma margem espacial onde desfruta do monopólio da força (PINTO; FREITAS; PAGLIARI, 2018). Este território não é apenas entendido como um espaço físico delimitado, mas também como um “locus em que o poder inerente a uma relação é constantemente exercido e confrontado” (FERREIRA NETO, 2014, apud. MEDEIROS, 2018, p. 40, tradução própria).

A disseminação massiva do ciberespaço colocou em xeque o conceito de território como zona de poder, ou seja, o próprio conceito de soberania. Isso porque a delimitação territorial, juntamente com os fluxos fronteiriços, são os principais elementos que definem o processo de territorialização, segundo Haesbaert (2004). Porém, a medida em que os fluxos imateriais das infovias do ciberespaço superam o controle dos fluxos fronteiriço, cruzando fronteiras e penetrando em territórios sem maiores problemas, passam a assumir um caráter desterritorializante (HAESBAERT, 2004, apud. MEDEIROS, 2018). Segundo Medeiros (2018), esses

> fluxos do domínio cibernético podem ser entendidos como a territorialidade de diferentes atores expressa por um domínio artificial e parcialmente imaterial. O efeito territorializante dos fluxos no mundo globalizado por atores mais capazes é reconhecido por Milton Santos (2002) quando argumentando que as redes e territórios sofrem a transformação correspondente, 'sobretudo no interesse dos atores hegemônicos na economia, cultura e política, e são plenamente incorporados às novas tendências mundiais’ (MILTON SANTOS, 2002, apud. MEDEIROS, 2018).

A nível de estados, os efeitos práticos desse processo aparecem quando atos cibernéticos afetam dispositivos fisicamente localizados em seus territórios, podendo acentuar-se quando diferentes atores estatais operam conectados à mesma rede, afetando consequentemente outros domínios, e ameaçando a soberania desses estados. Segundo Medeiros, a lógica operacional do ciberespaço, que assume um caráter “reticular”, resulta no esgotamento parcial da lógica “zonal” da noção clássica de território físico - fator que demonstraria o aspecto desterritorializante do ciberespaço (MEDEIROS, 2018).

Os recursos tecnológicos modernos, com seus sistemas de redes interconectadas a diferentes dispositivos digitais e computacionais, somados a um mundo interconectado e à ascensão de novos atores ao sistema internacional, vem trazendo enormes desafios à criação de soluções que não coloquem em risco as liberdades individuais. A fim de criar fronteiras e delimitações no ciberespaço, com o intuito de garantir a soberania, a figura do Estado vem ameaçando a liberdade dos indivíduos sem antes trabalhar em medidas visando alcançar a origem do problema (PINTO; FREITAS; PAGLIARI, 2018).

Pode-se pensar no cenário, chinês, por exemplo, através da criação de uma enorme rede interna controlada e monitorada. Alguns outros exemplos são destacáveis, como:

> (...) o acesso cada vez mais controlado à Internet em estados menos democráticos, (...) a ascensão de filtros e regras da Internet nas democracias ocidentais. Os estados estão estabelecendo os limites de seu controle soberano no mundo virtual em nome da segurança e sustentabilidade econômica. (DEMCHACK; DOMBROWSKI, 2011, p. 32 apud PAGLIARI et al.).

Conforme elucidado, o estado continua sendo o principal detentor das capacidades cibernéticas - usando-as para fins bélico e políticos. A crítica das autoras está no fato de que as limitações impostas pela coerção do estado afetam mais as liberdades civis que de fato os malfeitores do mundo cibernético. Embora seja importante reconhecer o avanço do debate neste domínio, e das discussões acerca da criação de algum tipo de fronteira que se assemelhe à era westphaliana, ainda é incerto como a soberania dos estados será exercida em um contexto como tal (PINTO; FREITAS; PAGLIARI, 2018)

A Ucrânia não foge dessa lógica. Segundo a especialista em segurança cibernética na Ucrânia, Natalia Spînu (2020), o país ainda carece de uma abordagem sistemática nacional que englobe gerenciamento, proteção e segurança de todo o agregado desses sistemas, que inclui objetos, recursos e redes (SPÎNU, 2020). Além disso, ainda não existe um mecanismo para prevenir potenciais situações de crise envolvendo a infraestrutura crítica do país. Para a autora, é fundamental, portanto, repensar a atual estrutura. No entanto, mudanças desta natureza exigiriam uma “revisão profunda das práticas atuais existentes na Ucrânia, que atualmente são dominadas por abordagens departamentais”, em que falta a interação e coordenação adequadas entre as agências para analisar todo o conjunto de dados (SPÎNU, 2020, p. 9, tradução própria).

A autora acrescenta que as hostilidades na Região de Donbass também têm sido acompanhadas de um “desgaste dos bens de capital e graves problemas de segurança

ambiental e antropogênica". Tais desgastes são ameaças diretas à infraestrutura crítica do país, podendo levar a acidentes envolvendo "minas de carvão, infraestruturas energéticas, instalações fabris, as indústrias químicas e siderúrgicas, bem como as redes de utilidade" - seja como resultado de danos acidentais, perda de controle do processo, ou como consequência de atos terroristas de sabotagem (SPÎNU, 2020, p. 10, tradução própria).

Portanto, ainda é cedo para concluir de que maneira se definirá a fronteira cibernética ucraniana, dada a atual dificuldade em delimitar o próprio ciberespaço. Além disso, o desafio que se impõe à Ucrânia e outros países que se afirmam como democracias é o de como conciliar regulações mais sistemáticas no campo cibernético com as liberdades individuais. E essa questão é especialmente importante no caso da Ucrânia, dada a manutenção do atual conflito e da atual configuração do campo cibernético no país, que apesar de ter passado por melhorias e atualizações recentes, ainda permanece passível de críticas.

2.5 CONCLUSÕES PRELIMINARES

Neste capítulo buscou-se abordar inicialmente uma definição mais objetiva do campo cibernético, que cada vez mais tem adotado a característica de domínio dentro das RI - dada a sua evolução como importante ferramenta política.

A manutenção de uma ferramenta quase que onipresente nos dias atuais é respaldada por diferentes redes, tanto físicas, como imateriais - peopleware, hardware e software. É justamente através da interação com os usuários que essa rede tem assumido cada vez mais importância nas relações políticas.

Apesar de não haver um consenso quanto às definições que devem ser atribuídas ao conflito atual da Ucrânia, em termos cibernéticos, há um relativo consenso entre os autores observados que o elemento de sabotagem tem assumido um papel central, sobretudo a tentativa de se manipular a opinião pública, portanto, os próprios usuários destes sistemas de redes.

Quando aplicamos estas análises ao caso ucraniano, é impossível deixar de fora o protagonismo russo no processo de evolução do campo cibernético daquele país. O país vizinho tem defendido uma posição dura frente às escolhas geopolíticas recentes da Ucrânia,

sobretudo reafirmando a indisposição frente a uma possível aproximação do país com a OTAN e com a UE.

No entanto, apesar do extenso histórico da "guerra fria cibernética" entre os dois países, os ciberataques e ações maléficas nas redes não tem ocupado o centro do palco das ações militares, principalmente quando levamos em conta o gigante cibernético russo, que tem no campo cibernético um espaço destacável dentro da sua estratégia de segurança nacional.

Também é verdade que uma parte desta falta de protagonismo é resultado das próprias limitações inerentes ao ciberespaço e da configuração subversiva das ações cibernéticas. Além disso, outro enorme desafio atual é o de se definir uma fronteira mais concisa do ciberespaço, que colabore com a soberania, ao mesmo tempo que mantém as liberdades individuais.

Essas considerações são fundamentais para que comecemos a analisar a evolução do campo cibernético ucraniano desde uma perspectiva securitária e em que medida essas mudanças têm refletido o atual cenário geopolítico desenhado.

3 A EVOLUÇÃO DO CAMPO CIBERNÉTICO UCRANIANO: A PRESENÇA DE UMA AMEAÇA CONSTANTE

Como explorado no capítulo anterior, apesar das inerentes limitações do escopo das ações cibernéticas, tem-se observado um incremento nos esforços por consolidar este campo securitário, justamente para prevenir ações futuras mais contundentes.

O presente capítulo busca explorar, primeiramente, o imbróglio ideológico existente na Ucrânia, que a situa em meio de um conflito geopolítico maior entre o Ocidente de um lado, e a Rússia do outro. A Ucrânia, desde sua independência, tem-se aproveitado deste cenário para buscar ganhos políticos e aprimorar seu campo regulatório e legislativo quando se trata de cibersegurança.

Posteriormente, abordam-se os alicerces das políticas cibernéticas do país, que serviram como base para a atual legislação, podendo-se destacar a Constituição de 1996, a Lei Sobre a Fundamentos da Segurança Nacional da Ucrânia de 2003, a Estratégia de Segurança Nacional da Ucrânia e a Doutrina Militar da Ucrânia, ambas aprovadas em 2012. Também destaca-se, desde o princípio, a predisposição do governo ucraniano em buscar se aproximar das diretrizes regulatórias dos países ocidentais, buscando aprimorar seu campo regulatório pautando-se notadamente nas normativas da União Europeia e da OTAN - um claro exemplo explorado é a adoção da Convenção de Budapeste, com normativas compartilhadas pelos membros da União Europeia, que viria a ser uma importante diretriz às atuais emendas e regulações cibernéticas.

3.1 PARCERIAS ESTRATÉGICAS: O OCIDENTE VS. A RÚSSIA

Ostentar o status de “estado satélite pós-soviético”, mesmo após o reconhecimento oficial da independência, aprofundou ainda mais as posições conflitantes nos grupos político nacionais sobre se a Ucrânia deveria se inclinar mais para o Ocidente (União Europeia) ou para o Oriente (Federação Russa) (GIERCZAK, 2020). A Ucrânia não só é a segunda maior nação Europeia, mas também dispõe de uma posição geopolítica estratégica e, assim como outras ex-nações soviéticas, em termos geopolíticos, encontra-se na esfera de influência de

duas ideologias dominantes opostas, representadas pelo Ocidente de um lado (a UE, a ONU, a OTAN) e a Rússia do outro.

A União Européia, juntamente com a OTAN, a ONU, e muitas organizações não governamentais, bem como os Estados Unidos, representam a postura democrática liberal que é percebida pela Rússia como uma ameaça à sua existência e ao status de potência mundial. O Kremlin parece tentar minimizar a influência da ideologia ocidental sobre os ex-estados soviéticos, que em grande medida ainda são influenciados pelo gigante ex-soviético.

A inteligência russa e os altos comandos enxergam que a sobrevivência do modus operandi russo depende da manutenção do seu entorno estratégico, do qual faz parte a região de planície da Europa Oriental, que engloba ex-nações soviéticas como a Ucrânia, Polônia, Bielorrúsia, etc., e que representam uma importância vital para a defesa russa - segundo os cálculos estratégicos das altas autoridades. O posicionamento russo em relação à Ucrânia fica mais evidente quando a questão da soberania ucraniana em termos de política externa entra em jogo, e é uma visão de política de estado com raízes na antiga União Soviética. Segundo essa visão, e como vimos brevemente anteriormente, as ex-repúblicas soviéticas, incluindo a Ucrânia e os Estados Bálticos, historicamente pertencem à Rússia - pelo menos a nível de influência geopolítica. Portanto, o controle da região garante a manutenção de uma zona-tampão entre sua fronteira, sobretudo frente à crescente expansão da OTAN e UE, que, como vimos, pregam valores e uma visão de Estado diametralmente diferentes aos da Rússia (MEARSHEIMER, 2014).

Mearsheimer (2014) apontou que “a ferramenta final do Ocidente para separar Kyiv de Moscou tem sido seus esforços para difundir os valores ocidentais e promover a democracia na Ucrânia e em outros estados pós-soviéticos, um plano que muitas vezes envolve o financiamento de indivíduos e organizações ocidentais.” (MEARSHEIMER, 2014, p. 3-4, tradução própria). Dado o extenso histórico diplomático da Ucrânia envolvendo entidades ocidentais, percebe-se que de fato há uma preocupação por parte do Ocidente em disseminar um conjunto de valores no país - incluindo medidas para fortalecer a democracia liberal, os direitos humanos, o combate à corrupção - dentre outros valores tidos como historicamente ocidentais.

A intensificação do conflito é resultado de uma complexa inter-relação de interesses étnicos, religiosos, políticos e econômicos. Além disso, o papel do ocidente, marcadamente a União Europeia e a OTAN, como propulsor do conflito foi enfatizado por Lakomy (2016),

Mearsheimer (2014) e Zwolski (2018). É importante destacar esse ponto, porque o senso comum nos leva a uma espécie de reducionismo quando se trata do tema. Autores como Mearsheimer, aportam-nos uma análise de questionamento sobre as reais causas da escalada de tensões na Ucrânia, apontando os Estados Unidos e os seus aliados europeus como detentores de grande parte da responsabilidade - além, obviamente, da Rússia. Portanto, a hipótese de que os avanços na área de segurança cibernética na Ucrânia foram resultado direto das agressões russas é parcialmente verdade. Levando-se em conta uma visão realista ofensiva, respaldada por autores como Mearsheimer (2014), o massivo esforço do Ocidente em capturar a Ucrânia como zona de influência pró-OTAN e pró-EU não envolveu uma estratégia capaz de diminuir as tensões com a ex-potência soviética.

A ampliação da OTAN, portanto, passa a ser um elemento central de uma estratégia maior para tirar a Ucrânia da órbita da Rússia e integrá-la ao Ocidente, e claramente é um ponto que é percebido pelo Kremlin como uma ameaça a sua soberania regional. Mearsheimer (2014) destaca que, a expansão da UE para o leste e o apoio do Ocidente ao movimento pró-democracia na Ucrânia – começando com a Revolução Laranja em 2004 – foram elementos críticos para explicar a atual tensão entre a Rússia e a Ucrânia. O triunfo de Viktor Yushchenko nas eleições foi a derrota de Putin. De repente, as esperanças mais ambiciosas (a adesão à OTAN e à UE) já não pareciam tão distantes (SHERR, 2020). Segundo a própria OTAN (2022), o lançamento do Diálogo Intensificado com a Ucrânia em abril de 2005, na sequência da “Revolução Laranja”, foi um sinal claro dos Aliados da OTAN de que apoiavam as aspirações de adesão da Ucrânia - em claro sinal de distanciamento político da zona pós-soviética.

No entanto, até mesmo autoridades ocidentais, como o Ex-Secretário de Estado dos EUA, Henry Kissinger (2022), em reportagem ao The Washington Post, têm alertado que, para que haja uma relação minimamente harmoniosa com a Rússia, e uma geopolítica global equilibrada, a Ucrânia deveria ter sido reconhecida como um estado-tampão. Muitos no Ocidente pensam que com o Kremlin nenhuma concessão de princípios pode ser feita. De qualquer forma, a questão da adesão da Ucrânia à OTAN acabou por romper as relações Leste-Oeste e há a ameaça de aumento das tensões entre as partes. Moscou julga que o Ocidente quer enfraquecer e marginalizar a Rússia e fará tudo o que estiver ao seu alcance para impedir que a Ucrânia entre na Aliança Atlântica.

As relações com Washington foram azedando à medida que Putin não conseguia arrancar um acordo das potências ocidentais para deter a expansão da OTAN. A integração das repúblicas bálticas na Aliança Atlântica em 2004 foi o último movimento para o leste que o Kremlin estava disposto a conceder. As aspirações de incluir a Geórgia e a Ucrânia nos anos seguintes foi recebida com rechaço por parte dos russos (MEARSHEIMER, 2014). De acordo com Alexander Grushko, então vice-ministro das Relações Exteriores da Rússia: “A adesão da Geórgia e da Ucrânia à aliança é um grande erro estratégico que teria mostrado sérias consequências para a segurança pan-europeia” (GRUSHKO apud. MEARSHEIMER, 2014).

Para Moscou, esta era uma linha vermelha. Esse posicionamento também fica evidente em um discurso na Conferência de Segurança de Munique em 2007, em que Vladimir Putin acusa as potências ocidentais de violar um compromisso solene ao ampliar consideravelmente a OTAN – principalmente com os países bálticos que aderiram à Aliança em 2004 – perguntando: "O que aconteceu com as garantias que nossos parceiros ocidentais fizeram após a dissolução do Pacto de Varsóvia?" o presidente do Kremlin ainda acrescentou que “um mundo onde há um senhor e mestre... é prejudicial não apenas àqueles que são parte dele, mas também ao próprio mestre... A expansão da OTAN visa cercar a Rússia.” (apud. FRANCE24, 2022).

Os anos seguintes foram marcados pelas crises do gás natural, em 2006 e 2008-2009, que também foram elementos intensificadores do cenário que se montava. Os danos econômicos decorrentes da má gestão desta última crise, aliados com as repercussões políticas negativas da Revolução Laranja, colaboraram para o cenário econômico ucraniano pós-crise de 2009 - ano em que o PIB do país “diminuiu em 15%” (SHERR, 2020, p. 9). De acordo com o investigador do Instituto de Estudos Estratégicos, José Pardo Santayana, esse cenário

> (...) permitiu que Moscou recuperasse a iniciativa momentaneamente. A vitória de Viktor Yanukovych em 2010 parecia atender aos propósitos do Kremlin. O objetivo principal do novo presidente ucraniano era tornar sua própria posição e os interesses de sua “família” oligárquica inexpugnáveis. Abandonando qualquer intenção de integrar a Ucrânia na OTAN, ele esperava garantir uma mão livre com a UE. Moscou não tinha intenção de aceitar isso e aumentou excessivamente a pressão sobre o país vizinho, exigindo plena integração setorial e “sincronização” das relações socioeconômicas. O Acordo de Associação UE-Ucrânia tornou-se o novo casus belli – se Kiev se abrisse para a UE, o comércio russo-ucraniano seria severamente limitado e a União Econômica da Eurásia definharia. O presidente ucraniano teve que ceder, mas mais uma vez, a sociedade civil ucraniana virou a mesa e, em novembro de 2013, estourou a revolução Euromaidan. Tendo conseguido tudo o que queria de Yanukovych, Putin perdeu Yanukovych e também perdeu a Ucrânia (SANTAYANA, 2021, p. 10-11).

Mearsheimer (2014) destaca o fato de que, desde a queda da URSS, em meados da década de 1990, os líderes russos já se posicionavam veementemente contrários ao alargamento da OTAN e, nos últimos anos, suas ações demonstraram que não ficariam parados enquanto a Ucrânia, sua vizinha estrategicamente importante, transformava-se em um bastião ocidental. A derrubada do presidente ucraniano pró-Rússia Viktor Yanukóvich, em 2014, e a sinalização de adesão à União Europeia, foram dois dos principais pontos de inflexão na postura russa, e a resposta foi nada menos que a ocupação da Crimeia naquele mesmo ano e o continuado esforço de desestabilizar a Ucrânia até que ela abandonasse sua disposição em se juntar ao Ocidente (MEARSHEIMER, 2014).

O autor também sustenta que as ações dos Estados Unidos na região demonstram que o país tem sido incapaz de deixar a Guerra Fria para trás e que segue tratando a Rússia como uma ameaça potencial, notadamente desde o início dos anos 1990, ignorando seus protestos e objeções. Outros teóricos defendem esse posicionamento e afirmam que a Aliança frequentemente tem sido insensível aos interesses russos, e bastante inepta em avaliar com precisão a importância da Rússia na região (MEARSHEIMER, 2014). A indisposição da OTAN em avaliar questões como a objeção da Rússia à independência de Kosovo, a ampliação da OTAN e o projeto de defesa antimísseis dos EUA causou forte ressentimento entre a elite russa. A guerra Rússia-Geórgia foi em grande parte uma resposta ao Summit da OTAN de 2008, realizado em Bucareste, no qual o Ocidente confirmou a sua disposição em discutir questões processuais para a inclusão da Geórgia e da Ucrânia na OTAN, ignorando completamente as preocupações da Rússia (SUKHOV apud. OĞUZ, 2015).

Como tantas vezes acontece, não há uma explicação única e tampouco um consenso para o curso de ação político da Rússia, e segundo Giles (2015), a intervenção direta na Crimeia e na Ucrânia também pode ser analisada como uma resposta à ameaça representada aos interesses comerciais russos por uma integração mais próxima com a União Europeia (UE) já que, segundo o autor, "o modelo da UE de mercados abertos e negociações baseadas em regras contraria diretamente a maneira russa de fazer negócios no exterior, reforçando a crescente percepção russa da UE como um problema e não uma oportunidade". O autor ainda destaca que, contra o senso comum, foi a perspectiva de um Acordo de Associação à UE para a Ucrânia, em vez de qualquer envolvimento com a OTAN, que acabaria levando à manutenção da intervenção militar da Rússia. Outros autores rebatem, no entanto, e sustentam que a rejeição de alguns atores chaves da OTAN, como é o caso da França e Alemanha, à proposta do presidente Bush de iniciar a adesão da Ucrânia e da Geórgia à Aliança foi a

verdadeira provocação à Rússia, porque expôs a fraqueza e falta de consenso do Ocidente (BOLTON, 2008, apud. OĞUZ, 2015).

O arcabouço de teorias como a de Fukuyama (1992), que pregavam o "Fim da História", reverberou de maneira a "dar confiança à resiliência e autoridade moral da ordem internacional liberal presidida pelos EUA, e pensava-se em Washington que outros países, incluindo a Rússia, acabariam se submetendo a ela" (SANTAYNA, 2021, p. 9). Em Washington, acreditava-se que o breve período de acomodação com Moscou de meados da década de 1980 a meados da década de 1990 havia se tornado o novo normal para o relacionamento com a Rússia (GILES, 2015).

No entanto, esse período foi uma anomalia. De acordo com artigo intitulado "Como Chegamos Até Aqui: A Visão do Kremlin", a pesquisadora Nataliya Bugayova (2019), Diretora de Desenvolvimento e pesquisadora do portfólio da Rússia e da Ucrânia no Institute for the Study of War (ISW) defende que

> O fato é que a política externa do Kremlin - incluindo a anexação da Crimeia em 2014 e sua intervenção na Síria em 2015 - pegou muitos de surpresa. Esse curso de ação foi consequência da visão de mundo do presidente russo, Vladimir Putin, baseada em mais de duas décadas de insatisfação com o Ocidente, bem como de sua experiência acumulada na busca de seus objetivos centrais: a preservação do regime, o fim da hegemonia dos EUA e a restabelecimento da Rússia como potência global. (BUGAYOVA, 2019, p. 8).

Para Santayna (2021), o conflito iniciado em 2014 marcou "o fim de um esforço de 25 anos para 'sincronizar o desenvolvimento' das relações russo-ucranianas por meios pacíficos, embora indiretamente coercitivos" (SANTAYNA, 2021, p. 11). O autor ainda destaca que o cenário pós-invasão ainda seria marcado pela interrupção da cooperação militar industrial, a sanção de bancos russos e a redução dramática do comércio e das importações de gás natural. Como veremos mais adiante, a invasão da Crimeia marca o início de um período na Ucrânia marcado pelas constantes ameaças e ataques cibernéticos, marcaria também o início de uma política cibernética mais consistente, pautada em legislações que se prescreviam à medida em que o conflito evoluía.

3.2 OS ALICERCES DAS POLÍTICAS CIBERNÉTICAS UCRANIANAS

Para obter uma perspectiva mais clara sobre a estrutura regulatória e legislativa do campo cibernético ucraniano, primeiro é necessário tentar esclarecer o que o Estado ucraniano vê como cibersegurança e quais são suas principais características. Infelizmente, não é uma tarefa fácil, parcialmente devido à indissociabilidade entre segurança da informação e segurança cibernética na Ucrânia. Originalmente, este último era visto como parte do primeiro, que, por sua vez, era um elemento essencial da segurança nacional do Estado. Recentemente, entretanto, no plano regulatório, ocorre certa distinção.

A importância de aprofundar o tema se encontra na indissociabilidade da evolução do campo cibernético ucraniano e as implicações geopolíticas que tem com o vizinho russo. É destacável o fato de que, até a invasão da Crimeia, havia pouca legislação que tratasse sobre a questão cibernética no país (KOSTYUK, 2015). A Constituição Ucraniana, de 1996, por exemplo, não tratava diretamente sobre o tema, ficando subentendido. De acordo com Lev Streltsov (2017) - chefe do Grupo de Pesquisa de Especialistas Cibernéticos do Instituto de Pesquisa Humanitária Aplicada, localizado em Odessa, na Ucrânia - "não há menção direta à segurança cibernética. No entanto, a julgar pelas esferas de proteção que são vistas como mais importantes, é seguro supor que a cibersegurança se enquadra na área de segurança da informação" (STRELTSOV, 2017, p. 13, tradução própria). Isto porque a principal disposição da Constituição da Ucrânia que trata do domínio cibernético é o Artigo 17, que afirma que "a proteção da soberania e integridade territorial da Ucrânia, a provisão de sua segurança econômica e da informação, são as funções mais importantes do Estado, uma questão de toda a nação ucraniana" (UCRÂNIA, 1996).

Também fica evidente ao analisar a introdução da Constituição do país a clara predisposição política frente ao Ocidente e a introdução de valores pró-Ocidente, que mais tarde se materializaram em enormes esforços de cooperação técnica com entidades como a OTAN, UE e esforços multilaterais com outros países:

> O Supremo Conselho da Ucrânia ("*Verkhovna Rada* "), em nome do povo ucraniano - cidadãos da Ucrânia de todas as nacionalidades, expressando a vontade soberana do povo, com base na história secular da construção do Estado ucraniano e no direito à autodeterminação reconhecidos pela nação ucraniana, e por todo o povo ucraniano, garantindo a garantia dos direitos humanos e das liberdades e das condições dignas da vida humana, zelando pelo reforço da harmonia civil em solo ucraniano e confirmando a identidade europeia do povo ucraniano e a irreversibilidade do curso europeu e Euro-Atlântico da Ucrânia, esforçando-se para desenvolver e fortalecer um Estado democrático, social e baseado no direito (UCRÂNIA, 1996).

No entanto, a primeira provisão normativa consistente viria apenas sete anos mais tarde, com a Lei "Sobre os Fundamentos da Segurança Nacional da Ucrânia", de junho de

2003, que seria posteriormente modificada. Porém, à época, foi um marco na legislação de segurança nacional do país, já que serviu como base para as noções securitárias e abriu espaço para a posterior discussão cibernética (KUZIO, 2020). O Artigo 1. já deixa bem claro a preocupação do governo Ucraniano com as ameaças cibernéticas:

> Os termos dados nesta Lei são usados com o seguinte significado: segurança nacional - proteção dos interesses vitais do homem e do cidadão, da sociedade e do Estado, que garante o desenvolvimento sustentável da sociedade, detecção oportuna, prevenção e neutralização de ameaças reais e potenciais aos interesses nacionais na aplicação da lei, anticorrupção, fronteira e defesa, política de migração, saúde, infância, educação e ciência, política de ciência e tecnologia e inovação, desenvolvimento cultural, liberdade de expressão e segurança da informação e cibersegurança (UCRÂNIA, 2003).

Já o Artigo 2. estabelece em linhas gerais a Base Jurídica da Segurança Nacional, que destaca o papel da Estratégia de Segurança Cibernética:

> A base legal no campo da segurança nacional da Ucrânia é a Constituição, esta e outras leis da Ucrânia, tratados internacionais, cuja natureza vinculativa foi aprovada pela Verkhovna Rada da Ucrânia, bem como outros regulamentos emitidos para implementar as leis.
>
> De acordo com esta Lei, o Presidente da Ucrânia desenvolve e aprova a Estratégia Nacional de Segurança da Ucrânia, a Estratégia de Segurança Cibernética da Ucrânia e a Doutrina Militar da Ucrânia, doutrinas, conceitos, estratégias e programas que definem diretrizes para militares em construção, a fim de identificar, prevenir e neutralizar ameaças reais e potenciais aos interesses nacionais da Ucrânia. A Estratégia de Segurança Nacional da Ucrânia, a Estratégia de Segurança Cibernética da Ucrânia e a Doutrina Militar da Ucrânia são documentos vinculativos e a base para o desenvolvimento de programas específicos sob os componentes da política de segurança nacional do estado (UCRÂNIA, 2003).

A Lei "Sobre a Fundamentos da Segurança Nacional da Ucrânia" de junho de 2003 criou as bases para a posterior ratificação da Estratégia Nacional de Segurança da Ucrânia, da Estratégia de Segurança Cibernética da Ucrânia e da Doutrina Militar da Ucrânia, que viriam a ser aprovadas por decreto anos mais tarde. O Artigo 7 também passaria a definir as nove áreas principais de ameaças aos interesses nacionais e à segurança nacional da Ucrânia. Que incluem as esferas da "política externa, segurança do Estado, segurança militar e de fronteiras, política interna, economia, social e humanitária, ciência e tecnologia, defesa civil e segurança da informação". As ameaças ligadas à esfera da segurança da informação listadas na lei são: "limitações à liberdade de expressão e acesso à informação pública; divulgação dos cultos de violência, crueldade e pornografia pela mídia; manipulação da consciência pública (por exemplo, divulgando informações falsas, incompletas ou tendenciosas); divulgação de segredos de Estado ou outras informações restritas que sejam essenciais para a proteção dos interesses nacionais; 'crime informático' e 'terrorismo informático'". O autor destaca os

últimos três pontos como claramente pertencentes à área de segurança cibernética, tornando, portanto, a segurança cibernética efetivamente parte da segurança da informação já a partir de 2003 (STRELTSOV, 2017, p. 150, tradução própria).

No entanto, grande parte das regulações e avanços cibernéticos posteriores do país se dariam através das parcerias e esforços internacionais. À parte das diretrizes securitárias que fundaram a agenda de segurança cibernética do país (com destaque à Constituição de 1996), a Ucrânia passa a contar, já em 2005, com uma estrutura legal e regulatória mais consistente no campo da segurança cibernética - este ano é marcado pela ratificação da Convenção Internacional sobre Cibercrime (CGSS), através da Lei da Ucrânia de 7 de setembro de 2005 (SPÎNU, 2020), embora a Convenção tenha sido inicialmente assinada pela Ucrânia já em 2001. Também conhecida como “Convenção do Conselho da Europa sobre o Cibercrime” ou “Convenção de Budapeste", é o único tratado internacional vinculativo do mundo sobre cibercrime (NOVA ZELÂNDIA, 2020) e é considerado o acordo internacional mais relevante sobre crimes cibernéticos e evidências eletrônicas (CONSELHO EUROPEU, 2020) - contando com 66 signatários e 15 expectantes, incluindo o Brasil.

O intuito principal do memorando é o de prevenir, deter e detectar crimes cometidos através da Internet e de outras redes informáticas (NOVA ZELÂNDIA, 2020) - como veremos com a análise de outros documentos aprovados posteriormente, a incorporação da Convenção de Budapeste deu-se de maneira progressiva. Dentre as principais medidas cibernéticas da Convenção que colaboraram à formulação da legislação cibernética ucraniana podemos citar

> (…) aquelas que visam dotar os órgãos de aplicação da lei com autoridade para ordenar os titulares de dados informáticos para registar e armazenar imediatamente os dados informáticos necessários à resolução de um determinado crime; estabelecer um procedimento definido para emitir tais ordens; bem como requisitos para que os operadores e fornecedores de telecomunicações forneçam informações aos órgãos de aplicação da lei (a seu pedido), o que é necessário para identificar os fornecedores de serviços e as rotas pelas quais as informações foram transferidas; estabelecendo a possibilidade de emitir uma ordem judicial para bloquear (ou limitar) um recurso (ou serviço) informacional identificado por operadores e provedores de telecomunicações; estabelecer um mecanismo eficaz de utilização de provas eletrônicas (recolhidas no curso da atividade investigativa) no processo penal (STRELTSOV, 2017, p. 174-175, tradução própria).

Outros importante marco regulatório a nível cibernético foi a Reforma do Serviço de Segurança da Ucrânia, aprovada por Decreto do Presidente da Ucrânia em decisão do Conselho de Segurança e Defesa Nacional da Ucrânia, em 15 de fevereiro de 2008 (FLURI et al., 2013) e que teve como objetivo:

> (...) estabelecer o objetivo, as tarefas e as direções básicas de uma reforma adicional

> do Serviço de Segurança da Ucrânia como parte do setor de segurança do estado. Esta reforma deve ser realizada de acordo com as prioridades dos interesses nacionais da Ucrânia indicadas na Lei da Ucrânia 'Sobre os Fundamentos da Segurança Nacional da Ucrânia' e a Estratégia de Segurança Nacional da Ucrânia, particularmente, a integração à segurança europeia e euro-atlântica sistemas, o que implica uma cooperação mutuamente benéfica e a adesão à Organização do Tratado do Atlântico Norte (OTAN) e à União Europeia (UE) (UCRÂNIA, 2008).

Além disso, a reformulação postula, dentre diretrizes gerais de segurança, algumas das prioridades securitárias no campo da contra-inteligência - seção que abrange também algumas diretrizes cibernéticas e informacionais:

> Aprofundamento dos princípios organizacionais e legais da atividade de contra-inteligência; uso de uma série de medidas para melhorar a atividade de contra-inteligência levando em consideração a experiência dos principais estados democráticos; melhoria da proteção de contra-inteligência dos órgãos estatais, unidades militares, agências policiais e de inteligência, bem como o nível de cooperação entre todas as autoridades estatais; realização de atividades de contra-inteligência, investigação e busca com os mais modernos meios de telecomunicações e outros meios técnicos; criação de um sistema preventivo de recepção de informações sobre as ameaças à segurança nacional da Ucrânia com base em unidades de contra-inteligência de rádio; melhoria da proteção de contrainteligência dos recursos informacionais do Estado; **enquadramento legal ao sistema de repressão das operações informacionais especiais, formas de cibercrime e ciberterrorismo, circulação ilegal e utilização de hardware de recolhimento de informação encoberta** (UCRÂNIA, 2008, destaque nosso).

Em 2012, o Parlamento começou a propor emendas às leis existentes que tratavam sobre segurança nacional, e passou a ser um importante marco na evolução do campo cibernético na Ucrânia. Neste ano foram aprovadas concomitantemente uma Nova Versão da Estratégia de Segurança Nacional da Ucrânia e uma Nova Versão da Doutrina Militar da Ucrânia, ambas aprovadas por Decreto Presidencial.

O primeiro documento aborda o cibercrime como parte do Artigo 3 - que discorre acerca das “Ameaças reais aos interesses nacionais e à segurança nacional da Ucrânia” (mesmo antes da invasão da Crimeia, já no ano de 2012 se observam tendências potencialmente comprometedoras à segurança nacional). O Decreto Lei ainda prevê, através do inciso 3.3, o desenvolvimento e implementação de normas nacionais e regulamentos técnicos que apliquem tecnologias de informação e comunicação harmonizadas com as normas relevantes dos países membros da UE - incluindo aquelas exigidas pela Convenção sobre Cibercrime de Budapeste. Bem como a posterior criação de um sistema nacional de cibersegurança. (FLURI et al., 2013).

Já a Nova Versão da Doutrina Militar da Ucrânia aborda a questão cibernética na disposição nº II, que trata sobre a “Situação político-militar e sobre as características dos

conflitos armados contemporâneos", também aborda a ameaça de ciberterrorismo - em concreto a "Propagação do terrorismo (incluindo ciberterrorismo), pirataria, crime organizado, migração ilegal, comércio ilegal de armas e tráfico de drogas" (FLURI et al., 2013).

No universo realista, há uma clara tendência em ver a força militar como o elemento mais importante do poder nacional no curto prazo, e outros elementos, como a "força econômica, a habilidade diplomática ou a legitimidade moral", ou, no nosso caso, o domínio cibernético, como importantes na medida em que se combinam com o poder militar. (CHATTURVEDI, 2005, p. 165). Isso fica evidente ao analisar os documentos fundadores da atual Estratégia de Segurança Nacional Ucraniana, que abordaremos na Seção 4.4, em que a Estratégia de Segurança Cibernética é uma das bases que define as diretrizes militares. Além, é claro, da agressão russa, que tem servido como catalisador do processo de revisão e aprimoramento da legislação nacional cibernética, através de emendas e decretos que viriam a modificar a agenda de segurança ucraniana (SPÎNU, 2020). Mais adiante abordaremos a legislação mais atual, precisamente a partir de 2015, quando se aprova a nova Estratégia de Segurança Nacional da Ucrânia, que destaca o papel cibernético. Primeiro, no entanto, é importante analisar o papel das parcerias estratégicas da Ucrânia, que têm influenciado o processo de evolução do campo cibernético no país.

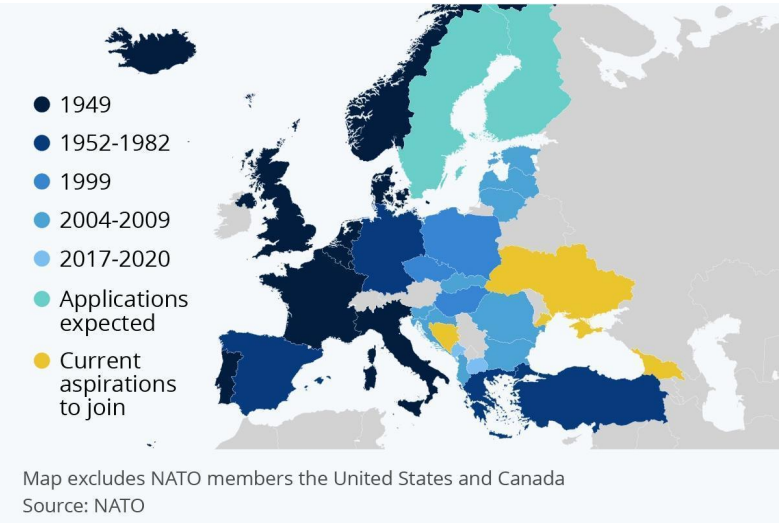
3.2.1 Diálogo continuado com a OTAN

A Rússia tem mantido uma postura firme desde o começo do processo de expansão da OTAN, e já alertava, desde 1995, quando da campanha de bombardeios da OTAN, contra os sérvios-bósnios, sobre a possibilidade da escalada de um conflito maior na região de disputa geopolítica. Na época, porém, os russos não eram fortes o suficiente para fazer frente e atrapalhar o movimento de expansão da OTAN em direção ao leste – o que, de qualquer forma, não parecia tão ameaçador - como destaca Mearsheimer, nenhum dos novos membros compartilhava uma fronteira com a Rússia, com exceção dos países bálticos (MEARSHEIMER, 2014).

Esse cenário mudou, e a OTAN começou sua expansão rumo ao leste em 1999 e trouxe consigo a República Tcheca, Hungria e Polônia. A segunda ocorreu em 2004 e incluiu

Bulgária, Estônia, Letônia, Lituânia, Romênia, Eslováquia e Eslovênia. Mais recentemente, e sobretudo após 2014, as conversações para a adesão da Ucrânia se intensificaram significativamente (MEARSHEIMER, 2014).

Figura 3 - Mapa de Adesão dos Países Europeus à OTAN por Ano



Fonte: OTAN (apud. BUCHHOLZ, 2022)

O ano de 2016 também foi importante para o amadurecimento do campo cibernético e o Summit anual da OTAN daquele ano centrou suas atenções na questão de infraestrutura e fortalecimento da defesa cibernética, sobretudo na questão de redes e indústrias nacionais estratégicas. A questão da abrangência cibernética dos demais domínios também passa a ser importante - registrando-se naquele ano uma série de operações envolvendo o ciberespaço, tido aqui já como um domínio de atuação estratégico - juntamente com o "terrestre, marítimo e aéreo". Mais recentemente, em 2018, o Summit de Bruxelas acrescentou à discussão dos ciberataques as ameaças híbridas, e a OTAN reafirmou a necessidade de levar as operações de ciberdefesa aos demais domínios de atuação. (CENTRE FOR GLOBAL STUDIES, 2015).

No caso da Ucrânia, e em termos bilaterais, os esforços de cooperação entre a OTAN e a Ucrânia na área da reforma do setor de defesa e de segurança são os mais extensos dentre as parcerias com países não-membros. As relações formais começam quando a Ucrânia adere ao Conselho de Cooperação do Atlântico Norte (mais tarde renomeado Conselho de Parceria Euro-Atlântico), imediatamente após alcançar a independência após o desmembramento da União Soviética. No entanto, o primeiro passo concreto visando uma maior aproximação com a OTAN ocorreu em 2004, com a criação do Diálogo Intensificado durante uma visita do

Secretário-Geral da OTAN a Kyiv, quando o governo ucraniano apresentou formalmente um documento de discussão inicial. O documento aborda questões-chave estabelecidas em um Estudo sobre o Alargamento da OTAN de 1995, incluindo política interna e externa, reforma do setor de defesa e segurança, bem como questões legais e de segurança (OTAN, 2022).

É possível destacar alguns esforços concretos de cooperação com a OTAN que abriram espaço para posterior discussões cibernéticas, notadamente: a adesão da Ucrânia ao Conselho de Cooperação do Atlântico Norte, em 1991, abrindo um canal de diálogo com a OTAN; a adesão em 1994 da Ucrânia na Parceria para a Paz (1994). "O programa representou um esforço inicial da OTAN de aproximar-se de maneira bilateral às ex-nações soviéticas e de promover parcerias militares em diferentes áreas" (OTAN, 2020). A assinatura da Carta de 1997 sobre uma Parceria Distinta também colaborou na aproximação, pois estabeleceu um importante marco ao criar a Comissão OTAN-Ucrânia (NUC), para levar a cooperação adiante. "Mais tarde, será essa a principal comissão de monitoramento e criação de outros programas conjuntos, como o Partnership for Peace programme, que seria aprimorado mais tarde, e o Annual National Programme (ANP)". (OTAN, 2022).

Além disso, a partir de 1998 deu-se a criação de diversas iniciativas bilaterais: o Grupo de Trabalho Conjunto OTAN-Ucrânia para a Reforma da Defesa Ucraniana (1998); a abertura do Gabinete de Ligação da OTAN em Kiev para facilitar a participação da Ucrânia no programa da Parceria para a Paz (Partnership for Peace Programme (1999); a criação do Plano de Ação Conjunta como resultado do NUC de 2002. O NUC do ano seguinte cementaria o início do Diálogo Intensificado (Intensified Dialogue), que tratou de abordar as aspirações da Ucrânia à adesão à OTAN e que propôs um pacote de ações de curto prazo para fortalecer o apoio a reformas importantes. Anos mais tarde, em 2008, e à ocasião do NUC daquele ano, criar-se-ia o Annual National Programme, que consistiria de um documento conjunto com descrições das reformas em áreas relevantes, definição de objetivos estratégicos e prioridades necessárias para garantir a implementação efetiva e sistemática do curso estratégico de adesão plena da Ucrânia no Tratado do Atlântico Norte Organização (OTAN, 2022).

Um importante marco das relações entre a Ucrânia e a OTAN foi a anexação russa da Crimeia em 2014, momento em que os Aliados da OTAN decidiram suspender toda a cooperação prática civil e militar com a Rússia. Concomitantemente, os ministros das Relações Exteriores da OTAN concordaram com medidas para aumentar a capacidade da Ucrânia de fornecer sua própria segurança. Decidiram também continuar a desenvolver o seu apoio prático à Ucrânia,

com base num reforço significativo dos programas de cooperação existentes, e com o compromisso de desenvolver novos programas substanciais. Portanto, neste mesmo ano cria-se o Fundo Fiduciário, que dentre suas prioridades encontram-se a questão cibernética.(OTAN, 2022). Segundo os autores do Centre for Global Studies, em trabalho analítico sobre a cooperação para combater ameaças híbridas na esfera cibernética entre a UE-OTAN-Ucrânia, o objetivo principal do Fundo Fiduciário é "o garantir o desenvolvimento dos grupos anti-ameaças cibernéticas dos países participantes - que no caso da Ucrânia envolve o aprimoramento da equipe de resposta a incidentes de segurança informática (CSIRT1), (...) do SSU (Serviço de Segurança da Ucrânia) e do Derzhspetszviazok (Serviço Estatal de Comunicações Especiais e Proteção da Informação da Ucrânia)" (CENTRE FOR GLOBAL STUDIES, 2015, p. 17, tradução própria).

Outras importantes iniciativas incluem o Programa de Aprimoramento da Educação em Defesa (DEEP), que é parte do Programa de Treinamento em Segurança Cibernética da OTAN de 2016. Em 2017 conclui-se a primeira fase do Fundo Fiduciário (CENTRE FOR GLOBAL STUDIES, 2015). Já em 2019, em projeto conjunto entre a Ucrânia e a OTAN, inaugura-se o Centro Situacional para prover segurança cibernética da SSU:

> A OTAN alocou mais de 1 milhão de dólares para este projeto. Outros ministérios ucranianos, incluindo o Ministério das Relações Exteriores da Ucrânia, também recebem equipamentos e softwares da OTAN necessários para a proteção da infraestrutura de informação (CENTRE FOR GLOBAL STUDIES, 2015, p. 18).

De acordo com o relatório *"Ukraine – EU – NATO Cooperation for Countering Hybrid Threats in the Cyber Sphere"*, publicado pelo Centre for Global Studies (2015), a cooperação cibernética entre a Ucrânia e a OTAN, marcadamente a partir de 2013, tem sido registrada anualmente. Na prática, parte da programação anual inclui a participação de especialistas militares ucranianos no campo da defesa cibernética no Treinamento Multinacional da OTAN em larga escala, chamado "CWIX" (*Coalition Warrior Interoperability Exercise*). A nível bilateral a cooperação também se dá através dos Programas Nacionais Anuais (ANP), sob regulação da Comissão OTAN-Ucrânia (NUC). A Comissão tem uma seção separada sobre Segurança Cibernética visando "melhorar o sistema nacional de segurança cibernética como componente do sistema de segurança da informação, sua estrutura conceitual legal e mecanismos práticos para combater a agressão russa no ciberespaço". O relatório ainda revela que "de acordo com os Programas Nacionais Anuais, a Ucrânia tem fortalecido a participação do Estado, incluindo órgãos policiais e especiais em coordenação com um setor privado de TI

- que atualmente corresponde às abordagens da UE e da OTAN para combater ameaças cibernéticas" (CENTRE FOR GLOBAL STUDIES, 2015, p. 17).

Como veremos a seguir, quando se trata de ciberdefesa, o foco na pauta aparece ao longo dos anos no âmbito das conversações da Aliança, à medida que o domínio ganha espaço, e aparece pela primeira vez nas deliberações da entidade em 2002, em um dos Summits da organização, em Praga. Algum tempo mais tarde, no Summit de Gales de 2014, a OTAN já contava com políticas estratégicas de ciberdefesa, que definiriam as atividades da Aliança nas áreas de "conscientização, educação, treinamento e exercício", bem como um plano para a sua implementação e a incorporação dessas políticas ao artigo 5.º do Tratado do Atlântico Norte, que define que " em que um ataque armado contra uma ou várias partes na Europa ou na América do Norte será considerado um ataque a todos" os membros da OTAN. (OTAN, 2017).

3.2.2 Esforços de cooperação internacional no campo cibernético ucraniano: a tríade OTAN-UE-Ucrânia

As relações desenvolvidas com a UE e com a OTAN acabaram por se fortalecer a partir do momento em que a Ucrânia não era mais capaz de resistir por conta própria às ameaças da Rússia. A garantia da estabilidade regional e da própria segurança interna da OTAN estão intimamente ligadas à ideia de garantia do território ucraniano. Essa ideia criou a base para um alinhamento securitário trilateral, visando fortalecer a estabilidade na Europa, no contexto da garantia de longo prazo da segurança dentro e ao redor da Ucrânia, buscando-se proporcionar "estabilidade regional, paz e prosperidade" (CENTRE FOR GLOBAL STUDIES, 2015, p. 4, tradução própria).

Essa parceria tem sido viável porque, historicamente, os objetivos de cooperação entre a UE e a OTAN nas áreas estratégicas de segurança têm coincidido - e isso fica evidente não apenas pelo fato de 21 países serem membros concomitantemente de ambas organizações - mas também pelos esforços conjuntos de preencher as lacunas existentes em termos de capacidades técnicas nas áreas de segurança. E recentemente tem-se dado ênfase à questão da cibersegurança. E fica claro que essa tem sido uma prioridade ao se analisar o histórico de

esforços conjuntos nesta área, que costuma incluir a interação com países não-participantes - notadamente com a Ucrânia (OTAN, 2022).

Como abordado na subseção 3.2, a expansão dos blocos para o Leste (tanto da UE e da OTAN) não tem colaborado para o arrefecimento das tensões geopolíticas. Fica cada vez mais evidente que a Rússia tampouco planeja abrir mão da sua presença na região (MEARSHEIMER, 2014). Um caso que nos demonstra claramente isso é o da Estônia - a série de ciberataques russos ao país motivados por questões geopolíticas alertaram os estados membros da OTAN e UE que eram necessárias melhorias urgentes nas práticas de segurança cibernética nos setores público e privado para reduzir o risco de interrupções digitais danosas (DEVANNY, 2022).

A nível da UE-OTAN em matéria de cibersegurança, a atual atualização das ameaças híbridas associadas à agressão da Rússia contra a Ucrânia tem servido como um impulso adicional para aprofundar a interação entre as duas organizações. A cooperação UE-OTAN tem sido marcada por frequentes summits e reuniões entre autoridades representantes dos dois grupos, surtindo efeitos práticos - com o aumento da colaboração em todas as áreas - desde ameaças híbridas e cibersegurança à cooperação marítima. A cibersegurança, por sua vez, está presente em grande parte dos documentos oficiais de segurança expedidos entre as duas entidades e na prática a cooperação é desenvolvida entre o Computer Emergency Response Team (CERT-EU), do lado da UE, e pelo Computer Incident Response Capability (NCIRC) da OTAN, que se tornaram signatários do acordo técnico entre as duas entidades (CENTRE FOR GLOBAL STUDIES, 2015).

Os esforços de coordenação securitária entre a UE e a OTAN também acabam por se refletir na Ucrânia, à medida em que se debatem as atuais ameaças e se avança a nível de políticas securitárias. Como vimos, mesmo antes de 2014 e dos ataques massivos à segurança cibernética ucraniana, o país já contava com uma certa estrutura legal e regulatória no campo da segurança cibernética (CENTRE FOR GLOBAL STUDIES, 2015). Devanny et al. (2022) corroboram com Mearsheimer (2014) e Giles (2015), ao argumentarem que a intensificação das negociações da Ucrânia com a União Europeia e com a OTAN, em 2013, foi fator decisivo para a operação de anexação da Crimeia e a desestabilização contínua do leste da Ucrânia, que posteriormente levaram a uma resposta diplomática da União Europeia e dos Estados Unidos.

Desde 2013, o presidente Putin tem investido na guerra cibernética visando inviabilizar infraestruturas críticas da Ucrânia (OGLOBO, 2022). A invasão da Crimeia no ano de 2014 ascendeu uma preocupação generalizada na Europa, sobretudo aos membros da UE e da OTAN que fazem fronteira com o ex-país soviético - isso fica evidente ao se analisar os documentos estratégicos das duas organizações, que introduzem a noção de "ameaças híbridas" nas discussões das Cúpulas da OTAN e nas conversações da Estratégia Global da União Europeia. Entre essas ameaças, há um enfoque nas campanhas de desinformação que visam "causar cisões em países e uniões, e intervenções em sistemas de informação e informática" (CENTER FOR GLOBAL STUDIES, 2015, p. 5, tradução própria).

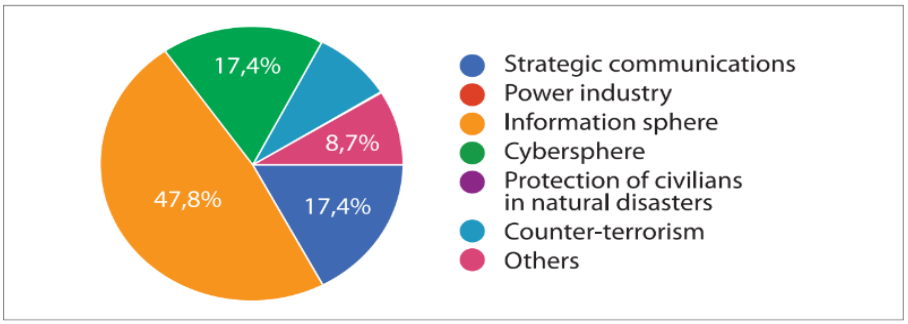
Mas, de fato, os generais russos foram alguns dos primeiros a implantar o conceito de guerra híbrida. O general Valery Gerasimov, hoje comandante das Forças Armadas da Rússia, em artigo de 2013, já defendia que guerras podem ser "vencidas sem a necessidade de extenso poder bélico, (...) o foco dos métodos aplicados de conflito mudou em direção ao amplo uso de medidas políticas, econômicas, informacionais, humanitárias e outras medidas não militares empregadas em coordenação com o potencial de protesto da população. Tudo isso é complementado por meios militares de caráter oculto, incluindo a condução de ações de conflito informacional e das forças de operações especiais" (GERASIMOV apud. OGLOBO, 2022). Com a mudança do contexto geopolítico, a cibersegurança tem estado no centro das prioridades securitárias não só da tríade Ucrânia – NATO – UE, mas também da Rússia. A Rússia, mais do que qualquer outro ator nascente no cenário cibernético, parece ter chegado a uma maneira de integrar as operações cibernéticas a uma grande estratégia capaz de alcançar objetivos políticos maiores (WIRTZ, 2015).

É justamente na Ucrânia que o Kremlin tem testado novos métodos e meios de conduzir guerras híbridas - o país tornou-se campo de ensaio para a Rússia testar novas formas e meios de guerra cibernética. Os ataques russos ao sistema eleitoral ucraniano geraram alertas ao Parlamento Europeu, devido ao receio de interferência nas eleições de países membros. Portanto, não apenas a União Europeia, senão também a OTAN, concetram-se em proteger suas próprias redes e fortalecer a estabilidade interna de seus Aliados, o que também é relevante para a Ucrânia - esse esforço tripartite torna-se especialmente relevante neste contexto (CENTRE FOR GLOBAL STUDIES, 2015).

O conceito de "guerra fria cibernética", usado por Pagliusi (2022), encaixa-se bem nesse contexto, porque ações de fortalecimento estratégico cibernético de um lado,

historicamente têm gerado uma resposta estratégica do outro. O que acaba por refletir-se nas áreas-chave da cooperação de segurança OTAN-UE, identificadas na Declaração Conjunta Sobre Cooperação, em que a segurança cibernética envolve indiretamente quase todos os pontos (incluindo respostas ao terrorismo e energia industrial), tornando-se um tópico altamente prioritário para ambas as organizações - esse diálogo viria a refletir-se nas áreas-chaves do combate comum entre a Ucrânia e a OTAN frente às ameaças híbridas. O gráfico abaixo foi extraído do artigo do Centre for Global Studies, e nos revela as áreas-chave de cooperação e a sua participação no debate entre a Ucrânia e a OTAN:

Figura 4 - Áreas-chave do combate da Ucrânia-OTAN às ameaças híbridas.



Fonte: *Centre for Global Studies*, 2015.

Tais esforços de cooperação também se deram através do diálogo direto da Ucrânia com a UE. De maneira direta, a União Europeia tem prestado assistência financeira à Ucrânia através da Missão Consultiva da UE na Ucrânia (EUAM). Dentre os objetivos, incluem-se a "melhoria de equipamento técnico das agências competentes, formação técnica, trocas de experiências de profissionais (incluindo a Europol) e painéis de discussão" (CENTRE FOR GLOBAL STUDIES, 2015, p. 16). De acordo com o site oficial da Missão Consultiva da UE na Ucrânia (EUAM Ukraine):

> Os eventos do Euromaidan em 2013-2014 aprofundaram a desconfiança do público ucraniano em relação ao governo e às forças de segurança após uma série de eventos violentos envolvendo manifestantes, policiais de choque e atiradores desconhecidos na capital Kyiv. É por isso que o governo pediu apoio à UE para reformar a aplicação da lei e as instituições do Estado de direito e restabelecer a confiança com o povo ucraniano. No âmbito da UE, a Missão Consultiva da UE na Ucrânia (EUAM Ukraine) interage com a polícia cibernética da Ucrânia, o Serviço de Segurança da Ucrânia e o Centro Nacional de Coordenação de Segurança Cibernética (EUAM Ukraine, 2022).

Os esforços também ficam evidentes durante a quinta reunião do Conselho de Associação em 17 de dezembro de 2018, em Bruxelas,

> (...) ambos os lados enfatizaram a necessidade de maior cooperação no combate a ameaças cibernéticas e híbridas no interesse da segurança de seus cidadãos. A este respeito, o Conselho de Associação congratulou-se com o compromisso da UE de continuar a apoiar a Ucrânia no domínio da cibersegurança. (...) A UE executou uma série de atividades ao abrigo do **Instrumento de Assistência Técnica e Intercâmbio de Informações da Comissão Europeia (TAIEX)** em três áreas: criação de um quadro legislativo adequado na Ucrânia; criação de parceria público-privada e promoção de aspectos organizacionais das estruturas nacionais de cibersegurança; apoio das capacidades e competências técnicas das autoridades estatais responsáveis pela cibersegurança (CENTRE FOR GLOBAL STUDIES, 2015, p. 17)

O ano de 2019 ficaria marcado pela ratificação do projeto conjunto da União Europeia e do Conselho da Europa. O **"Cybersecurity East"** visava atuar juntamente a países do Leste Europeu, incluindo a Ucrânia, a fim de "desenvolver mecanismos técnicos e de cooperação que aumentem a segurança cibernética e a preparação contra ataques cibernéticos, de acordo com os padrões da UE" (UNIÃO EUROPEIA, 2019). Pouco mais tarde, em 2021,

> a UE e a Ucrânia forneceram atualizações sobre suas respectivas configurações institucionais relacionadas à cibersegurança, responsabilidades, bem como desenvolvimentos políticos e legislativos, incluindo a atualização da **Diretiva de Segurança da Informação de Rede da UE (NIS)** e os esforços da Ucrânia para desenvolver suas políticas e legislações relacionadas à segurança cibernética, em alinhamento com o quadro jurídico e institucional da UE (UNIÃO EUROPEIA, 2021)

Voltando a lógica realista anteriormente abordada, a falta de "força militar", ou seja, recursos e meios suficientes para resistir à expansão geopolítica russa, aliada ao esforço de autodeterminação como nação soberana e independente, aumentam a importância de OTAN e da UE na elaboração da estratégia militar ucraniana e na assistência prática do desenvolvimento da capacidade militar do país na luta contra a chamada "guerra híbrida" e contra as ameaças modernas - e explicaria, em partes, os esforços de cooperação por parte da Ucrânia. Neste mesmo contexto das atuais ameaças, a cibersegurança tem estado no centro da cooperação Ucrânia–OTAN–UE, como nos revelam o histórico de documentos securitários de atuação conjunta.

3.3 CONCLUSÕES PRELIMINARES

A invasão da península da Crimeia marca o fim de um esforço de reaproximação russo-ucraniano desde a independência do país, em 1991. E é o resultado de anos de tensões geopolíticas na região que não envolvem apenas a Ucrânia, mas também o Ocidente. Desde a

sua independência, e com a queda da União Soviética, a Ucrânia tem buscado se aproximar mais da União Europeia e da OTAN.

Há um esforço não só do Ocidente, mas também da Rússia em capturar a Ucrânia como zona de influência. Autores como Mearsheimer (2014), no entanto, apontam que o massivo esforço do Ocidente em instituir um cenário pró-OTAN e pró-UE na região não envolveu uma estratégia capaz de diminuir as tensões com a ex-potência soviética. E conforme abordado, apesar da grande influência da Rússia na constituição do campo securitário ucraniano, esse avanço não se deu exclusivamente pautando-se nas tensões com os vizinhos. Ao menos não quando se trata da constituição da base legislativa e regulatória do campo informacional.

O Kremlin tem deixado bem clara a intenção de não aceitar as movimentações em direção ao leste da União Europeia e da OTAN - este posicionamento envolve uma visão histórica da Rússia de querer manter a zona de influência da antiga União Soviética. Também envolvem interesses comerciais estratégicos na região que podem ser comprometidos com a aproximação da Ucrânia com os blocos.

O esforço da Ucrânia em se aproximar dos blocos e manter uma política externa independente marcaria não só a interrupção da cooperação militar industrial russo-ucraniana, mas também a sanção de bancos russos e a redução do comércio e das importações de gás natural advindas da Federação Russa. Além disso, o ano de 2014 marcaria o início de um período de ameaças bélicas e ataques cibernéticos. Também serviria como base para o início de uma política cibernética mais consistente.

Essa política não viria desvinculada de um esforço cooperativo, notadamente junto à União Europeia e à OTAN, com a concretização de diversos projetos securitários conjuntos que cimentaram muitas das posteriores políticas atuais. A própria Constituição da Ucrânia de 1996 já menciona a predisposição frente ao Ocidente e seus valores, que mais tarde se traduziria em enormes esforços de cooperação técnica com as entidades supracitadas, além de esforços multilaterais.

4 O CENÁRIO CIBERNÉTICO NA ATUALIDADE

Este capítulo procura abordar o histórico de ameaças e ataques cibernéticos mirando as instituições ucranianas. A escolha temporal para a análise a partir do ano de 2013 é devido a um importante marco, representado pelo movimento do Euromaidan, que foi uma das respostas populares frente à suspensão das tratativas junto à União Europeia, visando a associação.

A partir deste ano, uma série de ataques começam a ser registrados - visando sobretudo instituições públicas, privadas e infraestruturas críticas. O impacto desses ataques será abordado, bem como a sua eficácia operacional. Buscar-se-á explorar também a atual estrutura regulatória do campo cibernético, além das recentes atualizações das legislações cibernéticas, notadamente a partir de 2015, para fazer frente às crescentes ameaças. Dentre as principais normativas abordadas, podemos citar: a Estratégia de Segurança Cibernética da Ucrânia, de 2016, o Projeto de Lei sobre os Fundamentos da Prestação de Segurança Cibernética da Ucrânia, de 2017 e a Estratégia de Segurança Nacional de 2015 e 2020.

Além disso, o capítulo buscou explorar e entender a atual organização do organograma de atores cibernéticos do país. Para tal fim, fez-se um esforço em responder às seguintes perguntas: quem comanda o campo cibernético no país e como se hierarquizam as funções dos diferentes atores?

Por fim, buscou-se explorar brevemente a relação da guerra em curso (desde 2014) com o processo de hipersecuritização, e em que medida o seu recrudescimento explica os esforços de readequação securitários observados na Ucrânia notadamente a partir do ano de 2014.

4.1 AMEAÇAS CIBERNÉTICAS RECENTES E AS RESPOSTAS ESTRATÉGICAS DA UCRÂNIA

Autores como Weedon (2015) e Pagliusi (2022) destacam que a arma cibernética russa intitulada "Ouroboros"existe desde 2005, e que consiste em um malware capaz de atacar

sistemas de redes e computadores ucranianos, através de uma enxurrada de operações cibernéticas operadas por hackers altamente “comprometidos e bem financiados” (WEEDON, 2015, p. 73, tradução própria). No entanto, os primeiros ataques a sistemas de informação de instituições públicas e empresas privadas da Ucrânia foram registrados durante os protestos que configuraram o Euromaidan, em 2013 (PAGLIUSI, 2022).

Em termos de infraestrutura, foram os primeiros ataques a sistemas de informação envolvendo empresas e o setor público e suas infraestruturas críticas que geraram alertas à integridade do sistema de segurança do país. Durante os protestos, a Operação Armageddon visou abrir um canal de espionagem cibernética russo aos “sistemas de informação de agências governamentais, policiais e agências de defesa, a fim de amparar a Rússia no campo de batalha” (PAGLIUSI, 2022).

O termo “guerra fria cibernética russo-ucraniana” anteriormente abordado, usada por Pagliusi (2022) no seu artigo “Guerra Cibernética Russo-Ucraniana – Lições para o Brasil e o Mundo”, deve ser entendido no contexto estratégico mais amplo, com base nas operações cibernéticas orquestrados de ambos os lados. O autor explica que:

> A trajetória dos ataques cibernéticos desferidos pela Rússia contra a Ucrânia, e vice-versa, demonstram que, embora conduzida de forma acobertada, esta guerra fria cibernética entre ambas as nações já vem se intensificando há quase uma década, sendo um componente precursor da posterior guerra convencional ostensiva, do início de 2022 (PAGLIUSI, 2022, p. 6).

O então Diretor do Centro de Excelência em Defesa Cibernética Cooperativa da OTAN, Sven Sakkov (2015), destaca que os incidentes cibernéticos relatados, como “desfigurações, vazamentos de informações ou ataques DDoS contra a mídia ou organizações governamentais” fizeram parte de uma intensa operação russa visando alvos na Ucrânia e no Ocidente. Outro elemento destacável é o fato de que ataques altamente danosos não tenham sido registrados (SAKKOV, CWinP, 2015, p. 8, tradução própria). No entanto, isso não significa que o elemento cibernético não tenha tido um papel estratégico importante no caso da Rússia - abordou-se anteriormente o fato de que o Kremlin parece se destacar no cenário internacional quando se trata de integrar as operações cibernéticas a uma grande estratégia capaz de alcançar objetivos políticos maiores, um ponto explorado por Wirtz (2015) e Maschmeyer (2021).

Uma outra consideração estratégica abordada por Sakkov (2015) no prólogo do livro Cyber War in Perspective é em relação à relativa eficácia das operações cinéticas tradicionais

no caso da Crimeia e do Donbass, onde não houve a necessidade de envolver operações cibernéticas ofensivas a fim de atingir infraestruturas críticas (SAKKOV, CWinP, 2015, p. 8). Esse ponto é sustentado por outros especialistas da área, como é o caso do pesquisador independente de cibersegurança e ex-consultor da Cruz Vermelha em Genebra, Lucasz Olejnik (2022) (apud. OGLOBO, 2022), que afirma que até mesmo no atual conflito de 2022 "não tivemos ciberataques de grande impacto. Eles não estão sendo aplicados, talvez com a exceção dos efeitos de alguns malwares de destruição de dados provocando problemas em sistemas de controle de fronteiras".

Portanto, apesar das políticas cibernéticas não serem o centro operacional da guerra híbrida que ocorre em solo ucraniano, elas têm servido como importante ferramenta por ambos os lados - e, como vimos no decorrer do trabalho, a Ucrânia tem respondido às tensões através dos esforços em construir uma política cibernética coerente e eficaz - isso se reflete nas respostas que se têm dado. Para Gills Vilar-Lopes (2022), da Universidade da Força Aérea,

> É possível que a Ucrânia tenha aprendido com os erros e identificado o modus operandi russo. A resiliência ucraniana parece ser bem-sucedida não apenas nas ruas, mas também na seara cibernética (VILAR-LOPES, 2022, apud. OGLOBO, 2022).

Pagliusi (2022), Weedon (2015) e Kostyuk (2015) destacam um importante marco na seara dos ataques cibernéticos - a Operação Armageddon - que surgiu em 2013 como uma campanha de ciberespionagem russa mirando sistemas de informação de entidades e instituições públicas da Ucrânia, como por exemplo os aplicadores da lei e as agências estratégicas de defesa. A estratégia russa serviu como um complemento bélico à invasão que tomaria lugar no ano seguinte (PAGLIUSI, 2022). Segundo Weedon (2015), analista de inteligência de ameaças estratégicas e consultora de gerenciamento de riscos cibernéticos na FireEye, "a Operação Armagedon provavelmente ajudou a fornecer uma vantagem militar à Rússia em relação à Ucrânia, a partir de segredos sistematicamente coletados através de espionagem cibernética" (WEEDON, 2015).

O período de 2013-2017 foi marcado por uma série de diferentes ciberataques desferidos contra a Ucrânia. A maioria envolveu malwares de diversos tipos e os principais foram "Snake, Uroboros, Sofacy / APT28, Epic Turla, Black Energy 2 e 3, Armageddon e outros" (CENTRE FOR GLOBAL STUDIES, 2019, p. 12). O relatório do Centre for Global Studies (2019) também indica que apesar da Operação Armageddon já estar ativa em 2013, é

apenas em 2014 que a Ucrânia de fato começará a sofrer ataques cibernéticos de grande escala, por ocasião do conflito na Crimeia. Em fevereiro daquele ano, após a invasão da península, centros de comunicação localizados na região foram tomados por forças russas e uma parte da infraestrutura foi comprometida - incluindo infraestruturas cibernéticas críticas, a exemplo dos cabos de fibra óptica que conectavam a península ao continente e que foram comprometidos.

Pagliusi (2022) também indica que houve um esforço em complementar essas ações com ataques a importantes sites de internet - incluindo veículos midiáticos e redes sociais do governo ucraniano. Lançaram-se ataques distribuídos de negação de serviço (DDoS) para tirar do ar páginas, ao mesmo tempo em que se hackeavam os celulares de parlamentares ucranianos. Segundo relatório do Parlamento Europeu, no mês seguinte, em março daquele mesmo ano, três dias antes do referendo sobre o status da Crimeia, a Rússia "lançou um ataque cibernético DDoS de oito minutos com o objetivo de desestabilizar as redes de computadores e comunicações ucranianas como forma de desviar a atenção do público da presença de tropas russas na Crimeia". (PRZETACZNIK et al., 2022, p. 3, tradução própria).

Weedon (2015) destaca que no final daquele ano, pesquisadores expuseram um grupo russo há muito ativo chamado "Sandworm", cujas vítimas incluíam a "OTAN, o governo ucraniano, governos da UE, empresas de energia e telecomunicações e uma organização acadêmica americana. O grupo (...) infectou vítimas por vários meios, incluindo anexos maliciosos de PowerPoint e o kit de ferramentas (vírus)[2] BlackEnergy" (WEEDON, 2015, p. 73, tradução própria).

Em 2015, pesquisadores identificaram dois grupos de hackers russos ativos na guerra cibernética russo-ucraniana: o APT29 (também conhecido como Cozy Bear ou Cozy Duke) e o APT28 (também conhecido como Sofacy Group, Team Czar, Pawn Storm ou Fancy Bear). (WEEDON, 2015, p. 71). No entanto, sabe-se que muitos destes grupos operam através de outros grupos de hackers, a fim de preservar a própria identidade. É o caso do CyberBerkut, uma organização hacker pró-russa que tem servido de fachada para outros grupos hacktivistas, como o GRU119 e APT28, e que possui destaque dentro do Departamento Central de Inteligência Russo (GRU).

No ano de 2014 o grupo foi responsabilizado pela tentativa de comprometer a legitimidade do processo eleitoral para decidir o novo presidente da Ucrânia. Em maio

[2] Nota do autor.

daquele ano, às vésperas das eleições, o grupo pró-russo realizou uma série de ataques cibernéticos para manipular o voto. O grupo foi capaz de invadir a rede e apagar arquivos na tentativa de alterar o resultado das eleições. O ataque, apesar de falho, conseguiu atrasar a contagem das eleições, gerando incertezas e colocando a validade do processo em dúvida em um primeiro momento (PRZETACZNIK et al., 2022).

Destaca-se aqui a noção do "trilema subversivo" proposto e explorado anteriormente por Maschmeyer (2021). Como tem-se observado, as principais operações cibernéticas têm oferecido à Rússia pouca utilidade estratégica mensurável. Um exemplo claro disso foram as tentativas de interferência nas eleições de 2014. Os hackers foram muito ágeis e rápidos na concepção desta operação em particular. O grupo por trás da operação cibernética para sabotar os computadores da Comissão Eleitoral Central (CEC) a desenvolveu em apenas dois meses, um tempo muito reduzido se comparado com os cinco anos que se levou para desenvolver o Stuxnet (MASCHMEYER, 2021).

Durante o ataque, buscou-se maximizar duas variáveis: efeitos intensos de baixa escala, mas de alto escopo - dada a natureza do ato, o de interromper um processo democrático vital. Mas, apesar da rápida ação dos hackers, eles tinham controle insuficiente sobre o sistema de computadores da CEC. O coletivo hacker Cyber Berkut, gabou-se na época de haver destruído o sistema computacional do CEC. No entanto, como previsto pelo trilema, eles tinham controle insuficiente sobre o sistema de computadores. E apesar dos ataques, a contagem de votos permaneceu inalterada porque a operação ignorou o fato de que o CEC poderia usar seus backups para restaurar o serviço. Essa evidência suporta o argumento H4 exposto pelo autor, em que aumentar duas variáveis tende a diminuir duplamente a variável restante (neste caso, velocidade e intensidade, em detrimento do controle). Consequentemente, a operação cibernética não ajudou a Rússia a atrapalhar a eleição da Ucrânia ou mudar o equilíbrio de poder. As eleições decorreram sem obstáculos e a sua legitimidade foi reconhecida (MASCHMEYER, 2012).

No ano de 2015, outra importante infraestrutura crítica ucraniana foi comprometida, quando dos ataques provenientes do vírus Trojan Black Energy, que tentou comprometer empresas de energia do país. Se bem-sucedido, o hack teria causado o maior apagão induzido cibernético de todos os tempos (O'NEILL, 2022). O portal de notícias ucraniano TEXTY relata o mal-estar do operador da central energética Prykarpattiaoblenergo, ao perceber que havia sido hackeado:

> O operador agarrou o mouse e tentou desesperadamente controlar o cursor, mas ele não respondeu. Então, quando o cursor se moveu na direção dos botões de outro interruptor, o computador desconectou inesperadamente o operador do painel de controle. E embora ele tentasse desesperadamente fazer login novamente, os invasores mudaram sua senha e bloquearam seu login.
> Tudo o que ele podia fazer era olhar impotente para a tela, onde os fantasmas da máquina desligavam um fusível após o outro, eventualmente "cortando" cerca de 30 subestações. Mas eles não pararam por aí. Ao mesmo tempo, mais dois centros de controle foram atacados, quase dobrando o número de subestações desativadas.
> Mais de 230.000 moradores locais foram deixados no escuro. E como se isso não bastasse, os atacantes também desligaram os sistemas de energia de backup em duas das três salas de controle - e os próprios operadores tiveram que tropeçar no escuro (ZETTER, 2016).

Além de Prykarpattiaoblenergo, também foram comprometidas as operações de outras duas centrais energéticas - Chernivtsioblenergo e Kyivioblenergo. As ações dos atacantes foram coordenadas e direcionadas à "infraestrutura de informação" e de acordo com informações de uma das centrais, os invasores se conectaram às suas redes de informações a partir de sub-redes da rede global da Internet pertencentes a provedores da Federação Russa (MINISTÉRIO ENERGIA E CARVÃO DA UCRÂNIA, 2016).

Após os incidentes, o Ministério de Energia e Carvão da Ucrânia criou um grupo de estudos para investigar potenciais ameaças futuras. De acordo com o grupo, as três operações foram capazes de "coletar informações sobre a estrutura das redes de informação, ferramentas de software utilizadas, informações sobre contas de acesso remoto à infraestrutura, senhas; pré-infecção de redes usando e-mails falsos; execução das operações de desligamento de subestações; danos a elementos de infraestrutura de TI (fontes de alimentação ininterruptas, modems, UTRs, switches); destruição de informações em servidores e estações de trabalho (utilitário KillDisk); ataques aos números de telefone dos call centers, com o objetivo de negar atendimento aos usuários destes serviços"[3] (UCRÂNIA, 2016).

O ano de 2017 também foi marcado pelo registro de um intenso "surto" de atividades maliciosas - período em que a Ucrânia passa a sofrer ataques do vírus de computador Petya-A (também conhecido como ExPetr, PetrWrap, Petya ou NotPetya) (CHEREPANOV, 2017). De acordo com o especialista em ameaças do tipo malware, o pesquisador Anton Cherepanov (2017), o grupo

> (...) montou ataques cibernéticos contra vários sistemas de computador na Ucrânia; sistemas que podem ser definidos como de infra-estrutura crítica. Além disso, esse grupo tem conexões com o infame grupo BlackEnergy, responsável pelas interrupções de energia de dezembro de 2015 na Ucrânia (...) As infraestruturas críticas envolvidas que tiveram o funcionamento afetado incluem órgãos estatais, aeroportos, bancos, empresas de mídia, serviços de entrega e até mesmo os sistemas

[3] Informação obtida através do site oficial do Ministério de Energia e Carvão da Ucrânia.

> de monitoramento de radiação na antiga usina nuclear de Chernobyl foram comprometidos (CHEREPANOV, 2017, tradução própria).

Empresas estrangeiras também sofreram danos, podendo-se destacar a unidade estadunidense do grupo farmacêutico Merck, a gigante russa Rosneft, do setor de gás natural e petróleo, a britânica WPP, do setor de publicidade e investimentos, a francesa Saint-Gobain, do ramo da indústria de engenharia de materiais, a filial australiana da Cadbury, da indústria alimentícia, entre outras (STRELTSOV, 2017, p. 2). De acordo com artigo do Centre for Global Studies, que também aborda o incidente:

> O criptografador do vírus penetrou em várias redes de instituições públicas e privadas ucranianas, em particular, o site do Gabinete de Ministros e vários ministérios, o Fundo de Pensões, o município de Kyiv, vários bancos, grandes empresas públicas e privadas. A Polícia Cibernética da Ucrânia conseguiu deter a próxima onda de ataques cibernéticos e estabelecer que foi precedida por uma coleta de dados sobre empresas ucranianas. Segundo especialistas, essa informação era o verdadeiro objetivo desse ataque cibernético para mais inteligência cibernética e ações subversivas. Devido a medidas preventivas, em outubro de 2017, os policiais ucranianos conseguiram evitar perdas e a disseminação em massa de ataques cibernéticos a determinados objetos, em particular, o aeroporto de Odessa, o metrô de Kyiv e o Ministério da Infraestrutura (CENTRE FOR GLOBAL STUDIES, 2019, p. 12).

O novo sistema cibernético ucraniano, renovado em 2016 com a nova Estratégia de Segurança Cibernética da Ucrânia, foi posto à prova em 2018, quando especialistas do SSU (Serviço de Segurança da Ucrânia) em segurança cibernética conseguiram bloquear cerca de 400 ataques cibernéticos. Alguns deles, segundo afirmam os especialistas, poderiam ter tido consequências iguais de graves que o vírus Petya-A (CENTRE FOR GLOBAL STUDIES, 2019). Desde a renovação da estratégia em 2016, a Ucrânia tem enfrentado novos desafios cibernéticos, o que culminou na posterior revisão legislativa da Estratégia de 2021, e a proposição da sua versão atualizada no mesmo ano.

De acordo com o Parlamento Europeu (2022), em relatório sobre a linha do tempo dos ataques cibernéticos desde 24 fevereiro de 2022, com a invasão Russa da Ucrânia

> tem-se notificado uma série de *malwares* e outros ataques cibernéticos às infraestruturas e organizações ucranianas e estrangeiras. O atual conflito tem sido marcado por um extenso histórico de ataques a infraestruturas críticas, sites do governo, empresas, organizações e cidadãos do país. Já em janeiro, logo antes da invasão, um relatório da Microsoft alegou que um *malware* mirando o governo e ONGs havia sido detectado - o vírus resultou no controle de 70 sites governamentais, que incluíram o Gabinete de Ministros e dos Ministérios da Defesa, Relações Exteriores, Educação e Ciência, que passaram a estar em mão de hackers russos, de acordo com o Ministério da Transformação Digital da Ucrânia, que responsabilizou a Rússia (PARLAMENTO EUROPEU, 2022, p. 3, tradução própria).

O relatório do Parlamento Europeu (2022) destaca que esse seria apenas o começo das atividades maliciosas do ano de 2022. No decorrer dos meses seriam registrados novos malwares e DDoSs visando bancos, estações de rádio, ministérios do governo, o setor financeiro, entidades não-governamentais, estações de controle fronteiriço. Além disso, foram registrados e-mails de phishing direcionados ao governo e militares, roubo de credenciais de usuário de cidadãos e organizações, incluindo dados bancários e pesquisas fraudulentas em redes sociais. Em fevereiro, no dia da invasão, também foram registrados hacks a sistemas de comunicação do Posto de Kyiv e da rede de satélites geoestacionários europeu, KA-SA, uma hora antes da invasão - resultando em interrupções da comunicação entre indivíduos e entidades públicas e privadas ucranianas (PARLAMENTO EUROPEU, 2022).

A ideia não é apenas a de comprometer a infraestrutura digital crítica de serviços financeiros e energéticos e interromper as redes. Como vimos, não apenas entidades governamentais têm sido alvo, importante parte desses ataques têm sido direcionado também a organizações não governamentais de caridade e ajuda humanitária. A obstrução da entrada de ajuda acaba dificultando a distribuição e a chegada de medicamentos, alimentos e suprimentos de socorro. A divulgação de fake news através de plataformas como o Telegram também tem sido uma constante. Destaca-se uma mensagem falsa que havia sido veiculada em março, e que foi ao ar em um canal de TV ucraniano, alegando que o presidente ucraniano, Volodymyr Zelenskyy, estaria suplicando à população que se rendesse (PARLAMENTO EUROPEU, 2022).

Apesar de todo o esforço russo, no entanto, Maschmeyer (2021) destaca que as operações cibernéticas tendem a ficar aquém de sua promessa estratégica e oferecem utilidade limitada. Todas as operações cibernéticas examinadas neste trabalho mostraram evidências claras do papel restritivo do trilema subversivo proposto por Maschmeyer. O autor defende que o sucesso das operações envolve mitigar as limitações do trilema sem aumentar os custos de alternativas diplomáticas ou militares. Para tal fim, os efeitos devem ser suficientemente intensos para contribuir para um determinado objetivo, enquanto a operação deve produzir esses efeitos dentro de um prazo curto o suficiente para evitar a sua descoberta, mas que seja longo o suficiente para aumentar a probabilidade de alcançar os efeitos pretendidos enquanto se evita consequências não intencionais. Além disso, requer condições de sucesso que raramente estão presentes:

> a disponibilidade de sistemas que controlam processos sociais, econômicos ou físicos de importância estratégica, mas que também contenham vulnerabilidades que

> os operadores podem explorar sem detecção prematura. Finalmente, o longo tempo de desenvolvimento envolvendo operadores altamente qualificados é caro; quanto mais intensos os efeitos físicos de uma operação, menos favorável será a relação custo-benefício. Além disso, mesmo sob condições ideais, o efeito potencial sobre o equilíbrio de poder ainda é provavelmente marginal (MASCHMEYER, 2021, p. 87, tradução própria).

O autor destaca, portanto, que as operações cibernéticas têm maior probabilidade de sucesso, neste caso, em um cenário de competição de longo prazo e de baixo risco entre adversários em desequilíbrio de poder. Porém, apesar da presença desta condição na Ucrânia, a série de operações cibernéticas não contribuiu de forma mensurável para ganhos aos objetivos estratégicos da Rússia. Portanto, provavelmente ainda são necessárias décadas para desenvolver uma operação cibernética bem-sucedida, o que dificulta a análise das ações cibernéticas de maneira isolada e o cálculo do seu impacto.

Independentemente do contexto estratégico, no entanto, qualquer operação cibernética é, em essência, subversiva e, portanto, está vinculada ao conceito explorado por Maschmeyer (2021). Consequentemente, pode-se esperar que esse trilema se aplique a vários contextos estratégicos. Por último, é importante ressaltar que a mudança de regime é, em última instância, a mudança mais significativa que a subversão tradicional pode alcançar. Apesar das operações cibernéticas por si serem provavelmente incapazes de tais efeitos, elas são propensas a fornecer utilidade se forem integradas à dita subversão tradicional. Assim como as operações subversivas tradicionais foram historicamente implementadas para contribuir com objetivos militares, as operações cibernéticas também são, portanto, capazes de potencializar-se ao serem incorporadas à subversão tradicional.

4.2 EMENDAS E NOVAS MEDIDAS: A ATUAL ESTRUTURA REGULATÓRIA

Está claro que antes da agressão da Rússia em 2014, a Ucrânia já tinha uma certa estrutura legal regulatória no campo da segurança cibernética, mas não se pode negar que o recrudescimento de tensões na região acelerou esse processo. O relativamente jovem estado independente da Ucrânia nos últimos anos foi repetidamente vítima de muitos casos de atividades maliciosas e de diversos ataques cibernéticos.

Como resposta à escalada de tensões e com o intuito de consolidar uma legislação cibernética, a partir de 2015, uma série de reformas políticas destinadas a desenvolver o

sistema de cibersegurança começaram a ser implementadas (STRELTSOV, 2017). Na seara destas reformas, promulga-se neste mesmo ano o documento base que guiaria a agenda de segurança do país, a revisada Estratégia de Segurança Nacional da Ucrânia, aprovada por decreto presidencial. Assim como as suas predecessoras, aprovada em 2003 e 2012, e previamente abordadas na Seção 3.1, o documento é composto por uma série de leis e normativas que tratam dos aspectos gerais da agenda de segurança do país. No entanto, contém um bloco separado sobre “ameaças cibernéticas e segurança de recursos informacionais". Nota-se que o Artigo 3 aborda o tema das “ameaças à segurança da informação” (Parágrafo 6) e “ameaças à segurança cibernética e segurança dos recursos informacionais” (Parágrafo 7) (UCRÂNIA, 2015, sp).

De acordo com artigo do Centre for Global Studies (2019), dentre as prioridades para fornecer segurança cibernética e segurança dos recursos de informação, pode-se destacar o aprimoramento do CERT-UA; a garantia de infraestruturas críticas e recursos de informação do estado - “evitando o uso de software, em particular, programas antivírus, desenvolvidos na Federação Russa”; “a intensificação da colaboração entre a Ucrânia e a OTAN, em particular no âmbito do Fundo Fiduciário da OTAN”, dentre outras medidas destacadas pelo documento visando aprimorar o sistema de coordenação de segurança cibernética (CENTRE FOR GLOBAL STUDIES, 2019, p. 10).

Além da efetivação da nova Estratégia de Segurança Nacional da Ucrânia em 2015, no mesmo ano seria proposto o primeiro documento oficial pertencente à esfera da segurança cibernética. No entanto, a Estratégia de Segurança Cibernética da Ucrânia só viria a ser aprovada no ano seguinte, em 15 de março de 2016, por decreto do presidente à época, Petro Poroshenko. Em essência, o documento descreve o sistema nacional de cibersegurança ucraniana e regula as respectivas responsabilidades decorrentes dos principais temas de cibersegurança (UCRÂNIA, 2016, s.p.).

Seguindo diretrizes ocidentais, o documento baseou-se nas disposições da Convenção de Budapeste e nos princípios de defesa cibernéticos adotados pela OTAN (CENTRE FOR GLOBAL STUDIES, 2019), e passa a descrever as principais ameaças na esfera da cibersegurança, incluindo o aspecto militar da cibersegurança, reconhecendo o “Ciberespaço” como um domínio de operações (juntamente com a tradicional “Terra”, “Ar”, “Mar” e “Espaço”) de crescentes hostilidades. (SPÎNU, 2020, p. 6).

Spînu (2020) nos revela que a nova Estratégia de Segurança Cibernética da Ucrânia também tem colaborado enormemente na promoção da cooperação internacional, com o objetivo de fomentar a "capacitação para lidar com a segurança cibernética" e para abordar "as necessidades e ameaças cibernéticas" (SPÎNU, 2020).

A pesquisadora também destaca a participação e liderança do país no desenvolvimento de iniciativas regionais através da criação de um grupo de trabalho sobre segurança cibernética no âmbito da Organização GUAM para a Democracia e o Desenvolvimento Econômico, do qual a Ucrânia é signatária desde 2006, junto com Azerbaijão, Geórgia e Moldávia. O trabalho se materializou no desenvolvimento de um Memorando de Entendimento, que tem servido como base para adoção de medidas conjuntas, como por exemplo a recente implementação de "um sistema de comunicação protegido que permite, entre outros, a troca segura de dados online e a realização de videoconferências" e atualmente, no âmbito cibernético, o GUAM possui Grupos de Trabalho em Tecnologias da Informação e Segurança Cibernética (SPÎNU, 2020, p. 11).

Os autores do artigo do Centre for Global Studies (2019) argumentam que a Doutrina Militar da Ucrânia, aprovada pouco antes da Estratégia de Segurança Cibernética, em 24 de setembro de 2015, ignora as questões de defesa cibernética e aborda apenas de maneira superficial disposições visando combater o ciberterrorismo. Somente a defesa cibernética de infraestrutura crítica é mencionada, como sendo parte da competência do Derzhspetszviazok (Serviço de Comunicações Especiais do Estado da Ucrânia) de: "garantir o funcionamento das comunicações do Governo, incluindo a segurança do Comandante Supremo e dos funcionários das Forças Armadas da Ucrânia, além de outras formações militares e agências de aplicação da lei de propósito especial, fornecendo, assim, segurança cibernética para pessoas e entidades consideradas como partes da infraestrutura crítica" (CENTRE FOR GLOBAL STUDIES, 2019, p. 13).

Além disso, no ano de 2016, deu-se a criação do Centro Nacional de Coordenação de Segurança Cibernética que, como visto, está a mando da coordenação da segurança cibernética da Ucrânia. Também propôs-se atualizar a legislação da época que tratava de crimes cibernéticos, para adequá-la às práticas previstas na Convenção de Budapeste, e a proposta de atualização da legislação de crimes cibernéticos para atender aos requisitos e melhores práticas previstas na Convenção, concretizando a compatibilidade com as normas

pertinentes da UE e da OTAN e o aprofundamento da cooperação com as mesmas (SPÎNU, 2020).

Com a escalada de agressões informacionais em forma de fake news, o Parlamento Europeu ficou imbuído da aprovação da sua própria resolução sobre o combate à propaganda anti-europeia disseminada por toda a UE e refletiu os princípios básicos dessa oposição no Documento intitulado "Comunicação estratégica da UE para combater a propaganda contra ela por terceiros" adotado em novembro 23 de agosto de 2016 (PARLAMENTO EUROPEU, 2016).

Seguindo o exemplo do Parlamento Europeu e respondendo aos desafios de hoje na Ucrânia, o Decreto do Presidente da Ucrânia nº 47/2017 de 25 de fevereiro de 2017 aprovou a Doutrina de Segurança da Informação da Ucrânia (STRELTSOV, 2017). A Doutrina define os interesses nacionais da Ucrânia na área da informação, as ameaças à sua implementação e os rumos e prioridades da política estatal nesta área. Além disso, o documento esclarece os princípios da formação e implementação da política de informação estatal, principalmente, relacionados ao combate à influência informacional exercida pela Federação Russa nas condições da guerra híbrida por ela desencadeada, com o uso das "mais recentes tecnologias de informação de influência sobre o consciência dos cidadãos e que visa incitar o ódio étnico e religioso, propaganda de guerra agressiva, mudança invasiva do sistema constitucional ou qualquer violação da soberania ou integridade territorial da Ucrânia" (UCRÂNIA, 2017, s.p.).

Streltsov (2017) destaca que a Doutrina de Segurança da Informação da Ucrânia, assim como outros documentos frutos da cooperação entre a tríade (UE-OTAN-Ucrânia), tem um forte ângulo "ideológico" - ao buscar enquadrar a legislação do país a princípios tidos como historicamente ocidentais: os princípios de respeito aos direitos e liberdades dos cidadãos, respeito à dignidade humana, proteção dos interesses legítimos dos indivíduos, da sociedade e do Estado, garantindo a soberania e integridade territorial da Ucrânia (UCRÂNIA, 2017).

No entanto, algumas disposições do documento situam-se na área da cibersegurança, um exemplo é o Art.5.1 que fala da "restrição da transmissão de informação através de redes informáticas em estado de lei marcial". Ainda, como regra geral, o parágrafo 3 do Art.1 afirma que "os princípios, prioridades e direções do estabelecimento da segurança cibernética são fornecidos por um ato normativo separado - a Estratégia de Segurança Cibernética da Ucrânia". Essa estratégia regula várias áreas de segurança cibernética, incluindo a proteção de

recursos de informação do Estado, infraestrutura-chave, combate ao cibercrime, etc. Além de estabelecer no Art. 1 que "o desenvolvimento e a segurança do ciberespaço, o estabelecimento da governança eletrônica, a segurança e o funcionamento sustentável da comunicação eletrônica e dos recursos estatais de informação eletrônica devem ser elementos da política estatal na área de desenvolvimento do espaço informacional e desenvolvimento da sociedade informacional na Ucrânia" (UCRÂNIA, 2017, s.p.).

No mesmo ano, em 5 de outubro, o Parlamento ucraniano, após muita deliberação e várias reformulações ao longo dos últimos anos, finalmente aprovou o Projeto de Lei sobre os Fundamentos da Prestação de Segurança Cibernética da Ucrânia (19.06.2015 Nº2126a). O documento leva em consideração a terminologia da UE e da OTAN, que permite uma distinção clara entre "tipos e objetos de atividade e fixa as áreas de responsabilidade dos participantes neste campo". Por exemplo, a lei reflete princípios como "abertura, acessibilidade, estabilidade e segurança do ciberespaço, bem como a necessidade de interação com o setor privado e a sociedade civil no campo da cibersegurança" (CENTRE FOR GLOBAL STUDIES, 2019, p.12).

Também define a base regulatória para proteger "os interesses vitais dos cidadãos, da sociedade e do estado, dos interesses nacionais da Ucrânia no ciberespaço, bem como os principais objetivos, direções e princípios da política estatal no campo da segurança cibernética, os poderes dos órgãos estatais, empresas, instituições, organizações, indivíduos e cidadãos neste campo, incluindo os princípios básicos de coordenação de suas atividades para garantir a segurança cibernética (UCRÂNIA, 2017, sp).

Streltsov (2017) destaca que esta lei é um verdadeiro marco na regulamentação ucraniana de segurança cibernética. No que diz respeito aos desafios que são apresentados no artigo, a adoção da minuta, de certa forma, resolve alguns problemas de inconsistências doutrinárias, sobretudo ao alterar o quadro jurídico de regulamentação desta área da segurança nacional para o legislativo. Apesar da mudança, o autor também destaca que as direções das políticas e os atores envolvidos na segurança cibernética, a distribuição de papéis entre eles, bem como vários outros aspectos da regulação, permanecem essencialmente os mesmos .

A Lei da Ucrânia "Sobre Segurança Nacional", do ano seguinte, mudaria o tipo de vinculação do Derzhspetszviazok no quesito prestação de segurança cibernética, e seria posteriormente revisada e revigorada em 2018, entrando em vigor em 21 de junho daquele ano, através de decreto presidencial. O Artigo 19 impõe a prestação de segurança cibernética

ao Serviço de Segurança da Ucrânia e o Artigo 22 da mesma Lei admite o papel especial do Serviço de Estado para Comunicações Especiais e Proteção de Informações da Ucrânia (Derzhspetszviazok) (CENTRE FOR GLOBAL STUDIES, 2019):

> O Serviço de Estado para Comunicações Especiais e Proteção da Informação da Ucrânia é um órgão estatal designado para garantir o funcionamento e desenvolvimento do sistema estadual de comunicações governamentais, sistema nacional de comunicação confidencial, formação e implementação de política estatal nas áreas de defesa cibernética de infraestrutura de informação crítica, recursos de informação do estado e informações, cuja proteção é exigida por lei, proteção criptográfica e técnica de informações, telecomunicações, uso do recurso de radiofrequência da Ucrânia, correio postal para fins especiais, comunicação do governo (..) e outras tarefas de acordo com a lei (CENTRE FOR GLOBAL STUDIES, 2019, p. 11, tradução própria).

Já o Artigo 31 da Lei da Ucrânia "Sobre Segurança Nacional" de 2018, dedicado à Estratégia de Segurança Cibernética da Ucrânia é tido como um

> planejamento de longo prazo, que define as prioridades dos interesses nacionais da Ucrânia no campo da segurança cibernética, ameaças cibernéticas existentes aos interesses vitais de uma pessoa e um cidadão, uma sociedade e um estado no ciberespaço (CENTRE FOR GLOBAL STUDIES, 2019, p. 11, tradução própria).

Além disso, a lei provê uma "Revisão Abrangente do Setor de Segurança e Defesa", que é conduzida por decisão do Conselho Nacional de Segurança e Defesa da Ucrânia, e que inclui "a revisão do status da defesa cibernética dos recursos de informação do estado e infraestrutura de informação crítica". Dito procedimento fez parte de uma revisão e um esforço de adequação maior do Derzhspetszviazok, por parte do Gabinete de Ministros da Ucrânia. O Artigo em questão também prescreve as necessidades de financiamento orçamentário, as direções prioritárias e abordagens conceituais para a formação e implementação da política estatal, e visa sobretudo melhorar a eficácia dos atores-chave na prestação de segurança cibernética (CENTRE FOR GLOBAL STUDIES, 2019, p. 11, tradução própria).

Mais recentemente, em setembro de 2020, o presidente Volodymyr Zelenskyy aprovou a decisão do Conselho Nacional de Segurança e Defesa da Ucrânia em reformular a Estratégia de Segurança Nacional da Ucrânia, que prevê o desenvolvimento da parceria distinta com a OTAN, com o objetivo principal de se tornar membro efetivo. No texto, os pontos chaves de garantia à segurança informacional e cibernética, que passam a ser aspectos cada vez mais integrantes das políticas do Estado, incluem a "segurança e desenvolvimento do ciberespaço, introdução da governança eletrônica, garantia de segurança e funcionamento sustentável das

comunicações eletrônicas e recursos nacionais de informação eletrônica" (UCRÂNIA, 2020, s.p.).

A Estratégia Nacional de Segurança de 2020 se baseia em três princípios norteadores apontados por Spînu (2020): deterrence, que envolve a prevenção de ataques; resilience, que envolve a capacidade de adaptação do estado e da sociedade a novas ameaças e por último, interaction, que prescreve o aprofundamento das relações com parceiros estratégicos, incluindo a União Europeia, a OTAN e seus estados membros, e os Estados Unidos (SPÎNU, 2020).

A Estratégia de 2020 também inclui novas diretrizes para a Estratégia de Cibersegurança, que visará, em especial,

> melhorar a segurança das redes e dos sistemas de informação; introduzir um sistema de gestão de risco; criar condições para fornecer recursos, incluindo a cibersegurança humana; aprimorar a infraestrutura crítica operacional e de segurança cibernética; combate ao cibercrime; usar os recursos de parceria público-privada e interação das partes interessadas para abordar questões de segurança cibernética e defesa cibernética e aumentar o nível de cultura online (SPÎNU, 2020, p. 7, tradução própria).

A nível legislativo, o ano de 2021 também representou um importante marco, com a outorgação da decisão do Conselho Nacional de Segurança e Defesa da Ucrânia (CNDS) em renovar a Estratégia de Segurança Cibernética, aprovada em 14 de maio. O Decreto Presidencial nº 447/2021 invalidou o artigo 2º do Decreto Presidencial nº 96 de 15 de março de 2016, sobre a decisão do Conselho de Segurança e Defesa Nacional da Ucrânia de 27 de janeiro de 2016, que abordava a estratégia de segurança cibernética da Ucrânia, descartando a anterior versão da estratégia, e propondo um modelo atualizado mais abrangente, que leva em consideração experiências e problemas anteriores, o estado atual do ambiente de segurança cibernética nos níveis nacional e internacional, bem como as disposições da Estratégia de Segurança Cibernética da UE para a Década Digital e as estratégias de segurança dos Estado-membro da UE e da OTAN (UCRÂNIA, 2021).

Outro ponto importante da Estratégia a destacar é a prerrogativa do desenvolvimento de um Plano Nacional de Resposta a Emergências Cibernéticas, que definirá mecanismos para responder a ataques cibernéticos nacionais em instalações críticas de infraestrutura de informação e medidas para posterior recuperação - uma medida visando fortalecer as diretrizes vinculativas sobre a proteção de infraestruturas críticas (UCRÂNIA, 2021).

A decisão do Conselho Nacional de Segurança e Defesa da Ucrânia (CNDS) também confere mais coordenação institucional, a medida em que passa a exigir do Centro Nacional de Coordenação de Segurança Cibernética o desenvolvimento e apresentação ao CNDS, em um prazo de dois meses, do Plano de Implementação da Estratégia de Segurança Cibernética da Ucrânia. Cabe às autoridades centrais, juntamente com o Serviço de Segurança da Ucrânia e o Serviço de Inteligência Estrangeira, garantir a implementação deste plano após a sua aprovação (UCRÂNIA, 2021).

A versão atualizada da estratégia cibernética que seria então proposta contém uma lista de desafios e ameaças que a Ucrânia enfrenta no campo da segurança cibernética, dentre elas propõe as bases para o desenvolvimento de um sistema nacional de proteção contra ameaças cibernéticas, determina as principais prioridades e objetivos estratégicos para garantir a segurança cibernética de Ucrânia, bem como as direções das atividades de política externa e tarefas estratégicas que o estado enfrenta nesta área (UCRÂNIA, 2021).

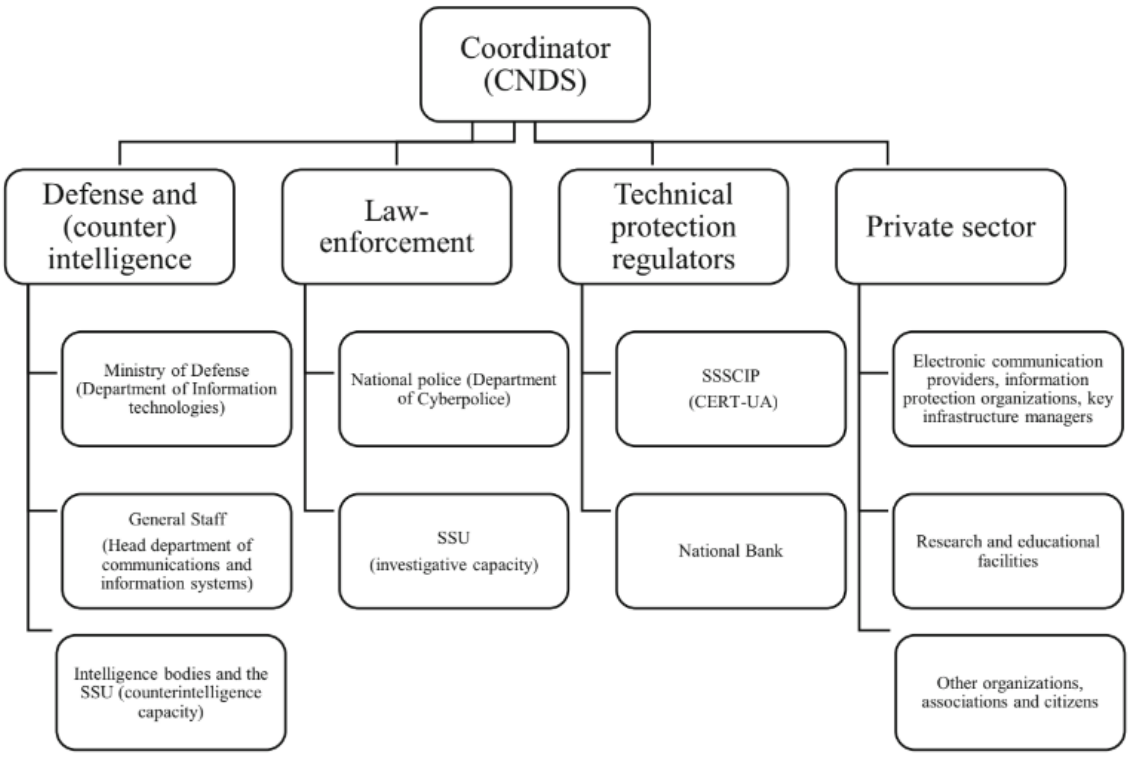
A Estratégia também leva em conta as ameaças e os desafios atuais, notadamente a pandemia do COVID-19, que mudou os processos econômicos e o comportamento social, obrigando os cidadãos a trabalhar remotamente usando cada vez mais serviços eletrônicos e tecnologias em nuvem. Esse ponto é particularmente importante porque a Rússia segue usado ciberataques para manipular a opinião pública e espalhar desinformação entre os cidadãos ucranianos, além de operar ataques destinados principalmente a atingir os sistemas de informação dos órgãos estatais da Ucrânia e infraestruturas críticas (UCRÂNIA, 2021).

4.3 OS ATORES CIBERNÉTICOS DA UCRÂNIA

Para fazer frente aos ataques que se intensificaram a partir de 2014, a Ucrânia não tem poupado esforços em desenvolver uma estrutura de segurança cibernética nacional mais coordenada. Como vimos na Seção 4.1, a nível regulatório, o parágrafo 3 do Art.1 da Doutrina de Segurança da Informação da Ucrânia afirma que os princípios, prioridades e direções do estabelecimento da segurança cibernética são fornecidos pela Estratégia de Segurança Cibernética da Ucrânia. Redigido em termos bastante gerais, no entanto, não aprofunda acerca das especificações de tarefas ou estabelece mecanismos de interação entre os atores.

No entanto, uma análise de suas disposições permite construir o quadro a seguir, baseado em quatro pilares: com um órgão coordenador, a base de cibersegurança do país é composta pelo “SSU (Serviço de Segurança da Ucrânia), o Derzhspetszviazok, ou SSSCIP (Serviço Estatal de Comunicações Especiais e Proteção da Informação da Ucrânia), o Ministério da Defesa e o Estado Maior das Forças Armadas da Ucrânia, a Polícia Nacional, o Banco Nacional da Ucrânia e as agências de inteligência” (CENTRE FOR GLOBAL STUDIES, 2019, p. 12, tradução própria). A Figura 5 esquematiza a estrutura base do esquema de cibersegurança ucraniano:

Figura 5 - Organograma dos Diferentes Atores que Compõem o Campo Cibernético Ucraniano



Fonte: (STRELTSOV, 2017)

A Tabela 1 é complementar à Figura 5, e ajuda a entender, de maneira resumida, as principais atribuições de cada um dos atores envolvidos supracitados

Tabela 1 - Atribuições dos Principais Atores Cibernéticos Ucranianos

	Principais Atores
Coordenação (CNDS)	O Conselho de Segurança e Defesa Nacional. O órgão específico da área do Conselho é o Centro Nacional de Coordenação de Segurança Cibernética.
Estrutura de Defesa	Ministério da Defesa, Estado-Maior General das Forças Armadas. As divisões especializadas dessas estruturas são a Divisão de Tecnologias da Informação do Ministério da Defesa e a Divisão-Chefe de Comunicações e Sistemas de Informação do Estado-Maior General. Além disso, o Ministro da Defesa da Ucrânia anunciou recentemente o desenvolvimento de uma nova unidade, considerando a experiência positiva da Lituânia e com a assistência da OTAN.
Contrainteligência	Serviço de Inteligência Externa da Ucrânia, o Órgão de Inteligência do Ministério da Defesa da Ucrânia e o Órgão de Inteligência da Guarda de Fronteiras do Estado, etc.
Agentes Aplicadores da Lei	Serviço de Segurança da Ucrânia Polícia Nacional da Ucrânia.
Reguladores da Proteção Técnica	Serviço Estadual de Comunicação Especial e Proteção da Informação (SSSCIP) Banco Nacional da Ucrânia
	A Estratégia não dá instruções diretas aos atores do setor privado, fala apenas da necessidade de criar as condições para sua participação nas seguintes capacidades. O primeiro tipo de ator aqui são organizações que realizam atividades na área de

Setor Privado	comunicações eletrônicas, proteção de informações e/ou são proprietárias (gerentes) de objetos de infraestrutura-chave.

Fonte: (STRELTSOV, 2017)

A maioria dos órgãos destacados acima são compostos por outras agências ou grupos especializados. Como é o caso do Setor de Segurança e Defesa da Ucrânia (SSU), que abrange órgãos militares, de inteligência, de segurança do Estado e de aplicação da lei, e são os responsáveis pela segurança cibernética do país - a nível legislativo e fiscalizador (CENTRE FOR GLOBAL STUDIES, 2019).

Também é o caso do Derzhspetszviazok, ou Serviço Estadual de Comunicações e Informações Especiais (SSSCIP), que foi a primeira agência ucraniana especializada em ameaças informacionais e cibernéticas - tendo a sua criação em fevereiro de 2006. Atualmente, é a única organização que trabalha exclusivamente em questões de segurança cibernética. De acordo com o website oficial do SSCIP, o órgão desempenha “93 tarefas e funções e molda a política do governo em 16 áreas” (SSSCIP, 2022). No entanto, vale destacar suas principais atribuições, que incluem: “interação com o domínio de administração ucraniana.; proteção dos recursos de informação do Estado; interação com autoridades estaduais; cooperação internacional na proteção de recursos de informação; manutenção de um sistema unificado de proteção antivírus; e determinação do nível de proteção dos sistemas das autoridades de informação e telecomunicações.” (KOSTYUK, 2015, p. 118, tradução própria).

Além disso, possui vários escritórios internos, incluindo o Centro de Proteção de Informações de Antivírus (CAIP), a Banca de Avaliação de Proteção de Recursos de Informações Estatais, o Sistema de Proteção Cibernética e o Registro de Sistemas das Autoridades de Informação e Telecomunicações” (KOSTYUK, 2019, p.119, tradução própria).

No entanto, dada a sua incidência nos documentos securitários cibernéticos, a Equipe de Resposta a Emergências de Computadores da Ucrânia (CERT-UA) é o órgão que mais se destaca dentro do SSSCIP, também a nível de cooperação internacional (KOSTYUK, 2015). A força-tarefa, criada em 2007, muito antes da aprovação da Estratégia de Segurança Cibernética da Ucrânia, é uma divisão especializada da Derzhspetszviazok que atua como coordenadora técnica de “órgãos estaduais, órgãos de governo autônomo local, formações

militares, empresas, instituições e organizações, independentemente da titularidade, na prevenção, detecção e eliminação dos efeitos de incidentes cibernéticos" (CENTRE FOR GLOBAL STUDIES, 2019, p. 12, tradução própria).

O aprimoramento e direcionamento do CERT-UA parecem refletir o atual cenário de manutenção das tensões com a Rússia. Segundo a pesquisadora Kostyuk (2015), a equipe tem se enfocado nos últimos anos quase exclusivamente no conflito com o país vizinho. Para fazer frente às ameaças, a Ucrânia tem-se aproximado cada vez mais das diretrizes ocidentais, como nos indicam alguns dos autores abordados neste trabalho, mais notadamente Giles (2015), Mearsheimer (2018), Gierczak (2020).

Os documentos oficiais também indicam um esforço de adequação às diretrizes ocidentais - parte dos regulamentos abordados incluem o aprimoramento e adequação do CERT-UA como uma prioridade. Notadamente, a Lei da Ucrânia "Sobre o Serviço de Estado para Comunicações Especiais e Proteção de Informações da Ucrânia", a Lei da Ucrânia "Sobre Princípios Básicos de Segurança Cibernética da Ucrânia", e a Estratégia de Segurança Cibernética (CERT-UA, s.d.).

O CERT-UA é especialmente interessante no nosso caso porque é através desta agência que grande parte das interações operacionais com parceiros estrangeiros e organizações internacionais têm-se dado. É importante destacar os esforços da OTAN e da UE, que têm adequado suas políticas através da cooperação entre o Computer Emergency Response Team (CERT-EU), do lado da UE, e pelo Computer Incident Response Capability (NCIRC) da OTAN (CENTRE FOR GLOBAL STUDIES, 2019). E no caso da UE e da Ucrânia, os incentivos para a adequação do CERT-UA têm-se dado sobretudo através da Parceria Oriental (COMISSÃO EUROPEIA, 2017).

Apesar do SSSCIP assumir um papel especializado a nível de regulação e proteção cibernéticas, o mais alto órgão de coordenação é o Centro Nacional de Coordenação de Segurança Cibernética, que é uma das ramas de atuação do Conselho de Segurança e Defesa Nacional (CNDS) (UCRÂNIA, 2021), assumindo a responsabilidade pela realização, coordenação e controle das atividades dos atores do Setor de Segurança e Defesa. As decisões do Conselho e as medidas tomadas pelos órgãos que coordena podem ter impacto em todos os demais atores envolvidos na oferta de cibersegurança, tornando efetivamente o Conselho, em última instância, o coordenador geral de implementação da Estratégia Cibernética. O Centro

Nacional de Coordenação de Segurança Cibernética (UCRÂNIA, 2021), por sua vez é composto por destacáveis atores políticos:

• Primeiro Vice ou Vice-Ministro da Defesa da Ucrânia

• Chefe do Estado-Maior General das Forças Armadas da Ucrânia

• Chefe do Serviço de Segurança da Ucrânia

• Chefe do Serviço de Inteligência Estrangeira da Ucrânia

• Chefe da Polícia Nacional da Ucrânia

• Chefe do Banco Nacional da Ucrânia

• Chefe da Direção Principal de Inteligência do Ministério da Defesa da Ucrânia

• Chefe do Gabinete de Inteligência da Administração do Serviço Estatal de Guarda de Fronteiras da Ucrânia

• Chefe do Serviço de Estado de Comunicações Especiais e Proteção Informacional da Ucrânia (SPÎNU, 2020, p. 7, tradução própria).

Em seu artigo sobre o sistema cibernético ucraniano, Streltsov (2017) elenca as principais atribuições do Centro Nacional de Coordenação de Segurança Cibernética, destacando "a análise do estado da cibersegurança e adequação dos diversos parâmetros da Estratégia; prognóstico e detecção de ameaças cibernéticas; desenvolvimento, implementação e supervisão de propostas de medidas de segurança cibernética (incluindo medidas de troca de informações entre atores e medidas de cooperação internacional), etc".

Apesar da centralidade de algumas agências governamentais, é válido dizer que atualmente os atores envolvidos na segurança cibernética e informacional da Ucrânia abrangem diversas áreas. A Figura 5 destaca que o setor privado também atua através das organizações de proteção de dados, dos gestores de infraestrutura, dos fornecedores de comunicação eletrônica, das entidades educacionais e de pesquisa, e através da própria sociedade civil.

4.4 PARCERIAS ATUAIS

Ao longo da crise geopolítica que já perdura por quase uma década, a realização do NUC tem-se mantido. Este ano, em janeiro de 2022, o secretário-geral Jens Stoltenberg recebeu a vice-primeira-ministra da Ucrânia para a Integração Europeia e Euro-Atlântica, Olga Stefanishyna, na sede da OTAN para uma reunião da Comissão OTAN-Ucrânia (NUC), focada em propor respostas ao contínuo desenvolvimento militar da Rússia (OTAN, 2022). Além desta última edição do NUC, conforme indicado anteriormente através do relatório do Centre for Global Studies (2015), têm-se realizado consultas anuais regulares da Comissão em vista das ameaças diretas enfrentadas pela Ucrânia à sua integridade territorial, independência política e segurança.

A guerra da Rússia com a Geórgia em 2008 acendeu alertas à UE em relação aos países da região e, segundo Pridham (2014), montava-se à época um cenário propício ao conflito em algum futuro próximo. Embora a UE às vezes parecesse relutante em admiti-lo. Desde a criação da Parceria Oriental, em 2008, visando fomentar a associação política e a integração econômica dos países da região (CONSELHO EUROPEU, 2022), tem havido extenso diálogo incluindo a Ucrânia, que mais tarde, em 2019, viria a se tornar, juntamente com outros países do Leste Europeu, parceira no projeto conjunto da União Europeia e do Conselho da Europa.

Intitulado “Cybersecurity EAST”, o projeto tinha como objetivo “desenvolver mecanismos técnicos e de cooperação que aumentassem a segurança cibernética e a preparação contra ataques cibernéticos, de acordo com os padrões da UE”, e possui atualmente uma dimensão regional, envolvendo todos os países da Parceria Oriental (ou seja, Armênia, Azerbaijão, Bielorrússia, Geórgia, República da Moldávia e Ucrânia) (UNIÃO EUROPEIA s.d.).

Como vimos, a nível de colaboração multilateral, a UE orienta-se na região principalmente através das diretrizes da Parceria Oriental e, mais recentemente, através Documento de Trabalho Conjunto dos Serviços, criado no âmbito da Parceria Oriental e intitulado “20 resultados para 2020” (em inglês “20 Deliverables for 2020: Bringing tangible results for citizens”), onde, na seção de Segurança, dos dez grupos das tarefas a serem cumpridas, três dizem respeito à cibersegurança, em particular, à “criação de unidades

operacionais de pleno direito para combater o cibercrime, ao desenvolvimento da cooperação público-privada e à cooperação internacional no domínio da cibersegurança'" (CENTRE FOR GLOBAL STUDIES, 2019, p. 16, tradução própria).

O canal de diálogo aberto pela Parceria Oriental envolveu, de um lado, parte da infraestrutura de atores da UE, como a Europol, a Comissão Europeia, Estados Membros, e do outro, os países parceiros supracitados, e os seus respectivos CERTs (Equipe de Resposta a Emergências de Computadores). O aprimoramento do CERT-UA, uma das principais equipes de monitoramento de riscos cibernéticos ucranianas, foi facilitado pela parceria (COMISSÃO EUROPEIA, 2017)

De acordo com a especialista em segurança cibernética ucraniana, Natalia Spînu (2020), o campo cibernético demonstra de maneira explícita a dependência da Ucrânia nos seus parceiros estratégicos ocidentais. Atualmente, pese aos esforços, há um problema considerável de coordenação interinstitucional na cooperação entre os setores público e privado - que, apesar de existente, encontra-se em um estágio inicial de desenvolvimento. Esse é um ponto importante, porque os esforços dos parceiros financiadores (notadamente OTAN e UE) dependem do nível de coordenação entre as agências ucranianas - e justamente o país enfrenta desafios porque carece de incentivos financeiros para atrair os melhores especialistas para trabalhar para o governo.

Como pôde-se observar, a OTAN também tem feito esforços de cooperação securitária com a Ucrânia, mais especificamente enfocando em estratégias que englobam pautas como mudanças na legislação, desenvolvimento de estratégias e políticas, fornecimento de apoio prático ao desenvolvimento de infraestrutura técnica e preparação e desenvolvimento da capacidade de defesa cibernética - notadamente através do Fundo Fiduciário para Defesa Cibernética, de 2014, e do Pacote de Assistência Abrangente, aprovado em 2016 (OTAN, 2022). Além disso, Spînu (2020) destaca que a Ucrânia tornou-se o principal beneficiário do Programa de Cooperação Científica para a Paz e Segurança (SPS). A autora destaca o papel da OTAN como financiadora do projeto:

> A OTAN alocou 2,2 milhões de euros para a cooperação SPS com a Ucrânia em 2014, contribuindo para um total projetado de 10 milhões de euros em 2014-2017. A assistência inclui o estabelecimento de um Centro de Gestão de Incidentes (IMC) para monitorar eventos de segurança cibernética, bem como laboratórios para investigar incidentes de segurança cibernética, juntamente com treinamento no uso desta tecnologia e equipamentos. O Serviço de Segurança da Ucrânia está assumindo o papel principal no quadro do Fundo Fiduciário, com o parceiro da OTAN, a Romênia, como a nação líder, com contribuições financeiras e adicionais

> da Albânia, Estônia, Hungria, Itália, Portugal, Turquia e os Estados Unidos. Juntamente com os parceiros da OTAN, a Ucrânia realizou exercícios e treinamento de defesa cibernética, onde todas as partes interessadas nacionais relevantes foram treinadas sobre como reagir a grandes ataques cibernéticos à infraestrutura de defesa nacional (SPÎNU, 2020, p. 11, tradução própria).

Spînu (2020) relata, no entanto, que os dois principais parceiros cibernéticos da Ucrânia alertam para a necessidade de ainda mais adaptação dos postulantes a beneficiários às suas normas securitárias. Isso porque, apesar dos esforço, na prática, a atuação ucraniana no domínio da cibersegurança tem estado separada da atuação da da UE e da OTAN, principalmente a nível de assistência prática - uma vez que este tipo de assistência demanda uma maior adequação aos princípios da UE-NATO de cooperação em cibersegurança - que inclui desde questões de ordem política, como instituições, legislações, adequação jurídica, até questões mais práticas do campo cibernético, como "certificação de software, o processo de comunicação e a introdução de padrões de responsabilização por ações no ciberespaço" (CENTRE FOR GLOBAL STUDIES , 2015, p. 16).

Autores como Mearsheimer (2014) enxergam nesses esforços de cooperação e de financiamento uma tentativa de tirar definitivamente a Ucrânia da órbita de Moscou e incorporá-la ao Ocidente. Entretanto, o autor tem alertado há anos sobre o potencial risco advindo de uma expansão rumo ao leste. Desde 2008, quando se sinalizou durante o Summit de Bucareste o interesse em conceder à Geórgia e à Ucrânia o Membership Action Plan (MAP), documento que prepara as nações para a adesão à OTAN, a Rússia tem se posicionado em diversas ocasiões afirmando que não estaria disposta a aceitar que os dois países aderissem sem que houvesse consequências. Além disso, o posicionamento da OTAN e os esforços de financiamento na região parecem refletir diretamente os interesses geopolíticos estadunidenses, visto que diferentes administrações - tanto democratas, como republicanos - têm-se preocupado em manter a expansão da Aliança rumo ao Leste como uma maneira de assegurar os interesses estadunidenses na região (MEARSHEIMER, 2014).

4.5 A GUERRA COMO PROPULSORA DO PROCESSO DE HIPER-SECURITIZAÇÃO CIBERNÉTICA?

As opiniões estão divididas sobre se o que está acontecendo dentro e ao redor da Ucrânia pode ou deve ser chamado de guerra cibernética. Como argumenta Jan Stinissen

(2015), as operações cibernéticas atuais não atendem a uma definição legal estrita de estado de guerra. Mas, ao mesmo tempo, de acordo com outros autores abordados, as operações na Ucrânia de fato contêm alguns elementos bélicos.

Apesar dos extensos registros de ataques cibernéticos envolvendo alvos ucranianos desde o início da "guerra cibernética", em 2013, e a sua escalada em 2022, no início da fase mais recente da invasão russa da Ucrânia, as operações cibernéticas parecem ter desempenhado um papel menos proeminente na estratégia russa mais ampla do que se poderia prever. Devanny (2022) avalia que ainda é cedo para avaliar quais fatores mais contribuíram para isso, porém o autor destaca, dentre outros, a "defesas cibernéticas ucranianas aprimoradas" e a "assistência de atores estrangeiros e corporativos;" (DEVANNY, 2022, p. 42, tradução própria).

Outros especialistas corroboram a tese de que a defesa da Ucrânia poderia estar por detrás do aparente silêncio cibernético russo, como aponta Villar-Lopes (2022, apud. OGLOBO, 2022). O professor destaca que a falta de danos mais sérios advindos de ataques cibernéticos não significa que estes não estejam ocorrendo, apenas que os ataques russos não têm tido sucesso em obstruir o vizinho pela via cibernética. Também parece-nos indicar, segundo o pesquisador, que a resiliência ucraniana parece ser bem-sucedida, ao menos na esfera cibernética (VILLAR-LOPES, 2022, apud. OGLOBO, 2022).

Como vimos no subcapítulo 3.3.2, a Rússia foi uma das pioneiras em incorporar o campo cibernético à uma estratégia mais ampla, que envolveu o conceito de "guerra híbrida". Giles (2015) defende que a postura russa impulsionou a transformação do ambiente de segurança na Europa Central e Oriental, tirando a maioria dos países de um estado de "inércia estratégica". Mais do que isso, a OTAN foi revitalizada, e o recrudescimento da postura russa reativou os objetivos centrais da organização, que encontravam-se relativamente dormentes desde a queda da União Soviética, em 1991 (GILES, 2015, p. 27, tradução própria). Giles (2015) ainda destaca que a postura ucraniana de desvincular-se politicamente da Rússia a aproximou da Europa e do Ocidente, através de um forte esforço de adequação aos valores e interesses ocidentais, incompatíveis com os da Rússia. O Ocidente, por sua vez, tem insistido em apoiar os vizinhos da Rússia na afirmação de suas soberanias.

O confronto com a Rússia, portanto, é o resultado de duas posições e visões de mundos em muitos aspectos incompatíveis. Isso também implica o reconhecer que o conflito que se estende desde 2014, e que tem incorporado elementos cibernéticos, não é uma

aberração nas relações entre Rússia e o Ocidente. O autor sustenta que “em vez disso, são os 25 anos anteriores de relativa quietude que eram a exceção à regra. (..) Na vizinhança da Rússia, o novo normal é um retorno aos velhos hábitos” (GILES, 2015, p. 28, tradução própria).

Como pôde-se observar através do estudo dos documentos oficiais ucranianos, o recrudescimento do conflito na Ucrânia tem sido o principal potencializador da doutrina cibernética do país. No entanto, ainda é muito cedo para se chegar a uma conclusão definitiva em relação à eficácia do sistema cibernético ucraniano frente às potenciais ameaças cibernéticas. Giles (2015) destaca que a abordagem cibernética ocidental adotada pela Ucrânia normalmente se concentra em respostas técnicas a ameaças técnicas, desconsiderando amplamente a interface com a guerra de informação em sentido amplo - como a Rússia tem feito.

> Essa abordagem é provavelmente insuficiente para quando surgir uma crise de segurança nacional, pois nesse ponto não haverá um confronto “cibernético puro”. Em outras palavras, o Ocidente pode estar bem preparado para a guerra cibernética, mas os eventos na Ucrânia mostram que também precisa estar preparado para a guerra de informações quando as operações cibernéticas são usadas como facilitador ou vetor de ataque (GILES, 2015, p. 27).

4.6 CONCLUSÕES PRELIMINARES

A análise dos ataques sofridos pela Ucrânia nos leva a algumas conclusões. Podemos começar pontuando que os ataques visando infraestruturas críticas e entidades estratégicas do governo são potencialmente muito perigosos. No entanto, até o momento, a Rússia não tem sido capaz de encabeçar ações cibernéticas mais contundentes, capazes de fugir da lógica do “trilema subversivo” explorado por Maschmeyer (2021). Outra alternativa, talvez igualmente válida, é a de que a Ucrânia tem sido capaz de fazer frente a tais ameaças com sucesso, neutralizando as ações mais danosas.

Essa última hipótese é reforçada pelo salto regulatório dado pela Ucrânia a partir de 2014, incluindo revisões de documentos críticos e estratégias de defesa cibernética e informacional. Esses documentos atualmente regulam as funções e estruturas dos atores cibernéticos do país, que incluem desde órgãos de defesa do setor público a entidades econômicas, como é o caso do Banco Central e agentes do setor privado.

Também pôde-se analisar as parcerias atuais no campo cibernético. Isso porque a influência da OTAN e da UE continuam a ser importantes à evolução do campo cibernético no país. Um exemplo concreto é o projeto Cybersecurty East, que tem servido desde 2019 como fonte de desenvolvimento técnico e cooperação direta. No entanto, as entidades supracitadas mantêm uma postura firme de exigência de mais adaptação por parte da Ucrânia, tanto às legislações dos países membros, mas também de adequação às questões mais práticas do ciberespaço.

Por fim, pode-se afirmar que a Rússia tem sido de fato o principal motivador das mudanças regulatórias pelas quais tem passado a Ucrânia nos últimos anos. No entanto, ainda é cedo para medir a extensão do sucesso defensivo da Ucrânia na seara cibernética.

5 CONCLUSÃO

Essa monografia buscou abordar quais as respostas estratégicas da Ucrânia frente às ameaças cibernéticas que o país tem enfrentado. Parte-se do suposto, portanto, que as medidas estratégicas tomadas pelo país nessa seara são influenciadas pelo entorno geopolítico. Para sustentar esta hipótese, procurou-se analisar não só a relação da Ucrânia com os seus vizinhos mais importantes - Rússia, EU e OTAN - mas também buscou-se trazer ao debate os resultados práticos do imbróglio existente entre a Rússia e o Ocidente, do qual a Ucrânia faz parte. Além da tentativa de se analisar em que medida as operações cibernéticas que têm a Ucrânia como alvo têm sido eficazes no objetivo de servirem como ferramenta bélica.

A fim de responder o problema de pesquisa, o Capítulo 1 começa por primeiramente definir o campo cibernético e alguns dos seus conceitos e componentes mais importantes, destacando o caráter político que esse campo tem assumido cada vez mais. Notadamente, as operações cibernéticas têm servido como importante ferramenta de sabotagem, mas, além disso, elas têm assumido um caráter subjetivo, ao servir como importante meio de manipulação da opinião pública.

Apesar das limitações operacionais enfrentadas pelas operações cibernéticas, a Rússia tem assumido a dianteira ofensiva, contabilizando uma série de ataques contra a Ucrânia. E além disso, a Rússia tem-se esforçado em exercer também uma espécie de soft power em diferentes níveis, envolvendo sobretudo a sociedade civil. A ideia é recuperar a Ucrânia como zona de influência histórica, frente às mudanças na condução da política externa ucraniana, que afetou negativamente a relação com a ex-república soviética.

Acontece que esse conflito geopolítico entre a Ucrânia e a Rússia não é o resultado de uma relação bilateral prejudicada pelo processo de independência daquele país, senão de um conflito maior envolvendo o Ocidente e a Rússia. Os protestos do Maidan, em 2014, podem ser observados como um estopim político que visou medidas mais contundentes. Esse posicionamento popular teria enorme impacto no posterior posicionamento da Ucrânia - cada vez mais favorável à adesão do país à União Europeia.

Apesar da predisposição de ambos os lados, a incorporação da Ucrânia ainda enfrenta resistência e pode levar anos, sobretudo devido à delicada situação com a Rússia, que insiste na sua visão do eurasianismo de enxergar a Ucrânia como importante zona de influência russa

que deve ser mantida como estado tampão frente às crescentes expansões da OTAN e da UE. Esse posicionamento tem colaborado com o recrudescimento do papel cibernético na guerra híbrida em curso.

Sabe-se que a Rússia é uma das principais potências cibernéticas da atualidade. Porém, como pontuado, não há nenhuma comprovação de que, de fato, a Rússia tenha dado protagonismo às operações cibernéticas nas ações contra a Ucrânia. Não se observou, por exemplo, ataques contundentes capazes de obstruir o fornecimento de serviços ou afetar as infraestruturas críticas. Inclusive na invasão do Donbass e da Península da Crimeia as operações cibernéticas não foram decisivas para o sucesso russo. Pelo menos não como se observou em outros momentos históricos, como por exemplo à ocasião dos ataques cibernéticos à Estônia e à Geórgia, respectivamente em 2007 e 2008, em que as operações cibernéticas de fato assumiram maior importância.

Porém, defende-se que a ausência de ataques mais contundentes não demonstra que a Rússia não tenha capacidade cibernética. De momento, suas ações cibernéticas parecem refletir uma decisão cautelosa, de não envolver toda a gama de capacidades cibernéticas, ao mesmo tempo em que incluem as operações cibernéticas como parte de uma campanha subversiva maior mirando a Ucrânia como um todo (MASCHMEYER, 2021). Pode que futuramente se descubra que de fato houve ataques de autoria russa que passaram despercebidos, devido à própria configuração do ciberespaço (LIBICKI, 2015). Outra tese é a de que estes ataques podem ter acontecido, mas que têm sido efetivamente neutralizados pelo sistema de defesa cibernético ucraniano. De todos modos, até o momento nenhum dos lados declarou abertamente o ciberespaço como parte central ou integral do conflito (PAST, 2015)

Outro enorme desafio enfrentado pela Ucrânia e outros países é o de se definir uma fronteira mais concisa do ciberespaço, que colabore com a soberania, ao mesmo tempo que mantém as liberdades individuais. Isto é, o desafio aqui é conciliar a manutenção das liberdades civis com o recrudescimento das políticas mirando definir os limites das ações dentro das redes.

O Capítulo 2 focou em explorar a evolução do campo cibernético ucraniano em si. Para realizar tal missão, começou-se por fazer uma rápida análise de onde a Ucrânia se situa frente ao conflito dissimulado envolvendo o Ocidente e a Rússia. Apesar do posicionamento da política externa ucraniana não ter sido sempre um consenso dentro do país, marcadamente desde o governo de Viktor Yushchenko, o país tem adotado oficialmente um discurso

pró-Ocidente, buscando distanciar-se cada vez mais da Rússia - a nível político, cultural e econômico.

Como não há um governo mundial para proteger os estados uns dos outros, as grandes potências são extremamente sensíveis a ameaças - especialmente perto de suas fronteiras - e às vezes agem impiedosamente para lidar com perigos potenciais. O direito internacional e as preocupações com os direitos humanos ficam em segundo plano quando questões vitais de segurança estão em jogo. Neste cenário, o Ocidente tem poucas opções para infligir dor à Rússia, enquanto Moscou tem muitas cartas para jogar contra a Ucrânia e o Ocidente. A mudança de postura em relação à Ucrânia e o seu papel como um importante fornecedor de gás são algumas das cartas das quais dispõe a Rússia neste momento. Não surpreendentemente, a maioria dos europeus não está muito entusiasmada com o emprego de sanções contra a Rússia. Mas mesmo que o Ocidente imponha custos significativos ao país, é improvável que Putin recue. Quando interesses vitais estão em jogo, os países invariavelmente estão dispostos a sofrer grandes dores para garantir sua segurança, e não há razão para pensar que a Rússia, dada a sua história, seja uma exceção.

Não só teóricos, mas também autoridades de outros países, como é o caso do Ex-Secretário de Estado dos EUA, Henry Kissinger (2022), apontam para a incapacidade, até o momento, do Ocidente fomentar uma aproximação com os ex-países soviéticos da região que ao mesmo tempo seja capaz de apaziguar as tensões com a Rússia, que vem alertando desde a queda da URSS acerca dos perigos de um movimento mais contundente da OTAN e da UE rumo ao leste. Tanto que a queda do ex-presidente do país, Viktor Yanukovich, em 2014, e a sinalização de adesão ao bloco econômico, foram dois dos principais estopins que resultaram na ocupação da Crimeia naquele mesmo ano, acompanhada do esforço que perdura de desestabilizar a Ucrânia até que ela abandone sua disposição em se aproximar do Ocidente (MEARSHEIMER, 2014).

Apesar da inexistência de um consenso quanto à solução ao conflito atual, alguns autores abordados defendem a manutenção da Ucrânia como estado neutro entre Oriente e Ocidente, o que implicaria um claro posicionamento dos Estados Unidos em não interferir nas futuras eleições ucranianas ou simpatizar com um governo anti-russo em Kiev. Além da garantia de futuros governos ucranianos em respeitarem os direitos das minorias, especialmente em relação ao status do russo como língua oficial. No entanto, dada a impossibilidade a curto prazo de uma resolução às tensões existentes, a manutenção do atual

cenário tem culminado em uma série de normativas regulatórias visando aprimorar a capacidade de resposta operacional do campo cibernético ucraniano.

Destaca-se o fato de que, até a invasão da Crimeia, havia pouca legislação que abordasse a questão cibernética no país (KOSTYUK, 2015). Porém, dada a enorme herança de infraestruturas soviéticas, já em 1996, quando da promulgação da Constituição Ucraniana, o país já mostrava certa preocupação em zelar pela segurança informacional, propondo normativas incipientes que serviriam de base para uma série de mudanças posteriormente.

Porém, a contribuição mais importante da Constituição de 1996 foi o destaque à predisposição do país em integrar o Ocidente, "confirmando a identidade europeia do povo ucraniano e a irreversibilidade do curso europeu e Euro-Atlântico da Ucrânia, esforçando-se para desenvolver e fortalecer um Estado democrático, social e baseado no direito" (UCRÂNIA, 1996). Essa postura serviria como base para a posterior aprovação de acordos e esforços junto à OTAN e a UE, incluindo um dos mais importantes - a ratificação da Convenção Internacional sobre Cibercrime, ou Convenção de Budapeste, firmado no âmbito do Conselho da Europa em 2005.

Uma análise da evolução do campo cibernético do país envolve necessariamente uma análise dos principais documentos oficiais promulgados pelo país visando regular a segurança cibernética e informacional. Destaca-se que a a Lei "Sobre a Fundamentos da Segurança Nacional da Ucrânia" de junho de 2003 foi a responsável por criar as bases para a posterior ratificação da Estratégia Nacional de Segurança da Ucrânia, da Estratégia de Segurança Cibernética da Ucrânia e da Doutrina Militar da Ucrânia, que viriam a ser aprovados por decreto anos mais tarde. Outros documentos abordados que serviram como base às atuais legislações incluem a Reforma do Serviço de Segurança da Ucrânia, aprovada por Decreto do Presidente da Ucrânia em decisão do Conselho de Segurança e Defesa Nacional da Ucrânia, em fevereiro de 2008, a Nova Versão da Estratégia de Segurança Nacional da Ucrânia e a Nova Versão da Doutrina Militar da Ucrânia, ambas aprovadas por Decreto Presidencial em 2012.

A predisposição ideológica frente à adesão ao curso europeu e Euro-Atlântico, sinalizada já em 1996, foi reforçada com o recrudescimento do conflito e das ameaças russas. Tanto que em matéria de cibersegurança, a agressão da Rússia contra a Ucrânia tem servido como um impulso adicional para aprofundar a interação da tríade Ucrânia-OTAN-UE, mantendo-se projetos conjuntos e encontros regulares entre os envolvidos.

A manutenção de um posicionamento intransigente, tanto por parte da Rússia, como também por parte do Ocidente da Ucrânia não tem levado a um arrefecimento das tensões. O terceiro capítulo busca abordar a série de tentativas de obstruções e sabotagem de setores críticos ucranianos que foram registradas notadamente a partir de 2014 - a maioria de autoria russa. Essas ações contribuíram para o processo de constituição da atual configuração do campo regulatório cibernético do país. Os principais documentos que atualmente regulam o campo incluem a Doutrina de Segurança da Informação da Ucrânia e o Projeto de Lei sobre os Fundamentos da Prestação de Segurança Cibernética da Ucrânia, ambos aprovados em 2017, a Lei da Ucrânia "Sobre Segurança Nacional", de 2018, a Estratégia de Segurança Nacional de 2020 e a outorgação da decisão do Conselho Nacional de Segurança e Defesa da Ucrânia (CNDS) em renovar a Estratégia de Segurança Cibernética, em 2021.

Além disso, o capítulo destaca os principais atores cibernéticos do país e os seus respectivos papéis securitários. Neste caso, é o Conselho Nacional de Segurança e Defesa da Ucrânia o órgão responsável pela coordenação cibernética. Este, por sua vez, é respaldado por atores de diferentes áreas estratégicas, incluindo a estrutura de defesa do país, o setor de contrainteligência, os agentes aplicadores da lei, os reguladores da proteção técnica e o setor privado.

Frente a um campo cibernético cada vez mais consolidado, as operações cibernéticas tendem a ficar aquém de sua promessa estratégica e oferecem utilidade limitada. Pelo menos até o momento, o que nos leva a repensar não só a eficácia e utilidade das operações, mas também o prazo dos seus resultados. Maschmeyer (2021) destaca que a real medição do impacto das ações cibernéticas pode levar décadas em se concretizar, dada a configuração subversiva do campo cibernético, que invariavelmente ainda recai na lógica do "trilema subversivo".

Para concluir, destaca-se a excepcionalidade do período compreendido pelos anos posteriores à queda da União Soviética, e antecessores à invasão da Crimeia. A tendência atual é a volta do "novo normal", em que a Rússia crescentemente busca restabelecer parte da sua influência na região. A análise dos documentos oficiais ucranianos confirma que o recrudescimento do conflito com o vizinho tem sido o principal potencializador da sua doutrina cibernética. No entanto, apesar de ser cedo para se chegar a uma conclusão definitiva em relação à eficácia do sistema cibernético ucraniano frente às potenciais ameaças

cibernéticas, pode-se atribuir parte do insucesso das operações russas a um campo securitário cibernético cada vez mais desenvolvido.

Apesar dos avanços, o campo cibernético ucraniano enfrenta alguns desafios. A abordagem cibernética adotada pela Ucrânia tende a se concentrar em respostas técnicas a ameaças técnicas, desconsiderando a guerra de informação em sentido amplo e a incorporação da seara cibernética a uma estratégia securitária mais ampla, como a Rússia tem feito (GILES, 2015). Além disso, autores como Spînu (2020) destacam que atualmente o campo cibernético ainda se encontra dominado por abordagens departamentais, que dificultam a interação e coordenação adequadas entre as agências envolvidas. Atualmente, por exemplo, há um problema considerável de coordenação interinstitucional na cooperação entre os setores público e privado. Esse é um ponto importante porque o envolvimento da OTAN e UE na seara cibernética do país depende do nível de coordenação entre as agências ucranianas e também porque o campo cibernético demonstra de maneira explícita a dependência da Ucrânia nos seus parceiros estratégicos ocidentais.

Dentre os principais desafios a serem superados daqui adiante podemos citar aqueles presentes na atual Estratégia de Cibersegurança e que incluem a melhoria da segurança das redes e dos sistemas de informação, a introdução de um sistema de gestão de risco, a criação das condições para fornecer recursos, incluindo a cibersegurança humana, o aprimoramento da infraestrutura crítica operacional e de segurança cibernética, o combate ao cibercrime, o uso de recursos de parceria público-privada e a interação das partes interessadas para abordar questões de segurança cibernética e defesa cibernética.

REFERÊNCIAS

BARINI, Filipe. O Exército de TI da Ucrânia: Kiev monta defesa, mas Rússia ainda não usou seu potencial cibernético. **OGlobo**. 2022. Disponível em: https://oglobo.globo.com/mundo/ucrania-convocou-exercito-de-ti-contra-acoes-ciberneticas-russas-mas-moscou-ainda-nao-usou-seu-potencial-na-guerra-atual-25428642. Acesso em: 01 de nov. de 2022.

BELLA, Timothy. Kissinger says Ukraine should cede territory to Russia to end war. **The Washington Post**. 24 de maio de 2022. Disponível em: https://www.washingtonpost.com/world/2022/05/24/henry-kissinger-ukraine-russia-territory-davos/. Acesso em: 01 de nov. de 2022.

BROWN, Chris; ECKERSLEY, Robyn: The Oxford Handbook of International Political Theory. *In:* VALERIANO, Brandon; MANESS, Ryan. **International relations theory and cyber security: Threats, conflicts, and ethics in an emergent domain.**

BUCHHOLZ, Katharina. **Will NATO Expand North?** Statista, 11 de maio de 2022. Disponível em: https://www.statista.com/chart/26674/european-countries-by-year-of-joining-nato/. Acesso em: 03 de outubro de 2022.

BUGAYOVA, Nataliya. How We Got Here With Russia: The Kremlin's Worldview. Washington: Institute for the Study of War and the Critical Threats Project.. Março de 2019. Disponível em: https://www.understandingwar.org/sites/default/files/ISW%20Report_The%20Kremlin%27s%20Worldview_March%202019.pdf. Acesso em: 31 de out. de 2022.

CATTLER, David; BLACK, Daniel. The Myth of the Missing Cyberwar: Russia’s Hacking Succeeded in Ukraine—And Poses a Threat Elsewhere,Too. Foreign Affairs, 6 de abril de 2022. Disponível em: https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar

CENTRE FOR GLOBAL STUDIES, “Strategy XXI”. **Ukraine – EU – NATO Cooperation for Countering Hybrid Threats in the Cyber Sphere**. Kiev, 2019. Disponível em: http://www.encouncil.org/wp-content/uploads/2019/10/ENG-Ukraine-EU-NATO-cooperation-to-counter-hybrid-threats-in-cyber-sphere.pdf. Acesso em: 31 de out. de 2022.

CERT-UA, Computer Emergency Response Team of Ukraine. **About CERT-UA**. Sem data. Disponível em: https://cert.gov.ua/about-us. Acesso em: 31 de out. de 2022.

CHATTURVEDI, J. C. **Political Governance: Comparative Politics**. Volume 2. Delhi: Isha Books, 2005.

CHEREPANOV, Anton. TeleBots are back: Supply-chain attacks against Ukraine. Welivesecurity. **ESET**. 03 de jun. 2017. Disponível em: https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/. Acesso em: 31 de out. de 2022.

CLAUSEWITZ,Carl Von. **On War**. Princeton: Princeton University Press, 1984.

COMPUTER EMERGENCY TEAM OF UKRAINE. **About CERT-UA**. Disponível em: https://cert.gov.ua/about-us. Acesso em: 01 de nov. de 2022.

CONSELHO SUPREMO DA UCR NIA (VERKHOVNA RADNA). **Lei da Ucrânia sobre os Princípios Básicos de Cibersegurança da Ucrânia**, Nº 2163-VIII. Lex: Vedomosti Verkhovnoi Rady (VVR), 2017, № 45, p.403. Publicado no site oficial do Conselho Supremo da Ucrânia. Disponível em: https://zakon.rada.gov.ua/laws/show/2163-19#Text. Acesso em 27 jun. 2022.

CONSELHO EUROPEU. The Budapest Convention on Cybercrime: benefits and impact in practice. **Cybercrime Convention Committee**. Strasbourg, 13 de jul. de 2020. Disponível em: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac. Acesso em 17 de oct. de 2022.

CPI Group (UK) Ltd, Oxford Univeristy Press, Nova York, março de 2018. p. 259-272.

DEVANNY, Joe; GOLDONI, Luiz Rogerio Franco; MEDEIROS, Breno Pauli. Strategy in an Uncertain Domain: Threat and Response in Cyberspace. **Journal of Strategic Security** 15, nº2, 2022, p. 34-47. Disponível em: https://digitalcommons.usf.edu/jss/vol15/iss2/3. Acesso em: 31 de out. de 2022.

ERIKSSON, Johan; GIACOMELLO, Giampiero. The Information Revolution, Security, and International Relations: (IR)relevant Theory?. Sage Publications. **International Political Science Review**, Vol 27, No. 3, 221-244, 2016. Disponível em: http://www.jstor.org/stable/20445053. Acesso em: 31 de out. de 2022.

EU4DIGITAL. Cybersecurity East. 2019. **União Europeia.** Disponível em: https://eufordigital.eu/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/. Acesso em: 04 de oct. de 2022.

EUROPEAN COUNCIL. **East Partnership.** 2022. Disponível em: https://www.consilium.europa.eu/en/policies/eastern-partnership/. Acesso em: 04 de oct. de 2022.

EUROPEAN UNION EXTERNAL ACTION. Cyberspace: EU and Ukraine launch dialogue on cyber security. **União Europeia**, Bruxelas, 2021. Disponível em: https://www.eeas.europa.eu/eeas/cyberspace-eu-and-ukraine-launch-dialogue-cyber-security_en. Acesso em: 04 de oct. de 2022.

EUROPEAN COMISSION. High Representative of the Union for Foreign Affairs and Security Policy. Joint Staff Working Document. **Eastern Partnership** - 20 Deliverables for 2020: Focusing on Key Priorities and Tanglible Results. Bruxelas. 09 de jun. de 2017. Disponível em: https://ec.europa.eu/neighbourhood-enlargement/eastern-partnership-20-deliverables-2020-focusing-key-priorities-and-tangible-results_en. Acesso em: 04 de oct. de 2022.

FLURI, Philipp; KOZIEL, Marcin; YERMOLAIEV, Andrii. The Security Sector Legislation of Ukraine. Segunda Edição. Kiev: **Center for Army, Conversion and disarmament studies**, 2013. Disponível em: https://www.dcaf.ch/sites/default/files/publications/documents/Book_LAW-engl_PRESS.pdf. Acesso em 17 de oct. de 2022.

GEERS, Kenneth. Cyberwar in Perspective: Russian Aggression against Ukraine. *In:* **GILES, Keir. Russia and Its Neighbours: Old Attitutes , New Capabilities.** NATO CCD COE Publications, Tallinn, 2015. p. 19-28. Disponível em:

https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Acesso em: 01 de nov. de 2022.

GEERS, Kenneth. Cyberwar in Perspective: Russian Aggression against Ukraine. *In:* **KOSTYUK, Nadiya. Ukraine: A Cyber Safe Haven**?. NATO CCD COE Publications, Tallinn, 2015. p. 113-122. Disponível em: https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Acesso em: 01 de nov. de 2022.

GEERS, Kenneth. Cyberwar in Perspective: Russian Aggression against Ukraine. *In:* **LEWIS, James A. 'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine**. NATO CCD COE Publications, Tallinn, 2015. p. 39-47. Disponível em: https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Acesso em: 01 de nov. de 2022.

GEERS, Kenneth. Cyberwar in Perspective: Russian Aggression against Ukraine. *In:* **STINISSEN, Jan. A Legal Framework for Cyber Operations in Ukraine**. NATO CCD COE Publications, Tallinn, 2015. p. 123-134. Disponível em: https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Acesso em: 01 de nov. de 2022.

GEERS, Kenneth. Cyberwar in Perspective: Russian Aggression against Ukraine. *In:* **LIMNÉLL, Jarno. Northern European Cyber Security in Light of the Ukraine War.** NATO CCD COE Publications, Tallinn, 2015. p. 145-151. Disponível em: https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Acesso em: 01 de nov. de 2022.

GEERS, Kenneth. Cyberwar in Perspective: Russian Aggression against Ukraine. *In:* **WIRTZ, James J. Cyber War and Strategic Culture: The Russia Integration of Cyber Power into Grand Strategy.** NATO CCD COE Publications, Tallinn, 2015. p. 29-37. Disponível em: https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Acesso em: 01 de nov. de 2022.

GEERS, Kenneth. Cyberwar in Perspective: Russian Aggression against Ukraine. *In:* **WEEDON, Jen. Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine**. NATO CCD COE Publications, Tallinn, 2015. p.

67-77. Disponível em: https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Acesso em: 01 de nov. de 2022.

GEERS, Kenneth. Cyberwar in Perspective: Russian Aggression against Ukraine. *In:* **LIBICKI, Martin. Beyond 'Cyber War': The Cyberwar That Wasn't**. NATO CCD COE Publications, Tallinn, 2015. p. 49-54. Disponível em: https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Acesso em: 01 de nov. de 2022.

GEERS, Kenneth. Cyberwar in Perspective: Russian Aggression against Ukraine. *In:* **PAST, Liisa. Missing in Action: Rhetoric on Cyber Warfare**. NATO CCD COE Publications, Tallinn, 2015. p. 49-54. Disponível em: https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Acesso em: 01 de nov. de 2022.

GEERS, Kenneth. Cyberwar in Perspective: Russian Aggression against Ukraine. *In:* **SAKKOV, Sven. Cyberwar in Perspective: Russian Aggression against Ukraine.** NATO CCD COE Publications, Tallinn, 2015. p. 8-11. Disponível em: https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/. Acesso em: 01 de nov. de 2022.

GIERCZAK, Bartosz. The Russo-Ukrainian Conflict. **Manhattan College**. p. 2- 33, maio de 2020. Disponível em: https://www.researchgate.net/publication/349948624_The_Russo-Ukrainian_Conflict. Acesso: 23 de out. de 2022.

KAGUBARE, Ines; MITCHELL, Ellen. Finland, Sweden's NATO moves prompt fears of Russian cyberattacks. **The Hill**. 14 de maio de 2022. Disponível em: https://thehill.com/policy/cybersecurity/3488518-finland-swedens-nato-moves-prompt-fears-of-russian-cyber-attacks/. Acesso em 17 de out. de 2022.

KUZIO, Taras. The Long and Arduous Road: Ukraine Updates Its National Security Strategy. **Royal United Services Institute**, 16 de out. de 2020. Disponível em: https://rusi.org/explore-our-research/publications/commentary/long-and-arduous-road-ukraine-updates-its-national-security-strategy. Acesso em: 31 de out. de 2022.

LAKOMY, Miron. 2016. “The Game of Ukraine: Conflict in Donbass as an Outcome of the Multilayered Rivalry.” Politeja 6. University of Silesia, Katowice, p. 280-315. Disponível em: https://doi.org/10.12797/Politeja.13.2016.45.13. Acesso em: 31 de out. de 2022.

MARTIN-VEGUE, Tony. Are we witnessing a cyber war between Russia and Ukraine? Don't blink - you might miss it. **Cyber Security for Business Leaders.** CSO Online. 24 de abr. de 2015. Disponível em: https://www.csoonline.com/article/2913743/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html

MASCHMEYER, Lennart. The Subversive Trilemma: Why Cyber Operations Fall Short of Expectation. President and Fellows of Harvard College and the Massachusetts Institute of Technology. **International Security**, Vol. 46, Nº2, 2021, p. 51–90, https://doi.org/10.1162/isec_a_00418.

MEARSHEIMER, John J. Why the Ukraine Crisis Is the West’s Fault: The Liberal Delusions That Provoked Putin. **Foreign Affairs.** 2014. Disponível em: https://www.mearsheimer.com/wp-content/uploads/2019/06/Why-the-Ukraine-Crisis-Is.pdf. Acesso em 04 jul. 2022.

MEARSHEIMER, John J. Getting Ukraine Wrong. The New York Times. The Opinion Pages. 13 de março de 2014. Disponível em: http://www.nytimes.com/2014/03/14/opinion/getting-ukraine-wrong.html?_r=0. Acesso em: 28 de nov. de 2022.

MEDEIROS, Breno P.; GOLDONI, Luiz R. F. The Fundamental Conceptual Trinity of Cyberspace. **Contexto Internacional**, vol. 42(1). Jan. de 2020.

NORMAN, Laurence. Zelensky Asks EU to Admit Ukraine as a Member. **The Wall Street Journal.** 28 de fev. de 2022. Disponível em: https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-02-28/card/zelensky-asks-european-union-to-admit-ukraine-as-a-member-CpG7RvYKhrSZ9RGF21yp. Acesso em 31 de out. de 2022.

NORTH ATLANTIC TREATY ORGANIZATION. **Relations With Ukraine.** 23 de set. de 2022. Disponível em: https://www.nato.int/cps/en/natohq/topics_37750.htm. Acesso em: 01 de nov. de 2022.

NORTH ATLANTIC TREATY ORGANIZATION. **Parternship for Peace Programme**. 23 de março de 2020. Disponível em: https://www.nato.int/cps/en/natolive/topics_50349.htm. Acesso em: 01 de nov. de 2022.

NORTH ATLANTIC TREATY ORGANIZATION**. NATO-Ukraine Commission.** 01 de set. de 2022. Disponível em: https://www.nato.int/cps/en/natohq/topics_50319.htm. Acesso em: 01 de nov. de 2022.

NORTH ATLANTIC TREATY ORGANIZATION**. Tratado do Atlântico Norte.** Washington, EUA. 4 de abril de 1949. Disponível em: https://www.nato.int/cps/su/natohq/official_texts_17120.htm?selectedLocale=pt. Acesso em: 01 de nov. de 2022.

NORTH ATLANTIC TREATY ORGANIZATION. **Relations with the European Union.** 26 de jul. de 2022. Disponível em: https://www.nato.int/cps/en/natohq/topics_49217.htm#:~:text=27%20EU%20member%20countries%3A%20Austria,%2C%20Slovenia%2C%20Spain%2C%20Sweden. Acesso em: 01 de nov. de 2022.

NORTH ATLANTIC TREATY ORGANIZATION. **NATO-Ukraine Commission meets at the start of "an important week for European security**. 10 de jan. de 2022. Disponível em: https://www.nato.int/cps/en/natohq/news_190540.htm

NOVA ZELÂNDIA. What is the Budapest Convention?. **New Zealand Government: Cybersecurity**. 15 de jul. de 2022. Disponível em: https://consultations.justice.govt.nz/policy/budapest-convention/user_uploads/1.-what-is-the-budapest-convention.pdf. Acesso em 17 de oct. de 2022.

OĞUZ, Şafak. **NATO's Mistakes That Paved The Way For Russia-Ukraine Crisis. Gazi University.** Faculty of Economical and Administrative Sciences. Deptment Of International Relations. Bahar, 2015.

O'NEILL, Patrick H. Russian hackers tried to bring down Ukraine's power grid to help the invasion. **MIT Technology Review**. 12 de abril de 2022. Disponível em: https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/. Acesso em: 01 de nov. de 2022.

PAGLIUSI, Paulo S. Guerra Cibernética Russo-Ucraniana – Lições para o Brasil e o Mundo. **Paulo Pagliusi**. 21 de mar. de 2022. Disponível em: http://www.pagliusi.com.br/2022/03/guerra-cibernetica-russo-ucraniana.html. Acesso em: 01 de nov. de 2022.

PARLAMENTO EUROPEU. **European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties**. Estrasburgo, França. 23 de nov. de 2016. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html. Acesso em: 01 de nov. de 2022.

PAVEL, Kazarin. Be afraid of your desires. **Crimea Realities**. 23 de abril de 2015. Disponível em: https://ru.krymr.com/a/26973631.html. Acesso em: 31 de out. de 2022.

PIFER, Steven. Ukraine, NATO, and Russia. **Center for International Security and Cooperation, Stanford University**, Volume 19, Número 2. Set. de 2020. Disponível em: https://fsi.stanford.edu/news/ukraine-nato-and-russia. Acesso em: 31 de out. de 2022.

PINTO, Danielle J. A.; FREITAS, Rita S.; PAGLIARI, Graciela C. Fronteiras Virtuais: Um Debate Sobre Segurança e Soberania do Estado. *In:* AYRES PINTO, Danielle J., et. al. **Fronteiras Comtemporâneas Comparadas: Desenvolvimento, Segurança e Cidadania**. Livro Coletânea, Universidade Federal do Amapá, Macapá, 2018. p. 39-52.

PRIDHAM, Geoffrey. EU/Ukraine Relations and the Crisis with Russia, 2013-14: A Turning Point. **The International Spectator**: Italian Journal of International Affairs, Londres. 12 de dec. 2014. Disponível em: https://www.tandfonline.com/doi/full/10.1080/03932729.2014.965587. Acesso em: 01 de nov. de 2022.

PRZETACZNIK; Jakub. TARPOVA, Simona. EUROPEAN PARLIAMENT: Russia's war on Ukraine: Timeline of cyber-attacks. **European Union**, 2022. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf. Acesso em: 04 de oct. de 2022.

RID, Thomas. **Cyber War Will Not Take Place**. Nova Iorque: Oxford University Press, 2013.

RÚSSIA. Address by the President of the Russian Federation. **The Kremlin**, Moscou, 21 de fev. de 2022. Disponível em: http://en.kremlin.ru/events/president/news/67828. Acesso em: 17 de out. de 2022.

SPÎNU, Natalia. Ukraine Cybersecurity: Governance Assessment. **Geneva Centre for Security Sector Governance**, Geneva, nov./2020. Disponível em: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf. Acesso em 27 jun. 2022.

STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE. **About the SSSCIP**. 01 jun 2022. Disponível em: https://cip.gov.ua/en/statics/pro-derszhpeczv-yazku. Acesso em 01 de nov de 2022.

SINOVETS, Polina; RENZ, Bettina. Russia's 2014 Military Doctrine and beyond: threat perceptions, capabilities and ambitions. **Research Division, NATO Defense College**, Roma, Número 117. Jul. de 2015.

SANTAYANA, José Pardo. Why is Russia so interested in Ukraine?. Instituto Español de Estudios Estratégicos. **Analysis Paper 25/2021**. 09 de maio de 2021. Disponível em: http://www.ieee.es/Galerias/fichero/docs_analisis/2021/DIEEEA25_2021_JOSPAR_Rsia_ENG. Acesso em: 31 de out. de 2022.

STRELTSOV, Lev. The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. **European Journal for Security Research**, p. 147–184, 2017. Disponível em: https://doi.org/10.1007/s41125-017-0020-x. Acesso em: 31 de out. de 2022.

SAUVAGE, Grégoire. Did NATO 'betray' Russia by expanding to the East?. **France24**. 30 de jan. de 2022. Disponível em: https://www.france24.com/en/russia/20220130-did-nato-betray-russia-by-expanding-to-the-east

STONE, John. **Cybewar Will Take Place!**. Department of War Studies , King's College. Journal of Strategic Studies, 2013. London, UK

SEEBECK, Lesley. Why the fifth domain is different. **Australian Strategic Policy Institute**, 5 de set. de 2019. Disponível em: <https://www.aspistrategist.org.au/why-the-fifth-domain-is-different/>. Acesso em: 16 de maio de 2022.

SHERR, James. Nothing New Under the Sun? Continuity and Change in Russia Policy towards Ukraine. **International Centre for Defence and Security**. Tallin: ICDS, julho de 2020. Disponível em: https://icds.ee/wp-content/uploads/2020/07/ICDS_EFPI_Report_Nothing_New_Under_the_Sun_Sherr_July_2020.pdf

TRIPATHI, Nikhil; MEHTRE, Babu. **DoS and DDoS Attacks: Impact, Analysis and Countermeasures.** School of Computer and Information Sciences Hyderabad Central University Institute for Development and Research in Banking Technology. Dez. de 2013, Hyderabad, Índia. Disponível em: https://www.researchgate.net/publication/259941506_DoS_and_DDoS_Attacks_Impact_Analysis_and_Countermeasures?enrichId=rgreq-d382ec4f0e72690a299a00d8fb449cb9-XXX&enrichSource=Y292ZXJQYWdlOzI1OTk0MTUwNjtBUzo5NzM0NzA1Mjc2OTI4MkAxNDAwMjIwNzU1NDAx&el=1_x_2&_esc=publicationCoverPdf. Acesso em: 31 de out. de 2022.

THE ECONOMIST. **War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?**. 1 de jul. de 2010. Disponível em: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain. Acesso em: 31 de out. de 2022.

UNIÃO EUROPEIA. EU4DIGITAL. Eastern Partnership. **União Europeia.** S.d. Disponível em: https://eufordigital.eu/discover-eu/eastern-partnership/. Acesso em: 04 de oct. de 2022.

UCRÂNIA. Constituição da Ucrânia de 1996. Kiev, Ucrânia. Disponível em: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text. Acesso em: 01 de nov. de 2022.

UCRÂNIA. **Decreto do Presidente da Ucrânia nº 96/2016**, de 15 de mar. de 2016. Decisão do Conselho Nacional de Segurança e Defesa da Ucrânia de 27 de jan. de 2016 "Sobre a Estratégia de Segurança Cibernética". Lex: Decreto do Presidente P. Poroshenko da Ucrânia nº 96/2016, publicado no site oficial do Presidente da República. Disponível em: https://zakon.rada.gov.ua/laws/show/96/2016#Text. Acesso em 27 jun. 2022.

UCRÂNIA. **Ministério de Energia e Carvão**. S.d. Disponível em: http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=245086886. Acesso em: 01 de nov. de 2022.

UCRÂNIA. **Decreto do Presidente da Ucrânia nº392/2020**, de 14 de set. de 2020. On the decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine. Lex: Decreto do Presidente Volodymyr Zelenskyy da Ucrânia nº 392/2020 Kiev, 14 de set. de 2020, publicado no site oficial do Presidente da República. Disponível em: https://zakon.rada.gov.ua/laws/show/392/2020#Text. Acesso em: 01 de nov. de 2022.

UCRÂNIA. **Decreto do Presidente da Ucrânia nº 447/2021**, de 14 de maio de 2021. Decisão do Conselho Nacional de Segurança e Defesa da Ucrânia "Sobre a Estratégia de Segurança Cibernética". Lex: Decreto do Presidente Volodymyr Zelenskyy da Ucrânia nº 447/2021, publicado no site oficial do Presidente da República. Disponível em: https://www.president.gov.ua/documents/4472021-40013. Acesso em 27 jun. 2022.

UCRÂNIA. **Sobre a decisão do Conselho Nacional de Segurança e Defesa da Ucrânia datada de 15 de fevereiro de 2008** "Sobre o Conceito de Reforma do Serviço de Segurança da Ucrânia". Kiev, 20 de março de 2008. Disponível em: https://zakon.rada.gov.ua/laws/show/249/2008#Text. Acesso em: 01 de nov. de 2022.

UCRÂNIA. **Decreto do Presidente da Ucrânia nº 287/2015**, de 26 de maio de 2015. On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 "On the National Security Strategy of Ukraine". Lex: Decreto do Presidente P. Poroshenko da Ucrânia nº 47/2017, Kiev. Publicado no site oficial do Presidente da República. Disponível em: https://www.president.gov.ua/documents/472017-21374. Acesso em 27 jun. 2022.

UCRÂNIA. **Decreto do Presidente da Ucrânia nº 47/2017,** de 25 de fevereiro de 2017. "On the Information Security Doctrine of Ukraine". Lex: Decreto do Presidente P. Poroshenko da Ucrânia nº 287/2015, Kiev. Publicado no site oficial do Presidente da República. Disponível em: https://www.president.gov.ua/documents/472017-21374. Acesso em: 01 de nov. de 2022.

UCRÂNIA. Lei da Ucrânia. **Sobre os fundamentos da segurança nacional da Ucrânia**. Verkhovna Rada da Ucrânia (VVR), Nº 39, Artigo 351, 2003. Disponível em: https://zakon.rada.gov.ua/laws/show/964-15#Text. Acesso em: 17 de oct. de 2022.

UCRÂNIA. THE LAW OF UKRAINE: **About the main principles of ensuring cyber security of Ukraine**. Information of the Verkhovna Rada (VVR), 2017, No. 45, Article 403), de 5 de out. de 2017. Disponível em: https://zakon.rada.gov.ua/laws/show/2163-19#Text

UCRÂNIA. **Ministério de Energia e Carvão da Ucrânia**. Міненерговугілля має намір утворити групу за участю представників усіх енергетичних компаній, що входять до сфери управління Міністерства, для вивчення можливостей щодо запобігання несанкціонованому втручанню в роботу енергомереж. Міністерство енергетики України. 12 de fev. de 2022. Disponível em: http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=245086886

VALERIANO, Brando; MANESS, Ryan C. **Russia's Coercive Diplomacy**: Energy, Cyber, and Maritime Policy as New Sources of Power. Palgrave MacMillan, 2015.

ZWOLSKI, Kamil. **European Security in Integration Theory:** Contested Boundaries. Palgrave MacMillan, 2018.

ZETTER, Kim. Хакерська атака Росії на українську енергосистему: як це було. **TEXTY.ORG.UA.** 17 de mar. de 2016. Disponível em: https://texty-org-ua.translate.goog/articles/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak-66125/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=wapp. Acesso em: 01 de nov. de 2022.