UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE FILOSOFIA E CIENCIAS HUMANAS
DEPARTAMENTO DE CIÊNCIA POLÍTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA POLÍTICA

FERNANDO HENRIQUE CASALUNGA

GUERRA HÍBRIDA CIBERNÉTICA:

Uma análise do conflito Rússia-Ucrânia (2014-2015) sob a perspectiva da tecnologia da informação

Recife
2020

FERNANDO HENRIQUE CASALUNGA

GUERRA HÍBRIDA CIBERNÉTICA:

Uma análise do conflito Rússia-Ucrânia (2014-2015) sob a perspectiva da tecnologia da informação

Dissertação apresentada ao Programa de Pós-graduação em Ciência Política do Centro de Filosofia e Ciências Humanas, Universidade Federal de Pernambuco como parte dos requisitos parciais para obtenção do título de mestre em Ciência Política.

Área de concentração: Relações Internacionais

Orientador: Prof. Dr. Marcos Aurélio Guedes Oliveira

Recife

2020

Catalogação na fonte
Bibliotecária Valdicéa Alves Silva, CRB4-1260

C334g Casalunga, Fernando Henrique.
Guerra híbrida cibernética : uma análise do conflito Rússia-Ucrânia (2014-2015) sob a perspectiva da tecnologia da informação / Fernando Henrique Casalunga. – 2020.
103 f. : il. ; 30 cm.

Orientador : Prof. Dr. Marcos Aurélio Guedes Oliveira.
Dissertação (mestrado) - Universidade Federal de Pernambuco, CFCH. Programa de Pós-Graduação em Ciência Política, Recife, 2020.
Inclui referências.

1. Ciência Política. 2. Tecnologia da informação. 3. Cibernética. 4. Sistemas de informação. 5. Segurança nacional – Rússia. 6. Hackers. . I. Oliveira, Marcos Aurélio Guedes (Orientador). II. Título.

320 CDD (22. ed.) (BCFCH2020-067)

FERNANDO HENRIQUE CASALUNGA

GUERRA HÍBRIDA CIBERNÉTICA:

Uma análise do conflito Rússia-Ucrânia (2014-2015) sob a perspectiva da tecnologia da informação

Dissertação apresentada ao Programa de Pós-graduação em Ciência Política do Centro de Filosofia e Ciências Humanas, Universidade Federal de Pernambuco como parte dos requisitos parciais para obtenção do título de mestre em Ciência Política

Aprovado em: 20/02/2020

BANCA EXAMINADORA

Prof° Dr. Marcos Aurélio Guedes de Oliveira (Orientador)

Universidade Federal de Pernambuco

Prof° Dr. Ricardo Borges Gama Neto (Examinador Interno)

Universidade Federal de Pernambuco

Prof° Dr. João Policarpo Rodrigues Lima (Examinador Externo)

Universidade Federal de Pernambuco

A minha querida mãe Cleonice Aparecida Casalunga, pelo apoio e dedicação.

A minha amada Natália Diniz Schwether, pelo companheirismo e respeito.

A minha avó Zelina Gonçalves que, por motivo de força maior, acompanha a finalização desta dissertação de um lugar mais tranquilo que o nosso (*in memorian*).

Dedico.

AGRADECIMENTOS

Ao orientador e amigo, Prof. Dr. Marcos Aurélio Guedes de Oliveira, pela competência e respeito com que conduziu este processo, do alvorecer da ideia até a sua síntese.

Aos professores Dr. Adriano Oliveira e Dr. Ricardo Borges, pelas valiosas contribuições durante toda minha trajetória neste departamento, desde a Graduação, passando pelo Exame de Qualificação até a conclusão do curso de Mestrado.

Aos queridos amigos que acompanham minha trajetória acadêmica desde muito: Natália Schwether e Kinn Peduti.

À Fundação de Amparo à Pesquisa do Estado de Pernambuco pela concessão da bolsa de mestrado e apoio financeiro para a realização desta pesquisa.

Um estado mafioso é mais perigoso do que uma superpotência comunista porque a ideologia não é mais o guarda-roupa da política, mas sim um conjunto de acessórios intercambiáveis e contraditórios (WEISS, 2014, p. 5).

RESUMO

O desenvolvimento da tecnologia da informação aumentou sobremaneira a preocupação dos Estados contemporâneos com a Segurança e Defesa cibernética. Apesar das medidas tomadas para proteção de dados e infraestruturas de rede, analistas indicam que, em geral, é grande a vulnerabilidade dos sistemas de informação. Levando em conta a crescente escalada de conflitos entre os países no espaço cibernético, este estudo utiliza como base o conceito de Guerra Híbrida para delinear uma possível ligação entre a estratégia de expansão de poder regional do estado da Rússia e os ataques cibernéticos ocorridos durante o recente conflito desencadeado entre este país e a Ucrânia (2014-2015). Utiliza, à luz da mudança institucional na estratégia da Política de Defesa e Segurança da Rússia, as técnicas de análise documental historiográfica, dependência da trajetória e rastreamento de processos para demonstrar a complexidade das operações conjuntas entre as forças especiais russas e hackers civis, bem como a sofisticação das principais ameaças utilizadas nos ataques cibernéticos. Nesse sentido, objetiva responder ao seguinte questionamento: como a tecnologia da informação amplia a assimetria de poder entre a Rússia e a Ucrânia? Para tanto, evidencia como a guerra híbrida cibernética travada tornou-se chave na desestabilização de territórios e consecução dos interesses russos em seu entorno estratégico.

Palavras-chave: Cibernética. Estratégia. Hacker. Rússia.

ABSTRACT

The development of information technology has greatly increased the concern of contemporary states with cybersecurity and security. Despite measures taken to protect data and network infrastructures, analysts point out that the vulnerability of information systems is generally high. Taking into account the increasing escalation of conflicts between countries in cyber space, this study uses the Hybrid War concept as a basis to delineate a possible link between Russia's regional power expansion strategy and cyber attacks during the recent conflict between this country and Ukraine (2014-2015). It uses, in the light of the institutional change in Russia's Defense Policy and Security Policy, the techniques of historiographic document analysis, trajectory dependency and process tracing to demonstrate the complexity of joint operations between Russian special forces and civilian hackers as well as such as the sophistication of the main threats used in cyber attacks.. In this sense, it aims to answer the following question: how does information technology extend the asymmetry of power between Russia and Ukraine? In order to do so, it shows how the hybrid cyberwar waged became a key in the destabilization of territories and attainment of Russian interests in its strategic environment.

Keywords: Cybernetics. Strategy. Hackers. Russia.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

APT	Ameaça Persistente Avançada
BE	BlackEnergy *Malware*
BB2	BlackEnergy 2 *Malware*
BB3	BlackEnergy 3 – *Malware*
BE.lite	BlackEnergy Lite *Malware*
CEC	Comissão Central de Eleições da Ucrânia
CEI	Comunidade de Estados Independentes
CERT-UA	Equipe de Resposta a Emergências de Computador da Ucrânia
CIM	Complexo Industrial Militar
D-DOS	Negação de Serviço
EUA	Estados Unidos da América
E-ISAC	Centro de Análise e Compartilhamento de Informações setor de Energia
FSB	Serviço de Segurança da Federal da Federação Russa
GHC	Guerra Híbrida Cibernética
GRU	Departamento de Inteligência Militar da Federação Russa
ICS-CERT	Sistema de Controle Industrial para Ciber Emergências
KD	KillDisk *Malware*
OCX	Organização para Cooperação de Xangai
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
OSCE	Organização de Segurança e Cooperação na Europa
OTSC	Organização do Tratado de Segurança Coletiva
PCO	Processo Causal Observável

PIB	Produto Interno Bruto
SANS	Sistema de Controle Industrial
SCADA	Sistema de Supervisão e Aquisição de Dados
UE	União Europeia
UEE	União Econômica da Eurásia

SUMÁRIO

1 INTRODUÇÃO

No âmbito internacional, o avanço da tecnologia da informação amplia a preocupação dos atores políticos e entidades privadas com questões concernentes à vulnerabilidade dos sistemas de informação a ataques externos, tais operações impõem novos desafios no âmbito aos Estados modernos. Em vista disso, a guerra regional entre Rússia-Ucrânia (2014-2015) é tratada como a crise de segurança mais importante desde o fim da Guerra Fria.

Provocada, por um lado, pela reformulação, ao longo dos últimos anos, dos principais documentos quer versam sobre a política de Defesa e Segurança da Federação Russa, e, por outro, pela reação do Kremlin frente ao estreitamento dos laços diplomáticos entre a Ucrânia e o Ocidente (CROWDSTRIKE, 2015; LOOKINGGLASS, 2015; USAOC, 2015). As evidências revelam que este conflito é o maior exemplo de uma guerra híbrida, que combina estratégias militares, econômicas e políticas para atingir os objetivos de um determinado Estado em território inimigo (LIMNÉLL, 2015, p. 521).

Nossa análise do conflito parte do pressuposto de que com o avanço das tecnologias da informação o ciberespaço se tornou fulcral para projeção de poder do Estado em seu entorno regional. Desse modo, intentamos demonstrar que a evolução da estratégia, somada a manifesta capacidade de atuação da agencia nesse ambiente, ofereceu vantagem considerável à Rússia para consecução de seus interesses estratégicos durante o conflito regional que eclodiu em território ucraniano.

Destarte, identificamos que mudança institucional russa, levada à cabo pela reformulação dos principais documentos quer versam sobre a Política de Defesa e Segurança, quando somada à atuação conjunta entre setores especiais das Forças Armadas russas e hackers civis, produziu o fenômeno da guerra híbrida cibernética (GHC), variante da guerra híbrida, ainda pouco estudado, e, que tem a simbiose hacker-Exército como mecanismo causal responsável por facilitar as operações militares que levaram à anexação do território ucraniano da península da Crimeia e apoiaram os movimentos separatistas que se formaram na região leste em Donbass, ampliando assim, em última instância, a assimetria de poder regional entre esses dois países.

Ao abordar o funcionamento do mecanismo que conecta as mudanças institucionais aos níveis tático e operacional militar do Estado russo, objetivamos responder ao seguinte questionamento: como a tecnologia da informação amplia a assimetria de poder entre a Rússia e a Ucrânia?

Ao analisar o conflito entre Rússia e Ucrânia (2014-2015) este estudo utiliza de modo concomitante três técnicas metodológicas de análise qualitativa orientada para estudo de caso '*within-case*'.

A técnica historiográfica de análise documental para comparar alguns dos principais documentos oficiais que versam sobre o emprego da estratégia de Defesa e Segurança da Federação Russa em seu entorno regional no intuito de indicar a dinâmica dos retornos crescentes no que concerne a incorporação da tecnologia de informação ao processo de mudança institucional revelado por estes documentos; a técnica de avaliação da dependência da trajetória para identificar pontos de inflexão nos eventos observados durante o conflito que possuem ligação direta com o fenômeno da GHC; e, por fim, a técnica de rastreamento de processos para testar as condições -necessária e suficiente- que ajudam a explicar o fenômeno que permitiu a consecução dos interesses estratégicos da Rússia neste conflito.

A fim de sustentar a validade da inferência descritiva que será construída, o ponto chave deste estudo será verificar se a simbiose entre hackers-Forças especiais atua como mecanismo causal que conecta o processo de mudança institucional da estratégia russa de atividade em seu entorno regional ao nível operacional e tático de ação no conflito desencadeado contra a Ucrânia (2014-2015), produzindo o fenômeno da GHC.

Destarte, o estudo presta-se a dois propósitos: 1) inferir a existência de um evento ou fenômeno observável, neste caso a GHC; 2) identificar o funcionamento mecanismo de conexão causal entre o evento e o processo de mudança institucional da estratégia e tática operacional russa em seu entorno estratégico com atenção especial ao emprego da tecnologia de informação no conflito.

A pertinência deste estudo é marcada ao elucidar como o processo de mudança institucional na estratégia de ação de um Estado contemporâneo em seu entorno regional quando somada a operações militares altamente sofisticadas, proporcionadas pelo avanço da tecnologia de informação, ampliam sobremaneira as capacidades de projeção de poder deste ente. Frente a isso, acreditamos contribuir para o avanço do debate sobre o impacto do emprego de novas tecnologias da informação em conflitos contemporâneos.

Inicialmente, a primeira seção apresenta os conceitos e o desenho de pesquisa que sustentam a análise desta dissertação.

Em seguida, a segunda analisa o processo de mudança pelo qual passaram as principais instituições responsáveis pela Defesa e Segurança da Federação Russa comparando

os documentos oficiais que versam sobre a Estratégia de Segurança Nacional e a Doutrina Militar.

Na sequência, a terceira, com atenção especial ao emprego da tecnologia de informação para consecução dos interesses estratégicos da Rússia em seu entorno regional, identifica o modo de operação de grupos hackers, as principais ameaças cibernéticas utilizadas e os principais alvos atingidos no conflito, a procura de evidências que permitam comprovar a hipótese de que as operações foram permeadas pela ação coordenada entre esses atores não estatais e agentes das forças especiais russas.

Finalmente, a partir da análise das evidências encontradas, no que se refere ao uso da tecnologia da informação em ataques cibernéticos durante o conflito, a quarta discute os resultados e revela o fenômeno da GHC como estratégia eficaz e consoante aos objetivos militares e geopolíticos expansionistas da Rússia.

2 DESENVOLVIMENTO

O desenvolvimento desta dissertação divide-se em quatro seções: a primeira apresenta o referencial teórico, aborda a construção do conceito de guerra híbrida, em específico, sua vertente cibernética e apresenta em detalhes o desenho de pesquisa empregado a partir de técnicas de análise qualitativa para estudos de caso único; a segunda analisa e compara os documentos oficiais que versam sobre Política de Defesa e Segurança Nacional da Federação Russa; a terceira apresenta uma breve descrição do contexto que envolve o conflito entre Rússia e Ucrânia e identifica a utilização do ciberespaço nas operações que empregam a ação conjunta entre atores estatais e não estatais como fator chave para o aumento da assimetria de poder entre estes países, por fim, a quarta seção apresenta e discute os resultados da pesquisa.

2.1 Conceitos

2.1.1 Guerra Híbrida, Guerra Cibernética e Guerra Híbrida Cibernética

Com o fim da Guerra Fria diversos conceitos foram propostos na tentativa de se explicar a realidade dos conflitos contemporâneos, em meio aos avanços tecnológicos e novos ambientes de ação. Termos como guerra tradicional, composta e de quarta geração, fundiram-se em um grande guarda-chuva teórico conceitual denominado guerra híbrida. Classificação que surge para preencher a lacuna conceitual existente.

O termo guerra híbrida tornou-se chave na descrição da interconexão entre as ações de agentes estatais e/ou não-estatais nos conflitos contemporâneos, desde o nível estratégico até o operacional. Porém, foi, ao mesmo tempo, responsável por produzir uma confusão na esfera acadêmica civil e militar.

Neste sentido, Chuka (2014) identifica que problemas na definição de termos que estão na base do conceito de guerra híbrida conduzem a imprecisão analítica dos processos de mudança nas estruturas institucionais que ocorrem frente aos novos desafios enfrentados pelos Estados contemporâneos. Tampouco este é um problema trivial, autores como Hoffman, Mansoor e Murray, cientes dos efeitos negativos produzidos na compreensão da guerra contemporânea e futura, protagonizaram importantes embates sobre a falta de rigor intelectual e precisão histórica da realidade e das justificativas defendidas por acadêmicos nesse campo.

Examinando de modo mais detido os termos que compõem o conceito de guerra híbrida, Hoffman (2007) discute como a guerra contemporânea trouxe mudanças

significativas à compreensão da dinâmica dos conflitos. Em vista disso, identifica que doravante a manifestação da chamada 4ª geração de conflitos não é mais possível aos Estados diferenciarem guerra e paz, combatentes de não combatentes, tal como era feito em sua origem westphaliana (HOFFMAN, 2007, p. 18).

De acordo com a descrição de Hoffman (2007) da quarta geração da guerra, seriam os agentes não-estatais os principais os atores desses conflitos na medida em que ao empregarem uma série de meios convencionais e não convencionais -terrorismo e desinformação- tornam-se capazes de desafiar a vontade do Estado e deslegitimá-lo, estimulando o colapso social interno e provocando sua derrota (HOFFMAN, 2007, p. 18).

Outro conceito discutido por Hoffman (2007) são as guerras compostas, grandes conflitos caracterizados por componentes regulares e irregulares em operações com direção unificada que, em geral, têm como alvos áreas frágeis que ao serem atacadas obrigam forças convencionais a se dispersar (HOFFMAN, 2007, p. 20). Diante desse cenário, "a força convencional geralmente induz o adversário a concentrar-se na defesa ou atingir a massa crítica em operações ofensivas decisivas" (HOFFMAN, 2007, p. 20, tradução nossa). As Grandes Guerras mundiais são exemplos desse tipo de conflito, bem como as guerras napoleônicas, a Guerra Civil norte-americana, a revolta contra o império otomano e a Guerra do Vietnã (HOFFMAN, 2007, p. 20-21).

Não obstante, Hoffman (2007) refere-se, também, ao conceito de guerras irrestritas ou além dos limites, conflitos marcados pela expansão dos domínios da guerra convencional. A guerra além dos limites ocorre quando a "fusão da tecnologia coloca os domínios da política, economia, militares, cultura, diplomacia e religião uns sobre os outros" (LIANG, 1999, *apu*d HOFFMAN, 2007, p. 22, tradução nossa), deixando de ser uma atividade exclusiva da esfera militar.

Diante disso, Hoffman (2007) define um modelo composto por esses conceitos que em sua percepção representa o futuro da guerra, o denominado modelo '*multi-modal*' ou de guerra híbrida[1] combina, portanto, elementos das guerras de quarta geração, composta e irrestrita.

[1] O guarda-chuva teórico conceitual da guerra hibrida conjura, portanto, a nova natureza dos conflitos contemporâneos frente a perda do monopólio da violência do estado da guerra de quarta geração, a omni-dimensionalidade e suas combinações das análises chinesas, o poder das redes, conforme definido por John Arquilla e T.X Hammes, a ideia de sinergia advinda da mistura entre as capacidades convencionais e não convencionais das guerras compostas em um grau de integração e coordenação que se dá entre os níveis micro e macro de uma forma nunca antes observada nos conflitos tradicionais (HOOFMAN, 2007, p. 29).

> As guerras híbridas misturam a letalidade do conflito de estado com o fervor fanático e prolongado da guerra irregular. O termo híbrida captura tanto sua organização quanto seu *modus-operantis*. Organizacionalmente, podem ter uma estrutura política hierárquica, juntamente com células descentralizadas ou unidades táticas em rede. [...] Em tais conflitos, futuros adversários (estados, grupos patrocinados pelo Estado ou atores autofinanciados) exploram o acesso a equipamentos militares modernos, incluindo sistemas de comando criptografados, mísseis de longo alcance, dentre outros sistemas letais [...] Isso inclui estados que combinam emprego de alta tecnologia como armas anti-satélites e ataques cibernéticos (HOFFMAN, 2007, p. 29, tradução nossa).

Todavia, embora seja capaz de descrever a crescente sofisticação e complexificação da agência de atores não-estatais nos conflitos contemporâneos, a exemplo daqueles desencadeados nos territórios da Chechênia, Líbano, Afeganistão e Iraque[2], Kjennerud e Cullen (2016) frisam que ao oferecer atenção à análise da insurgência de grupos terroristas, o modelo de Hoffman (2007) não explica a agência dos Estados nesses conflitos, à vista disso ressaltam que:

> A guerra híbrida do Estado envolve a plena integração dos meios militares e não-militares com o poder do Estado para alcançar objetivos políticos, nos quais o uso da força ou o papel da força desempenham um papel central. Estados com habilidades altamente centralizadas para coordenar e sincronizar seus instrumentos de poder (governo, economia, mídia, etc.) podem criar efeitos multiplicadores de força sinérgica (KJENNERUD; CULLEN, 2016, p. 1).

Sob essa perspectiva, a guerra híbrida pode ser entendida como o uso de todos os instrumentos de poder disponíveis ao Estado para atingir as vulnerabilidades do oponente. O modelo de Kjennerud e Cullen (2016) divide esses instrumentos nas categorias militar, política, econômica, civil e informacional, utilizados de forma sincronizada e coordenada contra os sistemas de infraestrutura crítica do oponente, almejando com isso "uma mudança no estado comportamental ou físico de um sistema ou elementos do sistema, de acordo com os objetivos políticos" dos Estados (KJENNERUD; CULLEN, 2016, p. 1, tradução nossa).

Frente ao exposto, embora o modelo de Hoffman (2007) tenha confirmado um importante aspecto da guerra contemporânea, no que diz respeito à sua composição, enquanto um misto de culturas estratégicas, legados históricos, realidades geográficas e meios

[2] O termo "híbrido" neste contexto de ator não-estatal foi usado para ilustrar como atores tais Hezbollah combinaram as características da guerra convencional e não convencional com outros modos de operação não-militares de modo inovador e inédito que desafiou tanto a prática militar ocidental quanto o pensamento estratégico (KJENNERUD; CULLEN, 2016, p. 1).

econômicos-, cenário no qual superioridade tecnológica é útil, porém insuficiente para conduzir os Estados à vitória sua abordagem excessivamente centrada na agencia de atores não-estatais torna seu modelo pouco atrativo para os propósitos desta dissertação.

Por essa lógica, a avaliação do processo histórico é capaz de dizer muito mais sobre a ação dos Estados em conjunto com atores não-estatais nos conflitos contemporâneos "embora haja um pouco de novidade na guerra híbrida, como um conceito é um meio útil para pensar sobre o passado, o presente e o futuro da guerra" (MANSOOR; MURRAY, 2012, p. 3, tradução nossa)[3].

O modelo analítico de Mansoor e Murray (2012) apresenta o pressuposto de que a guerra híbrida pode ser compreendida como uma combinação de forças militares convencionais e irregulares, atores estatais e não estatais, em prol de um objetivo político comum, podendo se desenvolver em todos os níveis de guerra (estratégico, tático e operacional) (MANSOOR; MURRAY, 2012, p. 3).

Sem embargo, neste modelo as forças militares convencionais conduzem as operações para derrotar oponentes regulares, enquanto que as forças paramilitares fazem uso de recursos interinstitucionais para eliminar as forças irregulares, controlar e pacificar os territórios e organizar a população (MANSOOR; MURRAY, 2012, p. 9).

Outrossim, compreende-se que a guerra híbrida sempre existiu e já ocorria nas décadas passadas, à vista disso, o termo é cunhado como uma explicação para a guerra não convencional, a qual acentuou o uso de expressões como atores híbridos, adversários híbridos, ataques híbridos e ameaça híbrida, abrindo espaço para diferentes fontes de interpretação (BOUJARD, 2016, p. 2).

Apoiados neste interstício da hermenêutica em que se encontra a delimitação do conceito de guerra híbrida, Vaczi (2016) salienta que após a eclosão do conflito entre russos e ucranianos em 2014 agências como a Organização do Tratado do Atlântico Norte (OTAN) publicaram documentos entre 2014 e 2015 nos quais é possível notar a dificuldade da organização em estabelecer um entendimento oficial acerca do conceito.

Nesse sentido, a Declaração de Wales, assinada em setembro de 2014, delimita a guerra híbrida como um conflito "onde uma ampla variedade de medidas militares, paramilitares e civis são empregados em um projeto altamente integrado" (WALES SUMMIT

[3] O termo guerra híbrida é útil para analisar os conflitos que envolvem forças regulares e irregulares que se encontram em combate simétrico e assimétrico. Embora possa haver algumas pequenas diferenças na maneira como os autores definem o termo, essas variações enfatizam ainda mais a complexidade do assunto (MANSOOR; MURRAY, 2012).

DECLARATION, *apud* VACZI, 2016, p. 3-4, tradução nossa). No entanto, ao abordá-lo enquanto "uma cadeia de táticas assimétricas que estão sendo realizadas apenas por meios não-militares e nas quais os meios militares têm apenas um papel de apoio" (VACZI, 2016, p. 23-24, tradução nossa) a definição deste documento deixa passar o papel estratégico do Estado nessa categoria de conflitos. De tal modo que, ao simplificar demais o fenômeno, o conceito perde em precisão, ainda que descreva bem sua essência assimétrica e não convencional (VACZI, 2016, p. 24).

Em vista disso, o Balanço Militar da OTAN (2015) publicado em janeiro de 2016 após dois anos de acompanhamento do conflito entre a Rússia e a Ucrânia pela organização demonstra uma mudança de entendimento do conceito, nele as guerras híbridas foram descritas de modo mais preciso enquanto "campanhas sofisticadas que combinam operações convencionais e especiais de baixo nível; ações cibernéticas e espaciais ofensivas; e operações psicológicas que usam a mídia social e tradicional para influenciar a percepção popular e a opinião internacional" (THE MILITARY BALANCE, 2015, *apud* VACZI, 2016, p. 38, tradução nossa).

Mediante análise dos documentos oficiais da OTAN, Vaczi (2016) identifica que a guerra híbrida, tal como a Rússia a emprega, é marcada pelo uso de guerras regulares e irregulares que combinam de forma coordenada atividades adaptáveis e flexíveis da guerra de diplomacia, informação, econômica e de comunicação estratégica (VACZI, 2016, p. 32). Outrossim, o apoio doméstico e internacional à guerra, conquistado por meio da guerra assimétrica e não linear capaz de criar um ambiente sociopolítico propício à destruição das estruturas econômicas e políticas do oponente é tomado como elemento chave da estratégia russa de ação em seu entorno regional (BERZINS, 2016, *apud* VACZI, 2016, p. 14).

No que tange às ações cibernéticas, a guerra cibernética ocorre mediante ações de espionagem avançada capazes de oferecer informações vantajosas para a tomada de decisão de atores estatais mediante a antecipação de movimentos de seus oponentes no cenário internacional "significa tentar saber tudo sobre um adversário enquanto este não sabe nada sobre nós mesmos. Significa virar o equilíbrio de informação e conhecimento ao nosso favor" (ARQUILLA; RONFELDT, 1997, p. 30, tradução nossa).

Nesta dissertação, na esteira do quadro teórico de Mansoor e Murray (2012), e, em consonância com a análise documental de Vaczi (2016), adotamos um modelo analítico por meio do qual ampliamos o foco da agência para abordar as diretrizes estratégicas, operacionais e táticas empregadas por atores estatais em conjunto com atores não-estatais na

guerra regional entre Rússia e a Ucrânia (2014-2015) sob a perspectiva do uso da tecnologia da informação no conflito.

Sem embargo, nos acercamos dos conceitos de guerra híbrida e guerra cibernética para delinear o conceito de Guerra Híbrida Cibernética (GHC) cunhado a partir da análise do mecanismo que conecta a ação estatal macro com o nível micro de grupos não-estatais, com ênfase na avaliação do processo de mudança institucional dos documentos oficiais que versam sobre a Estratégia Nacional de Segurança (2009; 2015) e a Doutrina Militar (2010; 2015) da Federação Russa e descrição das operações conjuntas realizadas durante o conflito entre as forças especiais russas e hackers civis através do espaço cibernético. Nossa definição alinha-se, igualmente, à visão institucional da OTAN, para a qual o conceito de guerra híbrida descreve:

> [...] uma combinação de meios convencionais, irregulares e assimétricos, incluindo a persistente manipulação de conflitos políticos e ideológicos, podendo incluir a combinação de operações especiais e forças militares convencionais; agentes de inteligência; provocadores políticos; representantes da mídia; intimidação econômica; ataques cibernéticos; '*proxies*'/substitutos, grupos paramilitares, terroristas e criminosos (VACZI, 2016, p. 34).

Frente ao exposto, operacionalizamos o conceito de guerra híbrida para descrever as ações do Estado russo que incluíram o uso de forças estatais para apoio de atores não-estatais insurgentes nos territórios da Criméia e Donbass. Convictos das capacidades manifestas pela Federação Russa para controlar as principais alavancas do poder nacional, força militar, paramilitar, equipamentos e capacidades para conduzir a guerra híbrida no espaço cibernético (CHUKA, 2014).

2.1.2 Ciberespaço, Segurança Cibernética e Ameaças Persistentes Avançadas

O final da Grande Guerra e a vitória dos aliados ocidentais sobre a ameaça totalitária deixou diversos legados, dentre eles, o primeiro domínio artificial inteiramente criado pela ação humana denominado de quinta fronteira, espaço de informação ou ciberespaço. Weiss e Jankauskas (2018) definem o ciberespaço como:

> O domínio das redes de computadores (e dos usuários por trás delas) em que as informações são armazenadas, compartilhadas e comunicadas on-line [...].

> Mas o ciberespaço não é puramente virtual. Ele compreende os computadores que armazenam dados, além dos sistemas e infraestrutura que permitem que ele flua (WEISS; JANKAUSKAS, 2018, p. 4, tradução nossa).

Neste ambiente cibernético as ameaças se multiplicam e modificam dia-a-dia, quase todas as hostilidades envolvem o uso de sofwares maliciosos que são de difícil detecção e rastreamento. Por essa razão, Kello (2013) define o ciberespaço como um ambiente anárquico que oferece ameaças à humanidade em três áreas: físicas, psicológicas e de infraestrutura crítica.

A emergência de uma sociedade amplamente conectada fez com que a importância deste domínio para os Estados se tornasse indiscutível. Por conseguinte, o fracasso na proteção do fluxo de dados via ciberespaço gera problemas que perpassam diferentes segmentos, desde o funcionamento do comércio e do sistema financeiro, a troca de informações entre órgãos públicos até a estabilidade de infraestruturas críticas, acarretando riscos à desestabilização de sociedades inteiras. Nesse sentido, o conceito de segurança cibernética, grosso modo, consiste em adotar medidas para proteger as operações de um sistema de computador ou a integridade de seus dados frente a uma ação hostil (CHOUCRI, 2012, p.39, *apud* WEISS; JANKAUSKAS, p. 4).

Em vista desse novo desafio, a comunidade acadêmica, civil e militar tem se debruçado sobre o problema fundamental da Defesa e Segurança no ciberespaço, a fim de compreender os movimentos da agência de atores estatais e não-estatais no que concerne às estratégias, táticas e operações utilizadas para atuarem no ciberespaço (GARTZKE, 2013; KELLO, 2013, LINDSAY, 2013). Na medida em que a pesquisa científica avança, novos enigmas teóricos emergem, refletindo a complexidade analítica e a dinamicidade do desafio cibernético (LINDSAY, 2015, GEERS; 2015; OLSZEWSKI, 2018; WEISS; JANKAUSKAS, 2019).

Nesse sentido, o campo de estudos sobre Segurança e Defesa cibernética analisa o conjunto de desafios ligados aos sistemas de informação que, cada vez mais, crescem em importância para a segurança interna dos Estados contemporâneos, uma vez que "[...] sistemas de informação de economia, de aprendizagem eletrônica e treino profissional, de gestão do conhecimento e, certamente, todos os componentes de infraestrutura de informação adversário podem ser considerados como alvos cibernéticos" (AZAROV; DODONOV, 2006, p. 7, tradução nossa).

Com pretensão de classificar os dilemas associados à Defesa e a Segurança cibernética, mais especificamente os riscos e as ameaças que circulam no espaço de informação, Weiss e Jankauskas (2018) constroem uma tipologia que se propõe a identificar a realidade fenomenológica da natureza desses problemas e evitar as "ambiguidades das ameaças cibernéticas à segurança nacional" (NYE, 2017, p. 46-49 *apud* WEISS; JANKAUSKAS, 2018, p.4).

Os riscos estariam, então, associados à vulnerabilidade das infraestruturas críticas, instalações físicas, redes, serviços e bens responsáveis por proverem recursos essenciais à vida humana - energia elétrica, gás e água potável -, sistemas altamente integrados interconectados via ciberespaço que podem ter seu funcionamento comprometido por ameaças virtuais (WEISS; JANKAUSKAS, 2019, p. 4-5).

De forma complementar, as ameaças são caracterizadas como os atores e as armas que "têm a capacidade de prejudicar a segurança de outros e que são percebidos por seus alvos potenciais como tendo intenção de fazê-lo" (WALLANDER; KEOHANE, 1999 *apud* WEISS; JANKAUSKAS, 2018, p. 5, tradução nossa). Nomeadas como Ameaças Persistentes Avançadas (APTs) são grupos com alto grau de especialização, alta capacidade de adaptação e recursos para atuarem por muito tempo (WEEDON, 2015). Contudo, embora "originalmente usada para descrever invasões cibernéticas contra organizações militares, a APT evoluiu e não está mais confinada às forças armadas" (OLSZEWSKI, 2018, p. 5, tradução nossa). Esses grupos pertencem a uma nova geração de ameaças que utilizam o ciberespaço para subtrair informações sigilosas que possam ser repassadas a terceiros ou mesmo utilizadas pelos setores de inteligência dos Estados (GARTZKE, 2013, p.70).

Tratam-se, portanto, de atores estatais e não-estatais como espiões, *hackers*, criminosos e terroristas cibernéticos que atuam em esquemas altamente organizados, capazes de orquestrarem ataques sofisticados sem que sua presença seja notada até que a ação tenha ocorrido e os danos causados (CAVELTY, 2013, *apud* WEISS; JANKAUSKAS, 2019, p. 5).

Todavia, para além de representarem ameaças à defesa cibernética das estruturas físicas, as APTs ganharam importância estratégica para essas potências também como ferramentas em operações ofensivas para projeção de poder "eficazes para a infiltração de sistemas de defesa estrangeiros ou roubo de segredos militares, principalmente devido à relativa facilidade de execução, bem como um baixo risco de revelar a fonte real e o beneficiário de tal ataque" (GAJEWSKI, 2013 *apud* OLSZEWSKI, 2018, p. 5, tradução nossa). Frente a esse cenário, antigos soldados cedem espaço aos engenheiros de combate

cibernético, ao mesmo tempo em que a infantaria se converte em invasores de rede, cujas armas principais são computadores munidos por *malwares*[4] (GEERS, 2015).

Essa percepção fomenta o debate sobre como a tecnologia da informação é utilizada em conflitos contemporâneos para ampliar a assimetria de poder entre Estados como a Rússia e a Ucrânia?

Para responder a este questionamento nesta dissertação procuramos identificar se o conflito que simboliza nosso fenômeno de interesse trata-se, de fato, de um exemplo da manifestação do que delimitamos como GHC, ou se representa um confronto de baixa intensidade com pouco potencial para causar danos de longo prazo ao inimigo. Desse modo, adentramos o debate teórico mais recente acerca da constituição deste fenômeno (SHARMA, 2011, GARTZKE, 2013, LINDSAY, 2013, 2015).

Sem embargo, se por um lado, parte dos acadêmicos defende a tese da Revolução nos Assuntos Militares (RMA) baseados na convicção do poder disruptivo produzido pela evolução técnica e tecnológica das capacidades e meios que os Estados contemporâneos dispõem para o conflito. Por outro, uma segunda vertente afirma que o emprego de tais capacidades se restringe aos Estados que dominam a tecnologia necessária para operar no ciberespaço, estando os demais Estados sujeitos à lógica das consequências estratégicas imposta pelo sistema internacional (LINDSAY, 2013, p. 3-4).

Frente a este debate, ao testar os pressupostos teóricos da lógica das consequências para a segurança cibernética em contraponto ao seu aspecto "revolucionário", Lindsay (2013, p. 6) identifica que os fatos empíricos advogam contra a tese de que ataques disruptivos via ciberespaço sejam de fato vantajosos para Estados mais fracos. O modelo de Lindsay (2013) indica que as capacidades cibernéticas i) aumentam o poder marginal de Estados fortes sobre os mais fracos; ii) devido a sua complexidade as ameaças cibernéticas mais eficazes estão restritas aos atores que dominam as tecnologias de informação; iii) as ameaças cibernéticas são mais atrativas do ponto de vista estratégico quando a dissuasão não é possível.

Outrossim, os efeitos dessas ameaças têm se mostrado insuficientes para consecução dos objetivos estratégicos dos Estados quando não são seguidos por ações convencionais de reforço, conduzidas por vias diplomática, econômica e militar que garantam a ampliação sinérgica do efeito da ação cibernética impetrada. Ademais, verifica-se uma correlação

[4] Definição de *malware*: termo utilizado para designar um software projetado para interferir na funcionalidade do computador ou para degradar a integridade dos dados. Engloba uma gama de códigos de computador maliciosos -vírus, worms, trojan, spyware, adware, etc-. Pode ser projetado para fornecer acesso a um sistema de computador adversário, e/ou para atacá-lo (KELLO, 2013, p. 18).

positiva entre o efeito dissuasório das operações ofensivas conduzidas no ciberespaço e a enorme disparidade entre as capacidades das grandes potências e os demais Estados que compõem o sistema internacional (GARTZKE, 2013).

Em linhas gerais, Lindsay (2013) argumenta que os ataques às infraestruturas são raros devido aos problemas que podem produzir ao mundo físico em termos de conflitos declarados entre os Estados. Assim sendo, se restringirmos o conceito da GHC ao uso de redes de computadores para atacar às infraestruturas físicas de um oponente com objetivo de conquistar ganhos políticos e estratégicos para o Estado agressor, então o fenômeno torna-se vantajoso para os entes que se encontram na vanguarda do desenvolvimento da tecnologia da informação e que contam com forças convencionais suficientes para garantir a defesa de seu território em caso de uma declaração de guerra.

Por deter expertise técnica que poucos Estados dispõem para combinar o emprego da força física às ações cibernéticas, uma potência como a Rússia têm maiores incentivos para utilizar o ciberespaço para explorar as vulnerabilidades de sistemas de informação complexos que lhe forneçam vantagens na consecução de seus objetivos estratégicos (LINDSAY, 2013).

Em termos de analise de riscos e ameaças à segurança cibernética, as evidências apontam que, em estando correto o pressuposto de que as capacidades convencionais de emprego da força pelos Estados fortes impõem restrições às ações ofensivas de entes mais fracos, então os riscos de que ocorram ataques cibernéticos capazes de causar danos graves às infraestruturas físicas de países militarmente mais fortes é menor (GARTZKE, 2013, LINDSAY, 2013). De tal modo que APTs de menor potencial de impacto, como aquelas especializadas em espionagem cibernética, despontam como estrategicamente mais atrativas aos Estados que pretendem utilizar o ciberespaço para atingirem seus objetivos estratégicos (LINDSAY, 2015, SHARMA, 2011, HJORTDAL, 2011, KENNEDY, 2013).

Fundamentados pela literatura exposta, entendemos que os ataques cibernéticos enquanto tática de ação empregada por atores não-estatais em conjunto com as operações militares convencionais podem garantir maior efetividade na consecução de objetivos estratégicos de grandes potências cibernéticas como a Rússia. Ou seja, ao empregarem a tecnologia da informação nos conflitos contemporâneos as operações militares produzem força sinérgica que contribui para o aumento da assimetria de poder entre os Estados.

Diante deste entendimento, defendemos que o fenômeno da GHC representa uma ferramenta instrumental, estratégica e tática, fundamental para os Estados contemporâneos, uma vez que pode ser iniciada sem jamais ter sido oficialmente declarada. De tal modo que, o

domínio do ciberespaço permite a redução da incerteza do processo decisório na medida em que a tecnologia fornece informações valiosas para a ação estratégica *ex-ante* dos tomadores de decisão, além disso, reduz a necessidade de um grande contingente humano e de recursos financeiros que de outra forma seriam desprendidos em ofensivas contra um oponente, tal dinâmica faz do espaço de informação uma arena chave para a dinâmica de retornos crescentes aos Estados que o utilizam para consecução de seus objetivos estratégicos.

2.2 Desenho de Pesquisa

2.2.1 Metodologia e Objetivos

Com intuito responder o questionamento que norteia esta dissertação, sustentamos que o aumento da assimetria de poder regional entre a Rússia e Ucrânia é consequência da guerra híbrida cibernética (GHC), fenômeno que resulta do funcionamento do mecanismo causal que conecta o emprego da tecnologia da informação no conflito ao processo de mudança institucional pelo qual passaram as Forças Armadas da Federação Russa.

Frente a esse desígnio, o objetivo principal desta dissertação é inferir que a mudança institucional na estratégia da Federação Russa, atrelada à simbiose entre as forças especiais e hackers civis, implicou na manifestação operacional e tática do fenômeno da GHC, o que favoreceu, em última instância, o aumento da assimetria de poder regional entre este país e a Ucrânia.

Destarte, os objetivos específicos deste estudo são: i) demonstrar os reflexos do processo mudança institucional na estratégia da Federação Russa a partir da comparação de documentos oficiais que versam sobre Defesa e Segurança; ii) coletar evidências que permitam a identificação dos agentes estatais e não-estatais, as operações, táticas, e as armas utilizadas nos ataques cibernéticos que permearam o conflito regional entre Rússia e Ucrânia (2014-2015); iii) inferir que a simbiose entre as forças especiais e hackers civis pode ser entendida como o mecanismo causal que conecta a GHC à mudança institucional.

Para tanto, utilizamos três técnicas de análise qualitativa, documental historiográfica, dependência da trajetória e o rastreamento de processos que serão apresentadas nesta seção.

Inicialmente, empregamos a técnica documental historiográfica para análise comparada das fontes oficiais que versam sobre a política de Defesa e Segurança da

Federação Russa com intuito de identificar a preponderância dada pelo Estado às questões relativas à tecnologia da informação.[5]

Uma vez que as relações político-militares exercem influência profunda no futuro da guerra, compreender o processo de mudança institucional pelo qual passaram os documentos que regulam a ação das Forças Armadas russas torna-se fator chave para avaliarmos o impacto da revolução tecnológica nas ações do Estado em seu entorno estratégico regional.

Fontes primárias analisadas: (documentos oficiais) Doutrina Militar (2010; 2014); Estratégia de Segurança Nacional (2009; 2015).

No que concerne à análise da consecução dos objetivos estratégicos regionais da Federação Russa, utilizamos a técnica da dependência da trajetória (*pathdependence)*[6] para compreender como o processo de mudança institucional produziu uma dinâmica de retornos crescente[7] no nível tático das ações do Estado (PIERSON, 2000).

> Em um processo de retornos crescentes, a probabilidade de ocorrer novas etapas no mesmo caminho aumenta a cada movimento nesse caminho. Isso ocorre porque os benefícios relativos da atividade atual em comparação com outras opções possíveis aumentam com o tempo (PIERSON, 2000, p. 252, tradução nossa).

Uma vez que a atenção à historicidade confere maior credibilidade aos argumentos que exploram processos de causais em estudos de caso, ao enfatizarmos a compreensão de um fenômeno que integra um processo histórico resultante da variação na vida política e social (PIERSON, 2000, p. 252) assumimos que "cada passo ao longo de um caminho específico produz consequências que o tornam mais atraente para a próxima rodada. À medida que esses efeitos começam a se acumular, eles geram um poderoso ciclo virtuoso (ou vicioso) de atividade de auto reforço" (PIERSON, 2000, p. 253, tradução nossa).

Por essa lógica, a mudança institucional e a atuação de atores estatais e não-estatais configuram evidências importantes para a identificação do papel exercido pela tecnologia da

---

[5] Os documentos originais em língua russa analisados nesta pesquisa foram traduzidos para língua portuguesa com ajuda da ferramenta GoogleTradutor.

[6] A dependência da trajetória significa que "uma vez que o Estado começa um movimento os custos de reversão são altos, existem outros pontos de escolha, mas o novo arranjo institucional impede um retorno fácil para o ponto inicial" (LEVI, 1997, *apud* PIERSON, 2000, p. 252, tradução nossa).

[7] O conceito de retornos crescentes -'*increasing returns*', '*self-reinforcing*' ou '*positive feedback process*'- é utilizado pela corrente do novo institucionalismo histórico para determinar padrões sequenciais específicos de tempo, pequenos eventos que podem ter grandes consequências, cursos de ação uma vez iniciados impõem alto custo para reversão, o desenvolvimento político pontuado por momentos críticos ou conjunturas que moldam os contornos básicos da vida social (COLLIER AND COLLIER 1991; IKENBERRY 1994; KRASNER 1989; *apud* PIERSON, 2000, p. 251).

informação no conflito entre Rússia-Ucrânia, a chave para compreensão do processo está, portanto, na análise da relação que se estabelece através da interdependência da matriz institucional observada e a ideia de produção de retornos crescentes (NORTH, 1990a; *apud* PIERSON, 2000, p. 255).

Não obstante, a elaboração do argumento sob a perspectiva da dependência da trajetória na medida em que pontua momentos críticos do conflito que refletem a mudança institucional observada durante a análise dos documentos oficiais, contribui para que possamos oferecer uma explicação razoável sobre as conjunturas históricas e as consequências do fenômeno de nosso interesse (PIERSON, 2000, p. 263) para o aumento da assimetria de poder regional entre Rússia e a Ucrânia.

À vista disso, esta dissertação encontra-se comprometida com o quadro teórico proposto pela comunidade epistêmica que emprega a análise histórica das instituições mediante avaliação de como as estratégias de ação do Estado são induzidas por mudanças nas diretrizes oficiais que organizam a agência, em nosso caso as Forças Armadas da Rússia que sofreram alteração nos parâmetros operacional e tático que "podem fossilizar-se ao longo do tempo e tornar-se visões de mundo, que são propagadas por organizações oficiais e terminam por moldar a imagem de si e as preferências dos interessados" (HALL; TAYLOR, 2003, p. 199, tradução nossa).

Justificamos assim o esforço deste estudo em extrapolar o horizonte temporal da análise ao investigarmos a operação do mecanismo causal -simbiose entre as forças especiais russas e hackers civis-, como agência que tornou possível o fenômeno da GHC.

> Os mecanismos de reprodução geralmente fornecem informações sobre os tipos de eventos ou processos que podem gerar importantes pontos de mudança subsequentes. Tais junções são geralmente atribuídas a 'choques exógenos'. Devemos esperar, no entanto, que esses pontos de mudança geralmente ocorram quando novas condições perturbam ou sobrecarregam os mecanismos específicos que anteriormente reproduziam o caminho existente (MAHONEY; THELEN (1999), *apud* PIERSON, p. 265, tradução nossa).

Cientes de que a abordagem institucionalista histórica estabelece que "muitas das implicações políticas contemporâneas desses processos temporais estão incorporadas nas instituições - sejam regras formais, estruturas políticas ou normas" (PIERSON, 2000, p. 265, tradução nossa), nossa a análise procura conectar as implicações políticas do processo de mudança institucional pelo qual passaram as regras formais que estruturam a agência das

Forças Armadas da Rússia aos momentos críticos que levaram a eclosão do conflito regional entre esse país e a Ucrânia.

Outrossim, pretendemos demonstrar que o processo causal observado é dependente da trajetória percorrida pela instituição das Forças Armadas que ampliou a capacidade de projeção de poder da Federação Russa em seu entorno regional mediante o investimento em tecnologia da informação e a inclusão de atores não-estatais nesses conflitos. Nesse sentido, a instituição militar figura como integrante permanente do contexto histórico, ao mesmo tempo em que representa um dos principais fatores que mantêm seu desenvolvimento sobre um conjunto de caminhos observáveis que permitem a análise de nosso fenômeno de interesse mediante a explicação de "como as instituições produzem esses trajetos, como elas estruturam a resposta de uma dada nação a novos desafios" (HALL; TAYLOR, 2003, p. 200, tradução nossa).

> No mesmo espírito, numerosos teóricos dessa escola tendem a distinguir no fluxo dos eventos históricos períodos de continuidade e "situações críticas", vale dizer, momentos nos quais mudanças institucionais importantes se produzem, criando desse modo "bifurcações" que conduzem o desenvolvimento por um novo trajeto. O principal problema consiste evidentemente em explicar o que provoca as situações críticas, e em geral os teóricos insistem no impacto das crises econômicas e dos conflitos militares (HALL; TAYLOR, 2003, p. 201).

Diante do exposto, ao testarmos nosso argumento causal hipotético-dedutivo que aponta para o impacto da GHC no aumento da assimetria de poder regional entre a Rússia e Ucrânia, coletamos e agrupamos as evidências em sequências de eventos temporais para sustentar as hipóteses condicionais levantadas, assim, diferentes evidências identificam as preferências e percepções dos atores, seus objetivos, propósitos e valores, bem como as especificidades do contexto analisado, as quais representam pistas importantes para compreensão do impacto de nosso fenômeno interesse na capacidade de projeção de poder regional da Federação Russa.

Fontes secundárias analisadas: (relatórios técnicos) empresas especializadas em segurança cibernética como CrowdStrike (2014; 2015; 2016); FireEeye (2014; 2016a; 2016b); F-Secure Labs (2014a; 2014b; 2016); LookingGlass (2015); Sistema de Controle Industrial para Ciber Emergências (ICS-CERT) (2016); Centro de Análise e Compartilhamento de Informações (E-ISAC) (2016); periódicos publicados em revistas de alto fator de impacto e diversos artigos de jornal escritos por analistas do tema.

A partir das fontes primárias e secundárias identificamos o processo que conecta a mudança institucional à atuação de grupos hackers em consonância com as forças especiais russas nas campanhas realizadas pela Rússia em território ucraniano.

Sem embargo, utilizamos a técnica do rastreamento de processos (*process tracing*)[8] para testar de modo sistemático as evidências selecionadas à luz das referidas hipóteses condicionais sobre as causas de um determinado fenômeno ora encontrado, ou seja, a guerra híbrida cibernética (GHC) (COLLIER, 2011, p. 823).

Inicialmente, a aplicação do rastreamento de processos requer a especificação da estrutura conceitual, sob a qual operacionalizamos nosso entendimento da GHC, somada à identificação de regularidades empíricas resultantes do fenômeno observado que permitam estabelecer a conexão causal entre as hipóteses que serão verificadas. Desse modo, o componente descritivo da série de momentos específicos que marcaram as principais etapas do processo é o ponto fulcral da técnica que permite uma boa análise da mudança e sequência do evento de nosso interesse (COLLIER, 2011, p. 824).

> Os testes nem sempre são fáceis de aplicar. Portanto, pode ser produtivo começar com uma boa narrativa ou com um tempo que lista a sequência de eventos. Pode-se, então, explorar as ideias causais embutidas nas narrativas, considerar os tipos de evidência que podem confirmar ou desconfirmar essas ideias e identificar os testes apropriados para avaliar essas evidências (COLLIER, 2011, p. 828-829, tradução nossa).

Por essa lógica, elencamos dois testes de hipótese condicional um de necessidade e outro de suficiência, ambos envolvem inferência descritiva e foram baseados, respectivamente, nos princípios de singularidade e certeza (BENNET 2010; COLLIER 2011; VAN EVERA 1997; *apud* CDI, 2015, p. 4)[9].

O primeiro refere-se à condição de necessidade (*hoop-test*), avalia como mudança institucional dos documentos oficiais que versam sobre a Política de Defesa e Segurança da Federação Russa resultou em redução quantitativa e aumento qualitativo das forças mediante

[8] O rastreamento de processos é uma técnica desenvolvida com intuito de sistematizar a análise qualitativa a partir de uma perspectiva capaz de explicar relações causais mediante a observação de como determinadas condições produzem um fenômeno social (CDI, 2015, p. 1). Trata-se de uma ferramenta útil para extrair inferências descritivas e causais a partir de evidências compreendidas como parte de uma sequência temporal de eventos ou fenômenos (COLLIER, 2011, p. 824).

[9] Os princípios indicam se a evidência coletada é necessariamente sólida para confirmar a hipótese DE singularidade (*uniqueness*) fomentada; se a evidência é suficiente para sustentar a certeza (*certainty*) da hipótese levantada, sendo então possível descartar explicações alternativas (BEACH; PEDERSEN 2013; BEFANI; MAYNE 2014, *apud* CDI, 2015, p. 4).

o crescimento nos investimentos em tecnologia da informação e segurança cibernética; o segundo diz respeito à condição de suficiência (*smoking-gun-test*), procura estabelecer a causação entre os eventos ou processos observados mediante a verificação da ocorrência do que denominamos como relação de simbiose entre as forças especiais e hackers civis enquanto mecanismo causal que favoreceu a condução das ações operacionais e táticas das Forças Armadas russas no território ucraniano.

Se por um lado o teste de necessidade pressupõe que uma evidência ou observação especifica do processo causal deve estar presente para que uma hipótese condicional seja válida, sua confirmação por si só não é suficiente para confirmar o argumento hipotético dedutivo que orienta a investigação empírica do impacto da GHC sobre a assimetria de poder regional entre a Rússia e a Ucrânia. Por outro lado, o teste de suficiência estabelece que, se uma determinada evidência - ou seja, um processo causal observável (PCO) específico - estiver presente, o argumento será válido, nesse sentido, o teste suficiência oferece apoio decisivo a favor de uma hipótese, embora falhar neste teste não a elimine como ocorre com o teste de necessidade (MAHONEY, 2012, p. 571).

> Em resumo, os testes de rastreamento de processo baseiam-se em informações sobre o mecanismo como base para inferência causal. Embora os testes geralmente não sejam realizados de forma explícita, eles geralmente são usados implicitamente por analistas que trabalham na pesquisa de histórico comparativa e de estudo de caso [...] Os testes de rastreamento de processo projetados para inferência causal sempre exigem que o analista localize e utilize mecanismos. Sem localizar PCOs que incorporam informações sobre mecanismo, não se pode usar testes de rastreamento de processo para ajudar a estabelecer se um evento causa outro (MAHONEY, 2012, p. 583-586, tradução nossa).

Com intuito de compreendermos como a GHC amplia a capacidade de projeção de poder da Federação Russa em seu entorno regional intentamos explicar como esse fenômeno se manifesta a partir da identificação do funcionamento do mecanismo causal que permite e / ou gera tal fenômeno (MAHONEY, 2012, p. 586).

Através da análise dos relatórios supracitados procuramos descrever os PCO's que compõem o mecanismo e conectam o fenômeno observado (Y: guerra híbrida cibernética) à causa inicial (X: mudança no modo de operação das Forças Armadas), desse modo, "as observações do processo causal (PCO's) são usadas em conjunto com uma generalização mais ampla relevante para o caso em análise" (COLLIER; BRADY; SEAWRIGHT, 2010; *apud* MAHONEY, 2012, p. 571, tradução nossa).

Por essa lógica, estabelecemos que se a mudança no modo de operação das Forças Armadas da Federação Russa for suficiente para produzir o fenômeno de nosso interesse, então será igualmente suficiente para o funcionamento do mecanismo causal, a simbiose que procuramos abordar como vetor observável do impacto da tática empregada pela Federação Russa para consecução de seus objetivos estratégicos regionais. Nesse caso ao avaliarmos a plausibilidade do mecanismo "a suposição é que se X realmente é suficiente para Y, também deve ser (de acordo com a lógica elementar) suficiente para todos os mecanismos intervenientes necessários para Y" (MAHONEY, 2012, p. 580, tradução nossa).

O quadro 1 sumariza os testes aplicados para construção de nosso argumento hipotético-dedutivo.

Quadro 1 Testes de Hipótese Condicional

Condição Necessária	
Mudança institucional na Política de Defesa e Segurança da Federação Russa	Variação nos investimentos em tecnologia da informação e segurança cibernética, redução quantitativa das forças e aumento qualitativo.
Condição Suficiente	
Simbiose forças especiais – hackers civis	Operações e táticas, ataques coordenados aos setores de infraestrutura crítica e alvos do governo ucraniano.

Fonte: Elaborado pelo autor (2020).

2.3 Análise documental

2.3.1 Doutrina Militar (2010)

Nesta seção apresentamos em detalhes os principais documentos oficiais que versam sobre Defesa e Segurança da Federação Russa com objetivo de corroborar a hipótese condicional de necessidade referente à mudança institucional na estratégia da Federação Russa para ação em seu entorno regional.

A Doutrina Militar (2010)[10], reformulada durante o primeiro governo de Vladmir Putin (2000-2008) e promulgada pelo então presidente eleito Dmitry Medvedev em 5 de Fevereiro de 2010, resultou de intensos debates entre os militares e a classe política sobre o futuro do desenvolvimento da organização militar da Federação frente aos conflitos regionais que eclodiram ao longo da primeira década do século vinte e um.[11]

Em sua primeira seção a doutrina (2010) estabelece o compromisso da Federação Russa com "o uso de instrumentos políticos, diplomáticos, legais, econômicos, ambientais, de informação, militares e outros instrumentos" para proteção dos interesses estratégicos o país e de seus aliados (RÚSSIA, 2010, art. 4, p. 1-2, tradução nossa).

No que tange aos conceitos básicos do planejamento estratégico na esfera militar, estabelece a percepção da guerra regional enquanto conflito entre "dois ou mais estados da mesma região, travada por forças armadas nacionais ou de coalizão usando armas convencionais e nucleares" (RÚSSIA, 2010, art. 6, item g, p. 3, tradução nossa).

Na segunda seção o documento apresenta percepção da Federação Russa acerca do atual estágio de desenvolvimento mundial, um contexto marcado pela redução da polarização ideológica frente à emergência de uma multipolaridade de centros de poder internacional que fragmentam o nível de influência econômica, política e militar de alguns Estados (RÚSSIA, 2010, art. 7, p. 3-4). Aponta, ainda, uma preocupação com o aumento de conflitos regionais em territórios que fazem fronteira com o território russo, sinalizando que as instituições e

[10] A Doutrina Militar (2010) apresenta conceitos que servem de base para a Segurança e Defesa da Federação Russa, o documento congrega elementos da Estratégia de Segurança Nacional (2009) e do Conceito de Política Externa da Federação Russa (2008) e está dividido em quarto seções, a primeira trata da base constitucional e jurídica dos conceitos adotados pelo planejamento estratégico militar (artigos 1-6); a segunda dos perigos e ameaças militares à Federação Russa (artigos 7-16); a terceira apresenta a Política Militar da Federação Russa (artigos 17-37); a última trata da segurança militar e econômica da Defesa (artigos 38-53) (RÚSSIA, 2010).

[11] A Federação Russa esteve envolvida em diversos confrontos regionais nesse período com destaque para os conflitos contra a Chêchênia (data) e Geórgia (2008) nos quais as Forças Armadas russas enfrentaram dificuldades para consecução dos objetivos estratégicos do país. Em 2008, os russos foram responsabilizados pela explosão do oleoduto em Baku Tbsilisi Ceyhan, a ação foi o estopim da guerra Russia-Geórgia que se iniciou dois dias depois do fato (THE CONVERSATION, 2016, p. 2).

mecanismos legais internacionais não apresentam a mesma eficiência, em termos de segurança, para todos os Estados, fator que representa uma ameaça de eclosão de novos conflitos em larga escala com possibilidade de envolver o emprego de armas convencionais e nucleares (RÚSSIA, 2010, art. 7, p. 4).

A doutrina (2010) salienta que a existência dessas ameaças externas é percebida pela Rússia como fatores que contribuem para a desestabilização de territórios e redução da estabilidade estratégica regional. Nesse sentido, o avanço da infraestrutura militar dos países membros da Organização do Tratado do Atlântico Norte (OTAN) sobre as fronteiras da Federação Russa é tido como uma das principais:

> A criação e implementação de sistemas estratégicos de defesa antimísseis que violam o equilíbrio de forças existente a na esfera dos mísseis nucleares comprometendo a estabilidade global, militarização do espaço sideral, implantação de sistemas estratégicos não nucleares de armas de alta precisão (RÚSSIA, 2010, art.8, item d, p. 4, tradução nossa).

No que se refere aos perigos militares internos, a doutrina (2010) estabelece as tentativas de alteração do sistema constitucional da Federação, a desintegração territorial e a desorganização da estrutura de funcionamento do estado, em especial de instalações militares e infraestrutura de informação (RÚSSIA, 2010, art. 9, p. 5).

A obstrução dos sistemas estatais e militares de comando e controle que podem ter seu funcionamento comprometido, afetando áreas de infraestrutura estratégica como “os sistemas de aviso de mísseis, controle espacial, instalações de armazenamento de armas nucleares, energia nuclear, química e outras instalações potencialmente perigosas” (RÚSSIA, 2010, art. 10, item h, p. 5, tradução nossa) é uma das principais ameaças militares à Federação Russa estabelecidas no documento.

De acordo com a doutrina (2010), os conflitos militares contemporâneos são marcados por uma combinação entre forças militares e meios de natureza não militar operando sistemas de armas e equipamentos de alta tecnologia, comparáveis, em termos de eficácia, às armas nucleares. Diante desse cenário, a guerra de informação é percebida como uma ferramenta que ajuda a reduzir o tempo de preparação do campo de batalha para operações militares, ampliando, consideravelmente, a eficiência da rede de sistemas de comando e controle de tropas e armas (RÚSSIA, 2010, art. 12, itens a-g, p. 6-7).

A guerra de informação é, portanto, descrita como uma característica dos conflitos militares contemporâneos que oferece vantagens aos Estados que pretendem “atingir objetivos

políticos sem o uso de força militar" (RÚSSIA, 2010, art. 13, item d, p. 7, tradução nossa) ao passo em que constroem "uma reação favorável da comunidade mundial" (RÚSSIA, 2010, art. 13, item d, p. 7, tradução nossa) às operações militares.

Ainda de acordo com a doutrina (2010), a Federação Russa prevê que a estratégia de utilização de grupos e tropas móveis para auxiliar na "garantia da supremacia em terra, no mar, no espaço aéreo e no exterior se tornarão fatores decisivos para a consecução dos objetivos" (RÚSSIA, 2010, art. 15, p. 7, tradução nossa). Dentre as principais armas de alta precisão utilizadas nas operações militares contemporâneas listadas no documento encontram-se "lasers eletromagnéticos, armas de infrassom, sistemas controlados por computador, drones, embarcações marítimas autônomas e modelos robotizados de armas e equipamentos militares" (RÚSSIA, 2010, art. 15, p. 7, tradução nossa).

Na terceira seção, o documento aponta para as ações da Federação Russa voltadas para prevenção de conflitos militares e proteção interna de acordo com as normas e tratados que regem o direito internacional. Dentre as principais tarefas estabelecidas estão a necessidade de "avaliar e prever o desenvolvimento da situação político-militar em nível global e regional [...] utilizando sistemas técnicos modernos e tecnologias da informação [...] neutralizar possíveis perigos militares e ameaças militares usando meios políticos, diplomáticos e outros meios não militares" (RÚSSIA, 2010, art. 19, itens a-b, p. 8, tradução nossa).

A doutrina (2010) manifesta, ainda, o interesse da Rússia em fortalecer o tratado de Organização do Tratado de Segurança Coletiva (OTSC) e intensificar a cooperação no campo da segurança internacional com as organizações da Comunidade de Estados independentes (CEI); Organização de Segurança e Cooperação na Europa (OSCE); Organização para Cooperação de Xangai (OCX), bem como ampliar as relações com a Organização do Tratado do Atlântico Norte (OTAN) e a União Europeia (UE) (RÚSSIA, 2010, art. 19, item e, p. 8-9).

O documento revela que a Federação Russa considera legítimo o uso das Forças Armadas e outras tropas para repelir ataques realizados contra o país e/ou seus aliados, com vistas à manutenção da segurança coletiva e garantia da "proteção de seus cidadãos localizados além das fronteiras da federação russa" (RÚSSIA, 2010, art. 20, p. 10, tradução nossa) em acordo com os princípios e normas reconhecidos pelos tratados de direito internacional dos quais o país é signatário. Dentre as medidas de dissuasão estratégica previstas, destacam-se o uso de armas de alta precisão e armas nucleares como reposta aos ataques que utilizem essa categoria de armamentos (RÚSSIA, 2010, art. 22, p. 10).

A preocupação com a defesa da soberania, integridade e inviolabilidade territorial russa estão entre as principais tarefas das Forças Armadas em tempos de paz. Nesse sentido, as forças devem se manter em "estado de prontidão e treinamento para combate e mobilização" (RÚSSIA, 2010, art. 27, item c, p. 11, tradução nossa). Outrossim, são responsáveis por garantir o funcionamento dos sistemas de comando e controle com vistas à garantir a Defesa e a Segurança contra as ameaças à Federação e a sociedade civil russa em quaisquer que sejam as condições (RÚSSIA, 2010, art. 27, p. 11).

A doutrina (2010) estabelece os principais objetivos para atingir o desenvolvimento da organização militar, dentre os quais, destacam-se:

> [...] aumentar a eficiência e a segurança do funcionamento de sistemas de administração estatal e militar [...] criar estruturas integradas para apoio material, técnico, social, médico e científico das Forças Armadas e outras tropas [...] melhorar o sistema de apoio à informação das Forças Armadas e outras tropas (RÚSSIA, 2010, art. 30, itens b, j, l, p. 13-14, tradução nossa).

Com o objetivo de responder à natureza dos conflitos contemporâneos, o documento apresenta uma série de procedimentos necessários para adequação das Forças Armadas aos novos desafios da era da informação. À vista disso, estabelece como prioridades para o desenvolvimento da estrutura e organização militar da Federação Russa: i) aprimorar o sistema de gestão da instituição e a eficácia de seu funcionamento; ii) desenvolver a base de mobilização das Forças Armadas e outras tropas; fornecer equipamento, provisão e treinamento às unidades militares; iii) melhorar a qualidade da educação militar e desenvolver o potencial científico da instituição (RÚSSIA, 2010, art. 31, itens a-d, p. 14-15, tradução nossa) Por conseguinte, estabelece o alinhamento do desenvolvimento da estrutura organizacional das forças e de outras tropas com o avanço da sofisticação das ameaças militares (RÚSSIA, 2010, art. 32, p. 15).

Outrossim, prevê melhorias nas armas de combate e treinamento operacional, o fornecimento e desenvolvimento de "modelos modernos de armas, equipamentos militares e especiais de alta qualidade" (RÚSSIA, 2010, art. 33, item e, p. 16, tradução nossa) e a garantia da "integração e o desenvolvimento coordenado de sistemas de apoio técnico, logístico e outras formas de apoio às forças armadas e outras tropas [...] treinamento e educação militar [...] ciência militar" (RÚSSIA, 2010, art. 33, item f, p. 16, tradução nossa).

A doutrina (2010) define que a instituição militar deve perseguir os objetivos de construção da organização e desenvolvimento das Forças Armadas e outras tropas adotando

medidas eficientes que permitam, dentre outros pontos: i) melhorar o nível qualitativo do complexo industrial militar; ii) manter o funcionamento do sistema de comando e controle; iii) garantir a base de mobilização em condições capazes de garantir o envolvimento estratégico das Forças Armadas e de outras tropas durante conflitos ou em tempos de paz; iv) constituir parceria entre instituições de ensino militares e federais para formação de profissionais de nível superior por programas de treinamento militar, equipados com material atualizado e base técnica (RÚSSIA, 2010, art. 34, itens c-d, f,k, p. 16-17, tradução nossa).

Em relação ao planejamento da instituição, os principais objetivos descritos na doutrina (2010) apontam para o "desenvolvimento da base científica, técnica e industrial" (RÚSSIA, 2010, art. 36, item a, p. 18, tradução nossa), a existência de uma correlação entre o "apoio de recursos para as Forças Armadas e outras tropas e as tarefas de construção organizacional, desenvolvimento e uso" (RÚSSIA, 2010, art. 36, item c, p. 18, tradução nossa) e a construção, ajuste e fiscalização dos marcos regulatório de curto, médio e longo prazo dos programas de desenvolvimento das Forças Armadas e outras tropas (RÚSSIA, 2010, art. 36, p. 18).

Na quarta seção o documento discute a criação de condições para oferecer suporte ao desenvolvimento militar, nesse sentido, prevê a construção de equipamentos de alta qualidade para as Forças Armadas e outras tropas, com objetivo, dentre outros pontos, de: i) otimizar os gastos com defesa garantindo o planejamento racional e a distribuição de recursos financeiros e materiais destinados para apoiar a organização militar, aumentando a eficácia de seu uso; ii) garantir a integração dos setores civil e militar da economia em esferas específicas de produção e coordenação das atividades econômico-militares do Estado, no interesse de apoiar a Defesa (RÚSSIA, 2010, art. 39, itens b,e, p. 19, tradução nossa).

Destarte, a tecnologia desempenha papel fundamental na construção do armamento das Forças Armadas e outras tropas da Federação, conforme consta na doutrina (2010), a Rússia busca fortalecer sua base de Defesa equipando as forças com armas modernas que incluem o desenvolvimento de "meios de guerra de informação" (RÚSSIA, 2010, art. 41, item c, p. 20, tradução nossa).

A estrutura do Complexo Industrial Militar (CIM) russo, responsável por oferecer sustentação para o desenvolvimento das forças, é outra evidencia presente doutrina (2010) na qual se verifica a importância da tecnologia da informação para as Forças Armadas. De acordo com o documento o CIM deverá "atender às necessidades das Forças Armadas e de

outras tropas por armamentos modernos e equipamentos militares especiais" (RÚSSIA, 2010, art. 45, p. 21, tradução nossa) que empreguem alta tecnologia.

Com objetivo de desenvolver o CIM, a doutrina (2010) propõe a criação de "grandes estruturas científicas e de produção" (RÚSSIA, 2010, art. 46, item a, p. 22, tradução nossa) que possam garantir a "independência tecnológica da Federação Russa na esfera da produção de modelos estratégicos e outros de armamentos" (RÚSSIA, 2010, art. 46, item c, p. 22, tradução nossa). Todavia, procura preservar o controle do CIM nas mãos do Estado enquanto agente patrocinador das atividades de "inovação e investimento, possibilitando a renovação qualitativa da base científica, técnica, manufatureira, e da base tecnológica" (RÚSSIA, 2010, art. 46, item g, p. 22, tradução nossa).

Não obstante, observa-se que a tecnologia desempenha papel importante no que tange a necessidade de assegurar o "desenvolvimento, a produção e a manutenção de modelos de armamentos e equipamentos militares especiais" (RÚSSIA, 2010, art. 46, item h, p. 22, tradução nossa) eficazes para emprego em conflitos contemporâneos.

No que tange a cooperação, militar-política e técnico-militar com estados estrangeiros e organizações internacionais, o documento sustenta o pragmatismo econômico da Rússia em acordo com a legislação federal e os tratados internacionais dos quais a Federação é signatária (RÚSSIA, 2010, art. 49, p. 25). Frente a isso, a principal tarefa das forças é reforçar a segurança internacional a partir do estreitamento dos laços com países da Organização do Tratado de Segurança Coletiva (OTSC) e da Comunidade de Estados Independentes (CEI) que tem por objetivo "desenvolver o processo de negociações para a criação de sistemas regionais de segurança" (RÚSSIA, 2010, art. 50, item c, p. 25, tradução nossa).

Nesse sentido, o documento expõe o interesse da Rússia em negociar a construção de sistemas regionais de segurança e fortalecer as relações com "organizações internacionais que possam ajudar a prevenir situações de conflito, preservar e fortalecer a paz [...] combater a proliferação de armas de destruição em massa" (RÚSSIA, art. 50, itens d-e, 2015, p. 25, tradução nossa).

Por fim, o documento estabelece como prioridade a cooperação militar com a Bielorússia para "desenvolvimento das forças armadas nacionais e uso da infraestrutura militar" (RÚSSIA, 2010, art. 51, item a, p. 26, tradução nossa), bem como com as comunidades CSTO, CEI e SCO, e, com a Organização das Nações Unidas (ONU) participando em operações de manutenção da paz, formulação, coordenação e implementação

de acordos internacionais na esfera do controle de armas (RÚSSIA, 2010, itens a-e art. 51, p. 26).

2.3.2 Análise comparada: Doutrina Militar (2010;2014)

Nesta subseção comparamos as doutrinas militares da Federação Russa (2010; 2014).

A Federação Russa promulgou sua nova Doutrina Militar (2014) assinada em 30 de dezembro de 2014 pelo presidente Vladmir Putin.

O documento destaca, dentre outras ameaças externas, o avanço militar da OTAN sobre os países fronteiriços que se encontram dentro do entorno estratégico regional russo como fator que impõe a necessidade de que a Federação Russa continue o processo de investimento em tecnologia para garantir a Defesa e a Segurança do país. A partir dessa diretriz, a doutrina (2014) destaca como primordial o aprimoramento do sistema de comando e controle de fluxo de informação e a construção de armas de alta precisão como vetores da Defesa nacional capazes de conter as ameaças à soberania e a integridade territorial da Rússia.

Em termos comparativos, a Doutrina Militar (2014)[12] guarda semelhanças com o documento anterior, porém acrescenta detalhes importantes que demonstram as conjunturas críticas do processo que conduziu ao conflito com a Ucrânia, acontecimentos que demonstram a importância crescente do uso da tecnologia nos conflitos militares contemporâneos.

A primeira seção do documento de 2015 mantém grande parte do texto anterior, no entanto acrescenta dois artigos que demonstram a importância dada pela Federação Russa ao controle dos perigos e ameaças militares que afetam os interesses não apenas da Federação, mas também de seus aliados (RÚSSIA, 2014, art. 2, p. 1) reforçando o compromisso com a proteção militar de tais interesses em caso de esgotamento das "possibilidades de usar instrumentos políticos, diplomáticos, legais, econômicos, informacionais e outros instrumentos não violentos" (RÚSSIA, 2014, art. 5, p. 2, tradução nossa).

No que concerne aos conceitos básicos do planejamento estratégico na esfera militar, a doutrina (2014) modifica a percepção da Rússia sobre a guerra regional (RÚSSIA, 2010, art. 6, p. 3) na medida em que retira a possibilidade de eclosão de conflitos nucleares nesse nível

[12] O documento congrega elementos da Estratégia de Segurança Nacional (2010) e do Conceito de Política Externa da Federação Russa (2013) e está dividido em quarto seções, a primeira trata da base constitucional e jurídica dos conceitos adotados pelo planejamento estratégico militar que servem de base para a Segurança e Defesa da Federação Russa (Artigos 1-9); a segunda dos perigos e ameaças militares à Federação Russa (artigos 9-16); a terceira apresenta a Política Militar da Federação Russa (artigos 17-42); e a última trata da segurança militar e econômica da Defesa (artigos 43-58) (RÚSSIA, 2015).

estabelecer o entendimento de um conflito travado por Forças Armadas nacionais ou de coalizão envolvendo importantes objetivos militares e políticos (RÚSSIA, 2014, art. 8, item g, p. 3). Ademais, delimita os conceitos de prontidão para mobilização e de sistema de dissuasão nuclear como importantes ferramentas para garantir a segurança da Federação Russa (RÚSSIA, 2014, art. 8, itens l-m, p. 3-4).

Na segunda seção a percepção da Federação Russa do contexto internacional também sofreu alterações com a inserção de três artigos que oferecem destaques ao processo histórico que se desenrolou desde a promulgação de seu documento antecessor.

O primeiro ressalta a instabilidade dos processos de desenvolvimento político e econômico global e regional que ocorrem em paralelo ao aumento da tensão das relações internacionais entre os Estados contemporâneos (RÚSSIA, 2014, art. 9, p. 4). Frente a esse cenário, o segundo descreve a preocupação das forças com a eclosão de conflitos regionais em zonas fronteiriças da Rússia que permanecem sem solução devido à insuficiência do sistema de segurança internacional em prover proteção equitativa aos Estados (RÚSSIA, 2014, art. 10, , p. 4). Por fim, o terceiro frisa o aumento dos perigos militares à Federação Russa e demonstra a percepção do ciberespaço como zona de combate proeminente dos conflitos contemporâneos ao inserir um alerta quanto a "tendência de transferir perigos e ameaças militares para o espaço de informação e a esfera interna da Federação Russa" (RÚSSIA, 2014, art.11, p. 4, tradução nossa).

Dentre os perigos externos, o documento mantém os itens anteriores (RÚSSIA, 2010, art. 8, p. 4), no entanto acrescenta uma preocupação fundamental com o avanço do uso de "tecnologias de informação e comunicação para fins político-militares" (RÚSSIA, 2014, art. 12, item l, p. 5, tradução nossa) e com a condução de operações especiais por "estados estrangeiros e suas coalizões" (RÚSSIA, 2014, art. 12, item m, p. 5, tradução nossa) a revelia do estabelecido por tratados de direito internacional, fatores que ameaçam a "soberania, independência política e integridade territorial dos Estados" (RÚSSIA, 2014, art. 12, item n, p. 6, tradução nossa) e contribuem para a instabilidade regional e global.

No que concerne aos perigos militares internos, há uma mudança significativa em comparação com seu documento antecessor que indica outra conjuntura crítica referente ao conflito com a Ucrânia. Nesse sentido, a doutrina (2014) reforça importância de manter o funcionamento das instituições estatais e da infraestrutura de informação (RÚSSIA, 2010, art. 9, item b, p. 5) e acrescenta uma preocupação fulcral com o impacto da manipulação da informação na opinião pública por agentes que objetivam "minar as tradições históricas,

espirituais e patrióticas no campo da proteção da pátria" (RÚSSIA, 2014, art. 13, item c, p. 6, tradução nossa).

Em relação às ameaças militares, a doutrina (2014) mantém a preocupação com o funcionamento do sistema de comando e controle estabelecido em seu documento antecessor (RÚSSIA, 2014, art. 15, item b, p. 7).

A descrição dos conflitos militares contemporâneos também sofreu modificações devido aos acontecimentos que marcaram a guerra regional entre Rússia e Ucrânia, sinalizando uma importância estratégica crescente dada à tecnologia e controle do espaço de informação. Diante desse cenário, a doutrina (2014) apresenta de modo objetivo a percepção da Federação Russa acerca da nova natureza dos conflitos, marcados pelo emprego integrado de tropas militares e não militares em conjunto com ações políticas, econômicas e informativas, "implementadas com amplo uso do potencial de protesto da população e das forças de operações especiais" (RÚSSIA, 2014, art. 15, item a, p. 7, tradução nossa).

Igualmente, traz uma descrição detalhada dos sistemas de armas e equipamentos militares utilizados nestes conflitos como "armas hipersônicas de alta precisão, armas de guerra eletrônica, [...] sistemas de controle de informações e veículos marítimos e aéreos autônomos não tripulados" (RÚSSIA, 2014, art. 15, item b, p. 7, tradução nossa), ferramentas capazes de produzir impacto significativo sobre um território inimigo através do "espaço global de informações, espaço aeroespacial, em terra e no mar" (RÚSSIA, 2014, art. 15, item c, p. 7, tradução nossa).

Por conseguinte, ressalta a preocupação fundamental com o fortalecimento da guerra de informação mediante a "participação nas hostilidades de grupos armados irregulares e empresas militares privadas" (RÚSSIA, 2014, art. 15, item h, p. 7, tradução nossa) enquanto "método de ação indireto e assimétrico" (RÚSSIA, 2014, art. 15, item i, p. 6, tradução nossa) capaz de aumentar a capacidade dos agressores em fazer uso de "forças políticas e movimentos sociais financiados e controlados externamente" (RÚSSIA, 2014, art. 15, item j, p. 7, tradução nossa) para atingir a estabilidade interna de um país.

Na terceira seção a política militar da Federação russa também recebeu algumas inserções que revelam o papel estratégico da instituição na dissuasão dos conflitos com vistas à garantia da Defesa e a Segurança do Estado e da sociedade (RÚSSIA, 2014, art. 18, p. 8).

As principais formas de dissuasão e prevenção de conflitos militares (RÚSSIA, 2010, art. 9, p. 8) foram mantidas, com o acréscimo de trechos que indicam a necessidade de garantir a segurança da Federação em tempo de guerra mediante preparação dos quadros do

serviço militar para os conflitos contemporâneos. Desse modo, a doutrina (2014) oferece preponderância ao desenvolvimento das capacidades de organização para mobilização da "economia, autoridades estaduais, governos locais e organizações" (RÚSSIA, 2014, art. 21, item e, p. 8, tradução nossa) bem como à implementação de medidas socioeducativas com permitam aumentar a "efetividade da educação militar-patriótica dos cidadãos" (RÚSSIA, 2014, art. 21, item f, p. 8, tradução nossa).

A doutrina (2014) reforça a intenção em conter e prevenir conflitos militares mediante ações diplomáticas com o objetivo de fortalecer a segurança internacional a partir da manutenção de tratados de cooperação com países signatários da OTSC; CEI; OCX; OTAN e UE (RÚSSIA, 2010, art.19, item e, p. 8-9), e acrescenta a intenção em aprofundar os laços com as Repúblicas da Abkhazia e da Ossétia do Sul (RÚSSIA, 2014, art. 21, item h, p. 9).

Todavia, o documento acrescenta a necessidade da Federação em investir em tecnologia para conter a ameaça à paz e a segurança global e regional representada pelo avanço da OTAN sobre países fronteiriços a fim de: i) neutralizar tentativas de estados individuais (grupos de estados) de alcançar superioridade militar, implantando sistemas estratégicos de defesa antimísseis, armas no espaço sideral e sistemas não nucleares estratégicos de armas de alta precisão; ii) reduzir o risco do uso de tecnologias da informação e comunicação para fins militares e políticos para a implementação de ações dirigidas contra a soberania, independência política, integridade territorial dos Estados (RÚSSIA, 2014, art. 21, itens l,s, p. 9-10, tradução nossa).

No que tange o uso legítimo das Forças Armadas e outras tropas para dissuasão estratégica e/ou conter ataques realizados contra a Federação, a doutrina (2014, art. 22-31, p. 10-12) mantém na íntegra o posicionamento descrito em seu documento antecessor (RÚSSIA, 2009, art. 20-26, p. 9-11). No entanto, as principais tarefas das Forças Armadas em tempos de paz (RÚSSIA, 2010, art. 27, p. 11) receberam inserções que, dentre outros pontos, indicam a relevância crescente da tecnologia para a instituição ao declarar o interesse pela construção de "novas instalações de infraestrutura militar e modernização das existentes [...] bem como a seleção de instalações de uso dual pelas tropas para fins de defesa" (RÚSSIA, 2014, art. 32, item, i, p. 12, tradução nossa).

No que se refere ao desenvolvimento da organização militar, a doutrina (2014) reforça o interesse estratégico (RÚSSIA, 2010, art. 30, p. 13-14) em garantir o funcionamento do sistema de comando e controle e manter a segurança do fluxo de informação entre os órgãos públicos federais e estaduais em nível que permita à Federação Russa solucionar problemas

relativos à Defesa e Segurança de forma eficiente e dinâmica (RÚSSIA, 2014, art. 35, item b, p. 14). Não obstante, insere uma preocupação fundamental com o desenvolvimento das bases de mobilização das Forças Armadas, outras tropas e órgãos para recrutar e preparar quadros de reserva (RÚSSIA, 2014, art. 35, item m, p. 14).

As prioridades para o desenvolvimento da estrutura e organização militar da Federação frente aos desafios da era da informação (RÚSSIA, 2010, art. 32, p. 15) foram mantidas. Entretanto, a doutrina (2014) insere um artigo importante que estabelece como principal objetivo das Forças Armadas o alinhamento de sua estrutura com modelos modernos de armas e equipamentos militares especiais que permitam o combate às ameaças previstas de acordo com a natureza dos conflitos militares que podem ocorrer em tempos de paz ou guerra, com vistas ao aprimoramento contínuo das "capacidades políticas, socioeconômicas, demográficas e técnico-militares da Federação Russa" (RÚSSIA, 2014, art. 37, p. 15-16).

No que tange o desenvolvimento das Forças Armadas (RÚSSIA, 2010, art. 33, p. 16) a doutrina (2015) acrescenta ao estabelecido a importância do "treinamento de militares altamente profissionais dedicados à Pátria e o aumento do prestígio do serviço militar" (RÚSSIA, 2014, art. 38, p. 16, tradução nossa).

Em relação aos objetivos de construção e desenvolvimento organizacional das Forças Armadas e outras tropas da Federação Russa (RÚSSIA, 2010, art. 34, p. 16-17) foram acrescidos pontos relativos à formação de quadros capazes de prover a defesa das instalações militares e garantir a segurança da informação e o funcionamento das estruturas críticas de setores como transportes, comunicação e energia (RÚSSIA, 2014, art. 36, itens h, l, p. 17).

A doutrina (2014) alterou o planejamento militar, inserindo dois artigos que enfatizam a necessidade de preparação das forças, autoridades federais, estatais, locais, e, da própria economia da Federação Russa para mobilização contra ataques armados que por ventura afetem a segurança do estado e da população em tempo de guerra (RÚSSIA, 2014, art. 41, p. 18). Para tanto, prevê o investimento em treinamento para mobilização e construção de armas modernas que permitam a manutenção do potencial técnico militar em alto nível de suficiência (RÚSSIA, 2014, art. 40, p. 18).

A preocupação da Federação Russa com a eclosão de novos conflitos é percebida de modo objetivo com a reformulação dos principais objetivos do treinamento para mobilização, o novo artigo difere completamente dos manifestos na doutrina (2010, art. 36, p. 18), todos os itens foram revistos para contemplar a necessidade de preparação para mobilização em tempos de guerra (RÚSSIA, 2014, art. 42, p. 19).

Nesse sentido, o documento (2014) estabelece dentre as principais metas a garantia de um governo sustentável capaz de regulamentar a "aplicação de medidas econômicas durante o período de mobilização, lei marcial ou guerra" (RÚSSIA, 2014, art. 42, item b, p. 19, tradução nossa) e garantir a capacidade operacional das Forças Armadas, outras tropas e órgãos, a necessidade de formação de unidades especiais que possam organizar a mobilização, fornecendo "recursos humanos e materiais técnicos das próprias Forças Armadas, outras tropa e órgãos para resolver problemas em condição de guerra" (RÚSSIA, 2014, art. 42, item d,f, p. 19, tradução nossa) e a necessidade de manutenção da capacidade industrial em nível que garanta a capacidade de restauração de instalações danificadas ou destruídas durante conflitos e o fornecimento de mercadorias para atender a sociedade em tempos de guerra (RÚSSIA, 2014, art. 42, itens g-h, p. 19).

Na quarta seção, os pontos centrais que tratam das condições para oferecer suporte ao desenvolvimento militar foram mantidos (RÚSSIA, 2010, art. 39, p. 19). No entanto, o conteúdo disposto no documento (2010) foi reformulado e incorporado a um texto conciso que adiciona às principais tarefas uma preocupação fundamental do Estado em garantir o investimento em "equipamentos militares e especiais baseados no desenvolvimento do potencial científico militar do país" (RÚSSIA, 2014, art. 44, item a, p. 19-20, tradução nossa) com objetivo de ampliar a eficiência das operações militares.

Ademais, estabelece a primazia organizacional do CIM no que tenciona o "treinamento operacional, de combate e mobilização de tropas [...] desenvolvimento do complexo industrial militar" em nível que permita a coordenação das atividades econômico-militares das Forças Armadas, outras tropas e órgãos, garantindo a "integração das áreas de produção dos setores civil e militar da economia, a proteção legal dos resultados da atividade militar intelectual, especial e de uso dual" (RÚSSIA, 2014, art. 44, itens c-d, p. 20, tradução nossa).

Dentre as principais tarefas da economia militar (RÚSSIA, 2010, art. 41 p. 20), no que concerne à tecnologia empregada para equipar as Forças Armadas e outras tropas, a Doutrina Militar (2014) acrescenta a intenção de construir "novos modelos de armas de alta precisão e meios de combatê-las" (RÚSSIA, 2014, art. 46, item f, p. 21, tradução nossa) com atenção especial ao uso da tecnologia para funcionamento de "sistemas de defesa aeroespacial, sistemas de comunicação, reconhecimento e controle, guerra eletrônica, complexos de veículos aéreos não tripulados, sistemas de ataque robótico" (RÚSSIA, 2014, art. 46, item f, p. 21, tradução nossa).

No que concerne à estrutura do CIM, a doutrina (2014, art. 45, p. 22) manteve a preponderância da tecnologia da informação para as forças conforme disposto em seu documento antecessor (RÚSSIA, 2010, art. 45, p. 21). Igualmente, em relação ao desenvolvimento do CIM, a doutrina (2014) manteve os principais objetivos do documento anterior (RÚSSIA, 2010, art. 46, p. 22-23), com acréscimo de um item que indica a importância da tecnologia da informação para o equipamento das forças mediante a necessidade de garantir a "produção e prontidão tecnológica das organizações do complexo para o desenvolvimento e produção de tipos prioritários de armas e equipamentos militares especiais" (RÚSSIA, art. 53, item o, 2014, p. 23, tradução nossa).

No campo da cooperação entre a Federação Russa e os estados estrangeiros, as intenções de fortalecer os tratados com as comunidades de países que compõem o CSTO, CIS e OCX através da construção de sistemas regionais de segurança (RÚSSIA, 2010, art. 51, p. 26) foram mantidas.

Por fim, apresenta a inclusão de dois pontos fundamentais para a compreensão da percepção russa acerca da importância da tecnologia nos conflitos regionais nas fronteiras da Federação, o interesse em estreitar os laços diplomáticos com as Repúblicas da Abkhazia e Ossétia do Sul (RÚSSIA, 2014, art. 55, item b, p. 24) , e, a intenção de estabelecer o diálogo com os Estados interessados acerca das "abordagens nacionais para combater os perigos e ameaças militares decorrentes do uso em larga escala de tecnologias de informação e comunicação para fins político-militares" (RÚSSIA, 2014, art. 55, item f, p. 24) fato que demonstra a preocupação crescente da Federação Russa com o uso da tecnologia da informação nos conflitos contemporâneos e sinaliza o forte caráter regional de sua política externa. O quadro 2 sumariza os principais temas abordados pela Doutrina Militar (2010; 2014).

Quadro 2 Principais Temas Abordados

Categorias	**Ameaças**	**Armas de Precisão**	**Eficiência**	**Complexo Industrial Militar**	**Cooperação**
Doutrina Militar (2010)	Art. 6 Art. 7 Art. 8 Art. 10 Art. 19 Art. 20 Art. 32	Art. 8 Art. 15 Art. 22	Art. 12 Art. 27 Art. 30 Art. 31 Art. 32 Art. 39 Art. 41 Art. 46	Art. 33 Art. 34 Art. 45 Art. 46	Art. 4 Art. 19 Art. 36 Art. 49 Art. 50 Art. 51
Doutrina Militar (2014)	Art. 2 Art. 6 Art. 8 Art. 10 Art. 11 Art. 12 Art. 13 Art. 15 Art. 22 Art. 41 Art. 55	Art. 15 Art. 21 Art. 44 Art. 46 Art. 53	Art. 15 Art. 21 Art. 35 Art. 42 Art. 44	Art. 27 Art. 32 Art. 35 Art. 36 Art. 37 Art. 38 Art. 44 Art. 53	Art. 18 Art. 19 Art. 20 Art. 44 Art. 51 Art. 55

Fonte: Elaborado pelo autor.

2.3.3 Estratégia de Segurança Nacional da Federação Russa (2009)

Promulgada pelo então presidente eleito Dmitry Medvedev em 13 de maio de 2009, a Estratégia de Segurança Nacional da Federação Russa (2009)[13] é o documento que serve de base para a Doutrina Militar, o documento estabelece as ações estratégicas adotadas para garantir a segurança nacional e o desenvolvimento sustentável do Estado e apresenta a percepção da Rússia acerca dos desafios que o século vinte e um impõe aos Estados em âmbito interno e externo. Nesse sentido, resulta da superação do processo histórico que conduziu ao esfacelamento da União das Repúblicas Soviéticas (URSS) em meados do século vinte.

A primeira seção apresenta a percepção da Federação do contexto histórico internacional que se constitui após o esfacelamento da União das Repúblicas Socialistas Soviéticas (URSS), no qual a Rússia se encontra inserida enquanto um país que conseguiu se recuperar da crise política e socioeconômica que ao final do século vinte e um havia reduzido, consideravelmente, a qualidade de vida de seus cidadãos (RÚSSIA, 2009, art. 1, p. 1).

Uma Rússia que não apenas resistiu à "pressão do nacionalismo, separatismo e terrorismo internacional, impediu o descrédito da ordem constitucional, preservou a soberania e a integridade territorial" (RÚSSIA, 2009, art. 1, p. 1, tradução nossa), como também soube reavivar a memória histórica do povo russo de acordo com "valores comuns – liberdade e independência do estado russo, humanismo, paz internacional e a unidade de culturas do povo multinacional da Federação Russa, respeito pelas tradições familiares, patriotismo" (RÚSSIA, 2009, art. 1, p. 1, tradução nossa).

A Estratégia de Segurança Nacional (2009) manifesta o interesse da Federação em inserir o país na ordem global como uma potência com peso significativo nos processos decisórios internacionais a partir da ampliação dos investimentos em tecnologia de modo a garantir a competitividade da economia nos mercados externos e melhorar a qualidade de vida do povo russo (RÚSSIA, 2009, art. 1, p. 1).

---

[13] O documento está dividido em seis seções, a primeira trata da implementação da política de estado com foco no desenvolvimento do sistema de segurança nacional para prevenir ameaças internas e externas a integridade e soberania territorial do Estado (artigos 1-7), a segunda ressalta o papel da Rússia em um contexto internacional marcado pelo avanço da globalização que constitui um novo modelo policêntrico da ordem mundial (artigos 8-20); a terceira apresenta as prioridades estratégicas que garantem a segurança nacional (artigos 21-24), e a quarta trata da segurança nacional em suas mais diversas áreas temáticas (artigos 25-96); a quinta apresenta a estrutura organizacional, regulamentar e informacional para implementação da estratégia (artigos 97-111); e a última revela os principais indicadores utilizados para mensurar o estado de segurança nacional do país (artigo 112) (RÚSSIA, 2009).

No que se refere à contenção das ameaças internas, a estratégia (2009) tem como principal objetivo fortalecer as agências estatais -Forças Armadas, outras tropas, unidades e órgãos do governo federal- responsáveis por garantir a segurança nacional interna e externa protegendo as liberdades constitucionais, a qualidade de vida dos cidadãos, a soberania e a integridade territorial da Federação Russa (RÚSSIA, 2009, art. 2, p. 2).

No que concerne aos meios para consecução dos objetivos estratégicos de segurança, o documento oferece destaque para o campo da ciência e educação com vistas à utilização de "tecnologias como meios técnicos, de software, linguísticos, legais, organizacionais, incluindo canais de telecomunicações, usados no sistema de segurança nacional para coletar, formar, processar, transmitir ou receber informações" (RÚSSIA, 2009, art. 6, itens i, iv, vii, p. 3, tradução nossa).

No âmbito internacional, a segunda seção apresenta a percepção russa sobre o as mudanças na condição geopolítica do século vinte e um que resultam do avanço do processo de interdependência dos Estados, marcado pelo desenvolvimento desigual entre os países e o fortalecimento de novos centros de crescimento econômico e influencia política. De acordo com a estratégia (2009) esse processo delimita uma "tendência para encontrar solução para os problemas existentes e resolver situações de crise em uma base regional sem a participação de forças não regionais" (RÚSSIA, 2009, art. 8, p. 4, tradução nossa).

Não obstante, a estratégia (2009) apresenta a intenção da Federação Russa de estabelecer, no médio prazo, "condições para sua consolidação entre os principais países da economia mundial" (RÚSSIA, 2009, art. 9, p. 4, tradução nossa) mediante o investimento do Estado nas áreas de Defesa e Segurança pública.

O documento demonstra uma preocupação fundamental da Federação Russa com o crescimento dos conflitos contemporâneos, questões relativas ao campo da alta tecnologia como o aumento de armas de destruição em massa e atividades cibernéticas ilegais são tomadas como entraves ao interesse nacional. Nesse sentido, aponta para o crescimento de conflitos globais envolvendo o espaço de informação como fator chave na desestabilização de territórios nacionais mediante a promoção de "sentimentos nacionalistas, xenofobia, separatismo e extremismo violento, inclusive sob os slogans do radicalismo religioso" (RÚSSIA, 2009, art. 10, p. 5, tradução nossa).

No que se refere em específico aos conflitos regionais, o documento expressa que a decisão dos Estados Unidos de instalar um sistema de defesa antimísseis nas regiões fronteiriças da Rússia é percebida como fator de instabilidade, em sequência, frisa que em

resposta a esse movimento as Forças Armadas russas poderão ser empregadas com intuito de restabelecer o equilíbrio de poder nessas áreas (RÚSSIA, 2009, art. 12, p. 5).

Igualmente, o documento reforça a percepção russa de que o avanço da infraestrutura militar da OTAN nas regiões fronteiriças da Federação, desconsiderando os interesses legítimos da Rússia nesses territórios, é fator preponderante para a redução da segurança na região euro-atlântica (RÚSSIA, 2009, art. 17, p. 7). No entanto, mesmo diante desse cenário, a Rússia manifesta interesse em "construir uma parceria estratégia igual e de pleno direito com os EUA" (RÚSSIA, 2009, art. 18, p. 7, tradução nossa) com foco no controle da proliferação de armas de destruição em massa e na cooperação para resolução de conflitos regionais.

A estratégia (2009) firma o compromisso da Federação Russa em exercer uma Política Externa marcada pela previsibilidade pragmática, com uso de instrumentos políticos, econômicos e militares para proteção da soberania do Estado e dos interesses nacionais. A fim de evitar danos causados por ameaças à segurança nacional. À vista disso, o documento propõe "aumentar o potencial de mobilização e crescimento da economia" (RÚSSIA, 2009, art. 20, p. 8, tradução nossa) e criar mecanismos eficientes de interação entre os órgãos públicos e a sociedade civil que permitam tornar efetivo o direito dos cidadãos russos ao acesso a "segurança, trabalho, moradia, saúde, educação, estilo de vida saudável e desenvolvimento cultural" (RÚSSIA, 2009, art. 20, p. 8, tradução nossa).

Na terceira seção, a estratégia (2009) apresenta os interesses nacionais e as prioridades estratégicas de longo prazo da Federação Russa para se consolidar como potência mundial, capaz de desempenhar papel fundamental na manutenção da estabilidade global e regional em um mundo multipolar, dentre as quais se destacam "o desenvolvimento da democracia e da sociedade civil, e o aumento da competitividade de economia nacional" (RÚSSIA, 2009, art. 21, p. 8, tradução nossa) com garantia dos direitos fundamentais regidos pela carta constitucional -integridade territorial e soberania- (RÚSSIA, 2009, art. 21, p. 8). Desse modo, pontua como prioridade interna e externa do Estado a garantia da eficiência da Defesa nacional e da Segurança pública (RÚSSIA, 2009, art. 23, p. 8).

A quarta seção está dividida em nove subseções que apontam para a correlação entre crescimento econômico e eficiência dos mecanismos legais e institucionais no que tange a garantia do sistema de segurança nacional (RÚSSIA, 2009, art. 25, p. 9). Destacamos algumas delas que demonstram a prioridade conferida pela Federação ao investimento em tecnologia, pesquisa e desenvolvimento.

A primeira subseção apresenta os objetivos estratégicos da Defesa nacional no que concerne a contenção de conflitos e guerras globais e regionais através do emprego da dissuasão estratégica que se dá através do desenvolvimento e implementação de medidas "políticas, diplomáticas, militares, econômicas, informacionais" (RÚSSIA, 2009, art. 26, p. 10, tradução nossa) para contenção das ameaças.

Nesta subseção a Estratégia de Segurança Nacional (2009) demonstra a importância do desenvolvimento da estrutura militar para a Defesa nacional, fundada sob os princípios de suficiência e eficiência. Por esse ângulo, frisa que a consecução dos objetivos estratégicos da Defesa nacional depende do estágio de "desenvolvimento da infraestrutura militar e da organização militar do Estado" (RÚSSIA, 2009, art. 28, p. 10, tradução nossa) para implementar medidas capazes de ampliar o reconhecimento do serviço militar enquanto atividade vital para o desenvolvimento da Federação. Todavia, sua base não engloba apenas meios militares, mas também mecanismos de diplomacia e cooperação internacional (RÚSSIA, 2009, art. 27, p. 10).

As principais ameaças à segurança militar, reconhecidas pela estratégia (2009) estão diretamente conectadas ao desenvolvimento da tecnologia de informação que, de acordo com o documento, auxiliam na implementação da política expansionista de países estrangeiros a partir do desenvolvimento e emprego de equipamentos militares -armas de alta precisão, guerra de informação, armas químicas, armas nucleares e a formação do sistema global unilateral de defesa antimíssil-, que podem levar a uma nova corrida armamentista devido a crescente militarização do espaço próximo à Rússia (RÚSSIA, 2009, art. 30, p. 10-11).

No médio prazo, a tecnologia se destaca como chave para consecução dos interesses da Federação Russa, assim, a estratégia (2009) expressa que o principal objetivo estratégico da Defesa nacional é a transformação qualitativa das Forças Armadas, meta perseguida, dentre outras ações, através do "desenvolvimento, criação e modernização de armas e equipamentos militares especiais, incluindo comunicações, inteligência, guerra eletrônica e gestão" (RÚSSIA, 2009, art. 31, p. 11, tradução nossa).

Não obstante, no médio prazo, reforça o papel fulcral da tecnologia para consecução dos objetivos estratégicos, na medida em que prevê o uso de "tipos modernos de armas e equipamentos especiais" (RÚSSIA, 2009, art. 34, p. 12, tradução nossa) não apenas pelas Forças Armadas da Federação, como também por outras tropas, unidades e órgãos paramilitares que assegurem a "manutenção de estoques de recursos materiais no estado e as

reservas de mobilização, bem como a cooperação com outros estados no campo da segurança militar" (RÚSSIA, 2009, art. 33, p. 12, tradução nossa).

A segunda subseção apresenta os objetivos estratégicos da Segurança pública no que concerne a garantia dos "fundamentos do sistema constitucional, [...] proteção da soberania e integridade territorial, [...] e preservação da estabilidade política e social" (RÚSSIA, 2009, art. 35, p. 12, tradução nossa).

As principais ameaças à segurança nacional, reconhecidas pela Estratégia de Segurança Nacional (2009) estão relacionadas às "atividades de inteligência e serviços especiais de Estados estrangeiros, [...] grupos e organizações terroristas, [...] atividades extremistas [...] e de grupos de criminosos transnacionais" (RÚSSIA, 2009, art. 37, p. 12, tradução nossa) com potencial para desorganizar o funcionamento da esfera pública, prejudicar o funcionamento de infraestruturas críticas, causar instabilidade social e aumentar o tráfico ilegal no país.

No longo prazo, para combater estas ameaças à estratégia (2009) propõe ampliar a presença do Estado enquanto ente garantidor da Segurança, reformar os mecanismos institucionais de combate a organizações criminosas e aplicar melhorar a eficiência do sistema de proteção de direitos dos cidadãos russos, inclusive daqueles que residem fora da Federação (RÚSSIA, 2009, art. 38, p. 13).

Para tanto, prevê o aprimoramento institucional das agencias policiais e serviços especiais responsáveis por garantir a aplicação da lei, o aumento da responsabilidade social do Estado e da segurança pública mediante a implementação de um plano nacional que contenha mecanismos para prevenir e combater o "terrorismo internacional e nacional, o extremismo político e religioso, e o separatismo" (RÚSSIA, 2009, art. 40, p. 14, tradução nossa), além do aprimoramento do "complexo industrial militar, nuclear, químico e de energia atômica do país" (RÚSSIA, 2009, art. 40, p. 14, tradução nossa).

Sem embargo, a estratégia (2009) apresenta uma preocupação fundamental com segurança das fronteiras da Federação Russa, ameaçada pela escalada de conflitos armados nessas regiões desencadeados pela ação criminosa de "organizações terroristas e extremistas internacionais" (RÚSSIA, 2009, art. 41, p. 14, tradução nossa) associados ao tráfico ilegal que exploram vulnerabilidades na infraestrutura e equipamentos técnicos dos quais dispõem as autoridades responsáveis pela segurança desses. Para resolver esse problema, o documento avalia a criação de "complexos fronteiriços multifuncionais de alta tecnologia" (RÚSSIA,

2009, art. 42, p. 15, tradução nossa) nas divisas de seu entorno regional com países como a República do Cazaquistão, Ucrânia, Geórgia e República do Azerbaijão.

No intuito de garantir a segurança nacional em casos emergenciais, o documento estabelece como imprescindível o aumento da eficiência do exercício dos poderes das autoridades locais, bem como o investimento na modernização de equipamentos de alta tecnologia que garantam o funcionamento dos sistemas de operação das infraestruturas críticas (RÚSSIA, 2009, art. 43, p. 15, tradução nossa).

A terceira subseção apresenta os objetivos estratégicos para conter ameaças a qualidade de vida dos cidadãos russos que podem ser causados por fatores como problemas em "sistemas financeiros bancários globais e regionais, aumento da concorrência na luta por matérias-primas escassas, energia, recursos hídricos e alimentares, atraso no desenvolvimento de estruturas tecnológicas avançadas" (RÚSSIA, 2009, art. 47, p. 16, tradução nossa).

Dentre as ações previstas para combater as ameaças à qualidade de vida dos cidadãos russos, a estratégia (2009) enfoca, dentre outras prioridades, a garantia de acesso da população aos veículos que empregam tecnologia da informação para tratar de questões relativas à "vida sócio-política, econômica e espiritual da sociedade" (RÚSSIA, 2009, art. 52, p. 16, tradução nossa), para tanto examina a criação de parcerias entre o setor público e a iniciativa privada capazes de alavancar os objetivos estabelecidos nesse campo.

Na quarta subseção o documento apresenta os objetivos estratégicos para garantir o crescimento econômico da Federação, pontua questões como "a entrada da Rússia no médio prazo entre os cinco maiores países em termos de produto interno bruto" (RÚSSIA, 2009, art. 53, p. 17, tradução nossa) e a necessidade de garantir "a segurança nacional nas esferas econômica e tecnológica" (RÚSSIA, 2009, art. 53, p. 17, tradução nossa).

O documento (2009) aponta dentre os principais riscos e ameaças à segurança nacional na esfera econômica: i) a necessidade de preservação do modelo de exploração de matérias-primas para exportação; ii) a redução da competitividade externa da industria nacional; iii) o crescimento da dependência externa; iv) a falta de controle dos recursos nacionais; v) a precarização da indústria de energia; vi) a desigualdade regional; vii) a escassez de mão-de-obra; viii) a instabilidade do sistema financeiro; ix) a migração ilegal (RÚSSIA, 2009, art. 55, p. 18, tradução nossa).

Com o intuito de garantir o crescimento econômico que sustente a segurança nacional, a Estratégia de Segurança Nacional (2009) prevê um alto investimento em desenvolvimento da ciência, tecnologia e educação através de parcerias público-privadas que auxiliem a

Federação Russa a atingir o grau necessário de "segurança nas Forças Armadas, indústria de Defesa e nas esferas internacionais" (RÚSSIA, 2009, art. 58, p. 18, tradução nossa).

Destarte, a estratégia (2009) revela que o combate às ameaças à segurança econômica depende da atuação conjunta entre as forças de segurança nacional e instituições da sociedade civil no que se refere ao apoio de políticas sociais e econômicas que objetivam, dentre os pontos, o aprimoramento do sistema nacional de inovação através da implementação de programas para o "desenvolvimento de setores de alta tecnologia da economia" (RÚSSIA, 2009, art. 61, p. 19, tradução nossa) que favoreçam a interação entre ciência, educação e produção. Por essa lógica, ressalta a importância do "desenvolvimento da indústria de tecnologias da informação e telecomunicações, instalações de informática, rádios eletrônicos, equipamentos e software de telecomunicações" (RÚSSIA, 2009, art. 61, p. 19, tradução nossa) como fator chave para o combate efetivo dessas ameaças.

No que tange a esfera política a estratégia (2009) registra como necessário o aprimoramento da regulamentação estadual com vistas ao crescimento econômico, ação executada a partir da reformulação de diretrizes institucionais para a construção de um sistema integrado de controle de riscos que permita ao Estado "estimular e apoiar o desenvolvimento do mercado de inovação, produtos de alta tecnologia e produtos de alto valor agregado, o desenvolvimento de tecnologias promissoras para fins gerais, duais e especiais" (RÚSSIA, 2009, art. 63, p. 20, tradução nossa).

A quinta subseção apresenta os objetivos estratégicos para garantia da segurança nacional nos campos da ciência, tecnologia e educação, realizados por meio da organização estatal enquanto ente responsável por orientar o desenvolvimento das organizações científico-tecnológicas. Á vista disso, o Estado é tido como principal responsável pela implementação de um sistema nacional de inovação que assegure a competitividade da economia e atenda as demandas da Defesa, igualmente, fixa como fundamental o investimento na formação de profissionais qualificados para atuarem nesses campos, ampliando as possibilidades de mobilidade da sociedade civil (RÚSSIA, 2009, art. 66, p. 21, tradução nossa).

No médio prazo, a estratégia (2009) sublinha os campos da ciência e educação como a principais vetores para sustentar o desenvolvimento e inovação industrial, desse modo, tenciona o treinamento de especialistas e trabalhadores altamente qualificados bem como a construção de parcerias público-privadas que permitam integrar os campos da ciência, inovação e indústria em prol da consecução dos objetivos estratégicos da "defesa nacional,

estadual e da segurança pública, bem como o desenvolvimento sustentável do país" (RÚSSIA, 2009, art. 68, p. 22, tradução nossa).

No longo e médio prazo, a fim de garantir a segurança nacional nos campos da ciência, tecnologia e educação, a estratégia (2009) estabelece como prioridade o investimento no desenvolvimento de produtos que empreguem alta tecnologia, a ser realizado através da rede de ensino superior com participação de instituições federais e nacionais de pesquisa atuando em conjunto para fornecer o treinamento de especialistas capazes de atuarem nesses campos em âmbito doméstico e internacional (RÚSSIA, 2009, art. 70, p. 22).

A nona subseção apresenta a estratégia russa para manter a estabilidade das relações internacionais fazendo uso de uma política externa ativa com foco na construção de "acordos bilaterais e multilaterais que sejam mutuamente benéficos" (RÚSSIA, 2009, art. 89, p. 27, tradução nossa) para os entes contratantes.

Com intuito de garantir a estabilidade estratégica, o documento propõe o avanço nos diálogos para construção de novos acordos que permitam a contenção da proliferação de armas nucleares e outras armas ofensivas, mediante a atuação pragmática e previsível das ações dos Estados nesse campo (RÚSSIA, 2009, art. 90-91, p. 27, tradução nossa). No entanto, sustenta o uso legítimo de "contingentes das Forças Armadas da Federação Russa com base no direito internacional" (RÚSSIA, 2009, art. 93, p. 27, tradução nossa) como agência de reforço na resolução de questões políticas e econômicas sem uso de força física, desse modo, defende o potencial de ação da instituição militar para "manter a estabilidade estratégica" e a "igualdade das parcerias" (RÚSSIA, 2009, art. 93, p. 28, tradução nossa) construídas entre os Estados contemporâneos.

No que se refere às ações para manutenção da estabilidade e construção de parcerias estratégicas a Federação Russa se compromete a honrar "tratados e acordos existentes no campo da limitação e redução de armas" e a discutir "condições para redução das armas nucleares" (RÚSSIA, 2009, art. 95, p. 28, tradução nossa), participar dos "processos de redução e limitação das forças armadas convencionais", fazer valer os "princípios constantes na Carta das Nações Unidas" (RÚSSIA, 2009, art. 95, p. 28, tradução nossa) e colaborar, no que tange a prestação de serviços e assistência humanitária, com as "ações organizadas pelas Nações Unidas e outras organizações internacionais" (RÚSSIA, 2009, art. 95, p. 28, tradução nossa).

Ainda no que concerne às ações para garantir a estabilidade estratégia, o documento estabelece a pretensão de construir acordos de "cooperação multilateral igual no cenário

internacional" (RÚSSIA, 2009, art. 96, p. 29, tradução nossa), no intuito de concentrar "esforços necessários no nível menos oneroso para manter a paridade com os EUA no campo das armas ofensivas estratégicas, no contexto da implantação de um sistema global de defesa antimísseis" (RÚSSIA, 2009, art. 96, p. 29, tradução nossa).

Na quinta seção, em relação ao controle de ameaças à segurança da informação, a estratégia (2009) prioriza a "segurança do funcionamento dos sistemas de informação e telecomunicações da infraestrutura crítica e instalações de alto risco" (RÚSSIA, 2009, art. 109, p. 31, tradução nossa) e estipula a criação de um "sistema unificado de suporte à informação e telecomunicações para as necessidades do sistema de segurança nacional" (RÚSSIA, 2009, art. 109, p. 31, tradução nossa) capaz de garantir a implementação dos objetivos traçados neste documento.

Por fim, a sexta seção apresenta as variáveis utilizadas para mensurar a segurança nacional: i) taxa de desemprego; ii) renda; iii) taxa de crescimento de preços; iv) dívida externa e interna em porcentagem do Produto Interno Bruto (PIB); v) nível de provisão de recursos em saúde, cultura, educação e ciência em porcentagem do PIB; vi) nível de produção anual de armas, equipamentos militares e especiais; vii) nível de segurança militar e de engenharia (RÚSSIA, art. 112, p. 31-32, tradução nossa).

2.3.4 Análise comparada: Estratégia de Segurança Nacional (2009;2015)

Promulgada pelo presidente Vladmir Putin em 31 de dezembro de 2015, a Estratégia de Segurança Nacional (2015)[14] aponta os resultados das medidas adotadas pela Rússia desde a publicação de seu documento antecessor e redefine alguns dos interesses nacionais e prioridades estratégicas estabelecidos no intuito de fortalecer a Defesa, a Segurança e garantir o desenvolvimento do país (RÚSSIA, 2015, art. 1, p. 2).

Inicialmente, a estratégia (2015) mantém o objetivo de consolidar os esforços da esfera pública para consecução dos interesses estratégicos da Federação Russa no que

[14] O documento (2015) está dividido em seis seções, a primeira apresenta disposições gerais da política estatal para formar e manter forças capazes de garantir a segurança nacional e prevenir ameaças internas e externas a integridade e soberania territorial do Estado (artigos 1-7); a segunda revisa o papel da Rússia na ordem mundial frente aos conflitos desencadeados entre este país e as potências ocidentais Estados Unidos e UE nos territórios fronteiriços da Federação (artigos 7-29); a terceira apresenta as prioridades estratégicas da segurança nacional (artigos 21-31); a quarta trata da segurança nacional em suas mais diversas áreas temáticas (artigos 32-107); a quinta apresenta a estrutura organizacional, regulamentar e informacional para implementação da estratégia (artigos 108-114); e a última revela os principais indicadores utilizados para mensurar o estado de segurança nacional do país (artigo 115) (RÚSSIA, 2015).

concerne a garantia da segurança nacional, compreendida como a defesa do país de "todos os tipos de segurança previstos na Constituição [...] estatais, públicas, informativas, ambientais, econômicas, transportes, segurança energética, segurança pessoal" (RÚSSIA, 2015, art. 6, p. 3, tradução nossa), para tanto prevê a continuidade da implementação de ações "políticas, militares, organizacionais, socioeconômicas, informacionais, legais e outras" (RÚSSIA, 2015, art. 6, p. 3, tradução nossa) para conter as ameaças diretas ou indiretas aos interesses nacionais.

Em termos comparativos, a primeira seção da estratégia (2015) apresenta um texto mais conciso e direto que oferece maior clareza aos conceitos adotados neste documento. Entretanto, alguns trechos foram propositalmente retirados dos conceitos básicos utilizados neste documento, evitando assim a menção direta a presença de atores não-estatais –outras tropas- nas forças de segurança nacional, bem como à tecnologia da informação enquanto meio de controle das ameaças à segurança nacional (RÚSSIA, 2015, art. 6, p. 3).

No âmbito internacional, a segunda seção sofreu reduções significativas no que concerne à percepção russa dos eventos recentes, a descrição do avanço do processo de interdependência dos Estados (RÚSSIA, 2009, art. 8, p. 4) deu lugar a dois artigos objetivos que se referem às capacidades demonstradas pela Federação Russa para ampliar seu potencial econômico, político, militar e espiritual (RÚSSIA, 2015, art. 7, p. 3-4) e contribuir para assegurar a estabilidade estratégica das relações interestatais mediante participação ativa nos processos de resolução de conflitos militares em observância aos princípios do direito internacional (RÚSSIA, 2015, art. 8, p. 4).

Por conseguinte, a estratégia (2015) busca reforçar o papel de destaque da Rússia naquilo que designa como uma ordem mundial policêntrica, cenário no qual se torna fulcral para a Federação garantir a "soberania, independência, integridade estatal e territorial e a proteção dos direitos de compatriotas no exterior" (RÚSSIA, 2015, art. 8, p. 4, tradução nossa).

Refletindo os acontecimentos históricos recentes -eclosão dos conflitos no leste ucraniano e anexação do território da Crimeia- que culminaram na imposição de sanções econômicas por parte da União Europeia (UE) e os Estados Unidos à Federação Russa, a estratégia (2015) retira os trechos que tratavam das intenções de médio prazo para inserção da Rússia entre os principais países da economia mundial (RÚSSIA, 2009, art. 9, p. 4) para ressaltar o potencial de sua economia para "manter e fortalecer seu potencial em condições de

instabilidade na economia mundial" (RÚSSIA, 2015, art. 9, p. 4, tradução nossa) em uma evidente declaração da capacidade de reação do país às sanções impostas.

No que se refere às preocupações com os conflitos contemporâneos, o documento (2015) apresenta trechos pouco específicos quando comparado a seu predecessor. De tal modo que a descrição do modelo de operação das ameaças com potencial para afetar os interesses nacionais através de atividades ilegais realizadas através do espaço de informação (RÚSSIA, 2015, art. 10, p. 5) foi retirada para apresentar de modo sucinto as ações positivas realizadas pela Federação para melhorar a qualidade de vida dos cidadãos russos, tais como medidas para garantir o crescimento demográfico e ampliar a expectativa de vida dos cidadãos russos (RÚSSIA, 2015, art. 10, p. 4).

O alerta presente na estratégia (2009) sobre o agravamento dos conflitos regionais próximos às fronteiras da Federação Russa causado pela instalação do sistema de defesa antimíssil norte americano nesses territórios (RÚSSIA, 2009, art. 12, p. 5) também alterado Nessa sequência, a estratégia (2015) passa a oferecer uma resposta clara ao confronto de interesses posto entre o país e os Estados Unidos e seus aliados no que se refere a questões globais na medida em que reforça a intenção da Federação Russa em atuar de modo independente nas esferas da política externa e doméstica como contrapartida à "pressão política, econômica, militar e de informações" (RÚSSIA, 2015, art. 11, p. 4, tradução nossa) imposta por seus adversários.

A preocupação russa expressa na estratégia (2009, art. 17, p. 7) com o avanço da infraestrutura militar da OTAN sobre as regiões fronteiriças ignorando os interesses legítimos da Rússia nesses territórios é contraposta de modo objetivo na estratégia (2015). De acordo com o documento, as tentativas do ocidente de conter o processo de integração da Ucrânia à Federação Russa, orquestrada por um 'golpe inconstitucional' apoiado pela UE e os Estados Unidos produziu o caos na sociedade ucraniana na medida em que contratirou diretamente os interesses nacionais russos na região da Eurásia (RÚSSIA, art. 17, 2015, p. 5).

Diante deste cenário, a estratégia (2015) frisa que o "fortalecimento da ideologia nacionalista de extrema direita e a formação intencional da imagem da Rússia como inimiga da população ucraniana" (RÚSSIA, 2015, art. 17, p. 56, tradução nossa) transformou a Ucrânia em um vetor de instabilidade na Europa, dando início às operações de uso da força por parte dos envolvidos.

Destarte, o interesse na construção de acordos estratégicos com os EUA para controle da proliferação de armas de destruição em massa e contenção de conflitos regionais, mediante

adoção do pragmatismo na política externa orientado para o controle das ameaças à segurança nacional, bem como a intenção de construir mecanismos de interação entre os órgãos públicos e a sociedade civil para o desenvolvimento da Federação Russa presentes na estratégia (2009, art. 17-18, p. 7-8) cederam lugar na estratégia (2015) à preocupação com as capacidades manifestadas pelos Estados contemporâneos para desestabilizar regimes políticos legítimos a partir do fomento ao "ódio étnico, ódio religioso e outras manifestações de extremismo" (RÚSSIA, 2015, art. 18, p. 6).

A estratégia (2015) acrescenta outros nove artigos à segunda seção que apontam para o impacto do uso do espaço global da informação pelos Estados contemporâneos para consecução de objetivos geopolíticos através do fomento aos conflitos internacionais. À vista disso, denuncia os anseios de alguns Estados em empregar as "tecnologias da informação e comunicação" para "manipulação da consciência pública e falsificação da história" (RÚSSIA, 2015, art. 21, p. 6).

Á face do exposto, o documento expressa uma preocupação fundamental com o crescimento da criminalidade cibernética "em particular com o uso de informação, comunicação e tecnologia de ponta" (RÚSSIA, 2015, art. 22, p. 6) por grupos transnacionais. Ademais, frisa que o uso da "tecnologia para resolução de conflitos geopolíticos" (RÚSSIA, 2015, art. 24, p. 7, tradução nossa) prejudica a estabilidade das relações econômicas internacionais e aumenta a incidência de novas crises financeiras em larga escala.

Frente a este cenário, para se proteger a Federação Russa manifesta interesse em investir no desenvolvimento de mercados regionais e sub-regionais (RÚSSIA, 2015, art. 25, p. 7) bem como adotar medidas que permitam fortalecer a "unidade interna da sociedade russa, garantindo estabilidade social, harmonia interétnica e tolerância religiosa" (RÚSSIA, 2015, art. 26, p. 7, tradução nossa). Nesse sentido, o fortalecimento da capacidade de Defesa do país figura como chave para ajudar a eliminar possíveis desequilíbrios na economia (RÚSSIA, 2015, art. 26, p. 7).

No que concerne à política externa, a estratégia (2015) mantém o compromisso com a defesa do pragmatismo previsível enquanto diretriz para frear uma provável corrida armamentista (RÚSSIA, 2015, art. 27, p. 7). No entanto deixa de lado a intenção de construir mecanismos domésticos de resolução de conflitos (RÚSSIA, 2009, art. 20, p. 8) para sustentar a necessária construção de acordos externos lastreados por princípios do direito internacional que permitam a diversificação das parcerias no intuito de fortalecer o comércio multilateral e a segurança nacional (RÚSSIA, 2015, art. 28, p. 7). Desse modo, prevê utilizar "instrumentos

políticos legais, diplomacia e mecanismos de manutenção da paz" (RÚSSIA, 2015, art. 29, p. 8-9, tradução nossa) como medida cautelar ao uso da força militar que só deverá ser empregada caso tenham se esgotados "todas as medidas de natureza não violenta adotadas" (RÚSSIA, 2015, art. 29, p. 8, tradução nossa).

A terceira seção sofreu alguns ajustes na estratégia (2015), com a redução de quatro para dois artigos que contemplam basicamente os mesmos interesses nacionais de longo prazo, dentre eles, a consolidação da condição de potência global do país, garantia da soberania e integridade do território, competitividade da economia, qualidade de vida dos cidadãos russos e melhoria dos mecanismos de interação entre o Estado e a sociedade civil (RÚSSIA, 2015, art. 30, p. 8). Para tanto, estabelece como chave a continuidade da implementação de uma série de prioridades estratégicas nos campos da economia, Defesa nacional e a Segurança pública (RÚSSIA, 2015, art. 31, p. 8).

A quarta seção, igualmente, dividida em nove subseções, sustenta que a segurança nacional depende da implementação eficiente das prioridades nacionais estratégicas da Federação Russa (RÚSSIA, 2015, art. 35, p. 9).

Na primeira subseção, referente aos objetivos estratégicos da Defesa nacional, houve alteração em todos os artigos. Contudo, embora seu conteúdo permaneça semelhante ao do documento de 2009, algumas informações foram modificadas, omitida e/ou reformuladas de acordo com o andamento dos conflitos que se desencadearam entre 2010 e 2015.

A contenção de conflitos regionais e globais por intermédio da dissuasão (RÚSSIA, 2009, p. 10) deixa de ocupar o centro dos objetivos da Defesa nacional, no documento (2015) o desenvolvimento socioeconômico e a segurança militar são estabelecidos como as principais metas estratégicas da Federação Russa (RÚSSIA, 2015, art. 33, p. 9).

A estratégia (2015) mantém e reforça a percepção da Federação Russa de que a consecução dos objetivos estratégicos da Defesa depende da implementação da política militar enquanto mecanismo capaz de proporcionar os meios para aumentar a eficiência da "organização militar do estado, formas e métodos de uso das forças armadas, outras tropas, unidades e órgãos militares" (RÚSSIA, 2015, art. 34, p. 9, tradução nossa).

A descrição detalhada do conjunto de medidas para emprego da dissuasão estratégica (RÚSSIA, 2009, art. 26, p. 9) foi reorganizada em um único artigo, às ações políticas, diplomáticas, militares e de informação (RÚSSIA, 2009, art. 26, p. 10) foram acrescentados trechos que ressaltam a importância da manutenção do "potencial de dissuasão nuclear em

nível suficiente" e a prontidão das "forças armadas, outras tropas, unidades e órgãos militares" (RÚSSIA, 2015, art. 36, p. 9, tradução nossa) para mobilização e uso em conflitos.

A estratégia (2015) indica que o aumento da eficiência da organização militar do estado depende da "identificação oportuna dos perigos e ameaças militares existentes e futuras" (RÚSSIA, 2015, art. 37, p. 9, tradução nossa). Contudo, o documento (2015) omite descrição detalhada dessas ameaças e perigos conforme estabelecido na estratégia (2009, art. 30, p. 10-11), em seu lugar oferece maior relevância ao desenvolvimento do CIM com vistas ao emprego da tecnologia para "fortalecimento das capacidades de defesa e equipamentos das forças armadas da Federação Russa, outras tropas, unidades e corpos militares especiais com equipamentos modernos" (RÚSSIA, 2015, art. 37, p. 9, tradução nossa).

Outrossim, a transformação qualitativa das Forças Armadas (RÚSSIA, 2009, art.31, p. 11) foi reformulada na estratégia (2015) que reforça a necessidade de que se aprimorem as "formas e os métodos de uso das forças armadas da Federação Russa, outras tropas, unidades e órgãos militares" (RÚSSIA, 2015, art. 38, p. 10, tradução nossa) em acordo com as novas "tendências da natureza das guerras modernas e dos conflitos armados" (RÚSSIA, 2015, art. 38, p. 10, tradução nossa). Nesse sentido, o documento frisa a preparação do terreno como chave para a consecução dos objetivos estratégicos da Defesa mediante a "realização das capacidades de combate das tropas (forças), o desenvolvimento de requisitos para formações promissoras e novos meios de luta armada" (RÚSSIA, 2015, art. 38, p. 10, tradução nossa).

A estratégia (2015) adiciona um artigo importante que confere atenção especial ao planejamento estratégico dos meios que garantam a mobilização das Forças Armadas e da sociedade civil da Federação Russa em caso de conflito armado, por essa lógica, prevê a atualização periódica do "potencial técnico-militar da organização do estado" (RÚSSIA, 2015, art. 39, p. 10, tradução nossa) e o emprego de ações que permitam "preparar a proteção da população, os valores materiais e culturais" do país das ameaças decorrentes dos conflitos militares (RÚSSIA, 2015, art. 40, p. 10, tradução nossa).

A estratégia (2015) reintera, ainda, a importância do desenvolvimento da estrutura militar para a Defesa nacional estabelecida em seu documento antecessor (2009, art. 27, p. 10), sustentada pelos princípios de suficiência e eficácia, movimento que não engloba apenas os meios militares, mas também mecanismos de diplomacia e cooperação internacional (RÚSSIA, 2015, art. 41, p. 10).

Os conflitos desencadeados durante o intervalo que separa a produção destes dois documentos ficam evidentes ao analisarmos as modificações inseridas na segunda subseção

da estratégia (2015) que trata dos objetivos do Estado no âmbito da Segurança pública. Nesta seção foram acrescidas às principais ameaças reconhecidas pela Federação Russa (2009, art. 37, p. 12), dentre outras, as ações envolvendo o "uso de tecnologias de informação e comunicação para divulgação e propaganda da ideologia do fascismo, extremismo, terrorismo e separatismo, danos à paz civil, estabilidade política e social da sociedade" (RÚSSIA, 2015, art. 43, p. 11, tradução nossa).

Outrossim, no longo prazo, no que concerne ao combate destas ameaças e garantia da Segurança pública e do Estado, à construção de mecanismos institucionais de controle (RÚSSIA, 2009, art. 38, p. 13) a estratégia (2015) acrescenta a necessidade de garantir e aprimorar o funcionamento do sistema de identificação, análise e combate de "ameaças na esfera da informação" (RÚSSIA, 2015, art. 47, p. 13, tradução nossa), bem como de implementar medidas aumentar a proteção dos cidadãos russos do "impacto destrutivo das informações de organizações extremistas e terroristas, serviços especiais estrangeiros e estruturas de propaganda" (RÚSSIA, 2015, art. 47, p. 13, tradução nossa).

Nesse sentido, a preocupação com a segurança das fronteiras permanece fulcral na estratégia (2015), o processo de implementação do plano nacional de aprimoramento institucional para combate e prevenção de ameaças (RÚSSIA, 2009, art. 40, p. 14) é descrito de modo detalhado ao apresentar as atividades que vem sendo realizadas pelos órgãos executivos federais no intuito de "identificar, impedir e suprimir a inteligência e outras atividades destrutivas de serviços especiais e organizações de estados estrangeiros que prejudicam os interesses nacionais" (RÚSSIA, 2015, art. 47, p. 12, tradução nossa).

Ao interesse manifesto pela implantação de sistemas multifuncionais de alta tecnologia na fronteira (RÚSSIA, 2009, art. 42, p. 15) foram acrescentados o aprimoramento do sistema de análise, identificação e combate de ameaças na esfera da informação (RÚSSIA, 2015, art. 47, p. 13) e o aperfeiçoamento da cooperação interagencias (RÚSSIA, 2015, art. 48, p. 13) com objetivo de garantir a eficácia das atividades e a segurança no espaço fronteiriço, apenas as citações diretas aos países envolvidos foram removidas.

Os meios para garantir a segurança nacional em casos emergenciais tais como a manutenção e atualização dos equipamentos tecnológicos, bem como dos sistemas de funcionamento das infraestruturas críticas foram mantidos na estratégia (2015) tal qual estabelecidos no documento anterior (RÚSSIA, 2015, art. 49, p. 13).

Na terceira subseção da estratégia (2015) dentre outros fatores reconhecidos como ameaças a qualidade de vida dos cidadãos russos (RÚSSIA, 2009, art. 47, p. 16) foi acrescido

a “introdução de medidas econômicas restritivas” (RÚSSIA, 2015, art. 51, p. 14, tradução nossa) contra a Federação Russa em uma clara alusão as sanções econômicas impostas pela União Europeia e Estados Unidos ao país após a anexação do território da Crimea.

No que concerne às ações previstas para combater tais ameaças, à garantia de acesso aos veículos de tecnologia da informação (RÚSSIA, 2009, art. 52, p. 16) a estratégia (2015) acrescenta a necessidade de que se garantam “o desenvolvimento da infraestrutura de informação, incluindo o uso de tecnologias de informação e comunicação” (RÚSSIA, 2015, art. 53, p. 15, tradução nossa).

Na quarta subseção, a estratégia (2015) que trata dos objetivos que visam garantir o crescimento econômico e ampliar as capacidades de se opor “à influência de ameaças externas” (RÚSSIA, 2015, art. 55, p. 16, tradução nossa) da Federação Russa, o detalhamento dos principais riscos e ameaças à segurança nacional na esfera econômica sofreu alterações, no lugar da preocupação com a migração ilegal e a desigualdade regional (RÚSSIA, 2009, art. 55, p. 18), a estratégia (2015) insere: i) a defasagem no desenvolvimento e implementação de tecnologias promissoras; ii) a vulnerabilidade da infraestrutura de informação; iii) registro de direito de propriedade de empresas estrangeiras (RÚSSIA, 2015, art. 56, p. 15, tradução nossa).

O interesse estratégico da Federação Russa em investir no desenvolvimento de pesquisa e tecnologia foi mantido na estratégia (2015), porém a forma de alcançar esse objetivo foi alterada dando origens a dois artigos que tratam do assunto.

Á vista disso, a intenção de construir parcerias público-privadas para garantir a segurança econômica (RÚSSIA, 2009, art. 58, p. 18) deu lugar ao protagonismo regulador do Estado enquanto entidade capaz de executar diversas ações, dentre as quais destacamos: i) manter a estabilidade do funcionamento e desenvolvimento do sistema financeiro; ii) combater a corrupção, a economia oculta e criminal; iii) proteger a industria militar, alimentícia, de informações e de segurança energética (RÚSSIA, 2015, art. 58, p. 17, tradução nossa); iv) desenvolver o mercado de trabalho, transporte, informação; v) investir em ciência e educação (RÚSSIA, 2015, art. 59, p. 17, tradução nossa).

No que concerne ao combate das ameaças à segurança econômica, a estratégia (2015) inclui uma série de novas medidas a serem adotadas pela Federação Russa, todavia, o interesse pelo desenvolvimento de novas indústrias de alta tecnologia permanece com acréscimo do interesse manifesto em aumentar os investimentos no aprimoramento do CIM

enquanto vetor da “modernização da produção industrial” (RÚSSIA, 2015, art. 62, p. 19, tradução nossa).

A descrição detalhada do conjunto de ações para melhoria da segurança econômica (RÚSSIA, 2009, art. 63, p. 20) foi removida da estratégia (2015) para dar lugar a uma diretriz abstrata que indica a necessidade de melhorar a administração pública enquanto fator preponderante para consecução deste objetivo sem mencionar o investimento em tecnologia de uso dual como fator relevante (RÚSSIA, 2015, art. 63, p. 20, tradução nossa).

Na quinta subseção, a estratégia (2015) reintera a importância do investimento no médio prazo em segurança tecnológica enquanto fundamento basilar para o desenvolvimento sustentável do país, com objetivo de garantir a “segurança nacional no campo da ciência, tecnologia e educação, inclusive na esfera da informação” (RÚSSIA, 2015, art. 69, p. 21, tradução nossa).

No que concerne à garantia da segurança nacional nos campos da ciência tecnologia e educação, a estratégia (2015) é mais específica que seu documento antecessor, contudo, o “desenvolvimento de alta tecnologia (engenharia genética, robótica, biológica, informação e comunicação, cognitivas, nanotecnologias)” (RÚSSIA, 2015, art. 70, p. 22, tradução nossa) permanece como condição necessária para consecução deste objetivo. Entretanto, o documento estabelece a primazia do suporte estatal na “interação entre organizações educacionais e centros de pesquisa com empresas industriais” (RÚSSIA, 2015, art. 70, p. 22, tradução nossa) bem como na melhoria da “qualidade do treinamento de cientistas, engenheiros e especialistas técnicos” (RÚSSIA, 2015, art. 70, p. 22, tradução nossa).

A nona subseção é a que recebe o maior número de alterações em função dos conflitos recentes desencadeados em territórios fronteiriços da Federação Russa. Nesse sentido, a estratégia (2015) reforça o compromisso da política externa do país com o cumprimento dos acordos estabelecidos pelos tratados de direito internacional dos quais o país é signatário, ademais considera a Organização das Nações Unidas (ONU) e o Conselho de Segurança (CSONU) como organismos centrais do sistema de resolução de conflitos das relações internacionais (RÚSSIA, 2015, art. 87, p. 30).

A estratégia (2015) sustenta o interesse da Federação Russa em fortalecer a cooperação com o bloco de países do “Brasil, Rússia, Índia, China e África do Sul (BRICS), o RIC, a Organização de cooperação de Xangai, a Cooperação Econômica Ásia-Pacífico, o G20 e outras instituições internacionais” (RÚSSIA, 2015, art. 88, p. 30, tradução nossa), bem como em construir novos acordos bilaterais e multilaterais com os Estados membros da

Comunidade de Estados Independentes (CEI), as Repúblicas da Abkhazia e da Ossétia do Sul, e, aprofundar processo de integração da Organização do Tratado de Segurança Coletiva (OTSC) e da União Econômica da Eurásia (UEE) (RÚSSIA, 2015, art. 89, p. 30). A preocupação em conter as ameaças regionais de natureza política e militar se manifesta na intenção da Federação Russa em transformar a OTSC em uma organização internacional com ramificações universais que a tornem capaz de combater a atuação dessas ameaças em diversas áreas, inclusive na esfera da informação (RÚSSIA, art. 90, 2015, p. 30-31).

A estratégia (2015) retira o foco das Forças Armadas como agente na resolução de questões política e econômicas (RÚSSIA, 2009, art. 93, p. 27), de acordo com o estabelecido no documento a estabilidade estratégia será buscada através do "fortalecimento da cooperação mutuamente benéfica com os estados europeus" (RÚSSIA, 2015, art. 97, p. 32, tradução nossa) com objetivo de construir um "sistema aberto de segurança coletiva na região euro-atlântica" (RÚSSIA, 2015, art. 97, p. 32, tradução nossa). Além disso, propõe um acordo de "parceria completa com os EUA com base em interesses coincidentes, inclusive na esfera econômica, levando em consideração a influencia fundamental das relações russo-americanas no estado da situação internacional como um todo" (RÚSSIA, 2015, art. 98, p. 32).

No que concerne à manutenção da estabilidade regional e global, a estratégia (2015) mantém as diretrizes objetivas anteriores (RÚSSIA, 2009, art. 95, p. 28) e acrescenta duas novas, o necessário controle da fragmentação do sistema jurídico internacional, levada a cabo pela aplicação seletiva das leis que compõem esse sistema, e, o interesse da Federação Russa em contribuir para a "formação de um sistema internacional de segurança da informação" (RÚSSIA, 2015, art. 104, p. 33, tradução nossa).

Embora a estratégia (2015) mantenha o compromisso em cooperar para "manter o potencial de dissuasão menos dispendioso no campo de armas ofensivas estratégicas" (RÚSSIA, 2015, art. 105, p. 33-34, tradução nossa) com objetivo de manter a estabilidade regional e global, o documento insere dois artigos que reinteram a preocupação da Federação Russa com a aproximação da infraestrutura militar da OTAN de suas zonas fronteiriças.

A vista disso, frisa que a construção do sistema de defesa antimísseis nesses territórios, bem como a intenção do bloco em adquirir funções globais que contradizem os tratados de direito internacional é o grande fator desestabilizador das relações entre a Federação e as potências ocidentais (RÚSSIA, 2015, art. 106, p. 34). A despeito disso, reintera o interesse em "fortalecer a segurança global na região euro-atlântica" (RÚSSIA, 2015, art. 107, p. 34) mediante a aproximação das relações com a OTAN desde que efetuadas

com base no respeito aos “interesses legítimos da Federação Russa na implementação do planejamento político-militar” nessas regiões (RÚSSIA, 2015, art. 107, p. 34).

Na quinta seção, a preocupação com o funcionamento dos sistemas de informação e a construção de um sistema unificado de suporte (RÚSSIA, 2009, art. 109, p. 31) foi mantida na estratégia (2015), no entanto a diretriz de ação tornou-se mais abstrata, o documento apenas estabelece como fundamental a “garantia da segurança da informação” (RÚSSIA, 2015, art. 113, p. 35, tradução nossa) para sua efetiva implementação sem que haja uma descrição detalhada das ações a serem tomadas pelo Estado nesse campo.

Por fim, a sexta seção que trata da mensuração dos níveis da segurança nacional apresenta a inclusão de novas variáveis: i) satisfação dos cidadão com o grau de proteção de direitos e liberdades constitucionais, interesses pessoais e de propriedade; ii) quantidade de armas modernas, equipamentos militares e especiais das Forças Armadas, outras tropas, formações e corpos militares ; iii) expectativa de vida; iv) PIB per capita; v) renda; vi) taxa de inflação; vii) taxa de desemprego; viii) parcela do PIB utilizado para desenvolvimento da ciência, tecnologia e educação; ix) gastos do PIB para cultura; x) áreas do território da Federação Russa que não cumpre as normas ambientais (RÚSSIA, 2015, art. 115, p. 35-36, tradução nossa). O quadro 3 sumariza os principais temas abordados pela Estratégia de Segurança Nacional da Federação Russa (2009; 2015).

Quadro 3 Principais Temas Abordados

Categorias	**Ameaças**	**Armas de Precisão**	**Eficiência**	**Complexo Industrial Militar**	**Cooperação**
Estratégia Nacional (2009)	Art. 1 Art. 2 Art. 8 Art. 10 Art. 17 Art.26 Art. 30 Art. 37 Art. 40 Art. 41 Art. 47 Art. 52 Art. 55 Art. 61 Art. 77	Art. 10 Art. 30 Art. 34 Art. 42	Art. 20 Art. 22 Art. 23 Art. 25 Art. 31 Art. 38 Art. 43 Art. 63 Art. 66	Art. 28 Art. 34 Art. 40	Art. 13 Art. 18 Art. 27 Art. 33 Art.58 Art. 68 Art. 70 Art.77 Art. 89 Art. 90 Art. 91 Art. 93 Art. 95 Art. 96 Art. 109
Estratégia Nacional (2015)	Art. 1 Art. 6 Art. 7 Art. 10 Art. 16 Art. 17 Art. 18 Art. 20 Art. 21 Art. 22 Art. 24 Art. 37 Art. 40 Art. 43 Art. 47 Art. 48 Art. 51 Art. 53 Art. 55 Art. 56 Art. 75 Art. 90	Art. 15 Art. 53 Art. 70	Art. 34 Art. 35 Art. 37 Art. 38 Art. 59 Art. 62 Art. 63 Art. 69 Art. 74	Art. 26 Art. 34 Art. 37 Art. 49 Art. 59 Art. 62	Art. 8 Art. 13 Art. 27 Art. 28 Art. 29 Art. 41 Art. 48 Art. 58 Art. 87 Art. 88 Art. 89 Art. 90 Art. 97 Art. 104 Art. 105 Art. 106 Art.107 Art. 113

Fonte: Elaborado pelo autor.

Frente à análise descritiva e comparativa realizada nesta seção, compreendemos que a reformulação dos principais documentos de Defesa e Segurança da Federação Russa, Doutrina Militar (2010; 2014) e Estratégia de Nacional de Segurança (2009; 2015) confirmam as pretensões da Federação em consolidar e expandir seu poder regional.

Atestamos que a mudança institucional identificada é condição necessária, porém não suficiente, para produzir o efeito estratégico ou militar através do emprego de armas eficientes e precisas, tais como as cibernéticas. Frisamos que, ao serem integradas às estruturas, doutrina e planejamento técnico e tático das operações militares, as armas cibernéticas produzem efeito sinérgico capaz de ampliar a assimetria de poder regional entre Federação Russa e a Ucrânia apenas se, e, quando em consonância com o mecanismo causal que será revelado na seção seguinte enquanto condição de suficiência para produção da GHC.

A orquestração sugerida é compatível os objetivos estratégicos russos que consideram as operações de rede de computadores como ferramentas a serem integradas em esforços mais amplos que objetivam manter o domínio político e militar nos conflitos contemporâneos (WEEDON, 2015, p. 68), conforme demonstraremos na seção subsequente.

2.4 A trajetória e o processo que envolve o conflito Rússia-Ucrânia (2014-2015)

Nessa subseção buscamos corroborar a hipótese condicional de suficiência, ao analisarmos o conflito cibernético entre os Estados da Rússia e Ucrânia (2014-2015). Para tanto, apresentamos um breve relado atento à historicidade na qual se desenrola o conflito, em seguida procuramos descrever a operação do mecanismo causal da GHC a partir da identificação das ações conjuntas perpetradas pelas forças especiais russas e hackers civis, bem como as novas armas cibernéticas utilizadas. Admitindo que em seu nível operacional e tático, o fenômeno se desenvolve mediante a sinergia proporcionada pela ação coordenada entre os esforços das agencias estatais e atores-não estatais.

Desse modo, partimos do pressuposto de que os ataques cibernéticos tem se tornado cada vez mais úteis às potências contemporâneas no que concerne ao alcance de seus objetivos estratégicos via ciberespaço. Uma vez que, por definição, a guerra híbrida favorece as estratégias das grandes potências em grande parte devido ao emprego de novas tecnologias no conflito, fator que se traduz, consequentemente, em um aumento da assimetria de poder regional em favor do Estado que a utiliza (HUNKER, 2014).

2.4.1 Contexto histórico

Em 2010 os ucranianos elegeram Viktor Yanukovych para ocupar o cargo de presidente do país. O novo presidente procurava demonstrar que estava aberto a estreitar os laços econômicos com a UE, embora negasse a plena integração do país À OTAN. Em suas declarações iniciais de política externa em 2010, o novo presidente expressava a intenção de tornar a Ucrânia um estado neutro, capaz de cooperar em questões de Defesa com a OTAN e a Rússia (USAOC, 2015, p. 26).

Entretanto, Yanukovych que mantinha laços estreitos com o Kremlin teve o mandato permeado por um conflito de interesses entre seus correligionários pró-rússia e os empresários ucranianos pró-ocidente. Diante desse cenário, o Partido das Regiões ao qual pertencia o presidente, desempenhou função importante nas tentativas de encontrar um equilíbrio que promovesse de modo equânime os interesses conflitantes.

A legenda constituída em 1997 que, inicialmente, simbolizava o regionalismo e a russofilia[15], ganhou força considerável em 2012 ao se unir ao Partido Ucrânia Forte que representava o interesse de atores transnacionais importantes como os bilionários Serhiy Tihipko e Oleksandr Kardakov (USAOC, 2015, p. 25).

No entanto, os esforços partidários malograram frente à pressão econômica e diplomática exercida pelo Kremlin que minou os interesses do grupo pró-ocidente, e, em novembro de 2013 Yanukovych rejeitou um grande acordo econômico que estava negociando com a UE e decidiu aceitar uma contra-oferta russa de 15 bilhões de dólares (MEARSHEIMER, 2015, p.3). O resultado foi uma guinada da política externa ucraniana no sentido de um maior aprofundamento das relações com a Rússia em detrimento do acordo com a UE.

A decisão foi recebida com protestos da oposição ao governo e manifestações pró-ocidente na Praça da Independência de Kiev (MEARSHEIMER, 2015, p.3) que ficaram conhecidas como 'novo movimento pró-ocidental Euromaidan'. Esse movimento que teve início de forma pacífica em 21 de novembro acabou se prolongando por três meses e chegou a reunir mais de 250.000 manifestantes que ocuparam a praça central, além de prédios do governo regional e o Ministério da Justiça (USAOC, 2015, p. 29-30).

Em fevereiro de 2014 a violência eclodiu, resultando em pelo menos oitenta e oito mortes entre os dias 18 e 20 em Kiev e centenas de manifestantes feridos pelo avanço das tropas governo (BBC, 2015, p. 2). Um dia depois, as tentativas de governo e oposição de costurar um acordo às pressas que mantivesse a legitimidade do presidente até a realização de novas eleições foram veementemente refutadas pelo parlamento culminando na fuga de Yanukovych e de vários deputados do Partido das Regiões da capital. Em 22 daquele mês, o parlamento decide dissolver a Berkut, unidade de elite da polícia culpada pela morte dos manifestantes na praça central, proibir o russo como segunda língua oficial do país e remover de Yanukovych do cargo, em seu lugar assume como presidente interino Oleksandr Turchynov (BBC, 2015; USAOC, 2015, p. 30).

O parlamento marcou novas eleições presidenciais para 25 de maio de 2014 quando os eleitores pró-ocidentais elegeram o oligarca Petro Poroshenko como o novo presidente da Ucrânia. Em 27 de junho de 2014 Poroshenko rapidamente assinou o Acordo de Associação

[15] Russofilia definição: sentimento de amizade, admiração, simpatia e empatia em relação à Rússia e aos russos. Sociedades ou indivíduos considerados russófilos são aqueles que expressam estes sentimentos em relação à cultura russa, ao idioma russo, à influência geopolítica e econômica russa em outros países e às atitudes russas na política (WIKIPEDIA, n/a).

que havia sido rejeitado por seu antecessor, concluindo assim o estreitamento dos laços da política externa ucraniana com o mundo ocidental (MEARSHEIMER, 2015, p. 5). Neste mesmo mês os ministros das Relações Exteriores dos países membros da OTAN decidiram que a aliança permaneceria aberta a novos membros, 'Nenhum país terceiro veta o alargamento da OTAN' (MEARSHEIMER, 2015, tradução nossa, p. 5).

No entanto a resolução do caso não foi um tão simples, as tentativas de formalizar o acordo de integração com a UE conduziram a Ucrânia a um impasse diplomático com a Rússia, cuja resolução do processo de tomada de decisão mediante a queda de Yanukovych que havia sido democraticamente eleito acarretou em um dos mais intrigantes conflitos contemporâneos desencadeados deste século.

A abordagem realista de Mearsheimer (2015) indica que os Estados Unidos e seus aliados europeus como os maiores responsáveis pela crise que se desencadeou na Ucrânia em 2014, em grande parte, devido ao programa liberal de alargamento da OTAN para os países do leste europeu que conduziu a um inevitável impasse estratégico com a Federação Russa a partir do momento em que se procurou integrar a Ucrânia à órbita ocidental. Nesse sentido, o apoio ao movimento pró-democrático que se iniciou na Ucrânia com a Revolução Laranja em 2004, é tido como um dos elementos críticos que despertaram a atenção da Rússia para a tentativa de ingerência ocidental no entorno estratégico regional russo (MEARSHEIMER, 2015, p. 1).

> Desde meados da década de 1990, os líderes russos se opuseram firmemente ao alargamento da OTAN e, nos últimos anos, deixaram claro que não permaneceriam sentados enquanto seu vizinho estrategicamente importante se transformasse em um bastião ocidental (MEARSHEIMER, 2015, p. 1, tradução nossa).

O processo de expansão da OTAN pode ser compreendido sob o prisma da política de contenção da antiga União Soviética que se iniciou durante a guerra fria, e, que teve por consequência um aumento do sentimento antiocidental na população de origem russa. Os russos se sentiram prejudicados pelos novos arranjos institucionais propostos pelos liberais ocidentais que obviamente afrontavam os interesses da Federação Russa, fator chave para se entender a "legitimidade de iniciativas antagônicas aos interesses ocidentais por parte de seu governo" (ARBATOV 1993; LYNCH 2001; *apud* MIELNICZUK 2014, p. 4).

Após Yanukovych deixar o cargo e seguir para a Rússia, o conflito iniciado pelo movimento Euromaidan se espalhou por toda a Ucrânia deixando claro que o país estava se

dividindo em duas metades, separadas pelo rio Dnieper, o lado pró-ocidental a oeste e o lado pró-russia a leste, “a crise mostra que a *realpolitik* permanece relevante e os estados que a ignoram o fazem por sua própria conta e risco” (MEARSHEIMER, 2015, p. 1, tradução nossa). A figura 1 ilustra a divisão étnica da Ucrânia.

Figura 1 Divisão étnica

Fonte: GGN (2014)

Na península da Crimeia, onde a grande maioria dos 2.3 milhões de habitantes é falante da língua russa e se identifica como russos étnicos (BBC, 2015, p. 3), o líder da força paramilitar Sergei Aksyonov solicitou ao presidente russo Vladmir Putin que intervisse com apoio militar (USAOC, 2015, p. 31) para garantir que a cidade de Sevastopol, base histórica da marinha russa no Mar Negro, se mantivesse dentro da jurisdição da Federação Russa.

Para Putin, a queda de Yanukovych na condição de presidente eleito e pró-russia forneceu a narrativa perfeita para o que ele justamente chamou de "golpe" (MEARSHEIMER, 2015, p.1). Imediatamente, veículos da imprensa russa passaram a disseminar informações sobre a queda de Yanukovych como resultado de um golpe de Estado orquestrado pela UE e os Estados Unidos que ameaçava os interesses regionais da Federação e colocava os russos que viviam na Ucrânia em perigo. Desse momento em diante:

> Grupos de homens armados não identificados começaram a aparecer em toda a região, frequentemente em coordenação com milícias pró-russas locais. Tanto o governo ucraniano quanto a maioria das fontes de inteligência ocidentais alegaram que os "homenzinhos verdes" eram agentes russos. As milícias da "autodefesa" da Crimeia apreenderam prédios do governo, bases aéreas e instalações militares, e o governo de Kiev, desejando evitar derramamento de sangue e outras provocações, ordenou que suas forças militares não resistissem (USAOC, 2015, tradução nossa, p. 31).

Os grupos armados e agentes de inteligência sem identificação são parte das forças de operações especiais russas, foram eles os responsáveis pelas operações militares que tomaram controle da península e por apoiar os movimentos separatistas do leste (GILES, 2015, p. 20). Essas tropas empregaram equipamentos fornecidos pelas Forças Armadas da Federação Russa que incluíam veículos blindados de transporte de pessoal e helicópteros (USAOC, 2015, p. 56). Embora o Kremlin tenha inicialmente negado envolvimento nas operações, pouco tempo depois a sede da frota russa do Mar Negro em Sevastopol admitiu que suas tropas haviam sido movidas para a Crimeia para garantir o controle do porto (USAOC, 2015, p. 56).

Em acordo com a intervenção russa, o parlamento da Crimeia decide pela união à Rússia e convoca um referendo para consulta popular (BBC, 2015, p. 3). Em 16 de março de 2014, o referendo organizado pelos governos locais da Crimea e de Sevastopol teve aprovação de mais de 90% da população (MIELNICZUK, 2014, p. 8), dois dias depois um tratado para anexação foi assinado e a Crimea passou a pertencer formalmente ao território russo (USAOC, 2015, p. 31). A tensão em torno da presença de militares ucranianos em bases localizadas na península foi dissipada por meio de acordos que garantiram sua retirada da região em segurança (MIELNICZUK, 2014, p. 8).

Destarte, a Rússia respondeu às ações do parlamento ucraniano contra Yanukovych anexando a Crimeia e "trabalhando para desestabilizar a Ucrânia até que abandonasse seus esforços para se juntar ao Ocidente" (MEARSHEIMER, 2015, tradução nossa, p. 1).

Os Estados Unidos e a UE reagiram aplicando sanções econômicas à Rússia[16], porém o conflito estava apenas em sua fase inical, uma vez que o sentimento antiocidental tomou força, o movimento de aproximação com a Rússia se espalhou exponencialmente para as regiões do leste ucraniano.

> Em essência, os dois lados têm operado com diferentes cartilhas: Putin e seus compatriotas têm pensado e agido de acordo com ditados realistas, enquanto seus colegas ocidentais têm aderido a ideias liberais sobre política internacional. O resultado é que os Estados Unidos e seus aliados, sem saber, provocaram uma grande crise sobre a Ucrânia (MEARSHEIMER, 2015, tradução nossa, p. 4).

[16] Em 17 de Março 2014 a UE e os EUA impõem restrições de visto e congelamento de vistos de oficiais russos e ucranianos atingindo cargos de alto escalão como o chefe do conselho Federal, o Primeiro Ministro e o assessor presidencial (IVAN, 2018).

Em 7 de abril, grupos de separatistas que classificavam o governo de Kiev como fascista organizaram um movimento para desvincular a região de Donbass, onde estão localizadas as cidades de Donetsk, Luhansk e Kharkiv, da Ucrânia (BBC, 2015, p. 4). Esses grupos tomaram prédios públicos e exigiram a realização de referendos regionais semelhantes ao da Crimeia, mediante a recusa do governo central em reconhecer a legitimidade desses grupos, os referendos foram organizados de modo informal e, em 11 de maio de 2014 os separatistas pró-russos declaravam a independência da República Popular de Donetsk e a autonomia dos territórios de Luhansk e Kharkiv do governo central (USAOC, 2015, p. 31-32). A figura 2 ilustra as áreas declaradas autônomas pelos separatistas do leste ucraniano.

Figura 2 Áreas declaradas autônomas

Fonte: BBC (2015)

Em 22 de maio, os separatistas do leste declararam o estabelecimento da Nova Rússia, uma área que incluía os territórios a sul a leste do rio Dnieper. A Federação Russa ofereceu apoio militar operacional e tático aos separatistas, o conflito e resultou na queda de um avião de transporte modelo Ily-ushin Il-76 em meados de junho, ocasionando a morte de 49 soldados ucranianos que estavam a bordo (USAOC, 2015, p. 32).

Em 20 de junho, o presidente Poroshenko anuncia um plano de paz de 15 pontos e declara um cessar-fogo que durou apenas uma semana até que um helicóptero militar ucraniano fosse derrubado no território do leste (BBC, 2015, p. 5). Em 5 de julho, as tropas do governo central de Kiev iniciaram uma contraofensiva e retomaram algumas cidades ocupadas pelos separatistas que deixaram Donetsk e Luhansk para se refugiar no sul (BBC, 2015, p. 6). A figura 3 ilustra o território controlado pelos separatistas do leste.

Figura 3 Território controlado por separatistas

Fonte: BBC (2015)

Em meados daquele mês os combates se intensificaram com as forças do governo avançando e acuando ainda mais os separatistas, em 17 de julho, um míssil é disparado contra o voo MH17 da Malaysian Airlines, causando a morte de 283 passageiros e 15 tripulantes civis. O ataque aos civis resultou em novas sanções econômicas[17] à Rússia por parte dos Estados Unidos e da União Europeia que atingiram atores transnacionais ligados ao governo russo e a alguns bancos, como diretores de empresas de energia e de defesa (MEARSHEIMER, 2015, p. 5). A figura 4 ilustra o local da queda do voo MH17.

Figura 4 Área da queda do voo MH17

Fonte: BBC (2015)

[17] Em 18 de julho o Banco Europeu de Investimento suspendeu o financiamento de projetos de infraestrutura na Rússia. No dia 29 daquele mês os Estados Unidos impõem sanções destinadas a setores da economia russa, incluindo armamentos, energia e finanças, em sequência a UE restringe o acesso ao mercado de capitais pelos bancos estatais russos, impõe um embargo ao comércio de armas e restringe as exportações de bens de uso dual e tecnologias sensíveis, especialmente no setor de petróleo (IVAN, 2018).

Em agosto, apoiado por tropas ocidentais o governo já havia recuperado cerca de dois terços do território ucraniano dominado pelos separatistas (USAOC, 2015, p. 33). As ações para retomada do leste pelo governo central resultaram em fortes baixas para os separatistas em termos de recursos humanos e território, abrindo espaço para a negociação de outro cessar-fogo que foi estabelecido em setembro 5 de 2014 com o apoio da Rússia e da UE (BBC, 2015, p. 7).

A OSCE coordenou as negociações de paz na cidade de Minsk, na Bielorússia, nesta ocasião o então presidente ucraniano Poroshenko conseguiu a aprovação plena por ambos os lados dos quinze pontos do plano de paz que havia sido proposto em junho (BBC, 2015, p. 7). Dentre os pontos do plano constavam itens como a garantia do governo central de conceder maior autonomia para a região de Donbass e o compromisso em proteger os falantes do idioma russo que habitam os territórios do leste, como contrapartida, equipamentos pesados de combate deveriam ser removidos das áreas de conflito e os prisioneiros de ambos os lados trocados (USAOC, 2015, p. 61).

No entanto, a trégua durou apenas dois meses. Em 2 de novembro os líderes separatistas do leste realizam novas eleições não reconhecidas pelo governo central, no dia 12 daquele mês as hostilidades foram retomadas e os territórios controlados pelo governo central a leste novamente declarados como autônomos pelos separatistas com apoio das tropas russas em uma clara demonstração de que o conflito não teria um fim breve. A figura 5 ilustra a área retomada pelos separatistas em janeiro de 2015.

Figura 5 Área sob controle separatista

Fonte: BBC (2015).

Em 22 de janeiro o aeroporto de Donetsk é retomado pelos separatistas, a estrutura destruída pelo intenso combate entre o movimento e as tropas do governo central precisaria ser recuperada, pois é considerada vital para que conseguir acesso ao equipamento de apoio russo como munições, e mão-de-obra transportados para a zona de conflito (BBC, 2015, p. 9).

Em 12 de Fevereiro um novo cessar-fogo é acordado em Minsk, entre Rússia, Ucrânia, Alemanha e França prevendo a retirada de armas, a troca de prisioneiros e a redução de armamento pesado entre as forças de artilharia envolvidas no conflito. Embora o acordo tenha sido assinado pelos separatistas, os conflitos não cessaram, o movimento continuou a avançar sobre o Debaltseve com intuito de unir as regiões de Donetsk e Luhansk, ato consumado nos meses seguintes. A figura 6 ilustra a área controlada pelos separatistas após a campanha de Abril (2015).

Figura 6 Área sob controle dos separatistas

Fonte: Conselho de Defesa e Segurança Nacional Ucrânia (2015)

Em 7 de agosto uma nova crise aumenta a tensão no conflito ao sul com a morte de um soldado e um agente de segurança federal da Rússia na Crimeia que foram classificados pelo Ministério das Relações Exteriores russo como “atos de terrorismo” realizados pelo governo central de Kiev, fato negado pela Ucrânia que respondeu com aumento da força militar na fronteira com a Crimeia e na linha de frente no leste (BBC, 2016, p. 1).

Os acontecimentos brevemente descritos nesta seção estão diretamente imbricados ao uso da tecnologia da informação no conflito, as operações e táticas empregadas demonstram a conexão entra a estratégia de ação regional e uso do ciberespaço enquanto zona de combate capaz de oferecer vantagens crescentes à Rússia que serão apresentadas na subseção seguinte, a partir da análise do funcionamento do mecanismo causal identificado nesta pesquisa.

2.4.2 A simbiose hacker-Exército: o emprego da tecnologia da informação no conflito

Conforme indicam relatórios de agências especializadas em segurança cibernética, durante o conflito as atividades do Exército russo estiveram vinculadas a uma série de ataques de negação de serviço (D-DoS), os quais paralisaram sistemas de computador, atingiram os setores de comunicação, sistemas bancários, interviram em eleições, e comprometeram o funcionamento de infraestruturas críticas (CROWDSTRIKE 2014; 2015; 2016; FIREEYE 2014; F-SECURE LABS 2014a; 2014b; 2016; LOOKINGGLASS 2015; ICS-CERT, 2016; E-ISAC 2016).

Os relatórios contêm uma série de evidências que indicam a ligação entre as atividades dos atores não-estatais com a agência estatal russa, simbiose que compõe o mecanismo causal aqui identificado enquanto condição de suficiência para promoção de nosso fenômeno de interesse, a GHC.

Nesta subseção, apresentamos as evidências descritas nestes relatórios mediante a congruência dos ataques cibernéticos com as ações físicas no conflito, em sequência, descrevemos algumas das principais armas cibernéticas utilizadas no conflito bem o modo de operação e tática de conjunta de hackers e atores das Forças Armadas russas, prática que identificamos como mecanismo causal da GHC.

> Basicamente, todos os meios e ferramentas empregados pela Rússia no âmbito da guerra híbrida fazem parte da antiga política externa e de segurança soviética, bem como da história da guerra assimétrica. A única novidade tem sido o alto grau de efetividade, em muitos casos, quase uma coordenação em tempo real de vários meios empregados, incluindo políticos, operações militares especiais e medidas de informação (RÁCZ, 2015 *apud* LIMNÉLL, 2015, p. 522, tradução nossa).

Sem embargo, o relatório Grupo de Inteligência sobre Ameaças Cibernéticas (CTIG) publicado pela LookingGlass (2015) apresenta a ligação entre a campanha de espionagem cibernética e atores estatais da agência do Serviço de Segurança Federal da Rússia (FSB) como fator chave para compreensão da vantagem militar russa sobre as forças ucranianas. Conforme declaração do Serviço de Segurança da Ucrânia (SBU), a subtração de informações do governo, policia e militares, pelos hackers forneceu detalhes dos planos de curto prazo delimitados pelo governo central de Kiev para conter o avanço das tropas do Kremlin (LOOKINGGLASS, 2015, p. 3).

A análise técnica e temporal do relatório concluiu, a partir da correlação observada entre os ataques cibernéticos e o conflito cinético, que a Rússia utilizou o ciberespaço para consecução de seus interesses estratégicos regionais em território ucraniano destacando "uma mistura alarmante entre espionagem cibernética, guerra física e as forças políticas por trás delas" (LOOKINGGLASS, 2015, p. 3, tradução nossa).

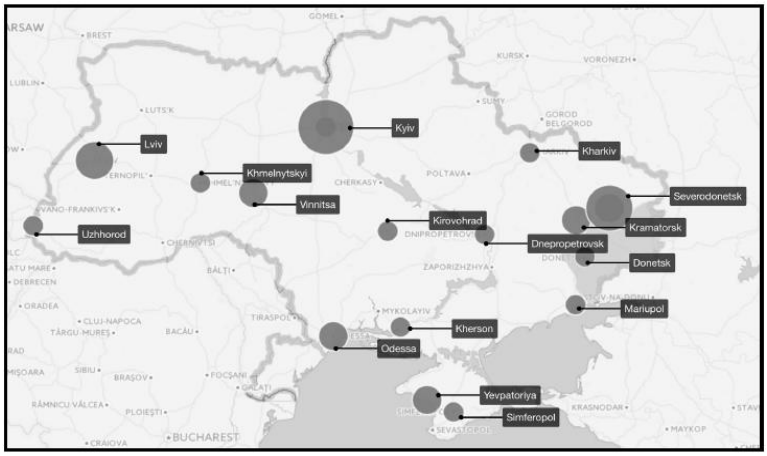
Classificado como operação 'Armagedon'[18] (escrito incorretamente) a campanha de intrusão cibernética teve inicio a partir da decisão do então presidente Viktor Yanukovych em aceitar o Acordo de Associação entre a Ucrânia e a União Europeia em 2013. A evidência encontrada indicou que os arquivos analisados em formato de documento formado Microsoft Word infectados com *malwares* datam de 26 de junho de 2013 e suas variações utilizadas na primeira onda de ataques *spear phishing*[19] contra alvos do governo central continham data e hora de modificação entre 12 de agosto e 16 de setembro daquele ano (LOOKINGGLASS, 2015, p. 4).

Cientes da dificuldade de atribuição das ações cibernéticas ofensivas, o SBU e a LookingGlass foram enfáticos em estabelecer a presença de duas agencias estatais russas envolvidas no conflito que fizeram uso tático do ciberespaço a 16º (ex-Agência Federal de Comunicações e Informações Governamentais) e o 18º Centro do FSB russo "além das motivações políticas e militares, a análise da linha do tempo dos ataques, juntamente com o mundo real e o contexto digital, sugere o envolvimento da Rússia" (LOOKINGGLASS, 2015, p. 4, tradução nossa). A figura 7 aponta as áreas onde se concentraram os ataques cibernéticos na Ucrânia do início do conflito até março de 2015.

[18] Definição 'Operação Armageddon': campanha russa de espionagem cibernética que visou alvos do governo ucraniano, policiais e militares - provavelmente ajudou a fornecer uma vantagem militar à Rússia em relação a Ucrânia, a partir de segredos sistematicamente coletados de espionagem cibernética (WEEDON, 2015, p. 73, tradução nossa).

[19] Definição de *spear phising*: e-mail contendo softwares maliciosos que roubam credenciais de acesso e documentos confidenciais, primeiro passo para penetrar mais fundo na infraestrutura de uma organização vítima. Na prática trata-se da coleta silenciosa de dados por um longo período de tempo capaz de fornecer acesso a contas pessoais favorecer o vazamento de informações sensíveis para causar danos à organização da vítima e influenciar a opinião pública e espionagem doméstica (HACQUEBORD, 2017, p. 8, tradução nossa).

Figura 7 Áreas mais afetadas por ataques cibernéticos



Fonte: LookingGlass (2015).

A partir da análise da infraestrutura de rede e as ameaças utilizadas pelos hackers foram identificados nomes de arquivo similares nos ataques cibernéticos o que facilitou o rastreamento das atividades das ameaças (LOOKINGGLASS, 2015, p. 18). O relatório (2015) traz detalhes sobre a ligação entre os ataques cibernéticos e os principais eventos políticos e militares que envolveram o conflito na Ucrânia (2014-2015) sumarizados no quadro 4.

Quadro 4 Cronograma da campanha de espionagem cibernética 'Armadegon'

2014	**Ação Física**	**2014**	**Ação Cibernética**
15 abril	Após separatistas tomarem o controle das cidades de Luhansk e Donetsk, o governo ucraniano anuncia uma 'operação antiterrorista' para retomada dos territórios	16 abril	'install_flashplayer_aih.exe' dropper SFX instalado em arquivo formato Microsoft Word disparado via spear phising para alvos militares, mídia e org. governamentais
14 Junho	Separatistas derrubam avião militar ucraniano com 49 oficiais	14 Junho	Novos ciberataques são detectados utilizando o mesmo malware e portas de entrada TTPs para buscar informações sobre como a Ucrânia iria responder ao ocorrido
20 Junho	Primeiro cessar-fogo (1 semana)	20 Junho	Os ataques cibernéticos cessam (1 semana)
17 julho	Queda do voo MH17 Malaysian Airlines (298 civis mortos), as forças armadas russas auxiliam a retomada das cidades ucranianas do leste que haviam sido tomadas pelas tropas do governo central	17 julho	'install.flashplayer_aih.exe' nova versão, o 123.cmd não inclui mais uma senha necessária para abrir o arquivo SFX de 'sex.exe'. Direcionado para alvos militares, mídia e org. governamentais, escrito em ucraniano, contém relatório legítimo para notificação diária da Administração do Presidente da Ucrânia sobre as operações antiterroristas na Ucrânia, dados sobre ataques terroristas contra o exército ucraniano e suas perdas

24 agosto	Após invasões das forças armadas russas nos territórios do leste as forças ucranianas são forçadas a se retirar	26 agosto	Os ataques cibernéticos cessam na região leste, inicio da retomada da operação de espionagem
12 setembro	SBU anuncia que identificaram movimento de forças especiais russas programando novos ataques cibernéticos contra a Ucrânia	30 outubro 26 novembro	Spear phising com 2 arquivos datados de 21 de agosto em endereços de email de contas pessoais e do Tribunal Internacional de Arbitragem Comercial da Câmara de Comércio e Indústria da Ucrânia são encontrados com links para páginas falsas de acesso ao Google Chrome
2015	**Ação Física**	**2015**	**Ação Cibernética**
15 janeiro 29 janeiro	Após um longo combate as tropas ucranianas perdem o controle do aeroporto de Donetsk para os separatistas	25 janeiro	Execução de arquivo SFX contendo malware indexado a documento oficial escrito em ucraniano com dados sobre equipamentos e batalhões de reconhecimento envolvidos no conflito em julho de 2014
8 fevereiro	Segundo cessar-fogo assinado	15 fevereiro	Os ataques cibernéticos não cessam até a retirada das tropas ucranianas do Debaltaseve, só então os ataques cibernéticos param e as ameaças são movidas para servidores de uma transportadora internacional de logística de carne e uma loja de eletrônicos
8 fevereiro	Chefe do centro antiterrorista da SBU divulga informações sobre os ataques das forças especiais russas	16 fevereiro	Dropper com relatório do centro antiterrorista da SBU sobre os territórios do leste é utilizado em novos ataques spear phising contra alvos militares
13 março	SBU divulga comunicado oficial sobre atividade cibernética russa atribuída ao 16th antiga agência do governo federal de comunicação e informação e ao 18th centro de segurança federal (FSB) da Rússia	25 março	Após a publicação do relatório oficial da SBU novos ataques spear phising são identificados, dessa vez com as entradas de servidor TTPs monitoradas pela SBU modificadas. Dois arquivos SFX com novos códigos “tron.cmd” contendo malwares

Fonte: LOOKINGGLASS (2015)

Dentre os principais atores não-estatais com alto nível organizacional envolvidos no conflito via ciberespaço estão grupos de hackers classificados como Advanced Persistent Threat (APT) (WEEDON, 2015, p. 69). Essas APT comprometeram sistemas de informação do governo, mídia e infraestrutura crítica da Ucrânia com ataques cibernéticos de negação de serviço e espionagem (CROWDSTRIKE, 2014; 2015; 2016).

Durante o conflito, esses hackers pró-rússia utilizaram táticas de intrusão sofisticadas para infectar não apenas as redes ucranianas, mas também alvos localizados na Europa e América do Norte, suas organizações de segurança, bem como governos, militares e centros

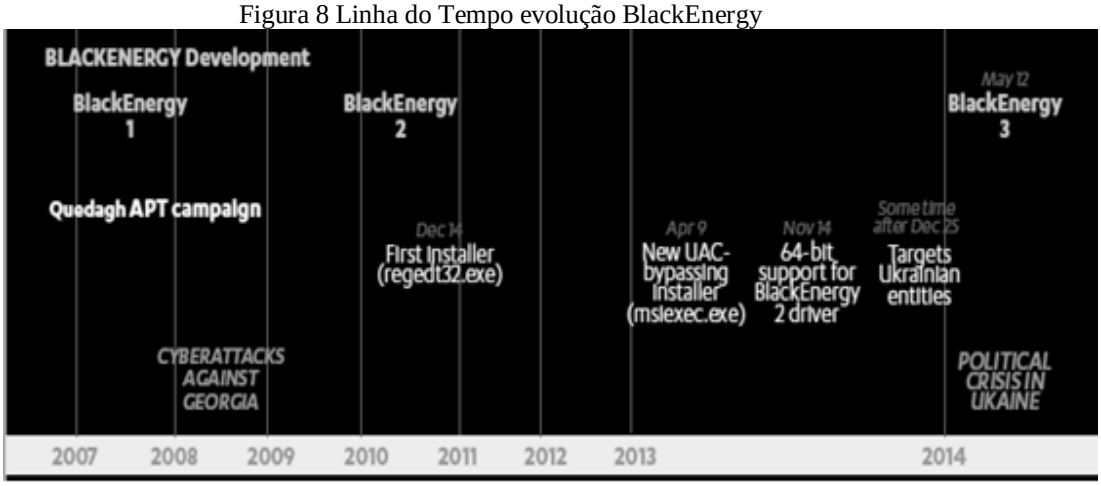
pensantes (WEEDON, 2015, p. 69), demonstrando alta capacidade para explorar vulnerabilidades de sistemas de informação até então não descobertas e corrigidas, destacam-se as APT28: CyberBerkut; FancyBear/Sofacy/Pawn Storm e Sandworm.

> O uso do ciberespaço no conflito ucraniano é particularmente interessante porque combina táticas cibernéticas e de guerra de informação. Isso inclui adulteração de cabos de fibra ótica e telefones celulares de parlamentares ucranianos, além de ferramentas maliciosas mais comuns, como ataques DDoS e falhas na web. O alcance dessa atividade ilustra como a guerra cibernética pode ser diferenciada da guerra de informação e sugere que as ações cinéticas futuras provavelmente serão acompanhadas por ambas (MAURER; JANZ; 2014, p. 1, tradução nossa).

Uma das armas cibernéticas utilizadas pelas APT na Ucrânia é o BlackEnergy (BE), sua evolução tem sido acompanhada por diversas empresas especializadas em segurança cibernética que emitiram relatórios apontando para a evidente convergência entre a atividade criminosa e espionagem russa através do ciberespaço (FIRE EYE, 2014; F-SECURE LABS, 2016).

Os especialistas do F-Secure Labs emitiram uma série relatórios associando a construção do BE ao grupo denominado Quedagh, organização em atividade desde 2010 com histórico de ataques a organizações políticas (F-SECURE LABS, 2016), no entanto, em sua versão mais recente essa arma atingiu, também, setores de infraestrutura crítica (ICS, 2016; E-ISAC, 2016).

Figura 8 Linha do Tempo evolução BlackEnergy



Fonte: F-Secure Labs (2016)

Em 2014, há um grande aumento nas referências a esse *malware* e seu uso crescente para atingir países europeus, e, em específico, na Ucrânia (FLOM, 2016). Analistas identificaram que no início do conflito variações denominadas BE.lite[20] e BlackEnergy2[21] atingiram alvos políticos na Ucrânia (2014-2015) e ocasionaram a queda de diversos sítios eletrônicos do governo, incluindo o do gabinete presidencial (MAURER, BERGEN, 2014). Curiosamente, ambas as versões derivam da mesma família de softwares maliciosos utilizados nos ataques cibernéticos contra a Geórgia (2008) (F-SECURE LABS, 2014a, p. 4; LIPOVSKY, 2014, p. 2-3).

Sem embargo, em fevereiro de 2014, após a queda do presidente ucraniano, uma onda de ataques cibernéticos utilizaram essas variações do BE para interferir nos serviços de telefonia celular dos membros do parlamento dificultando a comunicação e o processo de decisório de resposta à invasão russa ao território da Crimea, esses os ataques ocorreram em perfeita sincronia com as ações das forças especiais russas, os chamados pequenos homens de verde, principais responsáveis pela tomada de controle do território da Crimea.

De acordo com Maurer (2018), apenas quatro dias depois das operações no ciberespaço, as instalações da empresa de comunicações Ukrtelecom foram invadidas e os cabos de fibra ótica adulterados, evitando a conexão entre a península e o restante da Ucrânia (MAURER, 2018, p. 81), a operação de sabotagem evitou que o poder público tomasse uma atitude com relação ao movimento das forças russas na Crimea (WEEDON, 2015, p. 76), configurando, desse modo, uma forte evidencia da simbiose entre a ação dos hackers e forças especiais russas.

No mês de Março de 2014 após a anexação da península ucraniana, a APT CyberBerkut, grupo separatista pró-rússia composto por antigos membros das forças policiais ucranianas, assumiu a responsabilidade por atacar a página da rede do governo ucraniano que ficou fechada por três dias, além dos sites oficiais, telefones celular dos parlamentares ucranianos também foram invadidos (WEEDON, 2015, p. 76). Na ocasião o grupo vinculou

[20] Para atrair a atenção dos alvos, os hackers enviaram documentos do Ministério das Relações Exteriores ucraniano em formato Microsoft Word. A execução de dois arquivos em diretório temporário: o "*payload*" WinWord.exe e o documento com o nome "Embaixadores Russos para conquistar o world.doc", os arquivos eram abertos utilizando a função kernel32.WinExec, então, o WinWord.exe extraia e executava o BlackEnergy Lite. Essa variante não utiliza '*rootkit'* para ocultar objetos no sistema, e não utiliza *driver kernel* para descarregar arquivos, ao invés disso o *dll*. é carregado através do comando "*rundll32.exe*" (LIPOVSKY, 2014, p. 3).

[21] A variante mantém uma lista codificada de offsets em estruturas de *driver kernel* utilizada para as diferentes versões do Windows, o relatório aponta que a amostra foi desenhada tendo como base o Windows 8 e oferece acesso total às informações dos sistemas contaminados, além de ser capaz de esconder os processamentos de rotina utilizados pelo *malware* (F-SECURE LABS, 2014b, p. 1).

notícias contendo informações que indicavam a "ilegitimidade do governo que assumiu a Ucrânia após a expulsão do ex-presidente Viktor Yanukovych" (CROWDSTRIKE, 2014, p. 26-27, tradução nossa).

Ao utilizarem as variações do BE esses hackers foram capazes de subtrair informações sigilosas como códigos de execução e senhas de acesso remoto de seus alvos. Essa APT demonstrou possuir alta capacidade para utilizar o *malware* e afetar políticos do alto escalão do governo ucraniano procedendo com o vazamento periódico de documentos sigilosos em sua página na internet, "foram mais de 50 itens exclusivos, emails, relatórios, acordos, propostas, imagens aéreas e identificação pessoal" (CROWDSTRIKE, 2015, p. 29, tradução nossa). Embora a autenticidade dos documentos seja questionável a ação cibernética desse grupo foi capaz de atrair grande atenção da opinião pública e da mídia internacional (CROWDSTRIKE, 2015, p. 29).

Em abril de 2014, quando o conflito eclodiu em Donbass, as operações aumentaram exponencialmente acompanhando os eventos militares no que concerne à coleta de informações vitais para os setores de inteligência, o que ofereceu vantagem significativa às tropas russas no campo de batalha físico (LOOKINGGLASS, 2015, p. 4). Naquele mês, o alvo da CyberBerkut foram empresas militares privadas como Greystone, Triple Canopy e Academi que eles alegavam estar operando no conflito, novamente chama a atenção o grau de alinhamento das operações com as prioridades do estado russo que neste mês ofereceu apoio técnico e tático aos separatistas do leste conforme descrito na subseção anterior.

Os ataques cibernéticos seguiram uma dinâmica paralela às ações diplomáticas e estratégicas tomadas pelos Estados da Rússia e Ucrânia. Em 21 maio de 2014, logo após a declaração de independência dos territórios de Donbass em relação ao governo central de Kiev, a CyberBerkut assumiu a autoria dos ataques que atingiram a rede da Comissão Central de Eleições (CEC)[22], na ocasião a APT assumiu o controle da página que exibia a apuração eleitoral em tempo real, minutos antes do encerramento da contagem os hackers postaram no site da CEC uma foto anunciando a vitória do conservador Dmitry Yarosh nas urnas, notícia falsa que imediatamente foi compartilhada pelos canais de TV russos (KOVAL, 2015, p. 56).

> A cultura estratégica russa enfoca a guerra como atividade política; Para que o poder cibernético tenha um efeito verdadeiramente estratégico, a Rússia acredita que deve contribuir diretamente para moldar os resultados políticos,

[22] Um dia antes da eleição, o Serviço de Segurança da Ucrânia alertou sobre um vírus nos sistemas da Comissão Central de Eleições projetado para comprometer os dados coletados na apuração, revelando que hackers russos estavam tentando sabotar o pleito (MAURER; JANZ, 2014, p. 2-3, tradução nossa).

> alterando as percepções políticas de seus oponentes para melhor atender seus interesses (PETERSON, 2016, p. 6, tradução nossa).

No dia seguinte, após o final do pleito, quando o sistema teve seu funcionamento reestabelecido pelo serviço de segurança ucraniano (PETERSON, 2016), a CEC precisou confirmar a ação dos hackers para só então conseguir declarar a vitória do social democrata Petro Poroshenko que assumiu a presidência do país (KOVAL, 2015, p. 56).

O relatório da Crowdstrike (2014) aponta outra forte evidencia da ação russa em conjunto com os ataques cibernéticos, observada na medida em que coincidiram com as transmissões da mídia estatal russa que passou a divulgar a informação falsa vinculada pelos hackers em tempo real, conduzindo a opinião pública a colocar em dúvida a legitimidade do pleito (CROWDSTRIKE, 2014, p. 25-26).

> A coordenação da propaganda distribuída e da mídia russa foi particularmente reveladora no que diz respeito a como os serviços estatais russos podem direcionar muitas partes móveis em uníssono para alcançar seus objetivos. objetivos por meios cibernéticos [...] Os ataques DDoS contra o governo ucraniano instalaram um *backdoor*[23] nas máquinas das vítimas, presumivelmente permitindo que os serviços de inteligência russos criassem uma nova *botnet* com os "voluntários" comprometidos, que poderiam ser usados em futuros conflitos (CROWDSTRIKE, 2014, p. 26, tradução nossa).

Embora o relatório (2014) não afirme que a ação foi patrocinada diretamente pela Rússia ou se o grupo atuou de modo independente (CROWDSTRIKE, 2014, p. 27), analistas sustentam com convicção que “a quantidade e a gravidade dos ataques cibernéticos contra a Ucrânia aumentaram paralelamente aos eventos políticos em andamento” (KOVAL, 2015, p. 55, tradução nossa).

Nos meses seguintes, os ataques cibernéticos continuaram a atingir alvos do alto escalão do governo ucraniano como o ministro de Relações Exteriores, o ministro da Defesa, a administração executiva e as embaixadas no exterior, demonstrando grande potencial de intrusão das ações no ciberespaço.

> A totalidade desses eventos, de maio até o presente, exemplifica como os conflitos híbridos são conduzidos no espaço de batalha físico e de

[23] Definição de *Backdoor*: canais de comunicação como meio para que os servidores de Comando e Controle (C2) possam monitorar e controlar remotamente o sistema comprometido, geralmente são usados em conjunto com outros softwares maliciosos em ataques cibernéticos (SHRIVASTAVA, 2016, p. 3).

> informações, também conhecido como "o quinto domínio". Uma força capaz de causar efeitos físicos ao alavancar o quinto domínio é uma força a ser considerada (CROWDSTRIKE, 2015, p. 29, tradução nossa).

Outra APT identificada nas operações cibernéticas que atingiram a Ucrânia durante o conflito é o FancyBear/Sofacy/PawnStorm, grupo ativo desde 2000 apontado como responsável por atingir diversas organizações em todo o mundo através de armas cibernéticas multifuncionais enviadas via e-mail *spear phishing* para atingir setores “aeroespacial, defesa, energia, governo, mídia e dissidentes” (CROWDSTRIKE, 2016, p. 8, tradução nossa). Devido ao largo envolvimento com ataques cibernéticos a alvos políticos, essa ATP foi classificada como representante dos interesses da Federação Russa, vinculada ao Departamento de Inteligência Militar (GRU) (CROWDSTRIKE, 2016, p. 8,).

A campanha de espionagem cibernética atribuída a essa APT foi capaz de subtrair credenciais de acesso corporativo a sistemas de informação de importantes organizações governamentais da Ucrânia como forças armadas, ministério da defesa, indústria da defesa, partidos políticos, mídia e governos (HACQUEBORD, 2015, p. 3) e de segurança da Europa, como a Organização do Tratado do Atlântico Norte (OTAN) e a Organização de Segurança e Cooperação da Europa (OSCE) (FIREEYE, 2014, p. 14). A figura 9 apresenta um gráfico com os principais alvos atingidos por ataques cibernéticos *spear phishing* nas campanhas dessa APT.

Figura 9 Principais Alvos/Setor atingidos por ataques cibernéticos

Fonte: HACQUEBORD (2015).

Durante a campanha os hackers usaram ao menos seis ataques *zero-day*[24] (HACQUEBORD, 2015, p. 3) através de "provedores internacionais de webmail, como Yahoo e Gmail; bem como provedores de webmail para usuários ucranianos da Internet (Ukr. net) e usuários russos (Yandex e Mail.ru)" (HACQUEBORD, 2017, p. 9, tradução nossa), ao abrirem o e-mail aparentemente legítimo enviado por estes provedores, os usuários atingidos permitiam acesso irrestrito às suas contas, milhares de usuários foram alvo desse tipo de operação (HACQUEBORD, 2015, p. 5).

As ações cibernéticas do grupo conectam-se com às da CyberBerkut na medida em que facilitaram o intercambio de informações roubadas e o vazamento de documentos confidenciais (HACQUEBORD, 2017, p. 6). Todavia, embora a relação entre o Pawn Storm e a CyberBerkut tenha sido pouco explorada, analistas apontam que a "CyberBerkut publicou informações que foram roubadas durante as campanhas de *phishing* de credenciais do Pawn Storm" (HACQUEBORD, 2017, p. 8, tradução nossa). Outrossim, no caso do ataque ao CEC, o CERT-UA encontrou evidências de que os softwares maliciosos utilizados para espionagem do sistema da comissão correspondiam ao Sofacy, grupo conhecido por atingir alvos por longos períodos de tempo sem que suas ações sejam detectadas (KOVAL, 2015, p. 57).

Em julho de 2014, aproveitando a atenção da imprensa no caso do acidente envolvendo o voo MH17 da Malaysia Airlines que saiu de Amsterdã em direção à Kuala Lumpur e foi abatido pelos separatistas do leste, a APT passou a utilizar a notícia sobre o acidente como isca para atingir os alvos via em e-mails *spear phishing* que divulgavam a informação de que os conflitos no local do acidente haviam cessado após a queda da aeronave (CROWDSTRIKE, 2014, p. 40).

Em agosto de 2014 uma nova campanha de *spear phishing* foi identificada e atribuída ao grupo, o e-mail contendo uma lista com os nomes de membros do parlamento ucraniano que estariam oferecendo apoio aos separatistas do leste foi enviado em nome do primeiro ministro da Ucrânia Arzeniy Yatsenyuk aos órgãos de investigação como Ministério Público, Serviço de Segurança, Ministério de Assuntos Internos e o Ministério da Justiça, com diretrizes oficiais para que essas instituições verificassem a veracidade das informações (LIPOVSKY, 2014, p. 2). No entanto, o arquivo em anexo no formato Microsoft PowerPoint (PPSX) estava infectado com uma versão do BE.lite que ao ser aberto oferecia acesso aos hackers as contas dos servidores dessas instituições (LIPOVSKY, 2014, p. 3).

[24] Definição *zero-day*: vulnerabilidades ou falhas de software que deixam os usuários expostos a ataques cibernéticos por não serem conhecidas pelos sistemas de segurança (FIREEYE, 2016b, p. 3).

Outra arma cibernética associada a essa APT é o X-Agent, ferramenta de acesso remoto capaz de infectar sistemas operacionais diversos como Windowns, iOS e MacOS (MEYERS, 2016, p. 1). Identificada pela primeira vez em um aplicativo legítimo desenvolvido pelo oficial integrante da artilharia ucraniana Yaroslav Shertuk, prometia oferecer maior eficiência aos sistemas de artilharia do Exército, reduzindo o tempo de disparo de minutos para segundos (MEYERS, 2016, p. 2, tradução nossa).

A análise do X-Agent indicou uma série de artefatos em língua russa de natureza militar, evidencias da simbiose entre o FancyBear e o setor de inteligência militar russa (GRU) que opera em apoio aos separatistas no leste da Ucrânia (MEYERS, 2016, p. 2).

Em 2014, o aplicativo foi apresentado em fóruns militares ocorridos na Ucrânia que chegou a ser utilizado por quase 9.000 usuários, contudo, ao ser instalado a ferramenta implantava de modo sigiloso o X-Agent nos sistemas operacionais dos celulares desses usuários que, em grande, se tratavam de integrantes da artilharia ucraniana. Uma vez infectados os aparelhos forneciam aos hackers a localização exata em tempo real das tropas inimigas que de acordo com os analistas eram repassadas aos setores de inteligência russos permitindo que as Forças Armadas da Federação pudessem antecipar os movimentos do adversário no campo de batalha (MEYERS, 2016, p. 4).

Devido a sua estrutura modular a presença de variações do X-Agent foram, igualmente, identificadas em sistemas operacionais infectados do Comitê Nacional Democrata (DNC) e outras organizações políticas (MEYERS, 2016, p. 1). Nesse caso, a arma cibernética foi utilizada para execução remota de comandos, transmissão de arquivos e registro de chaves de acesso através de comandos rundll32, juntamente com a arma cibernética denominada X-Tunnel que ajuda a estabelecer conexões remotas em ambientes de acesso público que são de difícil detecção, combinadas essas ferramentas infectam os sistemas via RemCom, através da plataforma GitHub, com arquivos maliciosos compilados em bibliotecas que se encontram disponíveis para carregamento em software de análise de dados, (CROWDSTRIKE, 2016, p. 10).

Em que pese o fato de que as atividades de espionagem cibernética dos grupos APT28 foram classificadas como operações altamente qualificadas empregadas por “desenvolvedores e operadores que coletam informações sobre questões de defesa e geopolíticas que só seriam úteis para um governo” (FIREEYE, 2014, p. 3, tradução nossa).

As amostras de *spear phishing* coletadas pelo FireEye (2014) contêm códigos escritos em idioma russo e apresentam atividade em horário comercial de acordo com o fuso horário

das principais cidades da Federação Russa “evidências de operações focadas e de longa data que indicam um patrocinador do governo - especificamente, um governo com sede em Moscou” (FIREEYE, 2014, p. 3, tradução nossa).

> Mais de 96% das amostras de malware que atribuímos ao APT28 foram compiladas entre segunda e sexta-feira. Mais de 89% foram compilados entre 8h e 18h no fuso horário UTC + 4, que é paralelo ao horário de trabalho em Moscou e São Petersburgo. Essas amostras tiveram datas de compilação que variaram de meados de 2007 a setembro de 2014 (FIREEYE, 2014, p. 5, tradução nossa).

A análise dos arquivos enviados por *spear phishing* revelaram que o assunto dos e-mails infectados com softwares maliciosos foi adaptado aos temas de interesse dos destinatários, tratam-se, portanto, de iscas que fornecem pistas aos analistas sobre as metas e interesses dos grupos hackers. De acordo com o relatório (2014) esse tipo de estratégia precisa oferecer informações relevantes para que os usuários abram os e-mails, dentre iscas utilizadas foram identificados três temas relevantes para o governo russo como “O Cáucaso particularmente sobre a Geórgia; Governos e Militares do Leste Europeu; OTAN e outras organizações de segurança europeias” (FIREEYE, 2014, p. 6, tradução nossa).

> Nossa análise de algumas das ferramentas mais usadas pelo grupo indica que o APT28 atualiza sistematicamente suas ferramentas desde 2007. O APT28 provavelmente é suportado por um grupo de desenvolvedores que cria ferramentas destinadas ao uso e versatilidade a longo prazo, que se esforçam para ofuscar a atividade deles. Isso sugere que o APT28 recebe recursos financeiros e outros diretos e contínuos de uma organização bem estabelecida, provavelmente um governo estadual (FIREEYE, 2014, p. 19-21, tradução nossa).

O relatório indica que as amostras de ameaças analisadas “utilizam a mesma sequência de descriptografia e algoritmos semelhantes para codificação e decodificação” (FIREEYE, 2014, p. 21, tradução nossa). Para verificar as semelhanças encontradas os analistas identificaram um padrão nos códigos dos e-mails de *spear phishing*, “arquivos com nomes específicos, hashes MD5, carimbos de data e hora, funções personalizadas e algoritmos de criptografia, *backdoors* com endereços de IP e Comando e Controle similares e nomes de domínios incorporados” (FIREEYE, 2014, p. 29, tradução nossa).

> No nível mais básico, dizemos que dois eventos de intrusão são atribuídos ao mesmo grupo quando coletamos indicadores suficientes para mostrar, além de qualquer dúvida razoável, que o mesmo ator ou grupo de atores estava envolvido. Rastreamos todos os indicadores e vínculos significativos associados a grupos de ameaças identificados em um banco de dados próprio que compreende milhões de nós e vínculos entre eles. Dessa forma, sempre podemos voltar e responder "por que" associamos a atividade de ameaças cibernéticas a um grupo específico (FIREEYE, 2014, p. 29, tradução nossa).

A última APT identificada no conflito é o Sandworm, grupo apontado como responsável por obter códigos de execução e senhas de acesso remoto para atacar setores de infraestrutura crítica da Ucrânia em meados de 2015 (LIPOVSKY, 2014).

Os principais softwares maliciosos identificados nos ataques atribuídos ao Sandworm foram o BlackEnergy 3[25] (BB3) e o KillDisk (KD)[26], ao utilizar essas armas cibernéticas a APT infectou os sistemas operacionais dos computadores utilizados pelas vítimas, com a ação esses hackers foram capazes não apenas obter senhas pessoais de acesso ao sistema operacional das instalações elétricas como também destruir os caminhos utilizados para evitar a detecção do processo (WEEDON, 2015, p. 73).

Desde o ano anterior as atividades do Sandworm já estavam sendo monitoradas pelo FireEye (2014) que alertou sobre uma invasão em curso aos sistemas de energia de empresas polonesas e agências do governo ucraniano “o grupo parecia estar desenvolvendo métodos para atingir as arquiteturas especializadas de computadores usadas para gerenciar remotamente os equipamentos industriais físicos” (GREENBERG, 2017a, p. 11, tradução nossa).

Analistas frisam que a ameaça "Blackenergy tem sido considerado o cartão de visitas desse grupo hacker” (TUPUK; HAILES, 2016) indicativo de sua relação com a campanha de espionagem cibernética orquestrada pelo FancyBear/PawnStorm. Ao utilizar ataques de *zero-day*[27] para atingir alvos dessa natureza a APT inaugurou uma nova fase no conflito que revela a alta capacidade de ação da Rússia no ciberespaço (PAKHARENKO, 2015, p. 64-66).

---

[25] Definição *BlackEnergy 3*: arma de infiltração e roubo de informações, se diferencia das versões anteriores pois usa um componente de instalação mais simples e não possui um componente de *driver kernel*. O BB3 invade diretamente a pasta de dados do aplicativo local (não-móvel), em sequência um arquivo LNK é instalado com o nome de gerado com base no número de série do volume como ponto de ativação. O LNK é um atalho para executar a DLL principal usando o rundll32.exe (F-SECURE LABS, 2016, p. 11).

[26] Definição *Kill Disk*: arma desenvolvida para apagar o rastro dos processos de infiltração que utilizam a plataforma Windows conectados via *serial-to-ethernet* (E-ISAC, 2016, p. 6). O KD identificado nos ataques cibernéticos para sabotar os sistemas de controle industrial (ICS) não apenas encerra os processos como também tem a capacidade de substituir o arquivo executável por dados aleatórios (CHEREPANOV, 2016, p. 6).

[27] Os invasores interromperam o fluxo de eletricidade manipulando as IHMs de despachantes do sistema de distribuição - aplicativos que os operadores da rede usam para controlar o fluxo de energia para residências e

O desenvolvimento desse tipo de arma cibernética para exploração de vulnerabilidades nos sistemas de segurança de infraestrutura crítica requer alto nível de investimento, fator que indica a presença de um ente com capacidade de financiar tamanho esforço de engenharia da informação (F-SECURE LABS, 2014).

O ataque cibernético foi confirmado pelo relatório da Crowdstrike (2015) que acrescenta a importância do monitoramento das ações dessa APT na medida em que revela um alto potencial para causar impacto no nível tático do conflito ao utilizarem combinações de softwares maliciosos para conseguir acesso ao sistema operacional das usinas ucranianas da região de Ivano Frankvisk (CROWDSTRIKE, 2015, p. 26)[28].

O incidente na região de Ivano-Frankivsk foi reportado às 15:35-16:30, pela Kyivoblenergo (companhia regional de distribuição de energia elétrica) indicando que terceiros obtiveram acesso ilegal ao sistema de tecnologia de informação (TI), desconectando sete subestações 110kV e 23 subestações 35K, durante mais de duas horas o sistema teve de operar em modo manual e o serviço só foi restabelecido às 18:56 do mesmo dia (ICS, 2016, p. 1).

> Cada empresa informou que eles tinham sido infectados com o *malware* BlackEnergy, no entanto, não sabemos se o *malware* desempenhou um papel nos ataques cibernéticos. O *malware* foi supostamente entregue via spear phishing com anexos maliciosos do Microsoft Office. Suspeita-se que BlackEnergy pode ter sido usado como um vetor de acesso inicial para adquirir credenciais legítimas (LEYDEN, 2016, p. 3 , tradução nossa).

Em janeiro e fevereiro de 2016, o Sistema de Controle Industrial (SANS) e o Sistema de Controle Industrial para Ciber Emergências (ICS-CERT), respectivamente, emitiram relatórios que confirmaram que a interrupção no fornecimento de energia da cidade de Ivano-Frankvisk, em 24 de Dezembro de 2015, foi causada por uma série de ataques cibernéticos que indicavam a presença de hackers especializados em táticas de espionagem cibernética (E-ISAC, 2016; ICS-CERT, 2016).

---

empresas [...] exploraram duas vulnerabilidades desconhecidas em equipamentos de rede do sistemas de controle para inibir a capacidade das empresas de restaurar a energia e manter o controle da rede (FIRE EYE, 2016a, p. 10, tradução nossa).

[28] O relatório (2015) pondera que o ataque russo foi uma resposta cibernética de alto nível de sofisticação às ações do governo central de Kiev que no final de novembro de 2015 destruiu alvos físicos da região leste, na ocasião os ataques às linhas de energia que forneciam o serviço para península anexada da Crimea deixaram mais de dois milhões de pessoas que residem na região sem energia elétrica (CROWDSTRIKE, 2015, p. 27, 28).

O Departamento de Segurança norte americano (DHS) emitiu nota através alerta H-16-056-01, indicando que os ataques cibernéticos foram muito bem coordenados, e ocorreram de modo sincronizado em um intervalo de pouco mais de 30 minutos, atingindo instalações centrais e regionais, a similaridade entre os sistemas de controle afetados teria sido a razão para a escolha dos alvos.

Os resultados do relatório divulgado pelo ICS-CERT (2016) confirmaram o envolvimento de uma rede de planejamento e coordenação de difícil detecção, o ataque foi acompanhado de uma ação que destruiu todos os rastros nos dispositivos atingidos utilizando um software malicioso do tipo limpador de registros (ICS-CERT, 2016, p. 1-2).

O relatório divulgado pelo Centro de Análise e Compartilhamento de Informações do setor de Energia (E-ISAC) (2016) apontou que somadas as três diferentes estações atacadas o número de usuários afetados pelo comprometimento do sistema de energia elétrica foi de 225.000 mil (E-ISAC, 2016, p. 1).

Do ponto de vista internacional, que levou em conta o número de usuários afetados, a quantidade de infraestrutura elétrica envolvida e a duração da interrupção até a restauração completa do sistema os ataques foram classificados com nível moderado. No entanto, tendo em consideração a conjuntura regional, a exposição da vulnerabilidade do Sistema de Supervisão e Aquisição de Dados (SCADA) para infraestruturas críticas limitou a confiabilidade público-privada na segurança do mesmo, sob essa perspectiva, os ataques foram considerados críticos (E-ISAC, 2016, p. 3).

O relatório (E-ISAC, 2016) aponta, ainda, que o tempo estimado da operação que atingiu as estações elétricas da região foi de aproximadamente seis meses, entre o reconhecimento do sistema e o ataque propriamente dito, evidencia que indica o envolvimento de atores especializados em táticas de intrusão com acesso a recursos externos e treinamento profissional para subtrair credenciais e informações privadas e obter acesso aos controles da rede de energia sem que sua presença tivesse sido notada pelos sistemas de segurança (E-ISAC, 2016, p. 4).

Ainda de acordo com esse relatório, os detalhes do ataque cibernético comprovam o alto grau de complexidade técnica empregada para que a ação tenha sido considerada bem sucedida:

> Os atores demonstram experiência, não apenas em redes e infraestrutura online, como Fontes de Alimentação Ininterrupta (UPSs), mas também em operar os ICSs através de um sistema de controle de supervisão, como a

> Interface Homem Máquina (HMI). [...] A capacidade mais forte dos atacantes não estava na escolha das ferramentas ou na sua perícia, mas na sua capacidade de realizar operações de reconhecimento para aprender sobre o ambiente e executar um ataque múltiplo altamente sincronizado (E-ISAC, 2016, p. 4-5, tradução nossa).

O relatório E-ISAC (2016) ressalta que as etapas de planejamento e execução dos ataques ocorridos em Ivano-Frankivsk seguiram o modelo apresentado por Assante e Lee (2015, p. 2-8) em relatório da SANS. De acordo com o documento (2016), o primeiro estágio da invasão foi composto pelas fases de preparação e execução da intrusão cibernética, envolvendo a espionagem ou operação de inteligência para reconhecimento do sistema e armazenamento da ameaça (E-ISAC, 2016, p. 8).

No que tange o modo de operação da APT, durante a fase de planejamento do ataque, os computadores dos Kyivoblenergos foram infectados através de e-mails enviados a indivíduos na rede administrativa ou da T.I das empresas de eletricidade, a preparação envolveu o uso de e-mails *spear phising* contendo arquivos em formato Microsoft Office Excel e Word infectados com o BB3 que permitiram aos hackers extrair códigos de informação e senhas de acesso aos sistemas operacionais das instalações (E-ISAC, 2016, p. 8).

Após a infiltração os invasores atuaram no ambiente infectado como usuários autorizados, esse acesso irrestrito e indetectável permitiu que descobrissem as vulnerabilidades do sistema e extraíssem os dados necessários para formular um plano de ataque (E-ISAC, 2016, p. 6).

A fase seguinte refere-se ao desenvolvimento e execução do ataque cibernético às instalações elétricas. Primeiramente, os ataques cibernéticos ao sistema operacional de Prykarpattya Oblenergo danificaram aos sistemas de energia das estações e subestações de modo simultâneo, em sequência, para evitar o rastreamento, os hackers utilizaram os códigos de administrador remoto para modificar o firmware, o KD destruiu os arquivos corrompidos do sistema e o caminho dos invasores foi apagado (E-ISAC, 2016, p. 5).

Por fim, os hackers utilizaram um ataque do tipo de negação de serviço (D-DoS) no sistema de comunicação telefônica, congestionando o serviço de central de atendimento da empresa de energia com milhares de chamadas, garantindo que os usuários atingidos não conseguissem relatar as interrupções (E-ISAC, 2016, p. 12).

Uma vez conectado ao sistema de Comando e Controle (C2)[29], através de endereço IP, os hackers utilizaram a própria rede privada virtual (VPN) das estações para obter acesso aos dados administrativos das empresas e lançar comandos destrutivos à distância, desse modo a APT conseguiu estabelecer comunicação com o software malicioso e os sistemas infectados sem que fossem detectados pelo sistema de segurança (E-ISAC, 2016, p. 9-10). Em suma, a execução do ataque utilizou o controle do próprio sistema para cortar o fornecimento de energia em três empresas de infraestrutura crítica energética.

O relatório (2016) confirma que os softwares maliciosos BB3 e KD não foram os causadores da interrupção do funcionamento dos sistemas SCADA de energia elétrica, mas serviram de ferramentas para disparar e-mails maliciosos e conseguir informações de acesso privilegiado da administração da infraestrutura elétrica e apagar os rastros da ação (E-ISAC, 2016, p. 13).

No caso dos ataques à rede elétrica de Ivano-Frankvisk, o longo período de tempo em que os hackers interagiram nos três ambientes de gestão de documentos DMS[30] confirma o previsto pelo modelo de Assante e Lee (2015, p. 2-8). A ação imperceptível ofereceu tempo suficiente para que os hackers pudessem desenvolver um firmware malicioso para dispositivos *serial-to-ethernet* que foi capaz não apenas de danificar os disjuntores de 27 subestações elétricas dos sistemas SCADA, como também evitar que as estações fossem recuperadas com uso de comandos remotos (E-ISAC, 2016, p. 10-12).

Em Ivano Frankvisk a obtenção das senhas de acesso remoto foi o fator chave que permitiu aos atacantes enviar comandos administrativos capazes de comprometer o funcionamento do sistema de energia. De acordo com a análise do FireEye (2016a) "O sucesso desses incidentes ao comprometer sistemas-chave para atingir um objetivo político ou demonstrar as capacidades de um adversário nos faz esperar que os adversários de um Estado-nação explorem cada vez mais vulnerabilidades específicas da ICS" (FIREEYE, 2016a, p. 9, tradução nossa).

Destarte, analistas indicam que durante o conflito em questão os ataques cibernéticos multicoordenados que atingiram setores estratégicos excluindo dados, destruindo computadores e paralisando funções básicas das instituições governamentais da Ucrânia

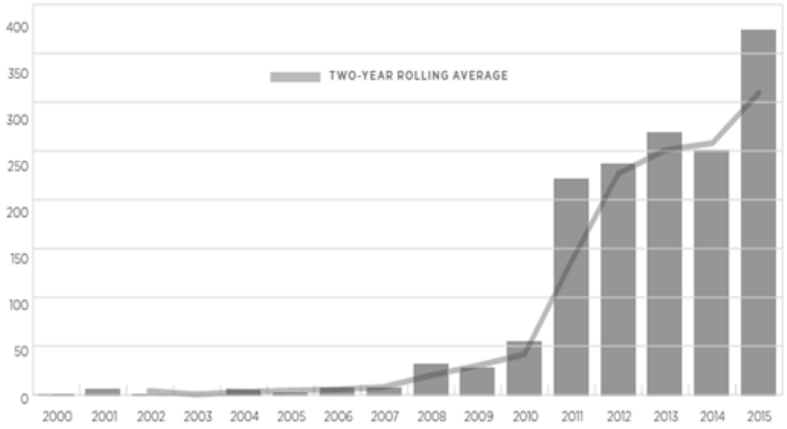
[29] Comando e Controle (C2) termo de uso comum dentro da indústria de segurança de computadores e no contexto da guerra cibernética, refere-se a um servidor locado em um computador controlado por um invasor que é utilizado para enviar comandos a sistemas comprometidos por softwares maliciosos [TRENDMICRO, 200-?]

[30] O Sistema de Gestão de Documentos (DMS) utilizado para rastrear, gerir e armazenar documentos, capaz de manter um registro das várias versões criadas e modificadas por diferentes usuários (histórico de rastreamento). (WIKIPEDIA, n/a).

não encontram precedente na história (GREENBERG, 2017a, p. 4). Além das estações de energia, alvos como companhia mineração e operadoras de transporte também foram atingidas pelo BlackEnergy, o que indica que o software malicioso não se limita ao uso em estações de distribuição de energia (LEYDEN, 2016).

De fato, conforme aponta a figura 10 os ataques aos sistemas SCADA que operam grande parte das infraestruturas críticas têm crescido de modo exponencial sinalizando a importância crescente para os Estados contemporâneos do estudo do fenômeno da GHC no que tange a segurança desses setores.

Figura 10 Vulnerabilidades específicas descobertas do ICS



Fonte: FireEye (2016a).

Apesar de a Rússia negar agir em consonância com os grupos hackers, a coincidência cronológica entre os ataques cibernéticos e as invasões por terra, a engenharia da informação por detrás dos códigos das armas identificadas e os horários de funcionamento das APT são fortes indícios do envolvimento simbiótico entre hackers e as Forças Armadas da Federação. Em geral, observamos que os ataques cibernéticos ocorreram em consonância com a ação de forças especiais que ao avançarem sobre as fronteiras ucranianas foram capazes de comprometer setores estratégicos mediante uso de informações privilegiadas coletadas por campanhas sofisticadas de intrusão e coleta e/ou destruição de dados.

Mediante a análise desta seção, atestamos a identificação do funcionamento do mecanismo causal investigado enquanto condição suficiente para oferecer retornos crescentes à Federação Russa frente seu adversário regional, fator que, em última instância, conectou a mudança institucional descrita nos documentos oficiais ao campo de batalha através do emprego da GHC.

3. DISCUSSÃO E RESULTADOS

Frente ao exposto, nesta seção apresentamos uma breve discussão dos resultados de nossa análise sobre o conflito que oferece resposta ao questionamento central desta pesquisa.

A análise buscou através da coleta de informações, análise de documentos, e, rastreamento das ações, estabelecer uma cadeia sucessória de eventos do uso da guerra assimétrica pelo Estado russo. A atenção à historicidade confere maior credibilidade aos argumentos e tal encadeamento sugere uma ligação entre o crime cibernético e as pretensões do governo russo de expansão regional.

Sob este prisma, abordou-se, primeiramente o fenômeno da guerra híbrida e as definições dos termos que compõem o conceito. Diante disso, analisamos, em paralelo à evolução da estratégia russa, o emprego da guerra híbrida em sua vertente cibernética, a GHC foi descrita pela ação coordenada entre atores estatais e não-estatais, de forma mais detida ao domínio militar e político do ciberespaço. Identificamos que o conflito cibernético reduziu significativamente o custo da ação, em um contexto de desaparelhamento das forças russas frente aos novos desafios dos conflitos contemporâneos.

A evolução da estratégia de Defesa nacional e Segurança da Federação Russa é envolta por tensões geográficas, antecedentes ideológicos, padrões tecnológicos e a relação das instituições com seus líderes (HEICKERO, 2010, p.12).

Nossa análise historiográfica descritiva e comparativa partiu do pressuposto de que a reformulação dos documentos oficiais Estratégia de Segurança Nacional (2009; 2015); Doutrina Militar (2010-2014) ampliou as capacidades do Estado para projetar poder em seu entorno regional mediante prioridade ofertada ao investimento em tecnologia, pesquisa e desenvolvimento de armas modernas e eficazes para uso nos conflitos contemporâneos que envolvem o ciberespaço como zona de combate proeminente.

Nesse sentido, compreendemos a Doutrina Militar e a Estratégia de Segurança Nacional como os documentos fundamentais que conectam a estratégia ao nível operacional e tático das ações do Estado. Tendo em vista a proteção do interesse nacional, defende a preservação da soberania enquanto princípio basilar na condução do processo de tomada de decisão. Desse modo, enquanto instrumento, configuram-se em uma série de crenças, interesses, regras e princípios que estão imbricados na política externa, ajudando o governo a cumprir sua missão e implantar seus interesses nacionais (MORIN; PAQUIN, 2018).

Nesta dissertação observamos que, nas últimas décadas, a Federação Russa deu inicio a um processo de mudança institucional descrito em detalhes na seção dois desta dissertação, com o objetivo de fortalecer as entidades responsáveis pela Defesa e Segurança do Estado para lidar com os desafios impostos pela era da informação.

Mediante a análise das fontes oficiais identificamos que esses documentos reconhecem a importância da guerra de informação como chave para disputa dos conflitos contemporâneos e a intensificação das atividades de guerra de informação como uma característica da guerra moderna. Neles, é flagrante o incentivo ao desenvolvimento de novos modelos de armas de combate e sistemas de inteligência, e, nítido a preponderância concedida à preparação do campo de batalha enquanto ação militar condizente com os objetivos estratégicos da Federação Russa.

No que tange a segurança cibernética, nas últimas duas décadas esses documentos confirmam a intenção da Federação Russa em estabelecer medidas substantivas para controle das ameaças como o aprimoramento das capacidades dos órgãos de comando e controle, o aumento da eficiência e poder de serviços de inteligência e a criação de novas divisões especializadas em segurança e defesa cibernética.

Os documentos reforçam o interesse do país em fortalecer seu Complexo Industrial Militar (CIM), conferindo à tecnologia papel de destaque para Defesa e Segurança do Estado e da sociedade civil. De tal modo que, para responder aos desafios da era da informação, a Federação Russa estabeleceu o desenvolvimento de alta tecnologia e profissionalização das forças militares como preocupação fundamental do Estado, no intuito de ampliar sua capacidade de operar em diversos terrenos, dentre os quais o espaço de informação tornou-se o mais promissor conforme verificamos na seção três desta dissertação.

Conforme verificamos na terceira seção, frente aos acontecimentos históricos que envolveram o conflito entre Rússia e Ucrânia e levaram a queda do presidente Yanukovych, o avanço das tropas russas sobre as fronteiras ucranianas, ação que resultou na anexação da Crimeia e suporte aos movimentos separatistas em Donbass demonstraram a alta capacidade das forças russas em empregar de modo inovador as diretrizes contidas nos documentos oficiais.

A análise das amostras das armas e ameaças cibernéticas bem como dos alvos físicos atingidos durante o conflito ajudam a identificar o impacto decisivo da estratégia russa de emprego da espionagem cibernética para oferecer suporte técnico e tático na preparação do

campo de batalha para operações militares a partir da mobilização das agências de inteligência em conjunto com atores não-estatais.

Identificamos que, em geral, na medida em que forneceram informações valiosas para que os setores de inteligência pudessem preparar as operações militares, as operações cibernéticas realizadas pelas APT28 ofereceram uma vantagem estratégica para as ações no mundo físico contra alvos como organizações políticas, militares e infraestruturas críticas. Desse modo, verificamos o aumento das capacidades qualitativas de ação tática das forças russas manifesta através da simbiose com ações de agentes não-estatais em ataques que comprometeram o funcionamento de setores estratégicos ucranianos e proporcionaram vantagens crescentes à Rússia sobre seu adversário ao longo do conflito.

Nesse sentido, os principais atores não-estatais identificados nos ataques cibernéticos foram o CyberBerkut, FancyBear/Pawn Storm/Sofacy e Sandoworm, bem como, respectivamente, as principais ameaças utilizadas, o Be.Lite, o BlackEnergy 2, Blackenergy 3, o X-Agent e os *spear phishing*.

A despeito de que as ações cibernéticas figurem como reforço aos movimentos da agência, e, portanto, não substituam a necessidade de emprego das forças cinéticas por parte do Estado (WIRTZ, 2015, p. 31-32), é cabal a evidência de que o funcionamento do mecanismo causal identificado nesta dissertação com ajuda da técnica de rastreamento de processos configure condição suficiente para integrar a tecnologia da informação às operações militares e produzir resultados políticos mediante a configuração do fenômeno da GHC.

Todavia é prudente observar que o dano causado à Ucrânia no início do conflito através das operações cinéticas e cibernéticas não exigiram grande esforço das forças russas, uma vez que grande parte da infraestrutura ucraniana como serviços de correio eletrônico e telecomunicações data do período da antiga URSS, razão pela qual os serviços de inteligência e segurança da Federação tiveram seu trabalho facilitado (GILES, 2015, p. 24).

A despeito disso, é flagrante que com a intensificação do conflito os ataques cibernéticos a setores de infraestrutura crítica do setor de energia aumentaram a complexidade das ações identificadas elevando a um novo patamar a disparidade de poder entre a Rússia e a Ucrânia.

Note-se, portanto, que a condição em que ocorre o conflito cibernético entre russos e ucranianos ensina valiosas lições sobre o potencial das ameaças cibernéticas quanto à exploração de complexos sistemas de informação para causar danos econômicos e sociais aos

adversários, ressaltando a importância da segurança cibernética dos sistemas que operam essas infraestruturas críticas.

Os resultados dessa pesquisa confirmam nossa hipótese de que a ação dos hackers em simbiose com as Forças Armadas resulta em ganhos crescentes para o Estado contemporâneo que utiliza a GHC para consecução de seus objetivos estratégicos em âmbito regional.

Torna-se, portanto, difícil refutar a suspeita de que a ação dos hackers parece ser impulsionada por um ente capaz de financiar esse tipo de campanha de longo prazo, mediante a verificação do alto grau de sofisticação dos ataques cibernéticos e a capacidade de atualização das ameaças, tamanha complexidade aponta para o envolvimento de um ente estatal robusto capaz de alavancar consideravelmente as ações no ciberespaço, uma vez que para ser efetiva, a ação cibernética requer largo investimento em tecnologia da informação e infraestrutura, bem como uma organização operacional profissional (WEEDON, 2015, p. 70-71).

Por fim, uma das vantagens oferecidas pelo emprego da metodologia qualitativa que orienta esta dissertação é que seu resultado pode ser generalizado para outros casos dependendo do grau de abstração utilizado (MAHONEY, 2012, p. 574). Desse modo, podemos confirmar a condição de suficiência do mecanismo causal identificado em estudos comparados futuros que permitam observar GHC em outras ações militares da Rússia e/ou outras potências contemporâneas em conflitos regionais.

4. CONSIDERAÇÕES FINAIS

A partir da análise documental dos documentos oficiais da Doutrina Militar e Estratégia Segurança Nacional identificamos o processo de mudança institucional dos órgãos responsáveis pela Defesa e Segurança da Federação Russa como condição necessária para que as forças russas pudessem se adaptar ao emprego da tecnologia da informação no conflito. Mediante a classificação dos principais temas explorados por esses documentos (quadro 2 e 3), verificamos artigos que indicam a preponderância dada ao controle das ameaças mediante investimento em infraestrutura do complexo industrial militar com intuito de aumentar a eficiência qualitativa das forças investindo em armas de alta precisão e no desenvolvimento do complexo industrial militar.

A preponderância dada ao emprego da tecnologia da informação no conflito confirma as diretrizes estabelecidas pelos documentos oficiais, tornando o ciberespaço uma zona de combate chave para aumento da assimetria de poder regional entre a Federação Russa e a Ucrânia. Não obstante, conforme apontam os relatórios de empresas especializadas em segurança da informação aqui analisados, o aumento da assimetria de poder regional foi identificado mediante o rastreamento do processo que descreve o funcionamento do mecanismo causal denominado como simbiose hacker-Exército, na qualidade de condição suficiente para a promoção do fenômeno revelado guerra híbrida cibernética, condição esta que conectou com primazia a estratégia descrita nos documentos oficiais às operações e táticas empregadas durante o conflito.

Nesse sentido é plausível afirmar que o avanço das tecnologias da informação empregadas no ciberespaço se tornou fulcral para projeção de poder da Federação Russa em seu entorno regional, uma vez que esta se tornou uma zona de combate inovadora para congregar estratégia, operações e tática de ação da agencia estatal e não-estatal para obter retornos crescentes ao Estado da Rússia para consecução de seus interesses estratégicos.

Ao lançarmos luz sobre o questionamento central deste estudo acreditamos que esta dissertação elucida a forma como o processo de mudança institucional na estratégia de ação russa em entorno regional, atrelado a operações militares altamente sofisticadas proporcionadas pelo avanço da tecnologia de informação, ampliou às capacidades de projeção de poder da Federação Russa. Encerramos, pois, convictos de nossa contribuição para o avanço do debate sobre um fenômeno ainda pouco estudado que representa o impacto do emprego de novas tecnologias da informação em conflitos contemporâneos. Fenômeno este aqui denominado guerra híbrida cibernética.

REFERÊNCIAS

ARQUILLA, John, RONFELDT, David. Cyberwar is Coming!. In:_____. **Athena's Camp: Preparing for Conflict in the Information Age,** Califórnia: RAND. 1997. p. 2-38.

ASSANT, M; LEE, Robert. The Industrial Control System Cyber Kill Chain. SANS **Institute Information Security Reading Room,** p. 1-21, 2015. Disponível em https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297. Acesso em: 28 abril 2018.

BBC. Ukraine crisis: key players in eastern unrest. **BBC NEWS,** 28, p. 1-21, agosto. 2014. Disponível em: http://www.bbc.com/news/world-latin-america-27211501. Acesso em: 17 junho 2017.

BBC**.** Ukraine crisis in maps. **BBC NEWS,** 18, p. 1-17, fevereiro. 2015. Disponível em http://www.bbc.com/news/world-europe-27308526. Acesso em: 18 dezembro 2017.

BBC. Ukraine crisis: What's going on in Crimea? **BBC NEWS,** 12, p. 1-14, agosto. 2016. Disponível em https://www.bbc.com/news/world-europe-25182823. Acesso em: 23 novembro 2017.

BERGEN, P., MAURES, T. **Cyberwar hist Ukraine.** CNN, 7, março. 2014. Disponível em: https://edition.cnn.com/2014/03/07/opinion/bergen-ukraine-cyber-attacks/. Acesso em: 02 outubro 2018.

BOUJARD, Oussima. **Hybrid wars / unconventional warfare and transnational terrorism.** (ongoing research). dezembro. 2016.

CENTER FOR DEVELOPMENT IMPACT PRACTICE PAPER. Straws-in-the-wind, Hoops and Smoking Guns: What can Process Tracing Offer to Impact Evaluation? **Institute of Development Studies**, Bringhton, UK. n. 10, abril. 2015. p. 1-8.

CHUKA, Neil. **Hybrid warfare implications for CAF force development**. Defence Research and Development Canada. 2014.

COLLIER, David. Understanding Process Tracing. **Political Science and Politics,** Berkley, v. 44, n. 4, p. 823-830, outubro. 2011..

CROWDSTRIKE. Global Threat Intel Report. **Crowdstrike,** p. 4-76, 2014. Disponível em: https://www.crowdstrike.com/2014-global-threat-report. Acesso em: 19 julho 2019.

CROWDSTRIKE. 2015 Global Threat Intel Report. **Crowdstrike,** p. 3-89, 2015. Disponível em: https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf. Acesso em: 26 setembro 2019.

CROWDSTRIKE. Cyber Intrusion Services Casebook 2016. **Crowdstrike,** p. 2-25, 2016. Disponível em: https://www.crowdstrike.com/resources/reports/crowdstrike-cyber-intrusion-services-casebook-2016/. Acesso em: 7 outubro 2019.

ICS-CERT INDUSTRIAL CONROL SYSTEMS. Cyber-Attack Against Ukrainian Critical Infrastructure. CISA Cyber Infraestructure. **Department of Homeland Security (IR-ALERT-H-16-056-01),** p. 1-5, fevereiro. 2016. Disponível em https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. Acesso em: 28.04.2018.

E-ISAC, ELETRICITY INFORMATION SHARING AND ANALYSIS CENTER. **Analysis of the Cyber Attack on the Ukranian Power Grid**. **SANS ICS TLP:White,** março. 2016. Disponível em https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. Acesso em: 30.07.2019.

FIREEYE. APT28: A Window Into Russia's Cyber Espionage Operations?. **FireEye,** p. 3-44, 2014. Disponível em: https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html. Acesso em: 15 outubro 2019.

FIREEYE. Overload Critical Lessons From 15 Years of ICS Vulnerabilities. **2016 Industrial Control Systems (ICS) Vulnerability Trend Report,** p. 3-11, agosto. 2016. Disponível em: https://www.fireeye.com/solutions/industrial-systems-and-critical-infrastructure-security/rpt-industrial-control-systems-vulnerability-trend-report-2016.html. Acesso em: 18 outubro 2019.

FIREEYE. Zero-Day Danger: A Survey of Zero-Day Attacks and What They Say About the Traditional Security Mode. **FireEye,** p. 2-15, 2016. Disponível em: https://www.fireeye.com/current-threats/recent-zero-day-attacks/wp-zero-day-danger.html. Acesso em: 15 outubro 2019.

FLOM, Z. Shedding Light on BlackEnergy With Open Source Intelligence. **Recorded Future,** p. 1- 10, março. 2016. Disponível em: https://www.recordedfuture.com/blackenergy-malware-analysis/. Acesso em: 20 julho 2018.

F-SECURE LABS. Beware BlackEnergy If Involved in Europe/Ukraine Diplomacy. **News From The Lab Archive,** p. 1-3, janeiro. 2014a, p. 1-3. Disponível em: https://archive.f-secure.com/weblog/archives/00002721.html. Acesso em: 20 março 2018.

F-SECURE LABS. BlackEnergy Rootkit, Sort Of. News From The Lab Archive. **News From The Lab Archive,** p. 1-2, junho. 2014b. Disponível em: https://www.f secure.com/weblog/archives/00002715.html. Acesso em: 29 março 2018.

F-SECURE-LABS. **Blackenergy & Quedagh: The convergence of crimeware and APT attacks.** F-Secure Labs Security Response Malware Analysis Whitepaper, p. 1-16, 2016. Disponível em: https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf. Acesso em: 21 abril 2018.

GEERS, K. Introduction: Cyber war in Perspective. NATO CCD COE / Atlantic Council / Taras Shevchenko National University of Kyiv. In: _____ **Cyber War in Perspective: Russian Aggression Against Ukraine.** ed. Tallinn: NATO CCD COE 2015. p. 13-18.

GILES, K. Russia and Its Neighbours: Old Attitudes, New Capabilities. Conflict Studies Research Centre. In: _____ **Cyber War in Perspective: Russian Aggression Against Ukraine.** ed. Tallinn: NATO CCD COE 2015. p. 19-28.

GREENBERG, Andy. Your Guide To Russia's Infrastructure Hacking Teams. Wired Security. **Wired Security,** p. 1-11, dezembro. 2017. Disponível em: https://www.wired.com/story/russian-hacking-teams-infrastructure/. Acesso em: 10 dezembro 2018.

GREENBERG. Andy. How na Entire Nation Became Russia's Test Lab For cyberwar. **Wired Security,** p. 1-30, junho. 2017. Disponível em: https://www.wired.com/story/russian-hackers-attack-ukraine/. Acesso em: 12 junho 2018.

HALPIN, E. et al. **Cyberwar, Netwar and the Revolution in Military Affairs**. New York: Houndmills, Basignstoke, 2006.

HALL, Peter A.; TAYLOR, Rosemary C.R. The Three Versions of Neo-Institutionalism. Lua Nova: **Revista de Cultura e Política**, n. 58, p. 193-223, 2003.

HACQUEBORD, F. Pawn Storm's Domestic Spying Campaign Revealed: Ukraine and US Top Global Targets. **Trendmicro Security Intelligence,** p. 1-7, agosto. 2015. Disponível em: http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storms-domestic-spying-campaign-revealed-ukraine-and-us-top-global-targets/. Acesso em: 03 janeiro 2018.

HACQUEBORD, Feike. Two Years of Pawn Storm Examing and Incresingly Relevant Threat. **A TrendLabs Research Paper,** p. 4-42, 2017. Disponível em https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf. Acesso em: 12 setembro 2018.

HACQUEBORD, Feike. Operation Pawn Storm Ramps Up its Activities. **Trendmicro Security Intelligence,** p. 1-2, abril. 2015. Disponível em: https://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/. Acesso em: 26 junho 2016.

HEICKERÖ, R. Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. **FOI Swedish Defense Research Agency,** Stockholm, p. 3-59, março. 2010.

HOFFMAN, Frank G. Conflict in the 21 Century The Rise of Hybrid Wars. Potomac **Institute for Policy Studies,** Arlington, p.5-62, dezembro. 2007.

HUNKER, Jeffrey. Cyber war and cyber power Issues for NATO doctrine. **Research Division NATO Defense College**, Rome, n. 62, p. 1-12, novembro. 2010.

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE. ICS Alert (IR-H16-05601) Cyber-Attack Against Ukrainian Critical Infraestructure. **ICS-CERT Alerts,** p. 1- 5, fevereiro. 2016. Disponível em: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. Acesso em: 12 dezembro 2018.

INDUSTRIAL CONTROL SYSTEMS. Confirmation of a Coordinated Attack on the Ukraine Power Grid. **SANS Industrial Control Systems Security blog,** p. 1-5, janeiro. 2016. Disponível em: https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid. Acesso em: 27 julho 2018.

IVAN, Gutterman. A Timeline Of All Russia-Related Sanctions: A detailed look at all the sanctions levied against Russia, and its countersanctions, since 2014. **RadioFreeEurope RadioLiberty,** setembro. 2018. Disponível em: https://www.rferl.org/a/russia-sanctions-timeline/29477179.html. Acesso em: 08 fevereiro 2019.

JANZ, Scott., MAUER, Tim. The Russia-Ukraine Conflict and Information Warfare in a Regional Context. **Swiss Federal Institute of Technology Zurich,** p. 1-4, outubro. 2014. Disponível em: https://www.files.ethz.ch/isn/187945/ISN_184345_en.pdf. Acesso em: 3 de março de 2016.

KELLO, L. The meaning of the Cyber Revolution Perils to Theory and Statecraft. **International Security,** v. 38, n. 2, p. 7-40, 2013.

KJENNERUD Erik, CULLEN Patrick. What is Hybrid Warfare? **Norwegian Institute of International Affaris,** n. 1, p. 1-4, 2016.

KOVAL, Nikolay. Revolution Hacking. Cys Centrum LLc, In: _____ **Cyber War in Perspective: Russian Aggression Against Ukraine.** ed. Tallinn: NATO CCD COE 2015. p. 55-58.

LIMNNÉL, J. The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War. **International Journal of Cyber-Security and Digital Forensics.** v. 4, n. 5, p. 521-532. 2015.

LIPOVSKY, Robert. Back in BlackEnergy: 2014 Targeted Attacks in Ukraine and Poland. **Welivesecurity ESET,** p. 1-12, setembro. 2014. Disponível em: https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014. Acesso em: 20 dezembro 2017.

LIPOVSKY, Robert. CVE-2014-4114: Details on August BlackEnergy PowerPoint Campaigns. **Welivesecurity ESET,** p. 1-7, outubro. 2014. Disponível em https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/. Acesso em 20 julho 2016.

LOOKINGGLASS. Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare. **Lookingglass Cyber Threat Intelligence Group,** p. 3-51, abril. 2015. Disponível em: https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf. Acesso em: 29 novembro 2018.

MAHONEY, James. The logic of Process Tracing Tests in the Social Sciences. **Sociological Methods & Research,** Evanston, p. v. 41, n. 4, p. 570-597. 2012.

MANSOOR, Peter, MURRAY, Williamson. **Hybrid Warfare**: **Fighting Complex Opponents from the Ancient World to the Present.** ed. Williamson Murray and Peter R. Manssor, 2012.

MAURER, Tim. Cyber Proxies and the Crisis in Ukraine. New America. In: _____ **Cyber War in Perspective: Russian Aggression Against Ukraine.** ed. Tallinn: NATO CCD COE 2015. p. 79-86.

MAURER, Tim; JANZ, Scott. The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context. **ISN ETH Zurich,** p. 1-4, outubro 2014. Disponível em: https://www.files.ethz.ch/isn/187945/ISN_184345_en.pdf. Acesso em: 13 julho 2018.

MEARSHEIMER, John. Why the Ukraine Crisis is the West Fault: The Liberal Delusion That Provoked Putin. **Foreign Affairs,** Set. p. vol. 93, n. 5, p. 1-15, setembro/out. 2014. p

MEYERS, Adam. Danger close: FancyBear Tracking of Ukrainian Field Artillery Units. **Crowdstrike blog,** p. 1-6, dezembro. 2016. Disponível em: https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/. Acesso em: 03 janeiro 2018.

MIELNICZUK, Fabiano. A crise ucraniana e suas implicações para as Relações Internacionais. **Conjuntura Austral**. v. 5, n. 23, p. 1-16, abril/mai. 2014.

OLSZEWSKI, B. Advanced Persistent Threats as a Manifestations of State Military Activity in Cyber Space. **Institute of International Studies**, v. 189, n. 3, p. 57-71, 2018.

PAKHARENKO, Glib. Cyber Operations at Maidan: A First-Hand Account. ISACA Kyiv; In: _____ **Cyber War in Perspective: Russian Aggression Against Ukraine.** ed. Tallinn: NATO CCD COE 2015. p. 59-66.

PETERSON, Nolan. How Russia's Cyberattacks Have Affected Ukraine. **The Daily Signal Security News,** p. 1-12, dezembro. 2016. Disponível em: http://dailysignal.com/2016/12/16/how-russias-cyberattacks-have-affected-ukraine/. Acesso em: 03 novembro 2017.

PETERSON, Nolan. Putin is Waging Cyberwar On The West. **Newsweek Opinion,** p. 1-12, dezembro. 2016. Disponível em: https://www.newsweek.com/nolan-peterson-putin-waging-cyberwar-west-534164. Acesso em: 27 novembro 2017.

PIERSON, P. Increasing Returns, Path Dependence, and the Study of Politics. **American Political Science Review,** v. 94, n. 2, p. 251-267, junho. 2000.

RÚSSIA. Presidência da República. **Doutrina Militar da Federação Russa**, Moscow, 2010. Disponível em: http://kremlin.ru/supplement/461. Acesso em: 21 novembro 2018.

RÙSSIA. Jornal Russo Edição Federal. **Doutrina Militar da Federação Russa,** 2014. Disponível em: https://rg.ru/2014/12/30/doktrina-dok.html. Acesso em: 26 novembro 2018.

RÚSSIA. Presidência da República. **Estratégia de Segurança Nacional da Federação Russa até 2020,** Moscow, 2009. Disponível em: http://kremlin.ru/supplement/424. Acesso em: 05 dezembro 2018.

RÚSSIA. Jornal Russo Edição Federal. **Decreto do Presidente da Federação Russa de dezembro de 2015 n 683 "Sobre a Estratégia de Segurança Nacional da Federação Russa",** 2015. Disponível em: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html. Acesso em: 10 dezembro 2018.

THE UNITED STATES ARMY SPECIAL OPERATIONS COMMAND. "Little Green Men" a prime on Modern Russian Unconventional Warfare Ukraine 2013-2014. **Johns Hopkins University Apllied Physics laboratory,** p. 1-65, North Carolina. 2015.

VACZI, Norbert. Hybrid Wafare: How to Shape Special Operations Forces, **U.S Army Command and General Staff College,** p. 3-88, junho. 2016.

WEEDON, Jen. Beyond Cyber War: Russia´s use of Strategic Cyber Espionage and Information Operations in Ukraine. FireEye. In: _____ **Cyber War in Perspective: Russian Aggression Against Ukraine.** ed. Tallinn: NATO CCD COE 2015. p. 67-78.

WEISS, M; JANKAUSKAS, V. Securing Cyberspace How States Design Governance Arrangements. **International Journal of Policy, Administration, and Institutions,** v. 32, n. 2, p. 259-275, 2019.

WIRTZ, James J. Beyond The Russian Integration of Cyber Power into Grand Strategy. Naval Postgraduate School. In: _____ **Cyber War in Perspective: Russian Aggression Against Ukraine.** ed. Tallinn: NATO CCD COE 2015., p. 29-38.

WIKIPEDIA. Document Management System. **Wikipedia The Free Encyclopedia**, n/a. Disponível em: https://en.wikipedia.org/wiki/Document_management_system. Acesso em 28 março 2018.

WIKIPEDIA. Russofilia Origem. **Wikipedia The Free Encyclopedia,** n/a. Disponível em https://pt.wikipedia.org/wiki/Russofilia. Acesso em: 10 agosto 2019.