Guerra Híbrida: o emprego da tecnologia da informação no conflito Rússia-Ucrânia (2014-2015).

Hybrid War: the use of information technology in Russia-Ukraine conflict (2014-2015).

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 9-36
DOI: 10.26792/RBED.v7n2.2020.75208
ISSN 2358-3932

MARCOS AURÉLIO GUEDES DE OLIVEIRA
FERNANDO HENRIQUE CASALUNGA

INTRODUÇÃO

Nossa análise da guerra híbrida desencadeada entre Rússia e Ucrânia (2014-2015) objetiva responder ao seguinte questionamento: como a tecnologia da informação amplia a assimetria de poder entre os Estados contemporâneos?

Sem embargo, partimos do pressuposto de que, com o avanço das tecnologias de informação, o ciberespaço se tornou fulcral para projeção de poder do Estado russo. O argumento está ancorado na descrição temporal das operações que ratificam a relevância deste novo engenho de força para consecução de objetivos estratégicos da Federação Russa em seu entorno regional.

Destarte, sustentamos que, ao utilizar o ciberespaço para auxiliar as operações militares, a simbiose inovadora entre setores especiais das Forças Armadas russas e *hackers* civis produziu efeito sinérgico que resultou em vantagem considerável à Rússia durante o conflito com a anexação do território da península da Crimeia e apoio aos movimentos separatistas que ocuparam a região leste da Ucrânia.

A fim de sustentar a validade da inferência descritiva construída, o ponto chave do artigo é marcado pela identificação do funcionamento desta

Marcos Aurélio Guedes de Oliveira — Doutor em Government pela University of Essex, Professor Titular do Departamento de Ciência Política na Universidade Federal de Pernambuco. Coordenador Geral do projeto CAPES/MD Pro-Defesa IV "Ciência, Tecnologia e Inovação em Defesa: Cibernética e Defesa Nacional".
Fernando Henrique Casalunga — Doutorando do Programa de Pós-Graduação em Ciência Política pela Universidade Federal do Rio Grande do Sul/UFRGS. Bacharel e Mestre em Ciência Política pela Universidade Federal de Pernambuco (UFPE); Bacharel e Licenciatura em História pela Universidade Estadual Paulista (UNESP). Bolsista Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

simbiose, compreendida em sua condição de mecanismo capaz de conectar a estratégia russa ao nível operacional e tático de ação militar — razão pela qual aplicamos o método qualitativo da dependência da trajetória em conjunto com a técnica de rastreamento de processos para analisar relatórios de empresas especializadas em segurança cibernética e instituições governamentais à procura de evidências que permitam desvelar o funcionamento deste mecanismo.

De modo que este artigo se divide em duas seções: a primeira discute a relevância da segurança frente aos riscos e ameaças do espaço cibernético para delimitar o conceito de guerra híbrida utilizado neste estudo; a segunda identifica o mecanismo responsável por conectar os níveis estratégico, tático e operacional militar ao verificar as ações conjuntas de atores estatais e *hackers* não-estatais envolvidos no conflito.

Ao elucidar como a tecnologia de informação amplia, sobremaneira, as capacidades de projeção de poder regional de uma grande potência como a Rússia, o artigo contribui para o avanço dos estudos sobre a relevância deste novo engenho de força para os Estados contemporâneos.

GUERRA HÍBRIDA: CIBERESPAÇO, SEGURANÇA CIBERNÉTICA E AMEAÇAS PERSISTENTES AVANÇADAS

Em vista da crescente relevância estratégica concedida ao ambiente cibernético, comunidades acadêmicas, civis e militares têm se debruçado sobre o problema fundamental da Defesa e Segurança no ciberespaço, a fim de compreender os movimentos de atores estatais e não-estatais no que concerne às estratégias, táticas e operações utilizadas para atuarem no ciberespaço. À medida que a pesquisa científica avança, novos enigmas teóricos emergem, refletindo a complexidade analítica e a dinamicidade do desafio cibernético (Gartzke 2013; Kello 2013; Lindsay 2013; 2015; Geers 2015; Kjennerud and Cullen 2016; Vaczi 2016; Olszewski 2018; Weiss and Jankauskas 2019).

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

Com o advento do século XXI, 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 tro-

ca de informações entre órgãos públicos e até a estabilidade de infraestruturas críticas, acarretando riscos à desestabilização de sociedades inteiras (Geers 2015).

Frente a este cenário, o conceito de segurança cibernética consiste, *grosso modo*, em adotar medidas para proteger as operações de um sistema de computador ou a integridade de seus dados frente a uma ação hostil (Weiss and Jankauskas 2019). Com pretensão de classificar os dilemas associados à segurança no espaço de informação, mais especificamente os riscos e as ameaças que circulam nesse ambiente, Weiss e Jankauskas (2019) constroem uma tipologia que se propõe a identificar a realidade fenomenológica da natureza desses problemas.

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. 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 and Keohane 1999, *apud* Weiss and Jankauskas 2019, 5).

Nomeadas como Ameaças Persistentes Avançadas (APA) estes grupos possuem alto grau de especialização, armas cibernéticas de difícil detecção, capacidade de adaptação e recursos para atuarem por longos períodos de tempo (Weedon 2015). Contudo, embora "originalmente usada para descrever invasões cibernéticas contra organizações militares, as APA evoluíram e não estão mais confinadas às forças armadas" (Olszewski 2018, 5). Pertencem, pois, 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, 70).

Trata-se, portanto, de atores 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 and Jankauskas 2019, 5). Todavia, além de representarem ameaças à segurança cibernética de estruturas físicas, as APA ganharam importância estratégica para os Estados contemporâneos como ferramentas úteis em operações ofensivas "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, 5).

No que concerne à análise dos riscos e ameaças à segurança cibernética, a literatura apresenta evidências que sustentam o pressuposto de que as capacidades convencionais de emprego da força pelos Estados fortes impõem restrições às ações ofensivas de entes mais fracos. Por essa lógica, 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). Desse modo, ameaças 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).

Frente a esse cenário, soldados dividem espaço com 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*[1] (Geers 2015). Em meio aos avanços tecnológicos que resultaram na produção destes novos engenhos de força, diversos conceitos foram propostos para explicar a realidade dos conflitos contemporâneos.

Inicialmente, termos como guerra convencional, irrestrita, composta e de quarta geração, fundiram-se em um grande guarda-chuva teórico conceitual denominado guerra híbrida, que se constitui com base nos postulados de diversas escolas de pensamento (Hoffman 2007, 30). O conceito formulado por Hoffman (2007) tornou-se chave para orientar o entendimento da literatura e de organismos internacionais dedicados ao estudo da interconexão entre as ações de agentes estatais e/ou não-estatais em conflitos contemporâneos, desde o nível estratégico até o operacional.

Neste ensejo, após a eclosão do conflito entre russos e ucranianos em 2014, documentos oficiais publicados pela Assembleia Parlamentar da Organização do Tratado do Atlântico Norte (OTAN) (2015) apresentavam um entendimento oficial do conceito semelhante ao proposto por Hoffman (2007), compreendido como "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, 23–24).

No entanto, embora capazes de descrever parte da composição da guerra contemporânea ao abordar a crescente sofisticação e complexificação da atuação dos atores não-estatais, tais entendimentos eram muito estreitos e desconsideravam o papel estratégico do Estado como ator fundamental das guerras híbridas (Kjennerud and Cullen 2016).

> A guerra híbrida do Estado envolve a plena integração dos meios militares e não-militares com o poder do Estado para alcançar obje-

> tivos políticos, nos quais o uso da força desempenha 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 and Cullen 2016, 1).

Kjennerud e Cullen (2016) ampliaram essa concepção e dividiram os instrumentos de poder nas categorias militar, política, econômica, civil e informacional, para identificar a relevância de sua utilização sincronizada e coordenada pelos Estados, com fins de atingir sistemas de informação e/ou infraestrutura crítica do oponente e produzir "mudanças no estado comportamental ou físico de um sistema ou elementos do sistema, de acordo com objetivos políticos" (Kjennerud and Cullen 2016, 1).

Por conseguinte, o International Institute for Strategic Studies (IISS) (2016), passou a descrever as guerras híbridas de modo mais preciso, na qualidade de "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" (IISS, *apud* Vaczi 2016, 38). Por essa perspectiva, a guerra híbrida é entendida como o uso de todos os instrumentos de poder disponíveis ao Estado para atingir as vulnerabilidades do oponente.

Frente ao exposto, adotamos o modelo analítico proposto por Kjennerud e Cullen (2016) em consonância com o Balanço Militar (2015) do IISS (2016) para operacionalizar o conceito de guerra híbrida tomando o uso do ciberespaço como ferramenta chave para consecução das diretrizes estratégicas, operacionais e táticas da Rússia no conflito com a Ucrânia (2014-2015).

Destarte, nossa análise do emprego da tecnologia da informação neste conflito destaca os movimentos conjuntos de atores estatais e/ou não-estatais no ambiente cibernético e cinético para compreensão da guerra híbrida conforme empregada pela Rússia, marcada pela coordenação de atividades adaptáveis e flexíveis para produzir força sinérgica capaz de auxiliar na consecução de seus objetivos estratégicos regionais.

A seção seguinte apresenta inferência descritiva sobre a ação conjunta de grupos *hackers* e forças especiais russas em ataques cibernéticos e ações físicas, e revela algumas das principais ameaças e armas cibernéticas utilizadas no conflito. Assim, fomentamos o debate sobre como novos engenhos de força podem ser utilizados para ampliar a assimetria de poder entre Estados contemporâneos.

A SIMBIOSE *HACKER*-EXÉRCITO: O EMPREGO DA TECNOLOGIA DA INFORMAÇÃO NO CONFLITO RÚSSIA-UCRÂNIA (2014-2015)

Nesta seção apresentamos evidências que comprovam a congruência dos ataques cibernéticos com as ações físicas durante o conflito Rússia-Ucrânia (2014-2015). A metodologia adotada contribui para que possamos oferecer uma explicação robusta sobre as conjunturas históricas e as consequências da guerra híbrida para o aumento da assimetria de poder regional entre estes Estados.

Ao aplicarmos a técnica da dependência da trajetória,[2] procuramos pontuar momentos críticos do conflito que sinalizem o modo inovador como o Estado russo utilizou o ciberespaço para consecução de objetivos estratégicos durante o conflito. Nesse ensejo, utilizamos o rastreamento de processos[3] para conferir se a incorporação da dimensão cibernética ao modo de operação das Forças Armadas russas (simbiose) foi suficiente para produzir força sinérgica neste conflito.

Deste modo, o componente descritivo da série de momentos específicos que marcaram as principais etapas do processo causal observável (PCO) torna-se o ponto fulcral da análise (Mahoney 2012, 586). Por essa lógica, a condição em que ocorrem os movimentos dos atores é identificada mediante a coleta de evidências que permitam verificar o funcionamento do mecanismo. Por essa razão destacamos como o ciberespaço foi utilizado para ampliar a capacidade de projeção de poder da Federação Russa em seu entorno regional.

Os relatórios de agências especializadas em segurança cibernética e de instituições governamentais analisados contêm uma série de evidências que indicam a ligação entre as atividades de atores não-estatais (APA) em conjunto com as forças especiais russas (Spetsnaz),[4] simbiose que compõe o mecanismo causal ora identificado enquanto condição suficiente para promoção de nosso fenômeno de interesse, a guerra híbrida.

Sem embargo, as atividades russas estiveram vinculadas a uma série de ataques de infiltração via ciberespaço, que fizeram uso de *spear phishing*[5] para instalar armas cibernéticas capazes de subtrair informações sigilosas e/ou causar danos cinéticos, paralisando sistemas de computador, setores de comunicação, bancários, eleitorais e de infraestruturas críticas (Crowdstrike 2014; 2015; 2016; FireEye 2014; 2016; F-Secure Labs 2016; LookingGlass 2015; ICS-CERT 2016; E-ISAC 2016).[6]

A partir da correlação observada entre os ataques cibernéticos e o conflito cinético, o relatório do Grupo de Inteligência sobre Ameaças Cibernéticas (CTIG) apresenta evidências que revelam como 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, 3).

Conforme aponta o relatório, a ligação entre a campanha de espionagem cibernética e atores estatais das agências do Serviço Federal de Segurança (FSB) e de Comunicações e Informações Governamentais (FAGCI) da Federação Russa é ponto chave para compreensão da vantagem militar russa sobre as forças ucranianas, "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, 6).

Cientes da dificuldade de atribuição das ações cibernéticas ofensivas, o Serviço de Segurança da Ucrânia (SBU) e a LookingGlass chamaram a atenção para o modo como as agências estatais russas envolvidas no conflito fizeram uso estratégico, tático e operacional do ciberespaço, destacando os movimentos da 16ª divisão da FAGCI e do 18º Centro do FSB. Não obstante, o SBU frisou que a subtração de informações do governo, polícia 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).

Os ciberataques utilizaram *spear phishing* com informações úteis para os alvos ucranianos, os *e-mails* continham arquivos de extração automática (SFX) que colhiam documentos com informações legítimas relativas ao conflito russo-ucraniano para depois serem usados como iscas na próxima onda de ataques. A análise da infraestrutura de rede e das ameaças utilizadas pelos *hackers* identificou nomes de arquivos similares e períodos de maior volume de ataques cibernéticos coincidentes com o horário de trabalho em Kiev, fatores que facilitaram o rastreamento das atividades dessas ameaças (LookingGlass 2015, 18).

O quadro 1 sumariza as informações do relatório, que apresenta em detalhes a ligação entre os ataques cibernéticos e os principais eventos políticos e militares que ocorreram durante o conflito entre russos e ucranianos.

Quadro 1
Cronograma da campanha de espionagem cibernética
operação "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. Arquivo 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, início da retomada da operação de espionagem

2014	Ação física	2014	Ação cibernética
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 dois arquivos datados de 21 de agosto endereçados via email para 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
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** Chefe do centro antiterrorista da SBU divulga informações sobre os ataques das forças especiais russas	15 fevereiro 16 fevereiro	Os ataques cibernéticos não param até a retirada das tropas ucranianas do Debaltaseve, só então os ataques cibernéticos cessaram. As ameaças foram movidas para servidores de uma transportadora internacional de logística de carne e uma loja de eletrônicos
			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 à 16ª antiga agência do governo federal de comunicação e informação (FAGCI) e 18º 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 identificados

Fonte: Elaborado pelos autores com base em LookingGlass (2015)

Durante o conflito, distintas APA pró-rússia utilizaram táticas de intrusão sofisticadas para comprometer sistemas de informação do governo, mídia e infraestrutura crítica da Ucrânia, com ataques cibernéticos de negação

de serviço e espionagem. Destacamos as APA28: CyberBerkut; FancyBear/Sofacy/Pawn Storm e Sandworm (Crowdstrike 2014; 2015; 2016).

> 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 (Janz and Maurer 2014).

Uma das armas cibernéticas mais utilizadas na Ucrânia foi o BlackEnergy (BE), a evolução deste *malware* têm sido acompanhada por diversas empresas especializadas em segurança cibernética que apontam a convergência entre as atividades criminosas e a espionagem russa através do ciberespaço (FireEye 2014; F-Secure Labs 2016). No início do conflito variações como o BE.lite[7] e BlackEnergy2 (BB2)[8] atingiram alvos políticos na Ucrânia, ocasionando a queda de diversos sítios eletrônicos do governo, incluindo o do gabinete presidencial (Bergen and Maurer 2018); em sua versão recente, o *malware* comprometeu setores de infraestrutura crítica (ICS 2016; E-ISAC 2016).

Em fevereiro de 2014, uma onda de ataques cibernéticos utilizou essas variações para interferir nos serviços de telefonia celular dos membros do parlamento ucraniano, dificultando a comunicação e o processo decisório de resposta à invasão russa ao território da Crimeia. Apenas quatro dias após as operações via ciberespaço, instalações da empresa de comunicações Ukrtelecom foram invadidas e os cabos de fibra ótica adulterados, inviabilizando a conexão entre a península e o restante da Ucrânia (Maurer 2015, 81). A operação de sabotagem evitou que o poder público tomasse uma atitude com relação ao movimento das forças russas na Crimeia (Weedon 2015, 76).

No mês de março de 2014, o CyberBerkut assumiu a responsabilidade por atacar a página da rede do governo da Ucrânia, que ficou fechada por três dias, além dos *sites* oficiais, telefones celulares dos parlamentares ucranianos também foram invadidos (Weedon 2015, 76). Na ocasião, o grupo composto por antigos membros das forças policiais ucranianas vinculou notícias na Internet contendo informações que denunciavam a "ilegitimidade do governo que assumiu a Ucrânia após a expulsão do ex-presidente Viktor Yanukovych" (Crowdstrike 2014, 26–27).

Ao utilizar as variações do BlackEnergy (BE.lite e BB2), a ameaça foi capaz de subtrair informações sigilosas como códigos de execução e

senhas de acesso remoto de seus alvos, demonstrando alta capacidade para afetar políticos do alto escalão do governo ucraniano por intermédio de operações conduzidas no ciberespaço. O vazamento periódico de documentos sigilosos em sua página na Internet prosseguiu durante os primeiros meses do conflito "foram mais de 50 itens exclusivos, emails, relatórios, acordos, propostas, imagens aéreas e identificação pessoal" (Crowdstrike 2015, 29).

Os ataques cibernéticos ocorreram em perfeita sincronia com as ações das forças especiais russas, os "homens de verde" (*Spetsnaz*), grupos armados e agentes de inteligência sem identificação, responsáveis pelas operações militares que tomaram controle da península e apoiaram os movimentos separatistas do leste (Giles 2015, 20).

> 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, 31).

As tropas especiais empregaram equipamentos das Forças Armadas da Federação Russa que incluíam veículos blindados de transporte de pessoal e helicópteros. Embora, o Kremlin tenha inicialmente negado envolvimento nas operações, pouco tempo depois, a sede da frota russa do Mar Negro em Sevastopol admitiu que a península havia sido ocupada para garantir o controle do porto (USAOC 2015, 56).

Em abril de 2014, quando o conflito eclodiu em Donbass, as operações cibernéticas aumentaram exponencialmente, acompanhando os eventos militares de coleta de informações vitais para os setores de inteligência, ações que ofereceram vantagem significativa às tropas russas no campo de batalha físico (LookingGlass 2015). Naquele mês, os alvos da CyberBerkut foram empresas militares privadas que operavam no conflito, novamente chama a atenção o grau de alinhamento das operações com as prioridades estratégicas do Estado russo que passou a oferecer apoio técnico e tático aos separatistas do leste (Crowdstrike 2014, 27).

Os ataques cibernéticos seguiam uma dinâmica paralela às ações diplomáticas e estratégicas tomadas pelos Estados da Rússia e Ucrânia. Foi assim que, em 21 maio de 2014, logo após a declaração de independência dos territórios de Donbass do governo central de Kiev, a CyberBerkut de-

clarava a autoria dos ataques que atingiram a rede da Comissão Central de Eleições (CEC) (Koval 2015).

Na ocasião, a ameaça 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, 56).

A coordenação da propaganda distribuída e das informações da mídia revelou como os serviços de inteligência da Federação Russa procuravam atingir seus objetivos estratégicos utilizando meios cibernéticos (Crowdstrike 2014, 26). O relatório Crowdstrike (2014) frisa a coordenação das 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, como indício dessa ação conjunta. No dia seguinte, quando o sistema da CEC teve seu funcionamento reestabelecido pelo serviço de segurança ucraniano, a comissão precisou confirmar a invasão do sistema pelos *hackers* para só então declarar a vitória do social-democrata Petro Poroshenko que assumiu a presidência do país (Koval 2015, 56).

Embora o relatório não afirme que a ação foi patrocinada diretamente pela Rússia ou se a CyberBerkut atuou de modo independente, Koval (2015, 55) destaca que "a quantidade e a gravidade dos ataques cibernéticos contra a Ucrânia aumentaram paralelamente aos eventos políticos em andamento". Tais ações atingiram alvos do alto escalão do governo ucraniano (ministro de Relações Exteriores, o ministro da Defesa, a administração executiva e as embaixadas no exterior), demonstrando o alto potencial de interferência no conflito causado por ações dessa ameaça via ciberespaço (Crowdstrike 2015, 29).

Igualmente identificada nas operações cibernéticas que atingiram a Ucrânia durante o conflito, a APA FancyBear/Sofacy/PawnStorm é apontada como responsável por atingir diversas organizações políticas com armas cibernéticas multifuncionais, enviadas via *e-mail spear phishing*. Classificada como representante dos interesses da Federação Russa, vinculada ao Departamento de Inteligência Militar (GRU) (Crowdstrike 2016, 8), a campanha de espionagem cibernética orquestrada por essa ameaça usurpou 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).

Em agosto de 2014, *e-mails spear phishing* foram identificados contendo uma lista com os nomes de membros do parlamento ucraniano que esta-

riam oferecendo apoio aos separatistas do leste. Enviados 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, a isca continha diretrizes oficiais para que essas instituições verificassem a veracidade das informações contidas nos documentos. No entanto, o arquivo em anexo estava infectado com uma versão do BE.lite que, ao ser aberto, oferecia acesso às contas dos servidores dessas instituições aos *hackers* (Lipovsky 2014, 2–3).

As amostras dos *malwares* presentes nos *e-mails* coletados 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, 3).

> Mais de 96% das amostras de malware que atribuímos ao APA28 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, 5).

O relatório indica que as amostras analisadas "utilizam a mesma sequência de descriptografia e algoritmos semelhantes para codificação e decodificação" (FireEye 2014, 21). Para verificar as semelhanças encontradas, os analistas identificaram um padrão nos códigos destes *e-mails*, "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, 29).

Não obstante, as ações cibernéticas do grupo Pawn Storm parecem se conectar com às da CyberBerkut ao facilitarem o intercâmbio de informações roubadas e o vazamento de documentos confidenciais. Embora a relação entre ambas as ameaças tenha sido pouco explorada, analistas revelam que a "CyberBerkut publicou informações roubadas durante as campanhas do Pawn Storm" (Hacquebord 2017, 8).

O X-Agent[9] é outra arma cibernética associada ao grupo. O relatório Crowdstrike (2014) apresenta indicadores técnicos, como localidades dos recursos e informações de registro em domínio de comando e controle (C2) que apontam para a relação da APA com a Federação Russa em operações conduzidas via ciberespaço contra entidades militares e instituições políticas contra a Ucrânia. Devido à sua característica modular, a forma de

infecção dos sistemas alvo pode mudar desde protocolos de transferência de hipertextos (HTTP), até *e-mails* e/ou mídias removíveis. Ataques mais recentes envolveram ofuscação de fluxo de código para impedir o rastreamento dos invasores (Crowdstrike 2014, 58-59).

Uma variante do X-Agent — desenvolvida em formato de aplicativo pelo oficial ucraniano Yaroslav Shertuk com a promessa de oferecer maior eficiência aos sistemas de artilharia do Exército, reduzindo o tempo de disparo de minutos para segundos — foi apresentada em fóruns militares ocorridos na Ucrânia, e chegou a ser utilizada por quase nove mil usuários (Meyers 2016). No entanto, ao ser instalada, a ferramenta implantava de modo sigiloso o *malware* nos sistemas operacionais dos celulares destes usuários que, em grande parte, integravam a artilharia ucraniana (Meyers 2016).

Uma vez infectados, os aparelhos forneciam aos *hackers* a localização exata, e em tempo real, das tropas inimigas. Este dados eram repassados aos setores de inteligência russos permitindo que as Forças Armadas do país antecipassem os movimentos do adversário no campo de batalha. A análise do *malware* apresentou uma série de artefatos em língua russa de natureza militar que indicam uma correlação entre o FancyBear e o setor de inteligência militar russa que operava em apoio aos separatistas no leste da Ucrânia (Meyers 2016).

A última APA identificada no conflito é o Sandworm, grupo apontado como responsável por atacar setores de infraestrutura crítica da Ucrânia em meados de 2015 (Lipovsky 2014). Os principais *malwares* utilizados nos ataques foram o BlackEnergy 3 (BB3)[10] e o KillDisk (KD).[11]

Instituições governamentais norte-americanas do Departamento de Segurança Interna (DHS), por intermédio da Equipe de Resposta a Emergências Cibernéticas de Sistema de Controle Industrial (ICS-CERT), atuando em parceria com o setor privado através do instituto SysAdmin, Auditoria, Rede, Segurança (SANS) e do Centro de Análise e Compartilhamento de Informações de Eletricidade (E-ISAC), produziram relatórios confirmando que a interrupção no fornecimento de energia foi causada por uma série de ataques cibernéticos, que indicaram a presença de *hackers* especializados em táticas de espionagem cibernética (E-ISAC, 2016; ICS-CERT, 2016).

O incidente na região de Ivano-Frankvisk, reportado em 24 de dezembro pela Kyivoblenergo (companhia regional de distribuição de energia elétrica), revelou que terceiros obtiveram acesso ilegal ao sistema de tecnologia de informação da rede elétrica, desconectando sete subestações 110kV e 23 35kV, por três horas (ICS 2016, 1). Os resultados do relatório confirmaram o envolvimento de uma rede de planejamento e coordenação

de difícil detecção, capaz de ocultar os rastros contidos nos dispositivos atingidos (ICS-CERT 2016, 1-2).

Não obstante, o relatório (E-ISAC 2016) revelou em detalhes o alto grau de complexidade técnica empregado nos ataques. Tratou-se de uma operação de longo prazo, estimada em aproximadamente seis meses, entre o reconhecimento do sistema e o ataque propriamente dito, que só poderia ser levada a cabo por 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, 4).

> 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 capacidade de realizar operações de reconhecimento para aprender sobre o ambiente e executar um ataque múltiplo altamente sincronizado (E-ISAC 2016, 1–2).

O relatório ressalta que as etapas de planejamento e execução dos ataques seguiram o modelo apresentado por Assante e Lee (2015). De acordo com o documento que descreve a operação, 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, 8).

Durante a fase de planejamento, os computadores da companhia regional de distribuição de energia elétrica foram infectados com o uso de *spear phising* enviados a usuários com acesso à rede administrativa das empresas. Os *e-mails* continham 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. Após a infiltração, os invasores atuaram no ambiente infectado como usuários autorizados; o acesso irrestrito e indetectável permitiu que descobrissem as vulnerabilidades do sistema e extraíssem os dados necessários para um ataque efetivo (E-ISAC 2016, 6-8).

Uma vez conectados ao sistema de Comando e Controle (C2), 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 APA conseguiu atingir os alvos físicos sem que fossem detectados pelo sistema de segurança (E-ISAC 2016, 9–10).

A fase seguinte resultou no desenvolvimento e execução do ataque cibernético que danificou os sistemas operacionais das estações e subestações elétricas de modo simultâneo, impactando mais de 225 mil clientes. Após o feito, para evitar o rastreamento, os *hackers* utilizaram o KD para destruir os arquivos corrompidos do sistema e apagar o rastro dos invasores (E-ISAC 2016, 5). Em arremate, 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 para garantir que os usuários atingidos não conseguissem relatar as interrupções (E-ISAC 2016, 12).

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 das subestações elétricas dos sistemas SCADA, como também evitar que as estações fossem recuperadas com uso de comandos remotos (E-ISAC 2016, 10-12). O relatório confirma que os *softwares* maliciosos BB3 e KD não foram os causadores da interrupção do funcionamento dos sistemas SCADA de energia elétrica, mas serviram como ferramentas sofisticadas para obtenção de informações de acesso privilegiado da administração dos sistemas operacionais dessas infraestruturas (E-ISAC 2016, 13).

Em suma, a execução do ataque utilizou o controle do próprio sistema para afetar o funcionamento de uma infraestrutura crítica. Todavia, desde o ano anterior à operação, 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 2017, 11).

Ao utilizar ataques para atingir alvos dessa natureza, a ameaça inaugurou uma nova fase no conflito, que explicitou a alta capacidade dos atores envolvidos para causar danos cinéticos via ciberespaço, aumentando os ricos à segurança das infraestruturas críticas. De acordo com o relatório do FireEye (2016),

> 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 2016, 10).

Mediante a verificação do alto grau de sofisticação dos ataques cibernéticos e a capacidade de atualização das ameaças, é difícil refutar a suspeita

de que a ação dos *hackers* tenha sido impulsionada por um ente capaz de financiar esse tipo de campanha de longo prazo. 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, 70–1).

Não obstante, o relatório da Crowdstrike (2015) anuncia que o alto potencial dessa APA para empregar combinações de *softwares* maliciosos visando obter acesso ao sistema operacional de setores da infraestrutura crítica, sinaliza o envolvimento russo nessa operação (Crowdstrike 2015, 26). A ação representou uma resposta 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 a península anexada da Crimea deixaram mais de dois milhões de pessoas que residem na região sem energia elétrica (Crowdstrike 2015, 27–8).

Apesar de a Rússia negar agir em consonância com os grupos *hackers*, as evidências descritas pela análise dos relatórios apresentados nesta seção são fortes indícios do funcionamento do mecanismo de simbiose entre *hackers* e as Forças Armadas da Federação Russa. Destacamos as seguintes evidências: a coincidência cronológica entre os ataques cibernéticos e as invasões por terra; os horários de funcionamento das APA; a engenharia da informação por detrás dos códigos das armas identificadas; e, o alto grau de sofisticação e complexidade das operações realizadas.

CONCLUSÃO

Frente ao exposto, apresentamos uma breve discussão dos resultados de nossa análise sobre o funcionamento do mecanismo e o emprego da tecnologia da informação no conflito com intuito de oferecer uma resposta ao questionamento central deste artigo.

Ao aplicarmos as técnicas de análise qualitativa, identificamos como as operações cibernéticas realizadas pelas APA28 ofereceram vantagens estratégicas para as operações militares no mundo físico.

As principais agências estatais russas envolvidas com as operações cibernéticas identificadas foram: o Serviço Federal de Segurança (FSB); o Serviço de Comunicações e Informações Governamentais (FAGCI); e o Departamento de Inteligência (GRU), órgão ao qual estão subordinadas as forças especiais russas (*Spetsnaz*). Já as ameaças identificadas nos ataques cibernéticos foram: CyberBerkut, FancyBear/PawnStorm/Sofacy e Sandoworm; as armas cibernéticas: BlackEnergy; X-Agent e o KillDisk.

Os relatórios publicados por empresas especializadas em cibersegurança e instituições governamentais apresentam evidências de como se deu o uso destas armas e o modo de operação das ameaças cibernéticas. A análise destes relatórios verificou um aumento das capacidades qualitativas de ação da Federação Russa, manifestada por meio da sinergia produzida pela simbiose entre os atores estatais e não-estatais, compreendida como condição suficiente para comprometer o funcionamento de setores vitais da Ucrânia, como organizações políticas, militares e infraestruturas críticas.

Neste ensejo, a guerra híbrida conforme empregada pela Rússia contra a Ucrânia, em geral, envolveu ataques cibernéticos que ofereceram suporte à ação das forças especiais russas 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. De tal modo que as operações cibernéticas desvelam como o domínio da tecnologia da informação contribuiu para ampliar a assimetria de poder entre estes Estados, conectando os níveis estratégico, tático e operacional, de modo a facilitar a anexação do território da península da Crimeia e apoiar os movimentos separatistas que ocuparam a região leste da Ucrânia.

Note-se, portanto, que a condição em que ocorre a guerra híbrida entre russos e ucranianos reflete o potencial das ameaças cibernéticas na qualidade de novos engenhos de força para exploração de complexos sistemas de informação, capazes de causar danos cinéticos significativos aos adversários. Por essa lógica, a inferência descritiva do processo sustenta o pressuposto da centralidade que assume o ciberespaço na projeção regional do poder nacional russo. Ressaltamos, pois, a importância da segurança cibernética como fator chave para os Estados contemporâneos.

REFERÊNCIAS

Assant, Michael and Lee Robert. 2018. "The Industrial Control System Cyber Kill Chain." *SANS Institute Information Security Reading Room*: 1–21.

https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

Bergen, Peter and Tim Maurer. 2018. "Cyberwar hist Ukraine." *CNN*: 1–3. https://edition.cnn.com/2014/03/07/opinion/bergen-ukraine-cyber-attacks/.

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

Collier, David. 2011. "Understanding Process Tracing." *Political Science and Politics* 44, no. 4 (Outubro): 823–30.

Crowdstrike. 2014. "Global Threat Intel Report." *Crowdstrike*: 4–76.

https://www.crowdstrike.com/2014-global-threat-report.

Crowdstrike. 2015. "Global Threat Intel Report." *Crowdstrike*: 3–89. https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf.

Crowdstrike. 2016. "Cyber Intrusion Services Casebook." *Crowdstrike*: 2–25.

https://www.crowdstrike.com/resources/reports/crowdstrike-cyber-intrusion-services-casebook-2016/.

E-ISAC. Electricity Information Sharing and Analysis Center. 2016. "Analysis of the Cyber Attack on the Ukranian Power Grid." *SANS ICS TLP:White*: 1–29.

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

FireEye. 2014. "APA28: A Window Into Russia's Cyber Espionage Operations?" *FireEye*: 3–44. https://www.fireeye.com/current-threats/APA-groups/rpt-APA28.html.

_____. 2016. "Overload Critical Lessons From 15 Years of ICS Vulnerabilities." *Industrial Control Systems (ICS) Vulnerability Trend Report*: 3–11. https://www.fireeye.com/solutions/industrial-systems-and-critical-infrastructure-security/rpt-industrial-control-systems-vulnerability-trend-report-2016.html.

F-Secure Labs. 2014. "BlackEnergy Rootkit, Sort Of. News From The Lab Archive." *News From The Lab Archive*, 1-2. https://www.f-secure.com/weblog/archives/00002715.html.

F-Secure Labs. 2016. "Blackenergy & Quedagh: The convergence of crimeware and APA attacks." *F-Secure Labs Security Response Malware Analysis Whitepaper*: 1–16. https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2: 41–73.

Geers, Kenneth. 2015. "Introduction: Cyber war in Perspective." *NATO CCD COE / Atlantic Council / Taras Shevchenko National University of Kyiv*: 13–8. In: _____. "Cyber War in Perspective: Russian Aggression Against Ukraine". Tallinn: NATO CCD COE.

Greenberg, Andy. 2017. "Your Guide to Russia's Infrastructure Hacking Teams. Wired Security." *Wired Security*: 1–11. https://www.wired.com/story/russian--hacking-teams-infrastructure/.

Hacquebord, Feike. 2015. "Pawn Storm's Domestic Spying Campaign Revealed: Ukraine and US Top Global Targets." *Trendmicro Security Intelligence*: 1–7. http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storms-domestic-spying-campaign-revealed-ukraine-and-us-top-global-targets/.

_____. 2017. "Two Years of Pawn Storm Examing and Incresingly Relevant Threat." *A TrendLabs Research Paper*: 4–42. https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf.

Hoffman, Frank. 2007. *Conflict in the 21 Century The Rise of Hybrid Wars*. Arlington, Virginia: Potomac Institute for Policy Studies.

ICS-CERT, Industrial Control Systems. 2016. "Cyber-Attack Against Ukrainian Critical Infrastructure". *Department of Homeland Security (IR-ALERT-H-16-056-01)*: 1–5. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Janz, Scott and Maurer, Tim. 2014. "The Russia-Ukraine Conflict and Information Warfare in a Regional Context." *Swiss Federal Institute of Technology Zurich*: 1–4. https://www.files.ethz.ch/isn/187945/ISN_184345_en.pdf.

Kello, Lucas. 2013. "The meaning of the Cyber Revolution Perils to Theory and Statecraft." *International Security* 38, no. 2: 7–40.

Kjennerud, Erik and Cullen, Patrick. 2016. "What is Hybrid Warfare?" *Norwegian Institute of International* Affaris 1 (Jan): 1–4.

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

Lindsay, Jon. 2013. Stuxnet and the Limits of Cyber Warfare. *Security Studies* 22, no. 3: 365-404.

Lindsay, Jon. 2015. The impact of China on Cybersecurity. *Journal of Strategic Security* 39, no. 3: 7-47.

Lipovsky, Robert. 2014. "Back in BlackEnergy: 2014 Targeted Attacks in Ukraine and Poland." *Welivesecurity ESET*: 1–12. https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014.

LookingGlass. 2015. "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare." *Lookingglass Cyber Threat Intelligence Group*: 3–51. https://www.lookingglasscyber.com/wpcontent/uploads/2015/08/Operation_Armageddon_Final.pdf.

Mahoney, James. 2012. "The logic of Process Tracing Tests in the Social Sciences." *Sociological Methods & Research* 41, no. 4: 570–97.

Maurer, Tim. "Cyber Proxies and the Crisis in Ukraine." *New America*, 79–86. In: _____. "Cyber War in Perspective: Russian Aggression Against Ukraine". Tallinn: NATO CCD COE.

Meyers, Adam. 2016. "Danger close: FancyBear Tracking of Ukrainian Field Artillery Units." *Crowdstrike blog*: 1–6. https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

Olszewski, Boguslaw. 2018. "Advanced Persistent Threats as a Manifestations of State Military Activity in Cyber Space." *Institute of International Studies* 189, no. 3: 57–71.

Pierson, Paul. 2000. "Increasing Returns, Path Dependence, and the Study of Politics." *American Political Science Review* 94, no. 2: 251–67.

USAOC. The United States Army Special Operations Command. 2015. "Little Green Men: a prime on Modern Russian Unconventional Warfare Ukraine 2013-2014." *Johns Hopkins University Apllied Physics laboratory*: 1–65.

Vaczi, Norbert. 2016. "Hybrid Wafare: How to Shape Special Operations Forces" *U.S Army Command and General Staff College*: 3–88.

Weedon, Jen. 2015. "Beyond Cyber War: Russia's use of Strategic Cyber Espionage and Information Operations in Ukraine." *FireEye*: 67–78. In: _____. "Cyber War in Perspective: Russian Aggression Against Ukraine". Tallinn: NATO CCD COE.

Weiss, Moritz and Jankauskas, Vytautas. 2019. "Securing Cyberspace How States Design Governance Arrangements." *International Journal of Policy, Administration, and* Institutions 32, no. 2: 259–75.

NOTAS

1. *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, 18).
2. Técnica que analisa um determinado período de tempo para indicar como mudanças institucionais dificultam a reversão ao ponto inicial de movimentos iniciados por um Estado (Pierson 2000, 252).
3. Técnica que sistematiza uma análise qualitativa a partir de uma perspectiva capaz de explicar relações causais mediante a observação de como determinadas condições produzem um fenômeno observável. 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, 824).
4. Spetsnaz (Спецназ): grupos especiais de intervenção da polícia, dos ministérios de justiça e assuntos internos russos, Serviço Federal de Segurança (FSB), Serviço de Inteligência Estrangeira (SVR), Agência Federal de Comunicações e Informações Governamentais (FAGCI), bem como do exército russo.
5. *Spear phishing*: comunicação eletrônica direcionada a indivíduos, organização ou negócios específicos com intenção de instalar *malwares* espiões nos computadores dos alvos.
6. Os relatórios analisados representam fontes secundárias que contêm informações produzidas por especialistas em segurança cibernética reconhecidos mundialmente. Tratam-se, pois, de um recurso central para coleta de evidências sobre as operações envolvendo atores estatais e ameaças cibernéticas.
7. Arma cibernética que utiliza diretórios temporários para executar arquivos iscas infectados com o *malware* que são carregados por comandos "rundll32.exe", a variante não utiliza *rootkit* para ocultar objetos no sistema ou *driver kernel* para descarregar os arquivos (Lipovsky 2014, 3).
8. Arma cibernética capaz de esconder os processamentos de rotina utilizados nos ataques, mantém uma lista codificada de *offsets* em estruturas de *driver kernel* que oferece acesso total às informações dos sistemas contaminados (F-Secure Labs 2014, 1).
9. Arma cibernética de acesso remoto capaz de infectar sistemas operacionais como Windowns, iOS e plataformas móveis. Possui arquitetura modular que combina a funcionalidade de implante necessária de acordo com o equipamento utilizado pelo alvo escolhido (Crowdstrike 2014, 59).
10. Arma cibernética utilizada para infiltração e roubo de informações que não utiliza componente de *driver kernel*, invade diretamente a pasta de dados do

aplicativo local e instala um arquivo LNK para executar o malware usando o "*rundll32.exe*" (F-Secure Labs 2016, 11).

11. Arma cibernética desenvolvida para apagar o rastro dos processos de infiltração conectados via *serial-to-ethernet* e substituir o arquivo executável por dados aleatórios (E-ISAC 2016, 6).

GUERRA HÍBRIDA: O EMPREGO DA TECNOLOGIA DA INFORMAÇÃO NO CONFLITO RÚSSIA-UCRÂNIA (2014-2015).

RESUMO

Como a tecnologia da informação amplia a assimetria de poder entre os Estados contemporâneos? Com o objetivo de responder ao questionamento, o artigo descreve o processo de utilização do ciberespaço para consecução dos objetivos estratégicos da Federação Russa em seu entorno regional, durante o conflito desencadeado com a Ucrânia (2014-2015). A partir da análise de relatórios de empresas especializadas em segurança cibernética e instituições governamentais, aplicamos as técnicas qualitativas da dependência da trajetória e rastreamento de processos para explicitar a complexidade das operações conjuntas entre as forças especiais russas e *hackers* civis, bem como a sofisticação das principais ameaças e armas utilizadas nos ataques cibernéticos. Desse modo, identificamos o mecanismo responsável por conectar os níveis estratégico, tático e operacional militar ao verificarmos o processo de ação simbiótica entre os atores envolvidos no conflito. As evidências coletadas indicam como a guerra híbrida empregada pela Federação Russa incorporou a dimensão cibernética como peça chave para a desestabilização de territórios e consecução de interesses em seu entorno estratégico.

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

ABSTRACT

How does information technology expand power asymmetry between contemporary states? In order to answer this question, the article describes a process of using cyberspace to achieve strategic objectives of the Russian Federation in its regional environment, during the conflict unleashed with Ukraine (2014-2015). Based on analysis of reports from companies specialized in cybersecurity and government institutions, we apply qualitative techniques of path dependence and process tracing to explain the complexity of joint operations between Russian special forces and civilian *hackers*, as well as the sophistication of main threats used in cyber attacks. In this way, we identified a mechanism responsible for connecting strategic, tactical and military operational levels when verifying the process of symbiotic action between the actors involved in this conflict. The evidence collected indicates how hybrid warfare employed by the Russian Federation incorporated cyber dimension as a key point to destabilizing territories and achieving interests in its strategic environment

Keywords: Cyber War. Strategy. Hacker. Russia.

Recebido em 01/07/2020. Aceito para publicação em 19/04/2021.