Guerra Cibernética Russo-Ucraniana: os ataques russos às Infraestruturas Críticas ucranianas e lições para o Exército Brasileiro

Rachel Camilly Soares de Souza, Murilo Gustavo de Paula e Thays Felipe David de Oliveira

Universidade Estadual da Paraíba (UEPB), João Pessoa/PB – Brasil; 2 Centro Universitário Estácio de Sá, Goiânia/GO – Brasil; 3 Universidade Federal da Paraíba (UFPB), João Pessoa/ PB - Brasil / Centro Universitário Estácio do Recife, Recife/PE – Brasil

Resumo - Quais lições sobre Defesa Cibernética no que tange aos ataques às Infraestruturas Críticas podem ser retiradas do conflito entre Rússia e Ucrânia para o Exército Brasileiro? Com a evolução do uso do ciberespaço, houve um aumento significativo de ataques que visam afetar as Infraestruturas Críticas de um Estado. O objetivo deste trabalho é analisar quais lições que o Exército Brasileiro pode obter a partir dos ataques russos às Infraestruturas Críticas ucraniana. Desse modo, através da metodologia exploratória, o texto concentra-se em entender quais foram os antecedentes do conflito, quais ações estão sendo utilizadas pela Rússia para afetar a Ucrânia e como as ações dentro do teatro de operações podem ser relacionadas com a Estratégia Nacional de Segurança Cibernética do Brasil. Portanto, o texto aponta as mudanças na estratégia russa ligadas ao uso e à adaptação dos ataques cibernéticos às infraestruturas críticas, abordando, possíveis lições que o Exército Brasileiro pode absorver.

Palavras-Chave: Guerra Russo-ucraniana, Infraestruturas Críticas, Exército Brasileiro.

I. INTRODUÇÃO

Quais lições sobre Defesa Cibernética no que tange aos ataques às Infraestruturas Críticas podem ser retiradas do conflito entre Rússia e Ucrânia para o Exército Brasileiro? Com o avanço tecnológico e a demonstração da fragilidade do espaço cibernético, têm sido registrados cada vez mais ataques nessa área com potencial de comprometer as Infraestruturas Críticas de um Estado, englobando setores como telecomunicações, energia, finanças, entre outros. Os serviços prestados por essas infraestruturas possuem dimensão estratégica, pois são essenciais para cidadãos, organizações e para o Estado, visto que desempenham um papel imprescindível tanto para a Segurança e soberania nacional como para a integração e o desenvolvimento econômico sustentável do Estado [1].

A invasão da Ucrânia pela Rússia em 24 de fevereiro de 2022 desencadeou a crise de Segurança mais importante na Europa desde a Segunda Guerra Mundial [2]. Para além da Guerra Cinética tradicional, a Rússia conduziu operações cibernéticas em grande escala na Ucrânia antes e depois do início do combate [3]. Desde o começo deste embate, pelo menos seis grupos diferentes de *crackers* ligados ao Estado realizaram cerca de 240 operações informáticas contra alvos civis e militares ucranianos [4].

Foi empregado um *malware*, uma designação ampla que abrange todos os tipos de softwares maliciosos utilizados para causar danos, combinado com ferramentas e táticas sofisticadas de *hacking*, em prejuízo das infraestruturas públicas. Os grupos de *Advanced Persistent Threat* (APT) ligados às agências de informação russas são os atores por detrás desta campanha em curso. Um ciberatacante é designado como *APT,* quando há o ataque a uma rede ou um sistema de forma direcionada durante um longo período de tempo, com o objetivo de extrair informações sensíveis, obter acesso privilegiado ou causar danos significativos. Os ataques APT são caracterizados por sua natureza furtiva, persistência ao uso de técnicas avançadas de invasão e exploração de vulnerabilidades, bem como pela capacidade de evadir a detecção das medidas de segurança tradicionais. Normalmente, este ator é bem treinado e frequentemente ligado a um Estado ou mesmo controlado por ele [5].

O sucesso da Ucrânia até agora na defesa contra a ofensiva cibernética russa pode ser atribuído a três elementos: os preparativos do governo nos anos anteriores à guerra, a assistência à ciberdefesa da Organização do Tratado Atlântico Norte (OTAN) e dos países da União Europeia. Em suma, para operacionalizar essa pesquisa foi realizada uma pesquisa qualitativa e de forma complementar é um estudo de caso único. Assim, o objetivo deste trabalho é analisar quais lições que o Exército Brasileiro pode obter a partir dos ataques russos às Infraestruturas Críticas ucranianas [7].

2. ANTECEDENTES HISTÓRICOS EM RELAÇÃO AOS CIBERATAQUES RUSSOS

A Rússia tem recorrido sistematicamente aos ciberataques contra a Ucrânia. Os *crackers*, indivíduos que invadem sistemas computacionais com propósitos ilegais, ligados aos serviços secretos russos, têm conduzido operações ciberofensivas na Ucrânia, pelo menos desde a anexação da Crimeia pela Rússia em 2014. Os seus alvos incluíam Universidades, Empresas de Eletricidade, o Setor Bancário e outras Infraestruturas Críticas. Inicialmente, o Estado Russo tinha como objetivo causar frustração pública e enfraquecer os seus adversários no sistema político ucraniano. Em alguns casos, os atacantes utilizaram *malware KillDisk*, fazendo da Ucrânia um banco de ensaio para o desenvolvimento de novas armas cibernéticas [2].

A partir de 2014, o grupo hacktivista pró-russo [5] *CyberBerkut*, ligado à agência de informações militares estrangeiras do Estado-Maior General das Forças Armadas russas, comprometeu o sistema eleitoral central ucraniano instalando um *malware BlackEnergy* no sistema para minar a confiança no processo eleitoral e causar instabilidade política [5]. O ataque não foi bem-sucedido, uma vez que não deslegitimou o vencedor das eleições em 2014. No entanto, a contagem final dos votos foi adiada por duas horas [6].

O pior incidente cibernético na Ucrânia ocorreu em 2017, quando o grupo APT russo *Telebots*, também ligado ao *Sandworm*, implantou o *malware NotPetya* contra os setores financeiro e energético ucranianos [8]. Espalhou-se pelo país por meio de um popular programa de preparação de impostos. Embora o ataque visasse de empresas dentro do Estado ucraniano, o *malware* ficou fora de controle e afetou empresas multinacionais em toda a Europa e nos Estados Unidos. O impacto exato na economia da Ucrânia não é claro, mas as perdas econômicas globais estimadas excederam os 10 milhões de dólares [9].

No dia 23 de fevereiro de 2021, véspera da invasão russa, foi lançado um ciberataque maciço utilizando o *malware HermeticWiper* nas máquinas do governo ucraniano e nos setores financeiros, da aviação, das TI e da energia [11]. Embora não existam provas concretas que liguem os autores deste ataque à Rússia, o momento e a metodologia utilizados sugerem fortemente essa ligação. No dia seguinte, poucas horas depois da invasão, houve outro ciberataque significativo contra a rede *KA-SAT* da *Viasat*, amplamente utilizada pelas forças armadas e pela polícia ucraniana [12]. Como resultado, a maioria dos modems *Viasat* ficou inoperacional e o serviço de Internet de banda larga para centenas de milhares de ucranianos e militares foi interrompido. Um efeito secundário deste ataque foi o fato de o *AcidRain* ter atravessado fronteiras e ter afetado outros países europeus, tal como no caso do *NotPetya* [12].

O seguinte grande incidente foi registrado em abril de 2022, quando a infraestrutura energética da Ucrânia foi atacada pelo *malware Industroyer II*, visando especificamente subestações elétricas de alta tensão [13]. É preciso salientar que, ao contrário do seu antecessor, o *Industroyer II* foi utilizado como uma arma autônoma, não necessitando da intervenção de um operador remoto [14]. O incidente obteve uma rápida resposta das autoridades ucranianas de ciberdefesa, que adquiriram uma experiência significativa nos últimos anos, e à assistência da *Microsoft* e da *ESET* [14].

3. LIÇÕES PARA O EXÉRCITO BRASILEIRO

A guerra cibernética entre Rússia e Ucrânia, especificamente os ataques russos às Infraestruturas Críticas ucranianas, oferece uma série de lições valiosas para o Exército Brasileiro. Esses eventos destacam a importância da preparação e capacitação para enfrentar ameaças cibernéticas direcionadas a setores estratégicos do país. Uma das principais lições é a necessidade de investir em capacidades de ciberdefesa. O EB deve desenvolver e aprimorar suas habilidades na proteção de sistemas de energia, comunicação, transporte e outras áreas estratégicas do país. Isso requer uma abordagem abrangente que envolva tecnologia, especialização em cibersegurança e treinamento adequado para suas equipes [16].

Torna-se fundamental destacar a necessidade contínua de aprimoramento e implementação regular de exercícios e simulações, como o “Guardião Cibernético 3.0” realizado pelo Comando de Defesa Cibernética Brasileiro – COMDCIBER. Essas atividades desempenham um papel crucial ao testar e fortalecer a prontidão cibernética do Exército, permitindo identificar lacunas, aperfeiçoar procedimentos de respostas a incidentes cibernéticos e aprimorar a colaboração entre as equipes envolvidas [17]. A força armada terrestre pode desempenhar um papel ativo em fornecer um orientações sobre medidas cibernéticas, como a implementação de sistema de detecção e intrusão, políticas de autenticação, proteção de dados e treinamento de funcionários de empresas privadas que fornecem serviços essenciais para o País, tais como bancos, empresas energéticas e telecomunicações.

Além disso, é fundamental investir em recursos ofensivos de cibersegurança. Os ciberataques russos à Ucrânia exigiram uma capacidade de resposta rápida e eficaz a esse tipo de agressão. O EB deve ter a capacidade de identificar, rastrear e neutralizar atores hostis que buscam prejudicar às Infraestruturas Críticas do país [18]. Outro ponto a ser destacado é a cooperação e intercâmbio com parceiros internacionais, pois, a Guerra Cibernética é uma ameaça transnacional que requer esforços definidos para combatê-la. Devendo assim, o Brasil, buscar parcerias estratégicas com outras nações, compartilhando conhecimentos, tecnologias e experiências para fortalecer os recursos de resposta a ataques cibernéticos. Além disso, a colaboração com organizações internacionais, como a OTAN, pode fornecer um quadro estratégico para lidar com essa ameaça a nível global [18].

4. CONCLUSÃO

Apesar da existência dos ramos cibernéticos nas forças singulares, a exemplo do que ocorreu com os antigos ramos aéreos dos Exércitos e da Marinhas, que foram unidos para a criação das Forças Aéreas, há uma possibilidade da construção de uma nova Força Armada, composta por cibercombatentes, advindos da junção dos ramos cibernéticos das Forças Singulares hoje existentes. Afinal, a organização, os tempos, os meios e as táticas de combate exploradas no quinto domínio da guerra são bem distintos. Observa-se o que ocorre na guerra russo-ucraniana, em que uma batalha cibernética dura poucas horas, enquanto batalhas terrestres, marítimas e aéreas duram dias ou semanas. Logo, a busca por lições aplicáveis ao Exército Brasileiro são imprescindíveis para o desenvolvimento de novas políticas de Defesa Cibernética além de uma atualização mais frequente da Estratégia Nacional de Segurança Cibernética, pois o Brasil, levando em consideração suas potencialidades internacionais e a quantidade de recursos naturais integrados ao território, não pode negligenciar seu segmento de defesa e a importância do desenvolvimento do quinto domínio na atualidade.

REFERÊNCIAS

1.Célio Taquary Segundo. “A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos**”**. Escola Superior de Guerra, 2019.

2.Leila Fonseca. "A guerra cibernética e o conflito Rússia versus Ucrânia". Revista de Relações Exteriores, 24 de fevereiro de 2023.

3.Matthias Schulze e Mika Kerttunen, “Cyber Operations in Russia’s War against Ukraine”, SWP Comment, April 2023.

4.Laurens Cerulus. “How Ukraine became a test bed for cyberweaponry”, February 14, 2019.

5.National Cyber Security Center (NCSC). “Reckless campaign of cyber attacks by Russian military intelligence service exposed”, 3 october 2018.

6.Americas Cyber Defense Agency. “Russian State-Sponsored and criminal cyber threats to critical infrastructure”. April 20, 2022.

7.Robert Yin. “Estudo de Caso: Planejamento e métodos”. Bookman editora, 2015.

8.Anton Cherepanov e Robert Lipovsky. “Industroyer: Biggest threat to industrial control systems since Stuxnet”, ESET, June 12, 2017.

9.“New WannaCryptor-like ransomware attack hits globally: All you need to know”, ESET. June 27, 2017.

10.A. Greenberg, ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’, Wired, 22 August 2018.

11.Juan Andrés Guerrero-Saade, “HermeticWiper. New Destructive Malware Used In Cyber Attacks on Ukraine”, Sentinel One (23 February 2022)

12.“KA-SAT Network cyber attack overview”, Viasat. March 30, 2022.

13.Computer Emergency Response Team of Ukraine. “Cyber attack of the Sandworm group (UAC-0082) on energy facilities of Ukraine using malware INDUSTROYER2 and CADDYWIPER”. December 12, 2022.

14.Victor Zhora, “The potential of Russian hackers is probably overestimated”, State Service of Special Communications and Information Protection of Ukraine. March 16, 2022.

15.Estratégia Nacional de Segurança Cibernética – E-Ciber, Presidência da República, DECRETO nº 10.222, 2020-02-05.

16. Política Nacional de Segurança de Infraestruturas Críticas – PNSIC, Presidência da República, DECRETO nº 9.573, 2018-11-22.

17. M. Harknett, "Defending cyberspace and other metaphors," Journal of Strategic Studies, vol. 32, no. 1, pp. 5-31, 2009.

18.J. P. Buchan, "Protecting national critical infrastructure against cyber threats," Computers & Security, vol. 28, no. 3, pp. 191-198, 2009.