O emprego de ataques cibernéticos no conflito Rússia-Ucrânia: um alerta à necessidade de capacitação em guerra cibernética

*Filipe Ramos Gajo**

Introdução

O nascimento da cibernética como ciência está associado aos trabalhos de Norbert Wiener (1894-1964). Na Segunda Guerra Mundial (1939-1945), ele foi encarregado pelo governo norte-americano de resolver problemas de controle automático da direção do tiro na artilharia antiaérea (FILHO, 2007, p. 137).

O primeiro grande ataque cibernético de que se tem notícia ocorreu apenas em 2007. Após divergências sobre a remoção de um memorial da Segunda Guerra entre o governo estoniano e o governo russo, a Estônia sofreu ataques cibernéticos em massa direcionados aos órgãos do governo, bancos e imprensa. Em decorrência desses ataques, o governo estoniano desativou o acesso de IP externos e levou meses para retornar à normalidade (ARAÚJO, 2022). Tal ataque reverberou no mundo e marcou o início da implantação de políticas de segurança cibernética e estratégias de defesa cibernética (CASSIANI, 2002, p. 5).

Atualmente, o conflito Rússia-Ucrânia reitera o massivo uso da guerra cibernética nos conflitos armados, deixando um alerta flagrante às nações para a necessidade de investimento e capacitação técnica em guerra cibernética no âmbito das forças armadas.

No Brasil, a Estratégia Nacional de Defesa (END), em 2008, estabeleceu prioridade em três setores estratégicos, sendo um deles o cibernético (BRASIL, 2008). O Ministério da Defesa, visando cumprir a END nos setores estratégicos da defesa, incumbiu ao Exército a coordenação e integração do setor cibernético (BRASIL, 2009).

Desenvolvimento

Guerra cibernética no conflito Rússia x Ucrânia

Antes mesmo da invasão russa à Ucrânia, em fevereiro de 2022, diversos ataques cibernéticos foram observados. Pesquisadores descobriram, em janeiro, um mês antes, um *malware* destrutivo circulando na Ucrânia. Após isso, uma onda de ataques derrubou brevemente *sites* bancários e governamentais. No início da ofensiva russa, nas primeiras horas do dia 24 de fevereiro de 2022, milhares de *modems* que forneciam internet aos ucranianos foram paralisados (PEARSON, 2022).

Outro conceito que pode ser observado no atual conflito é o de guerra híbrida. Esse tipo de guerra se caracteriza quando as ações de combate convencional ocorrem simultaneamente com operações de guerra cibernética, guerra irregular, dentre outras (BRASIL, 2018).

Nesse contexto, em 1º de março de 2022, ocorreu um ataque de míssil russo contra a torre de TV de Kiev, que coincidiu com ataques cibernéticos na mídia

*Cap Inf (AMAN/2011, EsAO/2021). Atualmente, é instrutor do Curso de Infantaria da EsAO.

da capital. Enquanto os militares russos ocupavam a usina nuclear de Zaporizhzhya, na Ucrânia, um grupo de *hackers* foi detectado nas redes de uma empresa de energia nuclear. Dessa forma, os russos estão integrando ataques cinéticos e atuadores não cinéticos (PEARSON, 2022).

Guerra cibernética no Brasil

O Ministério da Defesa, em 2009, emitiu diretriz para cumprir a END nos setores estratégicos da defesa. A responsabilidade pela coordenação e integração do setor cibernético coube ao Exército. Em cumprimento à diretriz, foi ativado, em agosto de 2010, o Núcleo do Centro de Defesa Cibernética. Em setembro de 2013, foi atualizada a Estratégia Nacional de Defesa e aprovado o *Livro Branco de Defesa Nacional*, que afirma que a proteção do espaço cibernético abrange áreas como: capacitação; inteligência; pesquisa científica; doutrina; preparo e emprego operacional; e gestão de pessoal (BRASIL, 2014).

A escalada de ataques cibernéticos aumentou em ritmo acelerado. O número de ataques, apenas no primeiro trimestre de 2021, foi superior a todos os ataques ocorridos no ano de 2020. Com vazamentos de informações sigilosas, sequestro de dados, invasões de sistemas, dentre outros, o Brasil foi o quinto país que mais sofreu crimes cibernéticos em 2021 (PRADO, 2021). Em maio de 2021, o frigorífico JBS, gigante mundial do setor de carnes, foi alvo de um ataque cibernético que ocasionou a paralização de sua produção em algumas fábricas.

O Brasil norteia suas relações internacionais pelos princípios da defesa, da paz, da não intervenção e da solução pacífica dos conflitos. Nenhum Estado, entretanto, pode ser pacífico sem ser forte (BRASIL, 2008). Nesse sentido, apesar de não sofrer ameaças militares diretas, a capacidade de se proteger frente a ataques cibernéticos é fundamental para qualquer Estado.

Conclusão

O Exército Brasileiro possui um papel importante na conjuntura de defesa cibernética nacional. Anualmente, militares realizam cursos na área cibernética. No ano de 2017, 50 militares, entre oficiais e sargentos, realizaram os cursos de Guerra Cibernética e Inteligência Cibernética. Em 2023, serão abertas 72 vagas para os cursos de Guerra Cibernética, Inteligência Cibernética, Planejamento de Guerra Eletrônica e Guerra Cibernética em Apoio às Operações e Proteção Cibernética.

O Brasil ainda precisa evoluir no campo da defesa cibernética. Desde 2008, porém, o país vem dando importância a essa área e nela se especializando. O número de militares capacitados para atuarem nessa área ainda é pequeno, mas podemos observar que, nos últimos anos, houve um incremento no número de vagas, bem como na diversificação dos cursos disponibilizados. Observando o cenário que se apresenta, entendemos que, além da oferta de cursos e formação de pessoal especializado, é urgente e imprescindível a criação de uma mentalidade de "contrainteligência cibernética". Importante inserir na rotina castrense o tema, buscando torná-lo mais palatável ao longo do tempo. Os usuários dos diversos sistemas ainda são os elos mais fracos nessa corrente.

Referências

ARAÚJO LISBOA, Cícero; ZIEBELL DE OLIVEIRA, Guilherme. **O Conceito de dissuasão cibernética: relevância e possibilidades**. OASIS n° 35, p. 53-78, maio 2022.

BRASIL. **Decreto n° 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Diário Oficial da União, Brasília, DF, 19 dez 2008. Seção 1, p. 4.

BRASIL. **Diretriz Ministerial n° 0014, de 9 de novembro de 2009.** Dispõe sobre a integração e coordenação dos setores estratégicos da defesa. Ministério da Defesa, Brasília, DF, 9 nov 2009.

BRASIL, Estado-Maior do Exército. **EB20-MF-03.109, Glossário de Termos e Expressões para uso no Exército**. 5. ed., 2018, Brasília, DF.

BRASIL, Ministério da Defesa. **MD31-M-08, Doutrina Militar de Defesa Cibernética.** 1. ed., 2014, Brasília, DF.

CASSIANI, Arthur Gonçales et al. **O Papel da Defesa Nacional em Casos de Ataques Cibernéticos: Uma Análise sobre a Necessidade de Protocolo(s) de Prevenção e Atuação**. Disponível em:<https://www.gov.br/defesa/pt- br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/oa_papela_daa_defesaa_nacionala_ema_casosa_dea_ataquesa_ciberneticosa_umaa_analisea_sobr ea_aa_necessidadea_dea_protocolos.pdf> Acesso em: 30 abr 2022.

FILHO, Cléuzio Fonseca. **História da computação: o caminho do pensamento e da tecnologia**. Porto Alegre: Editora EDIPUCRS, 2007. 204p.

PEARSON, James; BING, Christopher. **The cyber war between Ukraine and Russia: An overview.** Disponível em: <https://www.reuters.com/world/europe/factbox-the- cyber-war-between-ukraine-russia-2022-05-10/> Acesso em: 28 maio 2022.

PRADO, Filipe. **Brasil foi 5º país com mais ataques cibernéticos no ano: relembre os principais.** Disponível em: <https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com- mais-ataques-ciberneticos-no-ano-relembre-os-principais/> Acesso em: 29 maio 2022.