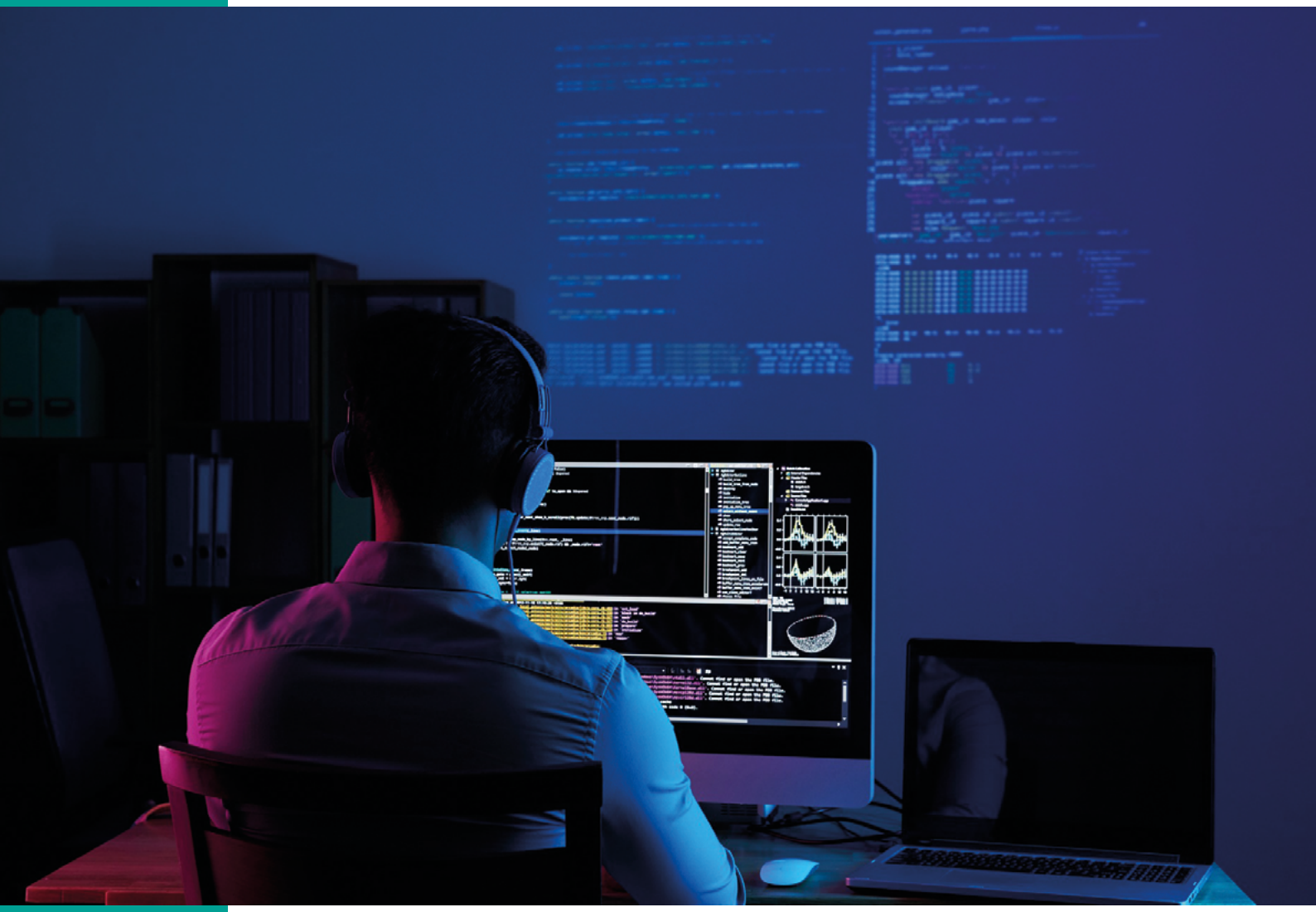
A CIBERNÉTICA COMO FERRAMENTA DE ESPIONAGEM: EXPLORANDO AS IMPLICAÇÕES DA CIBERNÉTICA NA SEGURANÇA NACIONAL BRASILEIRA



Carlos Eduardo Rabelo Amaral

2º Sargento de Infantaria do Exército Brasileiro. Escola de Aperfeiçoamento de Sargentos das Armas (EASA). Possui o Curso de Inteligência Cibernética, possui o Curso Básico de Inteligência, possui a certificação Off Sec Certified Professional (OSCP) pela OffSec, possui a certificação Desec Certified Penetration (DCPT) pela Desec Security, possui a certificação Certified Secure Computer User (CSCU) pela EC-Council.

ST Alan dos Santos

Orientador

O artigo de Rocha, F. C. W. (2013) intitulado "Espionagem e internet", aborda a crescente preocupação com relação à privacidade e segurança na internet, especialmente após as revelações feitas por Edward Snowden sobre as práticas de espionagem da Agência de Segurança Nacional dos Estados Unidos (NSA).

O autor discute como a internet se tornou uma ferramenta indispensável para a comunicação, o comércio e a troca de informações em todo o mundo e, sobretudo, propiciou um terreno fértil para atividades de espionagem e vigilância. É analisado como as empresas de tecnologia coletam informações sobre seus usuários para fins comerciais e como os governos podem usar essas mesmas informações para fins de Inteligência.

Também é destacado pelo artigo como as revelações de Snowden levantaram preocupações sobre a soberania nacional e a privacidade dos cidadãos, especialmente em países como o Brasil, onde a presidente Dilma Rousseff foi alvo de espionagem pela NSA. Ele discute as implicações legais e políticas dessas práticas de espionagem e as medidas que estão sendo tomadas para proteger a privacidade dos cidadãos na internet.

Rocha (2013) aborda um tema extremamente relevante e atual sobre as práticas de espionagem na internet e como isso afeta a privacidade e a segurança dos usuários. O autor chama a atenção para a importância de proteger a privacidade na internet, por meio de profissionais mais bem preparados, e discute as implicações legais e políticas das práticas de espionagem.

O artigo do autor está alinhado ao Manual de Campanha do Exército Brasileiro EB70-MC-10.220 – Contrainteligência, que traz as principais motivações que são exploradas por indivíduos e Estados para cooptar terceiros, a saber: dinheiro, ideologia, coerção e ego. Contextualizando, são apresentados diversos exem-

plos históricos de espionagens realizadas por traidores, coadunando com o Manual supracitado, que adverte sobre ações envolvendo o público interno da força.

J.Dailey (2017) reforça em seu artigo o que Rocha (2013) afirma acerca da existência de um acordo de colaboração entre

dia. Ambos os autores discorrem sobre a colaboração dessas agências justificarem sua existência sob o pretexto de combater as ameaças terroristas.

A Revista Em Discussão (2014), editada pelo Senado Federal, aborda especificamente a espionagem cibernética. Diver-

Figura 1 - Obtenção de dados de usuários.

Fonte: Bing Image Creator (2023).

países, chamado *The Five Eyes* (Os Cinco Olhos), integrado pelas agências de segurança: *National Security Agency* (NSA), dos Estados Unidos; *Government Communications Headquarters* (GCHQ), do Reino Unido; *Communications Security Establishment Canada* (CSEC), do Canadá; *Australian Sgnals Directorate* (ASD), da Austrália; e *Goverment Communicarions Security Bereau* (GCSB), da Nova Zelân-

sos artigos abordam as revelações feitas por Edward Snowden, ex-técnico da NSA, destacando a espionagem eletrônica perpetrada pelo governo norte-americano no Brasil e no mundo, conhecido como Projeto PRISM e tendo como pretexto a segurança nacional diante do terrorismo.

Segundo publicado pela Folha de São Paulo (2013), o Projeto PRISM foi fundamentado em uma legislação dos Estados

Unidos. Esse projeto se beneficiava da significativa concentração de empresas da área de tecnologia sediadas naquele país, o que, por conseguinte, permitia ao governo norte-americano obter acesso aos dados de usuários ao redor do mundo. Empresas como *Apple*, *Yahoo*, *Microsoft* e *Google* eram supostamente fornecedoras desses dados. Nesse contexto, observa-se que o aludido projeto corrobora com as argumentações escritas por Rocha (2013) em seu artigo, onde é mencionado que autoridades brasileiras, incluindo a ex-presidente, foram alvos dessa espionagem.

Assim como Rocha (2013), a Folha de São Paulo sugere propostas para que o Brasil possa melhorar a segurança de suas informações, as quais também foram contempladas no relatório final da Comissão Parlamentar de Inquérito (CPI) da Espionagem de 2013, instaurada pelo Senado Federal após as denúncias de Snowden.

Rocha (2013) também destaca que não apenas a ex-presidente do país, mas outras autoridades de alto escalão do Governo Federal foram monitoradas, como por exemplo: a Casa Civil, o Gabinete de Segurança Institucional, o Banco Central e o Ministério da Fazenda. Ainda, integraram esse grupo, autoridades de setores diplomáticos do Itamaraty, que também compuseram esse rol de monitorados por diversos anos.

Coadunando com esse tema, o *site* Terra postou um artigo intitulado: "*Wikileaks*: NSA espionou Dilma, Palocci e avião" (2015). Esse artigo detalhava como foi realizada uma vigilância em telefones oficiais, caracterizando a importância do Brasil no cenário mundial.

Em seu artigo, Rocha (2013) reitera os princípios estabelecidos pela Doutrina Militar de Defesa Cibernética (MD31-M-08), documento de alto nível de planejamento de defesa estabelecido pelo Ministério da Defesa (MD). Esse documento define objetivos e diretrizes para a atuação no Espaço Cibernético, com foco principalmente na defesa. O Brasil possui diversos interesses nessa área, incluindo infraestruturas críticas, que devem ser protegidas, por meio de um esforço cooperativo, conforme destacado na Doutrina Militar de Defesa Cibernética.

Rocha (2013) traz uma preocupação adicional sobre os meios tecnológicos em seu artigo. Corroborando com isso, esse apontamento também é caracterizado na Estratégia Nacional de Inteligência (ENINT) de 15 de dezembro de 2017, documento esse que decorre da Política Nacional de Inteligência (PNI), fixada por meio do Decreto nº 8.793, de 29 de junho de 2016. Esse autor reconhece os inegáveis benefícios e facilidades trazidos pela tecnologia, mas destaca que, como a ENINT também ressalta, o aumento da espionagem cibernética para fins econômicos e científicos é uma consequência preocupante. Ainda, reitera a importância do domínio das soluções tecnológicas por profissionais preparados para lidar com o espaço cibernético, o que proporcionará vantagens significativas. É importante notar que, de acordo com a ENINT, cabe à Atividade de Inteligência monitorar o ambiente interno e externo, a fim de identificar oportunidades, possíveis ameaças e riscos aos interesses do Estado e da sociedade brasileira.

Maroto (2009) reitera as informações apresentadas por Rocha (2013) que evidenciam a ampla utilização de recursos tecnológicos na prática de ciberespionagem, que podem se valer de dispositivos como: celulares, computadores, rádios, TV, satélites, sistemas de radiocomunicação e fibra ótica. Além disso, Maroto (2009) destaca a importância de equipamentos responsáveis pela manutenção de infraestruturas e serviços essenciais, muitas vezes importados, tais como meios de transporte, serviços de emergência, serviços bancários, universidades e forças armadas,

que são considerados elementos críticos para a segurança de um país.

Rocha (2013) ainda argumenta a atividade de espionagem é mais que um direito do Estado, é um dever e deve ser praticada internamente e externamente, visando à defesa dos interesses do país. Entretanto, afirma que nenhum poder, inclusive o de coletar e fazer uso de informações, pode ser absoluto, demandando uma permanente fiscalização. Dessa forma, o autor está em consonância com o que é preconizado na Política Nacional de Inteligência (PNI), que estabelece os parâmetros e limites para a atuação da Atividade de Inteligência e seus agentes no âmbito do Sistema Brasileiro de Inteligência (SISBIN), conforme estabelecido pela Lei nº 9.883, de 7 de dezembro de 1999.

Diante do exposto, evidencia-se na pesquisa realizada a importância de medidas como: a preparação de técnicos especializados em defesa e gestão do espaço cibernético brasileiro; e o emprego de ferramentas de proteção do espaço virtual, que podem reduzir significativamente os riscos aos ativos do Exército Brasileiro e os danos à imagem da Força Terrestre. Isso reforça a relevância do planejamento para enfrentar as ameaças ao espaço cibernético do Brasil, ainda pouco controladas e intensificadas pela modernização tecnológica.

Nessa perspectiva, o tema apresenta uma grande contribuição para o Sistema de Inteligência do Exército (SIEx), sugerindo fundamentalmente, por meio de estudos de acontecimentos, uma melhor preparação da defesa brasileira contra possíveis espionagens cibernéticas em ativos de interesse nacional, além de destacar a importância do Brasil no cenário mundial como alvo dessa prática.

Proteger e aprimorar a capacidade do Exército Brasileiro de resistir e responder a investidas cibernéticas deve representar uma das principais prioridades da Força, não obstante a carência global de talentos no campo da cibernética.

Nesse contexto, é digno de nota que o Exército Brasileiro seja capaz de atrair profissionais de alta qualificação para suas fileiras. Corroborando, como sugestão, o Sistema de Inteligência do Exército pode ajudar na tarefa de detectar, ainda dentre os quadros das Escolas de Formação, aqueles militares dotados de tais competências, de modo a recrutá-los para desenvolver seus talentos e evitar a evasão desse recurso humano qualificado.

REFERÊNCIAS

1. BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. **EB70-MC-10.220:** Manual de Campanha. Contrainteligência. 1 ed. Brasília, DF, 2019.
2. BRASIL. Ministério da Defesa. Gabinete do Ministro. **MD31-M-08:** Doutrina Militar de Defesa Cibernética. 1 ed. Brasília, DF, 2014.
3. BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. **Estratégia Nacional de Inteligência**, Decreto de 15 de dezembro de 2017.
4. BRASIL. Presidência da República. Secretaria-Geral. Decreto nº 8.793, **Política Nacional de Inteligência**, de 29 de junho de 2016.
5. BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. **EB70-MC-10.232:** Manual de Campanha. Guerra Cibernética. 1 ed. Brasília, DF, 2017.
6. DAILEY, Jeffrey. The Intelligence Club: A Comparative Look at Five Eyes. **Journal of Political Sciences & Public Affairs**. Texas, USA, jun. 2017. Disponible: https://www.longdom.org/open-access-pdfs/the-intelligence-club-a-comparative-look-at-five-eyes-2332-0761-1000261.pdf. Acesso em: 12 mar. 2023.

7. PUIME MAROTO, J. El ciberespionaje y la ciberseguridad. In: **CEDESEN**. **Madrid**: Ministerio de Defensa Nacional, 2009.
8. FÁVERO, Bruno. Falta de lei para internet expõe brasileiros à vigilância dos EUA. **Folha de São Paulo**, jun 2013. Disponível em: http://www1.folha.uol.com.br/tec/2013/06/1295459-prism---reacende-debate sobre-privacidade-na-internet-no-brasil-faltam-leis---sobre-o-assunto.shtml. Acesso em: 23 abr. 2023.
9. ROCHA, F. C. W. Espionagem e Internet. **Cadernos Aslegis**, n. 49, maio/ago. 2013.
10. SENADO FEDERAL. Espionagem cibernética: rede vulnerável. **Em Discussão!: os principais debates do Senado Federal**, v. 5, n. 21, jul. 2014. Disponível em: http://www2.senado.leg.br/bdsf/handle/id/503306. Acesso em: 12 mar. 2023.
11. **WIKILEAKS**: NSA espionou Dilma, Palocci e avião. TERRA, jul 2015. Disponível em: https://www.terra.com.br/noticias/brasil/politica/wikileaks-revela-lista-de-29-espionados-no-brasil--pela-nsa,4315c76a15b45b976fccd1651bfebc46qmigRCRD.html. Acesso em: 12 mar. 2023.