CICAD.I.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

SEGURANÇA CIBERNÉTICA: O OLHAR DA DEFESA NACIONAL E DA INTELIGÊNCIA DE ESTADO FRENTE ÀS VULNERABILIDADES DIGITAIS

Alexsandro Barreto Gois
Mestrando em Economia da Defesa pela Universidade de Brasília

RESUMO: O presente artigo trata sobre a segurança cibernética, um paradigma atual que está gerando uma crescente preocupação de entidades públicas e privadas em todo o mundo. Antigamente as ameaças eram, em sua grande maioria, visíveis e tangíveis. Mas, com o avanço das tecnologias de comunicação e informação, isso mudou. As ameaças atuais estão invadindo os sistemas eletrônicos das corporações, prejudicando suas atividades. Diante disso, surgem preocupações para uma nova forma de segurança e proteção frente às vulnerabilidades digitais: segurança cibernética. A segurança cibernética é uma preocupação atual e crescente de diversas instituições, tanto públicas quanto privadas. A preocupação é latente e já está normatizada nas políticas públicas de instituições de segurança pública, como é evidente nas Estratégias Nacional de Defesa e Nacional de Inteligência. Neste artigo, demonstra-se essa normatização e consequente preocupação, tanto da área de Defesa quanto da área de Inteligência. Ainda, comenta-se casos de ataques cibernéticos que ocorreram em algumas instituições públicas e privadas. A preocupação com uma nova forma de defesa é necessária para as instituições que trabalham com segurança. Como salvaguardar os sites e sistemas de suas instituições? É possível se defender desses tipos de ataques, ou estamos à mercê dos ataques cibernéticos?

Palavras-chave: Segurança cibernética. Vulnerabilidades digitais. Defesa Nacional. Estratégia Nacional de Defesa. Estratégia Nacional de Inteligência.

INTRODUÇÃO

Recentemente, uma sequência de ataques cibernéticos tem acometido diversas instituições, causando transtornos e prejuízos de grande soma. Por isso, o propósito deste artigo é analisar o olhar dos órgãos que se preocupam com Segurança Cibernética, como a Defesa Nacional e a Inteligência de Estado, tendo em vista as vulnerabilidades digitais existentes.

O fato de o Brasil ser um dos países que lidera o ranking de ataques cibernéticos, provoca grandes discussões sobre o aparato de proteção contra eles. A indagação de o Brasil estar preparado para a Defesa Cibernética é uma discussão feita neste trabalho.

Para responder a essa indagação, necessário se faz analisar a normatização estratégica de duas áreas de segurança: a Defesa Nacional e a Inteligência de Estado. Ambas demonstram, em suas Estratégias Nacionais, a preocupação com os ataques cibernéticos e propõem, em sentido similar, a capacitação de seu corpo técnico com conhecimentos e habilidades que auxiliem no combate ao crime em ambiente virtual.

1 SEGURANÇA CIBERNÉTICA

Considerando os atuais avanços das Tecnologias da Informação e Comunicação (TIC), foi constatado, pela presença cada vez maior de tecnologias no cotidiano da sociedade, o elevado uso de smartphones, tablets, relógios digitais, computadores, dentre outros equipamentos. Os quais fornecem acesso à internet, possibilitando a realização de trabalhos remotos, transações financeiras, ensino a distância (EaD), utilização de redes sociais,

disponibilização de documentos, fotos e vídeos na "nuvem" ou disponíveis para acesso sem restrições de usuários etc. Tudo disponível em um único clique, acessível a tudo e a todos.

Entretanto, isso requer cuidado, preocupação e medidas de segurança dos usuários das TIC. Tendo em vista essa preocupação, Canongia e Mandarino Júnior (2009) revelam que um dos grandes receios da atualidade é com a segurança no mundo digital. É evidente que a abertura de dados e a disponibilização de informações de forma ostensiva proporcionam fragilidades quanto à segurança de dados e informações.

Nesse sentido, seguindo as palavras de Mandarino Júnior (2009), que define segurança cibernética como a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas. Devemos nos preocupar com a segurança cibernética, reduzindo ao máximo vulnerabilidades disponíveis na rede mundial de computadores. Mas, como podemos nos proteger disso? Nós, como cidadãos, temos as "armas" necessárias para essa defesa? O Estado pode nos ajudar? A Segurança Pública se preocupa com essa nova forma de Defesa? As Forças Armadas também se preocupam com a segurança da informação? A Atividade de Inteligência reconhece essa fragilidade como uma ameaça a ser observada? Essas indagações são recorrentes e este artigo se propõe a respondê-las.

É crescente o cuidado dos governos em salvaguardar seus bancos de dados, com o fim de evitar cibercrimes, e em desenvolver e capacitar o seu corpo técnico para lidar com questões de segurança de dados e de informações (CANONGIA e MANDARINO JÚNIOR, 2009). Assim, considerando o elevado compartilhamento de dados e informações nas redes sociais, o aumento do armazenamento em "nuvens" e a importância das informações arquivadas em computadores, as questões ligadas à segurança, privacidade e confidencialidade tornam-se essenciais para a proteção de dados e de informações.

Nesse contexto, a segurança cibernética é uma preocupação global que objetiva assegurar ao máximo a disponibilidade, confidencialidade, integridade e autenticidade de dados e informações, haja vista a formulação de estratégias para o processo decisório nacional (CANONGIA e MANDARINO JÚNIOR, 2009). Além dos Estados, as organizações do setor privado e as pessoas físicas também estão preocupadas com a proteção de seus dados e informações, situação que cresce à proporção que se expande o número de usuários das TIC.

Por esse motivo, é importante a normatização de ações voltadas à Segurança Cibernética e à adoção de políticas públicas para essa área. Assim, a partir desse momento, iremos analisar as normas que estão voltadas a ações de proteção e salvaguarda contra ataques cibernéticos, que estão expressas na Estratégia Nacional de Defesa (END) e na Estratégia Nacional de Inteligência (Enint).

1.1 ESTRATÉGIA NACIONAL DE DEFESA

A END tem como propósito estabelecer diretrizes para a adequada preparação e capacitação das Forças Armadas, possibilitando a garantia da segurança do país em diversos cenários, tanto em tempo de paz quanto em situações de conflito. Uma congruente estrutura de defesa assegura maior estabilidade ao país e proporciona a devida proteção de seu território, de sua população e de setores considerados estratégicos da economia.

Esse documento definiu ações estratégicas num espectro de médio e longo prazos, objetivando a modernização da estrutura nacional de defesa. Dedica-se, também, a questões político-institucionais que assegurem os meios para fazer com que o governo e a sociedade empreguem decisivamente os conceitos inerentes à estratégia de segurança nacional. Além, é claro, de tecer temas propriamente militares, fixando orientações e paradigmas para

a atuação operacional do Exército, da Marinha e da Aeronáutica.

A referida estratégia foi estruturada em quatro eixos principais, os quais abordam: a) como as Forças Armadas devem se organizar e se orientar para melhor desempenharem sua destinação constitucional e suas atribuições na paz e na guerra; b) a reorganização da Base Industrial de Defesa, para assegurar o atendimento às necessidades de equipamentos das Forças Armadas apoiado em tecnologias sob domínio nacional, preferencialmente as de emprego dual (militar e civil); c) composição dos efetivos das Forças Armadas; d) o futuro do serviço militar obrigatório, observando a necessidade das Forças Armadas serem constituídas por cidadãos oriundos de todas as classes sociais.

Ainda, enumerou vinte e cinco diretrizes para nortear as distintas áreas de preocupação, com o fim de desenvolver ações estratégicas da Defesa Nacional. Dentre elas, a sexta diretriz pauta-se no fortalecimento de três setores de importância estratégica, quais sejam: o espacial, o cibernético e o nuclear.

O setor cibernético, que faz parte do escopo deste trabalho, se preocupa como as capacitações se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Integrarão, como prioridade, as TIC entre todos os agrupamentos das Forças Armadas, de modo a assegurar sua capacidade para atuar em rede. As prioridades do setor cibernético elencadas na END são as seguintes:

a) fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas;

b) aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à certificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças;

c) fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, Orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética;

d) desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;

e) desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais;

f) desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas;

g) incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e

h) estruturar a produção de conhecimento oriundo da fonte cibernética. (BRASIL, 2012).

As prioridades do setor cibernético citadas acima demonstram o norte de atuação das ações que as Forças Armadas devem dispensar para assegurar a defesa nesse setor. Das oito prioridades, percebe-se que é latente a preocupação com o fortalecimento, aprimoramento, desenvolvimento e capacitação por meio de conhecimentos, estudos e tecnologias que fomentem o fortalecimento dessa área. Nessa linha de raciocínio, Carvalho et al (2006) comentam a importância na capacitação em pesquisa e desenvolvimento:

> A manutenção da soberania nacional implica, basicamente, na capacitação em pesquisa e no desenvolvi-

> mento dos recursos humanos para que eles sejam capazes de contribuir com soluções organizacionais e tecnológicas específicas. Às vezes, torna-se necessária a geração do conhecimento por meio de importação de "pacotes tecnológicos" a serem posteriormente "abertos", adaptados às necessidades da instituição e otimizados por "engenharia reversa".

A pesquisa e desenvolvimento dos recursos humanos no setor cibernético são imprescindíveis, nos dias atuais, para promover a proteção do Estado, da sociedade e dos setores estratégicos da economia, com o intuito de capacitá-los com soluções e tecnologias recentes. Isso demonstra o valor de expressar na END a preocupação em desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas críticas. Também preocupa-se com a estruturação de produção do conhecimento proveniente de fonte cibernética.

1.2 ESTRATÉGIA NACIONAL DE INTELIGÊNCIA

A Enint é um documento que fixa a Estratégia Nacional de Inteligência a ser adotada no Brasil, para a orientação estratégica decorrente da Política Nacional de Inteligência (PNI) e servindo de referência ao Plano Nacional de Inteligência. Além de consolidar conceitos, identifica os principais desafios para a Atividade de Inteligência de Estado, define eixos estruturantes e objetivos estratégicos, de modo a criar as melhores condições para que o país possa se antecipar às ameaças e usufruir das oportunidades existentes.

Seguindo a ideologia da END, a Enint também expressa sua preocupação com a segurança cibernética, pois faz parte do seu escopo estratégico. Assim, no desenvolvimento de seu ambiente estratégico, pode-se extrair da Enint (2017) a preocupação com a espionagem cibernética que cresce à medida que se eleva a utilização das ferramentas de TIC:

> Os inegáveis benefícios e facilidades trazidos pela utilização da tecnologia são, contudo, acompanhados de vulnerabilidades. Como consequência, o mundo enfrenta o crescimento da **espionagem cibernética**, inclusive com fins econômicos e científicos. Da mesma forma, outros riscos surgem com a evolução tecnológica: a automatização e a interconectividade dos sistemas de infraestruturas críticas, por exemplo, tornam possíveis sabotagens pela via cibernética. (grifos nossos).

A disseminação das ameaças cibernéticas provocou na intensificação das procuras por soluções que fossem capazes de aumentar o nível de segurança da informação, das comunicações e das infraestruturas críticas. De outro lado, há soluções de segurança, como os recursos criptográficos, que podem ser utilizados por grupos distintos dos interesses nacionais para a própria defesa.

É perceptível que a preocupação da Enint converge com a da END, elegendo os ataques cibernéticos como ameaças a serem observadas. Nesse ponto, é oportuno citar os conceitos de ameaça e de ataques cibernéticos dessa Estratégia. Consideram-se ameaças "aquelas que apresentam potencial capacidade de pôr em perigo a integridade da sociedade e do Estado e a segurança nacional" (BRASIL, 2017) e ataques cibernéticos

> ações deliberadas com o emprego de recursos de TIC para interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado, a exemplo daqueles pertencentes à infraestrutura crítica nacional. (BRASIL, 2017).

As oportunidades que o Brasil está inserido proporcionam uma potencial capacidade de posicionar o país em um outro patamar competitivo e auxiliam na promoção e na defesa dos interesses do Estado e da sociedade brasileira. Uma delas, de acordo com a Enint, é a Inteligência cibernética, que evidencia a importância de se ter o domínio das soluções tecnológicas mais avançadas para lidar com o espaço cibernético, porque isso proporciona vantagens significativas às nações. Nesse

ambiente cibernético de ameaças e oportunidades, países que se desenvolvem mais rapidamente se tornam mais aptos a alcançar os objetivos nacionais.

Após as oportunidades serem definidas, desafios foram identificados, como por exemplo: a maior utilização de tecnologia de ponta, em especial no campo cibernético. Haja vista a necessidade de investimento para a atualização constante dos recursos tecnológicos indispensáveis à Atividade de Inteligência, que potencializam a eficácia do seu desempenho. Principalmente no espaço cibernético, a identificação de oportunidades e a previsão de fatos possivelmente danosos aos interesses nacionais são decisivos para elevar a efetividade do combate às ameaças virtuais.

A Enint definiu 33 objetivos estratégicos para o desempenho eficaz da Atividade de Inteligência, considerando um intervalo de 5 anos, tomando como base os desafios estratégicos identificados. Esses objetivos não seguem uma ordem de prioridade, mas retratam o foco estratégico para o direcionamento de esforços e a sinalização dos resultados essenciais a serem atingidos pelo Sistema de Inteligência Brasileiro. Dentre os objetivos, há dois que estão alinhados diretamente com este estudo: ampliar a capacidade do Estado na obtenção de dados por meio da Inteligência Cibernética; e promover a qualificação técnica para proteção e exploração do campo cibernético.

O primeiro objetivo estratégico tem como propósito ampliar a capacidade do Estado na obtenção de dados por meio da Inteligência Cibernética. Isso demonstra a preocupação em desenvolver a aptidão de fazer e compreender como obter dados no ambiente virtual, contornando o crescente aprimoramento das TIC. O segundo objetivo se propõe à promoção da qualificação técnica para o desenvolvimento e a exploração do campo cibernético. Os dois objetivos apresentados estão interligados, pois com a qualificação técnica há a possibilidade de ampliar a capacidade de obter, proteger e explorar dados e informações no campo cibernético.

Dessa forma, oportuno comentar que a Enint segue uma linha de raciocínio similar a da END, tanto a Atividade de Inteligência quanto a Defesa Nacional propõem a qualificação como uma orientação na obtenção de capacidade técnica na atuação de defesa contra ataques cibernéticos.

2 ATAQUES CIBERNÉTICOS

Os ataques cibernéticos têm ocorrido em todo o mundo, afetando diversas organizações do setor público e do privado, indistintamente, como Fundo Monetário Internacional (FMI), Lockheed Martin, Google, Sony, Playstation, Hyundai, Credicard, Hospital do Câncer de Barretos, bancos privados, instituições públicas, tribunais de justiça de diversos estados, Ministério Público estaduais, Instituto Nacional de Seguridade Social - INSS, Petrobrás, ministérios, bancos públicos etc (CORRÊA; BOCCHINI, 2017).

Os ataques atingiram sites do governo bloqueando o acesso a dados e sistemas, obrigando o pagamento de resgate dos dados por meio de moedas digitais, como a bitcoin. Também alvo de ataques, estabelecimentos comerciais tiveram seus sites e sistemas invadidos por hackers, como o caso de 28 de junho de 2017, em que alguns dos hospitais que tratam pacientes com câncer foram invadidos e tiveram seus computadores paralisados, atrapalhando o tratamento de quimioterapia em algumas regiões do Brasil. Os ataques em equipamentos paralisaram atendimentos de emergência, adulterando exames e induzindo médicos a erros e até impedindo que pacientes fossem medicados.

O Brasil é considerado o principal foco de crimes virtuais no mundo, sendo o 6º no ranking de ataques cibernéticos. Em 2017, o Brasil foi alvo de aproximadamente 205 milhões de ataques no ambiente virtual e estatísticas apontam que o país perdeu cerca de 22 bilhões com esses ataques. Sobre o assunto, Cortez e Kubota (2013) comentam que:

No Brasil, esse fato também vem ganhando importância após uma série de intrusões e ataques cibernéticos a bancos e a sistemas de órgãos do Governo Federal. Esses ataques revelaram ao grande público a existência de ameaças que têm o potencial de comprometer o pleno funcionamento de infraestruturas críticas.

Esses ataques são ameaças identificadas tanto pelo Estado quanto pela sociedade, os quais devem ser combatidos. Por isso, a Defesa Nacional e a Inteligência de Estado previram em suas estratégias essa preocupação. Ambos trabalham com o objetivo de capacitarem seu corpo técnico para a salvaguarda de dados e informações em âmbito nacional, evitando altos prejuízos decorrentes de ataques cibernéticos.

CONCLUSÕES

Este trabalho teve como objetivo analisar o olhar dos órgãos que se preocupam com Segurança Cibernética, como a Defesa Nacional e a Inteligência de Estado, tendo em vista as vulnerabilidades digitais existentes. Os ataques cibernéticos estão cada vez mais crescentes e provocam prejuízos de larga escala, comprometendo as economias afetadas. Por isso, a importância de se estudar esse assunto.

A normatização da Defesa Nacional e da Inteligência de Estado quanto à defesa cibernética demonstra a preocupação de ambas no combate ao cibercrime, por meio da obtenção, proteção e exploração de dados e informações no campo cibernético. Ficou evidente que ambas as instituições trabalham seguindo a mesma linha de raciocínio, tendo em vista que em suas estratégias objetivam promover uma maior capacitação do seu corpo técnico sobre assuntos relacionados à “defesa cibernética”, possibilitando elevar a capacidade de atuação nos momentos de crise. Essa evidência foi obtida por meio da análise das Estratégias Nacional de Defesa e de Inteligência.

Pelo fato desse assunto ser constantemente debatido e os ataques acontecerem corriqueiramente, o que justifica a elevada importância da temática, indicamos como sugestão a continuidade deste estudo, com novos olhares, evidenciando o impacto econômico desses ataques para a nação, os possíveis prejuízos financeiros e se esses ataques geram efeitos no produto interno bruto brasileiro.

CYBER SECURITY: THE VIEW OF NATIONAL DEFENSE AND STATE INTELLIGENCE IN THE DIGITAL VULNERABILITY

Abstract. This article is about cyber security, a current paradigm that is generating a growing concern of public and private entities around the world. In the past the threats were, for the most part, visible and tangible. But with the advancement of communication and information technologies, this has changed. The current threats are invading corporate electronics systems, hampering their activities. Faced with this, there are concerns for a new form of security and protection against digital vulnerabilities: cyber security. Cyber security is a current and growing concern of several institutions, both public and private. The concern is latent and is already standardized in the public policies of public security institutions, as is evident in the National Strategies of Defense and National Intelligence. This article demonstrates this standardization and consequent concern, both in the Defense area and in the area of Intelligence. Also, there are cyber attacks that occurred in some public and private institutions. Concern for a new form of defense is needed for institutions working safely. How to safeguard the sites and systems of your institutions? Is it possible to defend against these types of attacks, or are we at the mercy of cyber attacks?

Keywords: Cyber security. Digital vulnerabilities. National defense. National Defense Strategy. National Intelligence Strategy.

REFERÊNCIAS

BRASIL. Agência Brasileira de Inteligência. **Plano Nacional de Inteligência**. Disponível em: <http://www.abin.gov.br/acesso-a-informacao/legislacao-de-inteligencia/coletanea-de-legislacao/politica-nacional-de-inteligencia/>. Acesso em: 29 maio 2018.

BRASIL. **Decreto sem nº**, de 15 de dezembro de 2017. Aprova a Estratégia Nacional de Inteligência.

BRASIL. **Decreto nº 8793**, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília: 2012.

CANONGIA, Claudia; MANDARINO JÚNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, v. 14, nº 29, p. 21-46, jul-dez 2009, 2009.

CARVALHO, Antônio Ramalho de Souza; MASCARENHAS, Carlos Cezar de; OLIVEIRA, Edson Aparecida de Araújo Querido. Ferramentas de disseminação do conhecimento em uma instituição de c,t&i de defesa nacional. **Revista de Gestão da Tecnologia e Sistemas de Informação**, Vol. 3, nº 2, 2006, p. 77-92.

CORRÊA, Douglas; BOCCHINI, Bruno. **Ataque hacker global afeta órgãos de governo e da justiça no Brasil**, em 12/05/2017. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-05/ataque-hacker-global-afeta-orgaos-de-governo-e-entidades-no-brasil>. Acesso em: 29 maio 2018.

CORTEZ, Igor Siqueira; KUBOTA, Luis Claudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. **Revista de Administração**, v. 48, n. 4, p. 757-769, out./nov./dez. 2013.

MANDARINO JÚNIOR, Raphael. **Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro.** Monografia aprovada no Curso de Especialização em Gestão da Segurança da Informação e Comunicações. Brasília: Universidade de Brasília - UnB/ Departamento de Ciência da Computação, jun. 2009. p. 29.

O autor é mestrando em Economia da Defesa pela Universidade de Brasília – UnB, pós-graduado em Controladoria Governamental e em Gestão Pública pelo Instituto Federal de Brasília - IFB e graduado em Ciências Contábeis pela Universidade Federal de Sergipe - UFS. Possui cursos na área de Orçamento Público, Contabilidade, Administração, Inteligência e Fotografia. Atualmente, exerce a função de agente técnico em órgão do Gabinete de Segurança Institucional (GSI/PR). Já lecionou em cursos de nível técnico e superior as matérias de Contabilidade, Custos no Setor Público, Controladoria, Administração Financeira, Legislação Trabalhista, Gestão Bancária, Lei de Responsabilidade Fiscal e Ética Profissional. Pode ser contatado pelo e-mail prof.alexsandrobarreto@gmail.com.