O Boletim de Conjuntura (BOCA) publica ensaios, artigos de revisão, artigos teóricos e empíricos, resenhas e vídeos relacionados às temáticas de políticas públicas.

O periódico tem como escopo a publicação de trabalhos inéditos e originais, nacionais ou internacionais que versem sobre Políticas Públicas, resultantes de pesquisas científicas e reflexões teóricas e empíricas.

Esta revista oferece acesso livre imediato ao seu conteúdo, seguindo o princípio de que disponibilizar gratuitamente o conhecimento científico ao público proporciona maior democratizacão mundial do conhecimento.

BOLETIM DE CONJUNTURA

BOCA

Ano V | Volume 13 | Nº 39 | Boa Vista | 2023

http://www.ioles.com.br/boca

ISSN: 2675-1488

https://doi.org/10.5281/zenodo.7699102

BOLETIM DE CONJUNTURA

www.ioles.com.br/boca

JUSTIÇA DIGITAL E GUERRA CIBERNÉTICA: UM ATAQUE CRACKER AO PODER JUDICIÁRIO BRASILEIRO AUTORIZARIA O USO DA FORÇA MILITAR EM LEGÍTIMA DEFESA?

José Paes de Santana[1]

Roberto Luis Luchi Demo[2]

Resumo

O presente artigo discorrerá sobre o tratamento que poderá ser dado pelo Brasil, na hipótese de um ataque causado por crackers, que possa ser atribuído a outro Estado, e que neutralize o funcionamento da infraestrutura cibernética do Poder Judiciário brasileiro. Este artigo utilizará da metodologia de pesquisa bibliográfica, feita por meio de revisão de literatura em artigos especializados de plataformas científicas e de livros sobre o assunto, levantando aspectos conceituais e doutrinários, especialmente voltados para as tecnologias da informação, bem como de conceitos doutrinários do Direito Internacional Público. Ao longo do desenvolvimento deste trabalho se buscarão analisar, também, dados legais e fontes do Direito que respondam à pergunta do problema de pesquisa, sobre a justificativa ou não do uso de força militar, em resposta a esse tipo de ataque ao Poder Judiciário brasileiro. Esperamos, ao discorrer sobre essa pergunta de pesquisa, que levantemos dados tanto de importância acadêmica, quanto de importância para o fortalecimento do respeito mútuo entre os sujeitos de Direito Internacional, na proteção de sua infraestrutura cibernética dedicada às questões de Estado.

Palavras Chave: Ataque Cracker. Infraestrutura Crítica. Legítima Defesa. Uso da Força Militar.

Abstract

This article will discuss the treatment that may be given by Brazil, in the event of an attack caused by crackers, which may be attributed to another State, and which neutralizes the functioning of the cybernetic infrastructure of the Brazilian Judiciary. This article will use the methodology of bibliographic research, carried out through a literature review in specialized articles on scientific platforms and books on the subject, raising conceptual and doctrinal aspects, especially focused on information technologies, as well as doctrinal concepts of Law Public International. Throughout the development of this work, we will also seek to analyze legal data and sources of law that answer the question of the research problem, on the justification or not of the use of military force, in response to this type of attack on the Brazilian Judiciary. We hope, by discussing this research question, that we will raise data both of academic importance and of importance for strengthening mutual respect between subjects of International Law, in the protection of their cybernetic infrastructure dedicated to State issues.

Keywords: Cracker Attack. Critical Infrastructure. Self-Defence. Use of Military Force.

INTRODUÇÃO

Hodiernamente, além dos avanços tecnológicos, observamos, segundo Oliveira (2021), a integração na sociedade, dessa tecnologia subjacente, conectando as pessoas em rede e formando uma sociedade indissociável das tecnologias da informação. É uma verdadeira era digital que alcança as mais

[1] Professor do Centro Universitário de Desenvolvimento do Centro Oeste (UNIDESC). Doutor *Honoris Causa* pela Emil Brunner World University (EBWU). Doutorando pelo Instituto Brasiliense de Direito Público (IDP). E-mail: paesdireito1@gmail.com

[2] Magistrado da Justiça Federal de 1º Grau em Salvador (BA). Doutorando em Direito Constitucional pelo Instituto Brasiliense de Direito Público (IDP). E-mail: roberto.demo@trf1.jus.br

diversas manifestações das pessoas, tais como a forma de se comunicar, de negociar, de estudar, de trabalhar, de lazer, entre outros espaços da vida humana.

Para além dessas atividades, a tecnologia atualmente também faz parte, inclusive, das atividades militares e dos conflitos armados.

No Brasil, o Poder Judiciário brasileiro é considerado um dos mais avançados em termos de digitalização e de uso da tecnologia da informação. Consoante previsão da Organização do Tratado do Atlântico Norte (OTAN), na próxima década, os conflitos cibernéticos estarão entre as mais prováveis ameaças não convencionais, o que desperta preocupação quanto à proteção da infraestrutura cibernética do Poder Judiciário brasileiro.

Nesse sentido se indaga se essa infraestrutura cibernética pode ser considerada área prioritária da infraestrutura crítica brasileira e quais os limites para sua defesa, tendo em vista que pesquisadores como Barbosa (2018) admitem que um ataque contra uma infraestrutura crítica de um país membro da OTAN pode gerar uma resposta militar. Nas palavras de seu Secretário-geral atual, Jens Stoltenberg, contudo, tal ataque ensejaria uma resposta "firme e unida" (DIÁRIO DE NOTÍCIAS, 2022), mas ante as relações de poder que envolvem os países soberanos, chegar a uma resposta bélica pode ter efeitos irreparáveis.

Isso decorre obviamente da relação de direitos e deveres existentes entre os países soberanos, especialmente a de respeito mútuo, e ao fato de que a tecnologia hoje permeia todos os espaços da existência humana, o que traz implicações para as questões relacionadas entre Defesa Nacional e Segurança Pública, de modo que

> A Defesa Nacional, sempre que pensada por pessoas não especializadas, e não ligadas à área bélica, tende a voltar-se prioritariamente para as ações militares, desempenhadas pelas Forças Armadas. No entanto, para garantir a defesa de um país contra ações adversas estrangeiras, ou mesmo forças irregulares internas, são necessárias ações complexas muito além do emprego militar. (ROCHA, 2019, p. 3)

Nesse contexto, é preciso coadunar "resposta militar" com "resposta firme e unida" e procurar outros desfechos para as questões de segurança pública, que não sigam necessariamente os mesmos caminhos de uma resposta armada em se tratando de defesa nacional, de modo que o objetivo deste trabalho é indagar se um ataque cibernético que paralise o funcionamento do Poder Judiciário brasileiro autoriza o uso da força pelo Estado brasileiro em legítima defesa.

Desse modo procuraremos responder essa pergunta de pesquisa, dada sua relevância para o conteúdo da *soft law*, cujas preocupações já estiveram centradas no meio ambiente, o que continua despertando relevância, mas hoje devem enfocar também as questões da cibernética e da informática.

Para isso levaremos em conta as fontes do Direito Internacional, tanto as reais, quanto as formais, compreendidas estas, enquanto costumes e tratados, e aquelas, enquanto os princípios gerais do direito.

Faremos uma abordagem conceitual e dialogal entre os novos direitos que despontam à medida que novas tecnologias surgem, com o fito de responder à pergunta de pesquisa e alcançar a justificativa do artigo que é sua utilidade social e política, na compreensão deste fenômeno que é de grande relevância, especialmente no que diz respeito à segurança jurídica e à manutenção da ordem interna e do respeito mútuo entre as nações soberanas.

Além disso, apresentaremos, ao longo deste artigo, o conceito de infraestrutura crítica para o ordenamento jurídico brasileiro e sua segurança nacional, bem como se a infraestrutura cibernética do Poder Judiciário Brasileiro, pertence ou não a esse contexto de infraestrutura crítica para o Brasil.

Outro ponto de vista que precisa ser abordado é a origem do ataque, na identificação do agressor, especialmente devendo-se levar em conta se este for proveniente de uma nação soberana ou de grupos alheios aos interesses de determinada nação, vindo esse grupo a assumir a autoria desse ataque ofensivo ao Brasil.

OS SUJEITOS DE DIREITO INTERNACIONAL PÚBLICO

É cediço que sujeito de direito é toda pessoa capaz de contrair obrigações, adquirindo direitos em determinado contexto jurídico, e no caso do Direito Internacional Público poderemos, ora nos referirmos ao plano interno e, ora nos referirmos ao plano externo, o que no nosso caso é bem pertinente, tendo em vista que vamos abordar uma possível ofensiva sofrida pelo Estado brasileiro, proveniente de um ataque *cracker*, que possa ser atribuído a outro Estado, e que neutralize o funcionamento da infraestrutura cibernética do Poder Judiciário brasileiro.

Por esse motivo é pertinente abalizar quem são esses possíveis Sujeitos de Direito para o Direito Internacional, que para Cretella Neto (2019), apesar de suas características peculiares, especialmente dada a inexistência de um parlamento internacional, podem ser quaisquer sujeitos de direitos contraentes de direitos e obrigações na ordem internacional, tendo em vista que na ordem internacional a norma emana principalmente de tratados, costumes internacionais e decisões de tribunais internacionais, lembrando todavia, que nessa ordem inexiste um *gendarme internacional* que a todos subordina de forma coercitiva.

Muito embora não haja este força coercitiva ou órgão de coerção entre as nações, pois estas somente participam de acordos multilaterais abertos, por deliberação de seus representantes internos, na ordem internacional, existem órgãos supranacionais como a Organização das Nações Unidas (ONU) e

consolidações de normas de direitos internacional, como a Convenção de Viena sobre o Direito dos Tratados, que se estabelece como "norma imperativa de direito" (BRASIL, 2009), conforme dispõe seu artigo 53, além de sua hierarquia subjacente, de superioridade, aos acordos bilaterais ou mesmo plurilaterais fechados, expressa em seu artigo 64.

Retomando a questão dos Sujeitos de Direito na ordem internacional, há quem sustente pela doutrina clássica, ainda segundo Cretella Neto (2019) que somente os "[...] Estados como membros da comunidade internacional" poderiam ser sujeitos de Direito Internacional, mas "[...] em sentido diametralmente oposto, a escola sociológica sustenta que, apenas indivíduos, poderiam ser sujeitos de Direito Internacional," de modo que a possibilidade de sujeitos de direito, díspares na ordem internacional é perfeitamente possível, especialmente no caso de um hipotético ataque *cracker*, como é o caso da hipótese aqui levantada.

Sendo assim, neste artigo utilizaremos a classificação de Mazzuoli (2016), para quem podem ser sujeitos de Direito Internacional, além dos Estados e dos indivíduos particularmente considerados, também as coletividades interestaduais e as não estaduais.

A pertinência em adotar essa classificação, surge do fato de que certamente um grupo de *crackers*, ou um *cracker* individualmente, não teria capacidade para firmar tratado internacional, todavia suas ações poderiam ser discutidas no plano externo como ações de repercussão internacional e questionáveis desse mesmo ponto de vista, como acontece com os ataques do grupo *Jihad*, por exemplo, o conceito de sujeitos de direito internacional público não deve ser engessados, tampouco tratados como "[...] taxativos ou exaustivos em si mesmos," pois se assim o fizéssemos, "[...] a União Europeia ou o Mercosul, por exemplo, jamais poderiam celebrar tratados internacionais, porquanto não são enquadrados no conceito de Estado" (FERNANDES, 2021).

Essa abordagem sobre sujeitos de direito internacional, contudo não é nosso foco principal, mas é assunto que se faz necessário abordar, porque orbitaremos em seu redor ao longo da discussão em pauta, de modo que o referido conceito poderá, a depender da situação, ser estendido, até mesmo a uma empresa, além de outras organizações não estatais, mas em tese, o ataque que se imagina inicialmente, deve ser um ataque produzido por um ato unilateral de um Estado, e a partir de então, analisaremos como esses sujeitos de direito internacional resolverão suas controvérsias.

Da solução das controvérsias entre os sujeitos de direito internacional

Na ordem internacional, as controvérsias deverão ser resolvidas pacificamente, como alude o artigo 33, do Estatuto da Corte Internacional de Justiça (CIJ), ratificado pelo Brasil por intermédio do Decreto nº 19.841, de 22 de outubro de 1945, que prevê *in verbis:*

> Artigo 33. 1. As partes em uma controvérsia, que possa vir a constituir uma ameaça à paz e à segurança internacionais, procurarão, **antes de tudo, chegar a uma solução por negociação, inquérito, mediação, conciliação, arbitragem, solução judicial, recurso a entidades ou acordos regionais, ou a qualquer outro meio pacífico à sua escolha**.
> 2. O Conselho de Segurança convidará, quando julgar necessário, as referidas partes a resolver, por tais meios, suas controvérsias. (BRASIL, 1945) [destaque nosso]

Nota-se no texto retromencionado, que na ordem internacional, os Estados devem evitar ter na guerra um meio usual de resolução de disputas internacionais, preferindo soluções pacíficas.

A solução pacífica dos conflitos, assim na ordem internacional, nesse contexto, como na ordem interna, para o Brasil, é o ideal a ser alcançado, pois a Constituição Federal de 1988 – CF/88, também ressaltou sua importância, tanto no seu preâmbulo, como no seu artigo 4º, VII, enquanto princípio que rege a República Federativa do Brasil, em suas relações internacionais.

O Estatuto da CIJ, de contínuo, ainda ressaltou que se as partes em controvérsia não chegarem ao pleno acordo, pelos mecanismos efetivos de resolução de controvérsias, outrora chamados de meios alternativos de solução de conflitos, descritos no artigo supracitado, estas deverão apresentar o litígio ao Conselho de Segurança, que poderá, em qualquer fase da demanda, recomendar outra alternativa de solução do litígio, de modo que a ideia é sempre a da solução pacífica das controvérsias.

Desse modo, o Conselho de Segurança, analisará a gravidade dos atos unilaterais do Estado agressor para buscar uma solução não beligerante, especialmente quando julgar que a continuação dessa controvérsia poderá ser uma ameaça à paz e à segurança internacionais, recomendando os procedimentos já mencionados no artigo 33 do Estatuto da CIJ, ou outros que achar apropriados.

Atos unilaterais dos Estados no contexto das relações internacionais

A abordagem dos atos unilaterais, se faz necessária, pois, quando o Estatuto da CIJ, concluiu o capítulo da solução pacífica das controvérsias, não os mencionou, no contexto das fontes do Direito Internacional Público, no artigo 38 do Estatuto, o que segundo Mazzuoli (2009, p. 123-125), o seriam, razão por que assim como nos atos negociais, um Estado não poderia impor sua vontade a outro, inclusive o silêncio, tampouco poderia fazê-lo no contexto das relações da política internacional. Por isso" [...] a regência do seu valor obrigacional deve ser determinada pela ordem internacional, e não pela ordem jurídica do Estado que o manifesta." Isso deixa claro a necessidade e a importância da mediação do Conselho de Segurança como representante da Ordem Internacional na manutenção da ordem jurídica e da paz mundial, preferindo sempre a solução pacífica, em detrimento da *ultima ratio* belicosa.

Por esta razão, o Conselho de Segurança, nas conformidades do artigo 41 do Dec. 19.841/45,

> **[...] decidirá** sobre as medidas que, **sem envolver o emprego de forças armadas, deverão ser tomadas para tornar efetivas suas decisões e poderá convidar os Membros das Nações Unidas a aplicarem tais medidas.** Estas poderão incluir a interrupção completa ou parcial das relações econômicas, dos meios de comunicação ferroviários, marítimos, aéreos, postais, telegráficos, radiofônicos, ou de outra qualquer espécie e o rompimento das relações diplomáticas. (BRASIL, 1945) [destaque nosso]

Como se pode ver, e o mesmo decreto explica de contínuo, *a ideia é evitar o emprego de forças armadas*, sempre com a utilização de meios menos gravosos que sua utilização, e se no caso de todos os esforços implementados e até aqui explicitados, isso não surtir efeito, o artigo 42 do mesmo Decreto, ainda prevê, que mesmo as ações iniciais das forças aéreas, navais e terrestres, inicialmente poderão compreender apenas "[...] demonstrações, bloqueios e outras operações, por parte das forças aéreas, navais ou terrestres dos Membros das Nações Unidas".

Dessa forma se pode ver quão significativa é a utilização de forças armadas no combate bélico e, de um modo geral, a previsão é sempre de medidas preventivas, antes das medidas coercitivas, como prevê o artigo 50 do decreto em pauta, que aponta os esforços do Conselho de Segurança no sentido de evitar a utilização de forças armadas em um ataque por ato unilateral de um Estado a outro.

Numa situação de ato unilateral de um Estado que afronte a outro em sua soberania, é preciso analisar se ocorrem, entre outras, três situações que Carl Von Clausewitz (1790-1831) analisou no seu conceito de guerra, chamando-as de princípios, no entendimento de que "´[...] a guerra é a continuação da política por outros meios´, quais sejam: se além de **ser político**, o ato **é violento**, e tem o **propósito de submeter o adversário em sua volição**" (FERNANDES, 2022) [destaque nosso].

Presentes as situações acima descritas, o que caracterizaria um ato de guerra para Clausewitz (1790 - 1831), hoje se admite que,

> [...] Uma guerra cibernética pode vir a ocorrer com a constatação de ataques cibernéticos coordenados, efetuados com propósitos políticos e militares, **que venham a afetar as infraestruturas críticas**, a população ou os organismos de defesa de uma nação, ou que visem atacar diretamente a soberania de um Estado. (PINTO; GRASSI, 2020, p. 124) [destaque nosso].

Nesse contexto, é preciso saber se nosso hipotético ataque *cracker*, ao afetar ou neutralizar o funcionamento da infraestrutura cibernética do Poder Judiciário brasileiro, estaria afetando uma infraestrutura crítica brasileira no contexto da segurança nacional, pelo que passaremos a abordar a pertinência da relatada infraestrutura cibernética do Poder Judiciário à infraestrutura crítica brasileira, no contexto da Segurança Nacional.

INFRAESTRUTURA CRÍTICA BRASILEIRA NO CONTEXTO DA SEGURANÇA NACIONAL

O conceito de infraestrutura crítica e as áreas que prioritariamente a ela se relacionam, são tratados sistematicamente no Brasil, pela primeira vez que se teve notícia na busca de fontes primárias para a confecção desse artigo, na Portaria nº 2, de 8 de fevereiro de 2008, do Gabinete de Segurança Institucional da Presidência da República – Port. GSIPR nº 2/2008, que assim a definiu em seus artigos 2º e 3º, *in verbis:*

> Art. 2° Consideram-se IEC as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, **internacional ou à segurança nacional**.
>
> Art. 3º São consideradas áreas prioritárias de Infraestrutura críticas, sem prejuízo de outras que vierem a ser definidas: I - Energia; II - **Transporte;** III - Água; IV - Telecomunicações; e V - Finanças. (BRASIL, 2008) [destaque nosso].

Observa-se que o conceito de infraestrutura crítica diz respeito a impacto social, econômico, político, de caráter internacional ou ligado à segurança nacional, enquanto suas áreas de pertinência, estão relacionados aos serviços públicos como energia, transporte, água, telecomunicações e finanças, que aparentam natureza típica de serviços de Estado ou aqueles associados à natureza jurídica privada, como dispôs a CF/88, em seu artigo 173, § 1º, II, pelo seu pertencimento, também à ordem econômica nacional.

Desse modo situações de cunho privado e que muito embora possam estar ligadas à segurança pública, não podem se confundir com serviços de natureza típica de Estado, ligados à segurança nacional com repercussão internacional, pois se assim o fosse se correria o risco de confundir *infraestrutura crítica* com *atividades de natureza essencial* ao Estado, conforme menciona o artigo 10 da lei 7.783/89, que assim as definiu:

> Art. 10 São considerados serviços ou atividades essenciais:
> I - tratamento e abastecimento de água; produção e distribuição de energia elétrica, gás e combustíveis;
> II - assistência médica e hospitalar;
> III - distribuição e comercialização de medicamentos e alimentos;
> IV - funerários;
> V - transporte coletivo;
> VI - captação e tratamento de esgoto e lixo;
> VII - telecomunicações;
> VIII - guarda, uso e controle de substâncias radioativas, equipamentos e materiais nucleares;
> IX - processamento de dados ligados a serviços essenciais;
> ~~X - controle de tráfego aéreo;~~

> ~~X - controle de tráfego aéreo e navegação aérea; e (Redação dada pela Medida Provisória nº 866, de 2018) (Revogada pela Medida Provisória nº 883, de 2019) (Vigência Encerrada)~~
> ~~X - controle de tráfego aéreo;~~
> ~~X - controle de tráfego aéreo e navegação aérea; e (Redação dada pela Medida Provisória nº 866, de 2018)~~
> X - controle de tráfego aéreo e navegação aérea; (Redação dada pela Lei nº 13.903, de 2019)
> XI compensação bancária.
> XII - atividades médico-periciais relacionadas com o regime geral de previdência social e a assistência social; (Incluído pela Lei nº 13.846, de 2019)
> XIII - atividades médico-periciais relacionadas com a caracterização do impedimento físico, mental, intelectual ou sensorial da pessoa com deficiência, por meio da integração de equipes multiprofissionais e interdisciplinares, para fins de reconhecimento de direitos previstos em lei, em especial na Lei nº 13.146, de 6 de julho de 2015 (Estatuto da Pessoa com Deficiência); e (Incluído pela Lei nº 13.846, de 2019)
> XIV - outras prestações médico-periciais da carreira de Perito Médico Federal indispensáveis ao atendimento das necessidades inadiáveis da comunidade. (Incluído pela Lei nº 13.846, de 2019)
> ~~XV - atividades portuárias. (Incluído pela Medida Provisória nº 945, de 2020).~~
> XV - atividades portuárias. (Incluído pela Lei nº 14.047, de 2020) (BRASIL, 1989).

Veja-se que o próprio Poder Legislativo tem sido inconstante na definição das atividades de natureza essencial ao Estado, quando seu caráter privado se confunde com os serviços de natureza pública ou dele se aproxima, especialmente nas questões relativas a *tráfego aéreo* e *atividades portuárias*, sendo as que mais sofreram alteração legislativa, como identificado na referência retromencionada, pois estas, apesar de aparecerem como atividades de natureza essencial de Estado, podem também estar relacionadas à infraestrutura crítica, dada sua ligação à ordem econômica estatal e ao transporte, como se observa no art. 3º, II, da Port. GSIPR nº 2/2008, que mencionou a área de finanças como uma das prioritárias nas infraestruturas críticas.

Isso corrobora com os dizeres de Moteff *et al.* (2003), quando afirma que, o que constitui o conceito de infraestrutura crítica decorre de certa fluidez que pode "complicar a formulação de políticas e ações" governamentais.

Nesse contexto de semelhanças e dessemelhança, discute-se a seguir a pertinência da infraestrutura cibernética do Poder Judiciário à infraestrutura crítica brasileira.

INFRAESTRUTURA CIBERNÉTICA DO PODER JUDICIÁRIO E SUA PERTINÊNCIA À INFRAESTRUTURA CRÍTICA BRASILEIRA

A infraestrutura cibernética do Poder Judiciário brasileiro, apesar de sua importância significativa, e de estarem relacionadas à era digital, não se incluem taxativamente nos dispositivos que conceituam legalmente infraestrutura crítica, muito embora pudessem ser incluídas em áreas "[...] outras que vierem a ser definidas," conforme deixou em aberto a Port. GSIPR nº 2/2008, em seu artigo 3º.

Todavia, o legislador não fez ainda, pelo menos até o momento, menção expressa de que essa infraestrutura cibernética do Poder Judiciário componha o conceito de infraestrutura crítica do Estado Brasileiro.

Se observarmos a evolução do conceito legal de infraestrutura crítica de Estado, que depois da Port. GSIPR nº 2/2008, passa a ser mencionada pelo Decreto 8.793, de 29 de julho, de 2016 – Dec. 8.793/2016, este também não contemplou a inclusão da infraestrutura do Poder Judiciário no conceito de infraestrutura crítica, todavia fez menções que poderiam perfeitamente trazer uma interpretação extensiva do conceito, ao abordar os chamados temas globais e transnacionais, no contexto da complexidade global, que:

> [...] É necessário, ainda, **ampliar** o desenvolvimento de ações de proteção dos conhecimentos sensíveis e da **infraestrutura crítica nacional**, bem como **contrapor-se ao surgimento de ameaças representadas tanto por serviços de Inteligência**, quanto por grupos de interesse, organizações ou indivíduos que atuem de forma adversa aos **interesses estratégicos nacionais.** (BRASIL, 2016) [destaque nosso].

Especialmente se levarmos em conta que a infraestrutura cibernética do Poder judiciário é uma área digital de interesse estratégico nacional, especialmente porque o Programa Justiça 4.0, no Brasil, em 2022, é integrado por diversos projetos de Inteligências Artificiais (IA), mas essa não-inclusão parece estar ligada ao fato de que seu fito é a entrega da prestação jurisdicional e não o aspecto econômico diretamente, embora haja aspecto social no seu bojo. (BRASIL, 2021; 2022)

O Dec. 8.793/2016, ainda fez menções importantes a ações de sabotagem à infraestrutura crítica nacional, como veremos a seguir.

Ataque c*racker* a infraestruturas críticas brasileiras

Um ataque cracker à infraestrutura crítica brasileira, ou a parte dela, foi abordado pelo decreto em comento, e tratado como sabotagem, tendo em vista que foi por isso que nos referimos desde o início a um ataque *cracker* e não a um ataque *hacker*, levando em conta que o primeiro é uma espécie de sabotagem de sistema de segurança de forma ilegal, e o segundo causa modificações em nível de *software* e *hardware*, mas pode ter o intuito de melhorar *softwares* de forma legal (CASTRO, CHAMON, 1998, p. 258, 391).

Nesse caso, o ataque *cracker* estaria equiparado a uma ação de sabotagem com o intuito de comprometer ou inutilizar, parcial ou definitivamente dados ou sistemas de dados de infraestrutura crítica, conforme alude o Decreto 8.793/2016, ao mencionar que

> 6.2 Sabotagem
> É a ação deliberada, com efeitos físicos, materiais ou psicológicos, que visa a destruir, danificar, comprometer ou inutilizar, total ou parcialmente, definitiva ou temporariamente, dados ou conhecimentos; ferramentas; materiais; matérias-primas; equipamentos; cadeias produtivas; instalações ou sistemas logísticos, sobretudo aqueles necessários ao funcionamento da infraestrutura crítica do País, com o objetivo de suspender ou paralisar o trabalho ou a capacidade de satisfação das necessidades gerais, essenciais e impreteríveis do Estado ou da população (BRASIL, 2016).

O referido decreto, inclusive, associa a sabotagem a uma ação que não só prejudica interesses do Estado, no seu âmbito secundário, mas que também afeta a coletividade, no âmbito primário do interesse público, referindo-se à população civil, e criando mais uma questão complexa entre defesa nacional e segurança pública, como já aludido neste artigo, sendo a primeira afeta às Forças Armadas no contexto nacional, mas também internacional, e a segunda mais voltada a políticas econômicas, sociais, educacionais, mais voltadas a defesa civil interna, "[...] muitas das quais não implicam qualquer envolvimento das Forças Armadas" (ROCHA, 2019, p. 5).

O mesmo Decreto 8.793/2016 ainda se referiu diretamente a ataque cibernético à infraestrutura crítica nacional, ao mencionar que

> [...] 6.5 Ataques cibernéticos
>
> Referem-se a ações deliberadas com o emprego de recursos da tecnologia da informação e comunicações que visem a 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, 2016).

Ataques dessa natureza foram verificados na atual guerra entre Rússia e Ucrânia, mas se trata de uma situação bem avançada da guerra, diferentemente de uma resposta inicial, como aqui foi aludido por hipótese, apesar de que a Rússia, eufemisticamente a tem chamado de "operação militar," ofuscando sua tendência expansionista (VITTE; MORAES 2022).

Trata-se de uma guerra onde,

> [...] Além de tanques e mísseis, os hackers agora são parte integral de ofensivas que visam desmantelar a infraestrutura de um país e gerar choques de efeito psicológico na população. (SUZUKI, 2022).

Apesar de que o conceito de infraestrutura crítica, como política pública de Defesa Nacional, ainda evolui com o Decreto 9.819/2019, e com a Lei 13.844/2019, não os abordaremos aqui, pois nossa tônica não é necessariamente a das políticas públicas de Defesa Nacional, razão porque, nos voltaremos a discutir, a seguir, a possibilidade ou não, de uso das Forças Armadas como resposta a um ataque cibernético proveniente de origem estrangeira.

Possibilidade do uso das forças Armadas como resposta a um ataque cibernético

Já tendo abordado a evolução legislativa do conceito de infraestrutura crítica e suas áreas de interesse prioritário, verificamos que a infraestrutura cibernética do Poder Judiciário não se enquadra como infraestrutura crítica do Estado Brasileiro.

Vimos também posicionamentos doutrinários que admitem a possibilidade de resposta armada em caso de ataque cibernético ou guerra cibernética à infraestrutura crítica de um país (OLIVEIRA, 2021; PINTO; GRASSI, 2020, p. 124), como no caso da dos países da OTAN, mas ali vimos que seu atual Secretário-Geral, utilizou a expressão, resposta "firme e unida," que não traz em si um conceito claro de o que seria tal resposta.

Ao percorrermos o Estatuto da CIJ, vimos que este sempre pugna por uma solução pacífica dos conflitos como resposta aos atos unilaterais dos sujeitos de direito no Direito Internacional Público, e o Brasil em sua CF/88 apresenta o mesmo intuito nas suas relações internacionais.

Observamos também, numa citação de Suzuki (2022), que a Rússia, além de artefatos bélicos, vem utilizando contra a Ucrânia ataques ciberataques, comprometendo inclusive a segurança e o bem-estar da população civil, o que afeta diretamente a economia desse país, tendo em vista que "o bem-estar de seus cidadãos depende do funcionamento contínuo e confiável de seus sistemas de infraestrutura" (OUYANG, 2014, p. 43), no que tange ao comprometimento de sua infraestrutura crítica, pois,

> [...] Enquanto a entrada das tropas russas em território ucraniano começou em 24 de fevereiro deste ano, uma onda de ataques cibernéticos direcionados a infraestruturas críticas foram detectados alguns dias antes e, poucas horas após a entrada das forças russas, uma onda de ataques DDoS derrubou vários sites do governo e de bancos ucranianos (SOL, 2022, p. 1).

Esses ataques DDoS correspondem à "navegação de serviço distribuída", indisponibilizando websites ou tornando-os incapazes de operarem regularmente, ainda segundo Sol (2022), que apresenta também um conceito de infraestrutura crítica um pouco mais abrangente que o conceito legal, ao mencionar que

> A infraestrutura crítica de um país é definida como os sistemas, tanto digitais quanto físicos, que fornecem serviços essenciais à sociedade e que, se afetados por um ataque cibernético, podem ter um sério impacto sobre a segurança, economia, política, energia, saúde, comunicações, transportes, entre outros (SOL, 2022).

De qualquer modo um ciberataque deveria ser combatido pacificamente pela prática da cibersegurança, no sentido de proteger dados e sistemas de dados, computadores e servidores, no enfrentamento de ataques maliciosos, levando-se em conta que mesmo na solução coercitiva das

controvérsias, pela retorsão, o Estado ofendido deveria aplicar ao agressor "[...] as mesmas ou os mesmos processos que este empregou ou emprega contra ele [...]" (SILVA; CASELLA, 2012, p. 866).

Desse modo, não nos pareceria plausível que a resposta inicial, antes de quaisquer tratativas, fosse o ataque armado, pois ao longo desta discussão, observou-se que o Brasil, tendo como leme a CF/88 e vários tratados ratificados, está comprometido com a solução pacífica das controvérsias, assim na ordem interna, como em âmbito internacional.

CONSIDERAÇÕES FINAIS

Após realizar este estudo, se espera que os objetivos propostos tenham sido alcançados e que as hipóteses levantadas, bem como o problema de pesquisa tenha sido enfrentado em sua inteireza.

Espera-se que esta discussão colabore de algum modo com a questão do ciberataques e sua resposta, todavia se observou que uma resposta armada, inicialmente, seria prematura, desproporcional e de consequências irreparáveis, inclusive afrontando o respeito mútuo entre os sujeitos de direito, no direito Internacional Público.

Apesar de haver na doutrina posicionamentos aparentemente diversos, se os examinarmos com profundidade, veremos que um ciberataque não corresponde a um ato de guerra, como aqui foi discutido sob a perspectiva de estudiosos da arte da guerra, e que apesar de nos dias de hoje termos uma situação de guerra em curso, com a utilização de ataques maliciosos às infraestruturas críticas entre os conflitantes, é possível observar que eles ocorreram no curso do combate e não como uma resposta inicial.

Observa-se também que não se tem notícia de que uma guerra cibernética propriamente dita já tenha havido, mas o que há, como no caso entre Rússia e Ucrânia, é o incremento de inteligência digital a serviço da guerra, que, todavia, continua sendo política.

Não encontramos uma legislação ou convenção de órgãos supranacionais que tratasse especificamente do assunto e, enquanto novas tecnologias surgem, também novos direitos aparecem, e se espera que, com isso, novas disciplinas das relações internacionais também surjam, ou que enquanto isso, os princípios norteadores do Direito Internacional Público corroborem na interpretação da norma desse direito, no sentido de trazerem proteção e respeito mútuo entre os sujeitos de direito internacional, a exemplo da Cláusula Martens, da Convenção da Haia de 1907.

Como a pesquisa foi apenas qualitativa e bibliográfica, espera-se que novos estudos complementem nossas ideias aqui esboçadas e que a construção de novos direitos que emergem das inovações tecnológicas possam ser compreendidos de forma uníssona, levando-se em conta as fontes do

Direito Internacional, tanto as reais, quanto as formais, dos princípios gerais do direito, aos costumes e tratados, passando pela jurisprudência, doutrina, analogia, equidade, atos unilaterais do Estado, decisões de Organizações Internacionais, *jus cogens* e *soft law*.

REFERÊNCIAS

ALVES-MAZZOTTI, A. J.; GEWANDSZNAJDER, F. **O método nas ciências naturais e sociais**: pesquisa quantitativa e qualitativa. São Paulo: Editora Pioneira, 1998.

BARBOSA, M. S. "A guerra cibernética no ambiente marítimo". **Revista Marítima Brasileira**, n. 138, 2018.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Planalto, 1988. Disponível em: <www.planalto.gov.br>. Acesso em: 10/12/2022.

BRASIL. **Decreto n. 7.030, de 14 de dezembro de 2009.** Brasília: Planalto, 2009. Disponível em: <www.planalto.gov.br>. Acesso em: 10/12/2022.

BRASIL. **Decreto n. 8.793, de 29 de junho de 2016**. Brasília: Planalto, 2016. Disponível em: <www.planalto.gov.br>. Acesso em: 10/12/2022.

BRASIL. **Decreto n. 9.819, de 3 de junho de 2019**. Brasília: Planalto, 2019. Disponível em: <www.planalto.gov.br>. Acesso em: 10/12/2022.

BRASIL. **Decreto n. 19.841. de 22 de outubro de 1945**. Rio de Janeiro: Congresso Nacional, 1945. Disponível em: <www.planalto.gov.br>. Acesso em: 10/12/2022.

BRASIL. **Justiça em números**. Brasília: Conselho Nacional de Justiça, 2021. Disponível em: <www.cnj.jus.br>. Acesso em: 10/12/2022.

BRASIL. **Justiça em números**. Brasília: Conselho Nacional de Justiça, 2022. Disponível em: <www.cnj.jus.br>. Acesso em: 10/12/2022

BRASIL. **Lei n. 7.783, de 28 de junho de 1989**. Brasília: Planalto, 1989. Disponível em: <www.planalto.gov.br>. Acesso em: 10/12/2022.

BRASIL. **Lei n. 13.844, de 18 de junho de 2019**. Brasília: Planalto, 2019. Disponível em: <www.planalto.gov.br>. Acesso em: 10/12/2022.

BRASIL. **Portaria GSIPR n. 2, de 8 de fevereiro de 2008**. Brasília: Planalto, 2008. Disponível em: <www.planalto.gov.br>. Acesso em: 10/12/2022.

CASTRO, G.; CHAMON, V. **Microsoft Press**: Dicionário de Informática. Rio de Janeiro: Editora Campus, 1998.

CRETELLA NETO, J. **Direito Internacional Público**. São Paulo: Editora Letz, 2019

Diário De Notícias. “Nato promete a Rússia resposta firme e unida em caso de ataque a infraestrutura”. **Diário de Notícias** [2022]. Disponível em: <www.dn.pt>. Acesso em: 30/01/2023.

FERNANDES, A. C. S. “Sujeitos de Direito Internacional Público: um processo evolutivo de reconhecimento”. **Revista Jurídica Direito e Paz**, n. 1, 2021.

FERNANDES, C. “O conceito de Guerra de Clausewitz”. **Brasil Escola** [2022]. Disponível em: <www.brasilescola.uol.com.br>. Acesso em: 19/01/2023.

MAZZUOLI, V. O. **Curso de Direito Internacional Público**. São Paulo: Editora Revista dos Tribunais, 2016.

MAZZUOLI, V. O. **Curso de Direito Internacional Público**. São Paulo: Editora Revista dos Tribunais, 2009.

MOTEFF, J. *et al*. “Critical Infrastructures: what makes na infrastructure critical?” **Defense Technical Information Center** [2003]. Disponível em: <www.dtic.mil>. Acesso em: 24 fev. 2023

OLIVEIRA, N. F. “Acesso ao Poder Judiciário na era digital: uma abordagem sobre o impacto da tecnologia para pessoas que vivem na pobreza”. **Revista de Política Judiciária, Gestão e Administração da Justiça**, vol. 7, n. 2, 2021.

OUYANG, M. “Review on modeling and simulation of interdependent critical infrastructure systems”. **Reliability Engineering and System Safety**, vol. 121, 2014.

PINTO, D. J. A.; GRASSI, J. M. “Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil”. **Revista Brasileira de Estudos de Defesa**, vol. 7, n. 2, 2020.

ROCHA, P. C. C. **A Relação entre a Gestão De Riscos Integrada em uma Organização com Infraestrutura Crítica e as Questões de Defesa Nacional** (Trabalho de Conclusão de Curso em Altos Estudos em Defesa). Brasília: ESG, 2019.

SILVA, H. A. G. E. N.; CASELLA, P. B. **Manual de Direto Internacional Público**. São Paulo: Editora Saraiva, 2012.

SOL, G. “Ciberataques às infraestruturas críticas de um país e suas consequências”. **Welivesecurityby Eset** [2022]. Disponível em: <www.welivesecurity.com>. Acesso em 28 nov. 2022.

SUZUKI, S. “A guerra cibernética paralela entre Rússia e Ucrânia”. **BBC News Brasil** [2022]. Disponível em: <www.bbc.com>. Acesso em 14/01/2023.

VITTE, A. C.; MORAES, B. M. “A Ucrânia e o Pivot Geográfico De Halford Mackinder: permanências e metamorfoses de um conceito a partir da geografia física”. *In*: SENHORAS, E. M. (org.). **Ucrânia sob Fogo Cruzado**: a geohistória de uma guerra. Boa Vista: Editora IOLE, 2022.

BOLETIM DE CONJUNTURA (BOCA)

Ano V | Volume 13 | Nº 39| Boa Vista |2023

http://www.ioles.com.br/boca