UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

Alysson Araldi Boschi

A percepção de defesa do Japão no ciberespaço

Florianópolis
2023

Alysson Araldi Boschi

A percepção de defesa do Japão no ciberespaço

Dissertação submetida ao Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina para a obtenção do título de Mestre em Relações Internacionais.

Orientadora: Prof.ª Dr.ª Danielle Jacon Ayres Pinto

Florianópolis

2023

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Araldi Boschi, Alysson
A percepção de defesa do Japão no ciberespaço / Alysson Araldi Boschi ; orientadora, Danielle Jacon Ayres Pinto, 2023.
132 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Socioeconômico, Programa de Pós-Graduação em Relações Internacionais, Florianópolis, 2023.

Inclui referências.

1. Relações Internacionais. 2. Segurança Internacional. 3. Defesa cibernética. 4. Japão. I. Jacon Ayres Pinto, Danielle. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Relações Internacionais. III. Título.

Alysson Araldi Boschi

A PERCEPÇÃO DE DEFESA DO JAPÃO NO CIBERESPAÇO

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof.ª Danielle Jacon Ayres Pinto, Dr.ª
Universidade Federal de Santa Catarina

Prof.ª Graciela de Conti Pagliari, Dr.ª
Universidade Federal de Santa Catarina

Prof. Alexandre Ratsuo Uehara, Dr.
Universidade de São Paulo

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Relações Internacionais.

Documento assinado digitalmente
Danielle Jacon Ayres Pinto
Data: 25/06/2023 17:55:49-0300
CPF: ***.367.488-**
Verifique as assinaturas em https://v.ufsc.br

_____

Coordenação do Programa de Pós-Graduação

Documento assinado digitalmente
Danielle Jacon Ayres Pinto
Data: 25/06/2023 17:56:05-0300
CPF: ***.367.488-**
Verifique as assinaturas em https://v.ufsc.br

_____

Prof.ª Danielle Jacon Ayres Pinto, Dr.ª
Orientadora

Florianópolis, 2023

「土地の氏神様をな、古い言葉で産霊（むすび）って呼ぶんやさ。この言葉には、ふかーい意味がある。糸を繋げることもムスビ、人を繋げることもムスビ、時間が流れることもムスビ。全部、神様の力や。わしらの作る組紐もせやから神様の技。時間の流れそのものを表しとる。より集まって形を作り、ねじれて、からまって、時には戻って、途切れ、またつながり、それがムスビ、それが時間」

君の名は（新海誠の映画、２０１６年）

AGRADECIMENTOS

Agradeço primeiramente à Universidade Federal de Santa Catarina por me proporcionar uma experiência acadêmica excelente em seu Programa de Pós-Graduação em Relações Internacionais. Desse mesmo modo, ao PPGRI e à minha orientadora agradeço pela minha inserção no campo da segurança cibernética, o qual fundamenta esta pesquisa e pesquisas futuras. Agradecimentos indispensáveis à minha família, pois sem eles essa dissertação não seria possível. Aos meus amigos por terem feito da minha experiência na pós-graduação um período ainda mais marcante em minha vida e por me darem a motivação que me faltava em muitos momentos. Menção honrosa ao site sinonimos.com.br por facilitar e fazer fluir a escrita de qualquer pesquisa acadêmica.

RESUMO

O Japão vem desenvolvendo com veemência seu setor de defesa cibernética desde 2011, ano em que os ciberataques mais severos contra o país foram registrados. A partir desse momento, observou-se no Japão não só uma mudança estrutural nas agências e órgãos governamentais que tratam do tema, como também uma mudança política ampla envolvendo sua segurança e defesa cibernéticas. Esta dissertação, a partir de um estudo de caso hipotético-dedutivo, pretende aclarar como o Japão configura-se em termos de defesa no ciberespaço, haja vista a estrutura securitária que o país e demais agentes estão inseridos. Desse modo, inicialmente apresento o teatro de segurança que o Japão está inserido em sua região e como esse foi formado, para posteriormente abordar como a segurança cibernética surgiu e se encaixa nesse mesmo contexto securitário. Concluí que a ciberdefesa japonesa, nesse sentido, tem evoluído gradualmente e hoje é composta de três fundamentos de atuação, que focam na (1) proatividade política japonesa, que funciona em respeito aos limites constitucionais do país; na (2) público-privatização da ciberdefesa japonesa, muito por conta da necessidade de proteção das infraestruturas críticas nacionais que fazem parte do setor privado; e no (3) multilateralismo internacional do país para expansão de sua defesa cibernética e estabelecimento de normais internacionais que envolvam o ciberespaço, o que atualmente não existe.

Palavras-chave: Japão; defesa cibernética; segurança internacional.

ABSTRACT

Japan is vehemently developing its cyberdefense sector since 2011, the year that the most severe cyberattacks against the country were registered. Since this moment, it has been observed in Japan not only a structural change in the governmental agencies and bodies that deal with the theme, but also a broad political change involving its cyber security and defense. This dissertation, through a hypothetical-deductive case study, intends to clarify how Japan is set in terms of defense in cyberspace, taking into account the security framework that Japan is inserted in its region and how it was formed, in order to address how cybersecurity emerged in Japan and how it fits in this preexisting security context. I concluded that the Japanese cyberdefense has gradually evolved and today is composed by three principles of action, which focus on the (1) Japanese political proactivity, which respects the country's constitutional limitations; on the (2) public-privatization of its cyberdefense, largely due to the need to protect national critical infrastructures that are part of the private sector; and on the (3) international multilateralism of Japan that intends to expand its cyberdefense and to establish international norms involving cyberspace, which do not exist in the present.

Keywords: Japan; cyberdefense; international security.

LISTA DE FIGURAS

LISTA GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

ANPO – Tratado de Cooperação Mútua e Segurança entre os Estados Unidos e o Japão

APEC – Cooperação Econômica Ásia-Pacífico

APT – Ameaças Persistentes Avançadas

ARF – Fórum Regional da ASEAN

ASEAN – Associação de Nações do Sudeste Asiático

CCDCOE – *NATO Cooperative Cyber Defence Centre of Excellence*

CDC – *Cyber Defense Command*

CISO – Diretor de segurança da informação

CSIRT – Grupo de Resposta a Incidentes de Segurança em Computadores

CSNU – Conselho de Segurança das Nações Unidas

CSS – *Cybersecurity Strategy*

CSSH – *Cyber Security Strategic Headquarters*

CYDER – *Cyber Defense Exercise with Recurrence*

ELP – Exército de Libertação Popular

EUA – Estados Unidos da América

IA – Inteligência Artificial

IoT – *Internet of Things* (Internet das coisas)

ISPC – *Information Security Policy Council*

ISSPN – *Information Security Strategy for Protecting the Nation*

JAXA – Agência Japonesa de Exploração Espacial

JDA – *Japan Defense Agency*

JPCERT/CC – *Japan Computer Emergency Response Team Coordination Center*

LBD – Livro Branco de Defesa

LDP – Partido Liberal Democrata do Japão

METI – *Ministry of Economy, Trade, and Industry*

MHI – *Mitsubishi Heavy Industries*

MOD – Ministério da Defesa do Japão

MOFA – Ministério das Relações Exteriores do Japão

MTDP – *Mid-Term Defense Program*

NISC – *National Information Security Center* ou *National center for Incident readiness and Strategy for Cybersecurity*

NPA – National Police Agency

NDPG – *National Defense Program Guidelines*

NSC – *National Security Council*

NSIS – *National Strategy on Information Security*

NSS – *National Security Strategy*

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

ODA – Assistência Oficial ao Desenvolvimento

ONG – Organização não Governamental

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado do Atlântico Norte

PIB – Produto Interno Bruto

QUAD – Diálogo de Segurança Quadrilateral

SDF – Forças de Autodefesa do Japão

SIGINT – *Signal Intelligence*

URSS – União das Repúblicas Socialistas Soviéticas

WoG – *Whole of Government*

WoN – *Whole of Nation*

WoS – *Whole of System*

SUMÁRIO

INTRODUÇÃO

A partir da evolução dos sistemas de computadores e da expansão da internet, o ciberespaço começou a ser utilizado por numerosos agentes estatais e não estatais para disseminação de informações e influência. Contudo, a internet não fora projetada para um grande público, e devido ao acesso de milhões de usuários à plataforma suas fragilidades começaram a ser percebidas, dada a ausência de sistemas de segurança que comportassem esses grandes fluxos de acesso (PAGLIARI, AYRES PINTO e VIGGIANO, 2020). Em especial nas últimas duas décadas, essa disseminação de informações e influência tem sido extrapolada por demonstrações e uso de poder no ciberespaço, o que vem transformando essa esfera internacional em um novo ambiente securitizado de atuação, assim como os tradicionais domínios terrestre, marítimo e aéreo. Diferentemente desses âmbitos clássicos, entretanto, a dominação estatal no ciberespaço não é abrangente e soberana, dificultando o controle direto sobre as atividades realizadas nesse meio, por exemplo, visto que a maioria dos atores cibernéticos estão inseridos em um ambiente onde a aplicação de legislações e limites comportamentais ainda é nebulosa. Isso permite que os inúmeros agentes existentes nesse espaço exerçam ameaças cibernéticas sobre os demais sem restrições e punições claras a seus atos.

No caso específico do Japão, conforme indicado pela academia especializada, ciberespionagem é, a nível governamental, o maior risco à segurança cibernética nipônica, dado que esse é o tipo de manobra mais comum a afetar estruturas governamentais no tempo presente (SOESANTO, 2020; LEWIS, 2015). De maneira ilustrativa, os ataques registrados no Japão em 2011 se configuram como espionagem cibernética. Naquele ano ocorreram as mais severas incursões cibernéticas já observadas até hoje no país, contra a Mitsubishi Heavy Industries (MHI), principal fabricante de aparatos militares às Forças de Autodefesa do Japão (SDF), bem como contra o parlamento e embaixadas japonesas no exterior. Através desse movimento de ciberespionagem, foram ilegalmente consultados detalhes sobre a produção do sistema de defesa antimísseis do Japão, projetos de aviões de combate e veículos de lançamento espacial e outras armas estratégicas não divulgadas (GADY, 2017; KALLENDER e HUGHES, 2016).

Por outro lado, se ciberespionagem é a maior preocupação a nível governamental, cibercrimes são a principal ameaça contra a sociedade civil japonesa, especialmente empresas e grandes corporações, através dos quais se pratica *phishing* e extorsão de quantias milionárias do setor privado. No ano de 2020, por exemplo, mais de 100 empresas japonesas sofreram com tentativas de extorsão, das quais 33 pagaram uma quantia equivalente a JPY 123 milhões, ou

cerca de USD 1 milhão, por conta de vírus do tipo *ransomware* (SIRIPALA, 2020). Além disso, com o crescimento e o desenvolvimento de tecnologias centradas na *Internet of Things* (IoT) e em Inteligência Artificial (IA), o governo japonês teme que mais setores da sociedade fiquem vulneráveis a possíveis cibercrimes, dada a maior conectividade da vida diária de sua população à internet (BARLETT, 2020).

A vista disso, o governo japonês divide as infrações cibernéticas em duas grandes categorias: ciberataques e cibercrimes. Em sua definição de ciberataque, o Japão inclui atividades como "intrusão ilegal, roubo, alteração ou destruição de informações, parada ou mau funcionamento de sistemas de informação, execução de programas não autorizados, ataques DDoS" (MOD, 2021, p. 284), bem como Ameaças Persistentes Avançadas (APT), ataques contra sistemas de controle industriais e outras infraestruturas críticas que impactam uma variedade de atividades econômicas e sociais, e mesmo aqueles ataques contra processos democráticos, visando e interferindo em eleições (NISC, 2021). Observa-se, portanto, que a ciberespionagem está incluída na categoria geral de ciberataques. Em contrapartida, os cibercrimes são definidos pela *National Police Agency* (NPA) do Japão como sendo crimes de violação da *Unauthorized Computer Access Law*[1]; crimes contra computadores/dados[2]; e crimes relacionados à internet[3] (NPA, s.d.). Nesse escopo, a assinatura da Convenção de Budapeste em 2001, ratificada apenas em 2012, não só fortalece o comprometimento internacional do Japão contra o cibercrime como alinha traços de sua legislação interna com os demais países signatários.

Desse modo, haja vista a variedade de ameaças a permear o ciberespaço, assim como numerosos outros Estados, o Japão vem robustecendo suas políticas de segurança cibernética com o intuito de regular essa nova esfera de poder. A primeira institucionalização da questão ocorreu em 1996, com a criação do *Computer Emergency Response Team Coordination Center* para responder a incidentes e emergências cibernéticas que viessem a ocorrer no país (HATHAWAY et al, 2016). Já nos anos 2000, o ciberespaço começou a receber atenção maior do governo japonês por conta de uma série de ataques contra sites de Ministérios e agências governamentais japonesas (KSHETRI, 2014), ataques os quais apresentaram teor mais

[1] Promulgada em agosto de 1999, tendo recebido sua última emenda em 2013. Este tipo de crime faz menção a qualquer tipo de invasão não autorizada a computadores, seja por atividades hackers, seja por credenciais oficiais (NPA, s.d.).

[2] Nesta categoria encontram-se crimes como fraude, destruição ou produção ilegal de dados eletromagnéticos e obstrução de atividades empresariais pela destruição de computadores (NPA, s.d.).

[3] Incluem-se atos como difamação, intimidação, infração contra direitos autorais, pornografia e prostituição infantil e distribuição de materiais obscenos (NPA, s.d.).

sofisticado se comparados aos observados até aquele momento (GADY, 2017). Por conta desse evento, foram criados o *Information Security Policy Council* (ISPC), responsável por confeccionar a estratégia básica de cibersegurança do Japão, e o *National Information Security Center* (NISC), atuando como secretariado do ISPC, que trataria de desenvolver mapas estratégicos, estruturas de coordenação governamental e planejar o envolvimento internacional do Japão na questão cibernética (KALLENDER e HUGHES, 2016).

A década de 2010, não obstante, foi o momento histórico decisivo para que a segurança cibernética alcançasse um alto patamar estratégico nas políticas do Japão, quando parlamentares japoneses chegaram ao consenso de que a cibersegurança precisava ser tratada como assunto fulcral nas políticas de segurança do país (IBID, 2016). Após os ataques de 2011, anteriormente mencionados, o IPSC foi renomeado para *Cyber Security Strategic Headquarters* (CSSH) e movido para o Escritório do Gabinete do Primeiro-ministro, em 2014. Isso faz com que essa instituição hoje se encontre em um dos graus hierarquicamente mais altos da política japonesa no tema, acima do nível ministerial, por exemplo, capaz de controlar orçamentos de agências governamentais no que tange à segurança cibernética, por exemplo (KALLENDER e HUGHES, 2016). No mesmo ano, o NISC foi igualmente reformulado, passando a se chamar *National center for Incident readiness and Strategy for Cybersecurity* (ainda sob a sigla NISC), também atuando como secretariado ao CSSH e tratando, dentre outros pontos, da formulação da *Cybersecurity Strategy* (CSS) do Japão e de políticas de proteção a infraestruturas críticas (NISC, s.d.). À vista disso, em 2015 a primeira CSS japonesa foi oficialmente lançada, tendo sido revisada em 2018 e, mais recentemente, em setembro de 2021, sendo essa a versão que rege a segurança cibernética do Japão ao momento de escrita dessa dissertação. Através de sua Estratégia de Cibersegurança, especialmente na versão atual de setembro de 2021, o Japão esclarece como o ciberespaço é um domínio conflitivo e que ameaças tendem a aumentar em número e em complexidade nessa esfera de poder.

Por fim, na década de 2020, o país menciona abertamente pela primeira vez, em sua *Cybersecurity Strategy* de 2021, como a Coreia do Norte, a China e a Rússia são os países que apresentam as principais ameaças contra o Japão no ciberespaço. Indica-se que a China presumidamente volta seus ataques ao roubo de informações de companhias relacionadas à indústria militar para assim impulsionar sua posse de tecnologias avançadas; a Rússia, por outro lado, comete infrações no ciberespaço para exercer influência com o intuito de atingir objetivos políticos e militares; por fim, a Coreia do Norte, para além de conduzir ataques para alcançar objetivos políticos, tal como a Rússia, também tenta obter moedas estrangeiras com seus ataques. Além desses três países, Tóquio reconhece o envolvimento de organizações criminosas

por trás de ciberataques realizados contra o país (NISC, 2021). Nesse mesmo passo de internacionalização da cibersegurança japonesa, os Estados Unidos estão presentes desde a concepção da ideia de segurança cibernética no Japão até o momento atual, sendo o principal aliado do Japão neste ramo de sua defesa tal como nos âmbitos tradicionais de poder. Isso é exposto extensivamente nas políticas estratégicas japonesas, nos encontros bilaterais EUA-Japão e, mais marcadamente, em seu acordo de segurança mútua, o ANPO.

Na década de 2020 também ocorreram no Japão os Jogos Olímpicos de Verão, momento no qual o governo nipônico pôde pôr em prática diversas estratégias para proteger seu espaço cibernético. Nessa ótica, documentos governamentais, inclusive a CSS pioneira de 2015, apontaram o ciberespaço como um dos pontos mais sensíveis a se prestar atenção ao longo do evento, já que o Japão poderia sofrer uma série de ciberataques que ameaçariam sua integridade territorial. Ademais, o *Cyber Defense Command* (CDC), por vezes também chamado de *Cyber Defense Unit* ou *Cyber Defense Group* em documentos oficiais, foi reestruturado em março de 2022 e passou a contar com forças com potencial de ataque. Como indicado por Benjamin Barlett (2020), contudo, o CDC utilizará suas forças de ataque de modo a evitar ciberataques e interromper o uso do ciberespaço por atacantes, o que ainda recai no âmbito da autodefesa em conformidade ao Artigo 9 da Constituição japonesa.

Posto isso, esse trabalho tem como objetivo responder a seguinte pergunta: c*omo o Japão percebe o ciberespaço, enquanto nova esfera de poder, a partir de sua estrutura de defesa?* Como resposta a essa pergunta, divido minha hipótese em três momentos: a primeira visão de como o Japão percebe o ciberespaço a partir de sua estrutura de defesa indica que o país está passando por um processo de transformação em seu sistema defensivo para voltar a ter capacidades ofensivas, ao mesmo tempo que respeita seus atuais limites constitucionais até que isso não se concretize de fato. Nesse sentido, a percepção japonesa quanto à sua ciberdefesa assemelha-se em muito à sua percepção de defesa nos domínios tradicionais de poder, não podendo uma realidade ser desvinculada da outra, visto que a Constituição japonesa continua a impedir uma postura estatal ofensiva. Isso posto, apesar de o governo japonês respeitar o Artigo 9 de sua Constituição e restringir sua defesa no ciberespaço à autodefesa, certos grupos políticos estão constantemente em busca de uma reforma no sistema de defesa japonês para que o Japão volte a ser um "Estado normal"[4]. Em linhas gerais, a defesa japonesa no ciberespaço perpassa

[4] O conceito de Estado normal, no Japão, serve como contraponto ao pacifismo neutro instaurado no país pós-Segunda Guerra, através do qual se argumenta que o Japão deveria se tornar um Estado westfaliano "normal" como as demais nações do mundo (JESUS JUNIOR, 2008). Assim, os defensores desta visão utilizam-na especialmente para justificar que o Japão deveria se tornar um país com controle total sobre suas políticas de defesa, inclusive sobre o direito de se remilitarizar formalmente.

o entendimento de que o Japão precisa ter forças com potencial de ataque para enfrentar aqueles agentes que ameaçam a nação ciberneticamente, em especial Rússia, China e Coreia do Norte; em conformidade ao que vinha ocorrendo desde os mandatos de Shinzō Abe, no governo de Fumio Kishida ainda se observam indícios de que esta reforma pode se tornar realidade.

De outro modo, visto que parte considerável das ameaças à segurança cibernética do Japão recaem sobre entes privados constantemente atacados, como grandes empresas de tecnologia e mesmo produtoras de armamentos, minha segunda hipótese aborda como a postura defensiva do Japão no ciberespaço também considera uma expansão do guarda-chuva de suas Forças de Autodefesa para cobrir o setor privado. Isso ocorre não só pela incapacidade do setor privado em se autodefender por completo, dado que são alegadamente atacados por outros Estados com capacidades muito superiores, como também por estratégia governamental para proteger as infraestruturas críticas visadas pelos ciberatacantes e que põem em risco a segurança nacional japonesa. Dessa forma, observa-se no presente um constante aprofundamento das relações público-privadas no Japão, visto que para o governo a proteção da esfera privada é igualmente importante para a integridade nacional no ciberespaço. De quebra, esse tipo de cooperação público-privada resolve em parte a falta de mão de obra especializada a serviço da defesa cibernética do Japão, uma vez que trabalhadores do setor privado complementam o corpo estatal de ciberdefesa.

Por fim, o terceiro viés de minha hipótese indica que o Japão está expandindo seu multilateralismo internacional na questão cibernética, sendo esse o terceiro pilar que define a ciberdefesa japonesa. Nesse contexto, o bilateralismo com os EUA, cristalizado em seu acordo de segurança mútua, continua sendo o canal pelo qual o Japão define suas políticas securitárias na esfera internacional, inclusive quanto ao ciberespaço. A busca por multilateralismo no campo cibernético, nesse sentido, justifica-se pela necessidade de o Japão robustecer seu alinhamento internacional com países *like-minded*, o que resultaria na consolidação de um ciberespaço internacional livre, justo e seguro, em conformidade às atuais políticas securitárias do Japão.

Quanto ao segundo e ao terceiro momentos de minha hipótese, ambos se conectam à crescente utilização maliciosa do ciberespaço pelos rivais tradicionais do Japão: a China, a Coreia do Norte e a Rússia; nesse sentido, as ameaças à segurança cibernética do Japão são um reflexo das ameaças do país nos domínios tradicionais de atuação. Observa-se nessa conjuntura que tanto os documentos gerais de segurança do Japão, como sua *National Security Strategy*, quanto os documentos voltados à sua cibersegurança, como a *Cybersecurity Strategy* japonesa, apontam esses três países como suas principais ameaças no cenário internacional. Quanto a isso,

a Rússia começou a ser categorizada mais marcadamente como uma ameaça à segurança geral do Japão após o início da Guerra da Ucrânia, em fevereiro de 2022, mas antes desse evento o país já era ciberneticamente visado pelo Japão por conta dos tipos de guerra híbrida e de informação praticados pelos russos. A China e a Coreia do Norte, por outro lado, ao menos desde o início da Guerra Fria são securitariamente monitoradas pelo Japão, dado que mágoas historicamente estabelecidas entre as partes se traduzem em ofensivas também no ciberespaço contra o Japão.

Isso posto, o objetivo geral desta pesquisa é expor o que chamo de "os três fundamentos da ciberdefesa japonesa", em conformidade às três hipóteses acima, cada uma sendo um dos fundamentos. Assim, focarei em evidenciar como o Japão está atuando em conformidade à sua Constituição, sem abandonar seu intento de tornar a ser um Estado normal. Isso se justifica, pois, seja no âmbito de sua segurança tradicional, seja no âmbito cibernético, a Rússia, a China e a Coreia do Norte se apresentam como ameaças latentes contra o Japão, sobremaneira devido a construções identitárias historicamente conflitantes, exigindo evolução contínua de suas políticas securitárias e de defesa. Esses pressupostos são passíveis de verificação através da maior assertividade dos documentos estratégicos japoneses, da reestruturação do *Cyber Defense Command* japonês, em março de 2022, ou da expansão das relações público-privadas e do multilateralismo internacional do Japão nos últimos anos, por exemplo.

Em complementaridade ao objetivo geral, enquanto objetivos específicos indico o esforço de explorar (1) como a segurança cibernética se tornou uma vertente de segurança internacional relevante ao Japão e como isso se conecta ao complexo de segurança preexistente, envolvendo a Rússia, a China e a Coreia do Norte. Nesse sentido, o ramo da segurança cibernética japonesa conta, em linhas gerais, com os mesmos antagonistas historicamente estabelecidos na região do Leste Asiático devido a desavenças passadas que deram origem a identidades contrastantes entre essas nações. Por fim, abordar (2) como o Japão parece estar em um período de transição constitucional e legislativa e como isso impulsiona uma proatividade securitária no país, o que inclui sua esfera de defesa cibernética através de temas como multilateralismo e cooperação público-privada.

No que tange às variáveis da pesquisa, classifico como (I) *independentes*: ameaças crescentes advindas de países securitizados pelo Japão – China, Coreia do Norte e Rússia; (II) *dependentes*: o estabelecimento de uma política ciberdefensiva calcada em três fundamentos de atuação; (III) *condicional*: ciberespaço enquanto novo palco de ameaças internacionais.

Tratando-se da metodologia aplicada, esta dissertação é definida como um *estudo de caso hipotético-dedutivo*. Este método de procedimento se justifica, inicialmente, pela limitação

no número de casos analisados, restringindo-se apenas à segurança cibernética do Japão, além de majoritariamente se tratar de fatos atuais, eliminando a viabilidade de métodos comparativos ou históricos, por exemplo. Por outro lado, escolheu-se o método de abordagem hipotético-dedutivo por ser alinhado a estudos de Ciências Humanas; conforme apontado por Karl Popper (1975), estudos hipotético-dedutivos partem de um conhecimento prévio, a partir do qual surge uma pergunta problema que dá início a uma pesquisa. Esse problema é respondido através de conjecturas, ou hipóteses passíveis de verificação, as quais são, por fim, submetidas a testes de falseabilidade, como a observação. Assim, se as hipóteses resistirem às tentativas de refutação, tem-se um novo conhecimento formado; caso contrário, as conjecturas são falseadas e precisa-se reiniciar o processo de análise.

Enquanto ferramentas de pesquisa, utilizarei majoritariamente fontes primárias, como documentos confeccionados por agências e órgãos governamentais do Japão sobre segurança e defesa cibernéticas; ainda, analisarei fontes secundárias, especialmente produção científica na área de cibersegurança e Relações Internacionais.

Por fim, por ser um campo de estudo contemporâneo e ainda em pleno desenvolvimento, a justificativa do tema está centrada na necessidade de se entender como governos agem frente a ameaças cibernéticas em um âmbito internacional e o que essas ameaças e esse espaço de disseminação de poder representam aos Estados. Além disso, pouco se estuda sobre Japão na academia brasileira de Relações Internacionais, ocasionando, por consequência, pouco conhecimento gerado em língua portuguesa sobre o assunto e sobre o país como um todo. Dessa maneira, as particularidades envolvendo o estudo do Japão e a atual expansão do tema de cibersegurança no campo de Relações Internacionais tornam essa pesquisa um trabalho original no Brasil.

1. TEORIA E SEGURANÇA CIBERNÉTICA

O campo das Relações Internacionais conta com uma série de teorias, diversas em sua natureza e em seus pressupostos, as quais permitem entender o sistema internacional. A fim de compreender o domínio cibernético, entretanto, é essencial adotar lentes teóricas que compreendam sua complexidade e todas as suas facetas em constante transformação. Sendo assim, este trabalho será sumariamente guiado pela visão construtivista de Relações Internacionais, em especial pelos entendimentos elaborados por Alexander Wendt e por Glenn Hook et al. (2012); antes de justificar tal escolha, todavia, faz-se necessário entender até que ponto o aparato teórico da disciplina abrange a questão cibernética.

Segundo Breno Medeiros e Luiz Goldoni (2020), Thomas Kuhn aborda como campos de estudo estabelecem paradigmas para entender determinados fenômenos e resolver determinados problemas. A partir do momento que um paradigma falha em cumprir com esse objetivo, um novo é formulado, baseado em novos entendimentos; devido à mudança de paradigmas e da formação de novas interpretações para um determinado fenômeno, portanto, a ciência avança. Brian Schmidt (2013) observa que o campo das Relações Internacionais, tal qual o da Ciência Política, desenvolveu-se na perspectiva de Kuhn. Ao tempo da criação da disciplina, pesquisadores apressaram-se em desenvolver o primeiro paradigma de Relações Internacionais e consolidar uma teoria ao campo de estudo. Nesse quesito, a teoria realista é tida por muitos como a fundante das Relações Internacionais, referida como o "paradigma tradicional" da disciplina. Entretanto, essa vertente teórica trata de assuntos bastante costumeiros ao entendimento das relações internacionais, como sobrevivência estatal, anarquia internacional e o princípio da auto-ajuda.

Na medida que o campo da cibersegurança evolui, em concomitância às preocupações em ascensão por parte de Estados quanto a suas seguranças cibernéticas, o paradigma realista, e sua vertente mais atual neorrealista, não consegue explicar esse fenômeno em sua completude. Em primeiro lugar, ao realismo, apenas Estados apresentam-se como atores relevantes no sistema internacional, enquanto seus âmbitos domésticos são irrelevantes à interpretação dessa teoria. Neste sentido, o realismo falha em elucidar como, no ciberespaço e para a segurança cibernética, indivíduos e agentes não estatais compõem o universo da cibersegurança e podem vir a representar ameaças a Estados. Dessa forma, a multiplicidade de agentes, conforme apontado por Medeiros e Goldoni (2020), é uma das características do ciberespaço que está em desacordo com o realismo. Se a corrente realista não reconhece a atuação de agentes não estatais e a importância do âmbito doméstico ao espaço cibernético, falha em explicar, portanto, como

esses fatores representam ameaças internacionais envolvendo o ciberespaço, advindas de agentes por vezes pouco organizados e diversificados, e que afetam estruturas estatais tradicionais por completo.

A vista disso, o governo japonês identifica que organizações criminosas, para além da China, da Coreia do Norte e da Rússia, fazem parte dos atores que ameaçam o Japão através do ciberespaço (NISC, 2021). Apesar de as principais ameaças advirem, sim, de Estados, não se pode negar o reconhecimento por parte do governo das ameaças perpetradas por agentes não estatais. Além disso, o Japão reconhece em sua CSS mais recente como cooperação com o setor privado, em especial grandes empresas e corporações, é fulcral para expandir a defesa cibernética do país (IBID, 2021). Este fato volta a evidenciar a importância de agentes domésticos e, novamente, não estatais, na ótica cibersecuritária do Japão, tornando inviável adotar uma teoria que não reconheça tais atores para analisar a realidade cibernética japonesa. Menciono, entretanto, que preceitos realistas serão sim utilizados nesta pesquisa – ponto abordado mais adiante neste capítulo –, não por crer que o realismo se aplique integralmente ao caso japonês, mas sim por certos aspectos da teoria realista serem resultado de um constructo social e identitário no Leste Asiático, como o dilema de segurança.

Em segundo lugar, as teorias realistas pressupõem que as relações internacionais são hobbesianas, isto é, constantemente conflituosas, e que Estados apenas se aproximam uns dos outros por interesses e para cumprir determinados objetivos que, quando alcançados, resultam em seu afastamento. Essa realidade não reflete o alinhamento do Japão a parceiros estratégicos, com os quais o país mantém relações amistosas há décadas. Além disso, há prerrogativas construtivistas que indicam que o alinhamento japonês com seus parceiros, especialmente aqueles ocidentais, surge de identidades e interesses nacionais afins, o que não se relaciona com o entendimento realista de cooperação. Isso se traduz também no ciberespaço, por exemplo, na medida que o Japão tem uma aproximação mais marcada em cooperação cibernética com países do Ocidente e do Sudeste e Sul Asiáticos por fatores estratégicos e identitários, em detrimento daquelas regiões que não partilham a mesma mentalidade ou as mesmas ameaças contra o Japão.

Em relação à vertente liberal, por outro lado, as teorias mais recentes e consagradas do ramo neoliberal trabalham especialmente com a ideia de interdependência complexa enquanto um dos aspectos mais contundentes do sistema internacional, para além da dominância da economia enquanto uma das forças motrizes das relações internacionais. Para Robert Keohane e Joseph Nye (2008), principais autores que trabalham com esse conceito, interdependência complexa é a subversão dos conceitos centrais das teorias realistas. Assim, primeiramente,

Estados não são os únicos agentes no sistema internacional; nesse sentido, existem outros participantes que influenciam diretamente a política através de múltiplos canais que conectam sociedades, como laços informais entre elites governamentais e não governamentais, e organizações transnacionais, a exemplo bancos multinacionais e corporações. Em segundo lugar, relações interestatais não seguem uma agenda específica e clara, como a primazia da *high politics* em detrimento da *low politics*; isso é dizer que a ausência de hierarquia de questões significa que segurança militar, como no caso do realismo, não seja consistentemente a agenda dominante. Por fim, o uso da força é um instrumento ineficaz de política; a força não é utilizada, segundo Keohane e Nye, entre governos de uma mesma região em um cenário de interdependência complexa. Apesar de o poder ser eficaz na manutenção de relações políticas e militares com outros blocos, é irrelevante para resolver conflitos econômicos entre membros de uma aliança.

Ademais, para além da interdependência complexa, a interdependência econômica entre os Estados gere que tipo de relação esses países terão entre si, segundo a vertente liberal. Na medida que os Estados se tornam economicamente dependentes uns dos outros a probabilidade de conflito diminui, visto que suas economias estão interligadas a tal ponto que danos a países com os quais se tem dependência resulta em danos a si, reduzindo a probabilidade de uso da força. Diferentemente da teoria realista, que trata a cooperação internacional como algo extremamente pontual no sistema internacional, para a vertente liberal a cooperação se torna central nas relações internacionais, tendo em vista a necessidade de manutenção de um *status quo* cooperativo em um cenário de interdependência econômica para assim evitar danos a si.

Dessa maneira, apesar de a teoria liberal apresentar pressupostos consonantes ao estudo da segurança cibernética internacional, como a existência de demais agentes nas relações internacionais, as teorias liberais trabalham majoritariamente com assuntos econômicos e de cooperação. Apesar de o Japão de fato cooperar com Estados estratégicos no ciberespaço, observa-se que essa cooperação não tem os traços econômicos característicos da teoria liberal; essa cooperação é muito mais política para o tema cibernético. Ainda, as principais ameaças japonesas no ciberespaço dizem respeito à tentativa de roubo de informações confidenciais, especialmente aquelas vinculadas a novas tecnologias que possam ser aplicadas ao setor militar, bem como ao exercício de influência para que se atinjam objetivos políticos, segundo a CSS de 2021 (NISC, 2021). Dessa maneira, a vertente liberal de Relações Internacionais não se mostra adequada à análise da realidade cibernética do Japão, uma vez que o foco de atenção da estratégia japonesa não se concentra em fatores econômicos. A economia é sim mencionada nos documentos cibersecuritários do Japão como algo a ser protegido no ciberespaço, mas o

foco, como apontado acima, concentra-se no alcance de objetivos políticos e na expansão de arsenais militares por intermédio de novas tecnologias.

No que tange a teorias pós-positivistas, incluindo aquelas do sul global como a teoria da dependência, em sua maioria ancoradas no materialismo-histórico, poder-se-ia utilizá-las para explicar as disparidades de poder entre Estados mais desenvolvidos contra aqueles menos desenvolvidos e como isso afeta o acesso a tecnologias cibernéticas, por exemplo. Aproximadamente metade da população global ainda não tem acesso à internet, segundo pesquisa desenvolvida pelas Nações Unidas (2019), que aponta que 53,6% do planeta, ou 4,1 bilhões de pessoas, têm acesso ao serviço. A pesquisa da ONU indica também que os países menos desenvolvidos são os que têm menos acesso à internet, com uma média de apenas 20% da população utilizando o serviço digital. Tomando como exemplo a tecnologia 5G, a qual já está amplamente disponível em países como a Coreia do Sul, se cerca de metade da população global não tem acesso à internet, e que a maioria daqueles sem acesso estão localizados em países em desenvolvimento, que tipo de nação consegue ter acesso à tecnologia 5G? Em vista disso, tal como as relações de poder teorizadas pelo marxismo, há uma enorme lacuna entre os países que conseguem acessar tecnologias cibernéticas avançadas contra aqueles que têm sequer acesso a recursos digitais básicos. A mesma pesquisa aponta ainda que, dentre os usuários da internet, 48% das mulheres no mundo têm acesso ao serviço, contra 58% dos homens. Assim, existe ainda uma disparidade de gênero no mundo cibernético que poderia ser estudada à luz de vertentes feministas no âmbito das Relações Internacionais. Como Judith Tickner (1997) observa, teóricas feministas de Relações Internacionais preocupam-se em esclarecer como as desigualdades, neste caso de gênero, moldam os papéis dos indivíduos na sociedade e, como consequência, as relações internacionais. Nesse contexto, o gênero feminino representa um papel subalterno e marginalizado, pondo em risco a segurança de mulheres por conta da iniquidade formadora dos Estados contemporâneos. Similarmente a essa ideia, teorias deste espectro, como as materialistas-históricas, procuram explicar desigualdades sistêmicas entre países e como isso afeta as relações internacionais.

Desse modo, pesquisar relações de poder e desigualdades entre países do Sul e do Norte global no âmbito cibernético, portanto, utilizando teorias desse ramo, mostra-se promissor frente aos desafios que ambos os grupos de países enfrentam. Contudo, visto que essa dissertação não busca aprofundar tais debates, tais teorias não se aplicam ao caso do Japão proposto nesta dissertação. Assim, apesar de essas vertentes serem um instrumental teórico inovador tratando-se das desigualdades cibernéticas apresentadas, tendo em vista o tipo de insegurança cibernética que o Japão está submetido e considerando que o objetivo desta

pesquisa não é assinalar assimetrias entre o Japão e outros Estados, teorias materialistas-históricas não se aplicam propriamente ao objeto de estudo.

Por fim, para a vertente construtivista utilizada nesta pesquisa, enquanto aspecto basilar da teoria identifica-se que todos os processos desencadeados no sistema internacional são resultados de interações sociais, na base de significados e de legitimidade, particulares de um determinado contexto histórico e situação política (FIERKE, 2015). Neste sentido, analisando a anarquia do sistema internacional, Alexander Wendt (1992) propõe que essa anarquia é pautada nas relações que diferentes agentes constroem entre si, contrariamente ao preceito realista de desconfiança constante entre Estados. Dessa forma, a anarquia internacional representa aos Estados – e demais agentes, como consequência –, nada mais que o constructo social de suas relações com terceiros. Se essas relações forem pacíficas, não há razão para que a anarquia internacional opere em uma lógica beligerante, e vice-versa. Assim, para o construtivismo as relações de segurança não são dadas tal como no realismo, cuja principal preocupação securitária concernente aos Estados é a de sobrevivência[5].

Em suma, Glenn Hook et al. (2012) especificam que o construtivismo é uma teoria que aborda como os agentes que compõem o sistema internacional moldam suas definições de interesses e sua racionalidade tendo como base interações mútuas e padrões de comportamento de outros atores, diferentes uns dos outros. Assim, essa socialização é dotada de um conjunto de expectativas, normas e identidades que servem para constranger ou prover oportunidades para a definição de que comportamento adotarão internacionalmente. Dessa maneira, contrariamente às teorias tradicionais, não existe uma racionalidade imutável compartilhada pelos agentes do sistema internacional. Posto isso, essa estrutura internacional de relações na qual os agentes estão inseridos é o palco onde Estados e suas populações interagem, criam suas

[5] Mesmo Kenneth Waltz (1978), um dos fundadores da corrente neorrealista, com sua controversa colocação de que seria ridículo construir uma teoria de política internacional baseada na Malásia ou na Costa Rica, já deixava claro seu ponto: os Estados não são iguais e não têm as mesmas preocupações no sistema internacional. Desde o movimento dos não alinhados, durante a Guerra Fria, à política de Guerra ao Terror do ex-Presidente americano George W. Bush (2001–2009), percebe-se que Estados não apresentam o mesmo tipo de pensamento quanto a certos cenários de segurança e ameaças internacionais. Tendo como exemplo o último ponto, Eliézer Rizzo de Oliveira (2003) indica como a Guerra ao Terror de Bush representou uma radicalização de alguns conceitos de segurança nacional dos Estados Unidos por conta dos atentados de 11 de setembro. "O terrorismo já era concebido como o principal desafio. Agora, deve ser destruído em qualquer hipótese" (OLIVEIRA, 2003, p. 5). Essa postura deu início à Guerra do Iraque, caracterizada como preventiva, logo, contra o Direito Internacional, e sem aval do Conselho de Segurança das Nações Unidas (CSNU). Nesse contexto, países como o Brasil, ou mesmo grandes potências abarcadas pela teoria realista como França, Alemanha e Rússia, reafirmaram uma preferência pela lei internacional, pela valorização da ONU e pelo emprego da força em último recurso, segundo Oliveira. Esse tipo de postura é compreensível quando se considera o Brasil, dado que o país nunca tinha sido até aquele momento (e nunca foi até hoje) alvo do terrorismo islâmico internacional. Deparar-se com uma posição reticente vinda da França, no entanto, é algo que demonstra como mesmo as grandes potências não têm o mesmo entendimento sobre segurança e sobrevivência no sistema internacional, e que suas prioridades são, portanto, baseadas em contextos e construções sociopolíticas distintas.

expectativas em relação aos outros, moldam suas identidades e seus interesses nacionais e constrangem ou criam oportunidades de relação entre si. Qualquer mudança que ocorra na estrutura do sistema internacional criará novos constrangimentos e novas oportunidades de relacionamento, fazendo com que a estrutura na qual os agentes estão inseridos condicione as relações internacionais.

Os autores também esclarecem como o comportamento japonês no sistema internacional, amplamente ocupado por potências industrializadas, oscilou ao longo dos anos a depender da situação da estrutura na qual o país estava inserido. A partir dessa habitual interação com grandes potências, portanto, em um momento inicial houve um impulso de isolamento do restante do mundo por parte do Japão devido a diferenças e restrições impostas pelo sistema internacional; já em outro cenário, a tentativa japonesa de se tornar de fato uma das potências mundiais, ou ao menos uma potência regional, foi o tipo de ação conduzida pelos líderes políticos. No entanto, o alinhamento à potência de cada momento histórico e a formação de fortes relações bilaterais com esses países, como os Estados Unidos no presente, foi o comportamento mais usualmente adotado pelo Japão ao longo dos anos, uma vez que essas potências são as formadoras da estrutura internacional e há interesse por parte do governo japonês em se alinhar a essa realidade estrutural (HOOK ET AL., 2012).

Referindo-se ao que se pretende pesquisar nesta dissertação, o construtivismo também se aplica ao cenário de segurança do Japão por esse ter sido formado, em especial a partir do início do século XX, por fatores sumariamente identitários. Como apontam Hook et al. (2012), a bárbara herança colonial japonesa sobre a península coreana e sobre regiões da China foi fundamental para que esses países, uma vez independentes após a Segunda Guerra Mundial, temessem que o Japão se remilitarizasse e voltasse a representar uma ameaça à sua segurança. Os autores mencionam, inclusive, que tanto a Coreia do Sul quanto a do Norte formaram nacionalismos anti-nipônicos naquele período. Assim, argumentar-se-á aqui que, para além da esfera tradicional de segurança internacional, a segurança cibernética na região também se insere nessa construção identitária de constrangimentos impostos pelo Japão na estrutura do Leste Asiático.

Em adição ao passado imperial japonês que levou os países da região a desenvolverem identidades anti-nipônicas ao longo do século XX, o alinhamento japonês aos Estados Unidos, enquanto potência antagônica às nações supracitadas do Leste Asiático, também corrobora à co-construção de identidades contrastantes entre o Japão e seus rivais históricos China, Coreia do Norte e Rússia. O governo norte-coreano chegou a mencionar, nesse sentido, como os Estados Unidos estão construindo uma espécie de OTAN na Ásia devido a testes militares

conjuntos com a Coreia do Sul e o Japão, bem como demais arranjos cooperativos formados com os países, com o intuito de deter um possível avanço norte-coreano (SHIN, 2022). Esse posicionamento indica como, às nações do Leste Asiático, existe o entendimento que o Japão está localizado no espectro oposto e que essa conformação se dá graças a diferenças identitárias e interesses nacionais.

Para além das questões identitárias envolvendo o Japão e as três nações securitizadas pelo país, no contexto da segurança cibernética japonesa nota-se como o Japão reconhece a importância de constructos sociais na formulação de suas políticas securitárias. Para além da assídua participação japonesa em conferências internacionais sobre cibersegurança, seja em organismos internacionais, seja bilateralmente com parceiros estratégicos, o Japão procura alinhar determinadas políticas cibernéticas e sistemas de reconhecimento com aqueles dos Estados Unidos e de países europeus (SCHUETZE, 2020). Isso se deve, pois, o governo japonês entende que se necessita construir uma universalidade nas políticas cibernéticas para que se evite a disseminação de regras únicas a cada Estado, que se desencontrariam e distorceriam atividades de determinadas entidades, e essa universalidade política precisa ocorrer com o Ocidente. Assim, o alinhamento japonês a países ocidentais específicos demonstra como há uma percepção de que o Japão deve cooperar com certos Estados em detrimento de outros, haja vista visões de mundo semelhantes e percepções de ameaças afins, por exemplo. Dessa forma, seja em suas relações de segurança nos domínios tradicionais, seja no ciberespaço, as identidades desempenham nas políticas japonesas dois papéis: antagonismo aos Estados do Leste Asiático e alinhamento às nações ocidentais.

Dessa maneira, haja vista as diferenças identitárias históricas co-construídas no Leste Asiático, pressupostos da teoria construtivista me ajudarão a expor porque o Japão identifica as três nações mencionadas como suas principais ameaças no ciberespaço e porque o Japão, como consequência, é alvo recorrente desses países em termos de ciberataques. Há de se mencionar novamente que, para além as nações tradicionalmente securitizadas, o governo japonês reconhece que organizações criminosas não-estatais também realizam ciberataques contra o país e, portanto, compõem o espectro de ameaças cibernéticas; o setor privado, de mesmo modo, também é considerado como chave na ciberdefesa japonesa e está sendo inserido gradativamente nas tratativas nacionais quanto ao tema. Em conformidade, a vertente construtivista de Relações Internacionais reconhece uma variedade de atores para além daqueles estatais; analisar as relações securitárias em termos de cibernética através do construtivismo, logo, propicia o abarcamento de todos os agentes envolvidos nesse ambiente, sejam eles estatais, não governamentais, transnacionais, privados ou individuais.

Observo ainda que, ao longo dessa dissertação, serão utilizados certos conceitos realistas para explicar a relação do Japão com seus vizinhos no Leste Asiático. Há de se esclarecer, entretanto, que não assumo que os princípios realistas nas relações japonesas aqui utilizados são baseados nas justificativas da teoria realista para sua aplicabilidade. Argumento, desse modo, que a configuração das relações do Japão no Leste Asiático que tem como pilar concepções realistas, tal como o dilema de segurança, ocorrem se não por um constructo social desencadeado ao longo das décadas, conforme será explicado em detalhes no segundo capítulo, tendo como base o colonialismo no Leste Asiático iniciado na segunda metade do século XIX e que perdurou até o final da Segunda Guerra Mundial. Sendo assim, mesmo que o Japão se encontre em uma zona cinza no Leste Asiático caracterizada por um dilema de segurança, isso não ocorre pois as relações estatais são naturalmente conflituosas ou que os Estados naturalmente buscam por uma expansão de seu poder, como poria o realismo. Na verdade, as nações ali localizadas moldaram suas relações de tal forma haja vista diferenças identitárias, diferenças em interesses nacionais e constrangimentos que puseram esses Estados em uma situação de rivalidade.

1.1. Conclusões do capítulo

Em suma, identifico que a vertente construtivista de Relações Internacionais é a que melhor se enquadra na análise do ciberespaço, das ameaças que dele advém e da inserção do Japão nesse cenário, pois o construtivismo de suas relações é o componente formador do teatro de segurança no qual o Japão está inserido. Por um lado, neste contexto temos agentes com identidades historicamente construídas de maneira contrastante, o que criou identidades e nacionalismos antinipônicos no caso das Coreias e da China por motivos de dominação colonial, por exemplo, ou como no caso da Rússia, que estabeleceu com o Japão diferenças identitárias majoritariamente por motivos políticos, haja vista o alinhamento japonês ao Ocidente e o tipo de dependência dos Estados Unidos gerada disso. De outro lado, os constrangimentos mutuamente causados por esses agentes tornaram a estrutura que estão inseridos em uma zona cinza, onde existe cautela para se avançar em face à possibilidade de conflito tendo em vista seu histórico de relações.

De mesmo modo, as relações do Japão com suas contrapartes ocidentais também se dão em termos construtivistas, visto que existe uma prioridade por parte do Japão em cooperar com nações com pensamento similar, ou *like-minded*. Esse alinhamento a Estados com mentalidades afins não só indica o tipo de identidade internacional de preferência e, ao mesmo tempo, adotada

pelo país, como delineia o tipo de comportamento praticado pelo Japão em determinados temas, como seu setores de segurança tanto tradicionais quanto cibernéticos. No caso da segurança cibernética, por exemplo, observa-se um esforço para fazer convergir as práticas japonesas com aquelas de seus parceiros estratégicos, compondo uma espécie de grupo que trabalha a favor deste coletivo delimitado, em detrimento daqueles países que não fazem parte da identidade, já que com esses o conjunto de interesses nacionais e de afinidades diverge.

Por conseguinte, outras configurações da segurança tradicional e cibernética do Japão estão de acordo com os pressupostos da vertente construtivista, como a aceitação de outros agentes para além do ente estatal como componentes do sistema internacional. Nesse caso, o ponto de maior destaque no tema cibernético, especificamente, é a participação da esfera privada japonesa na vida securitária da nação, tema que será exposto com mais clareza no capítulo quatro. Inclusive, dentro da própria esfera privada japonesa existem vieses identitários, por exemplo, visto que os entes privados no Japão igualmente se alinham a uma determinada visão de mundo e a um determinado grupo de países com mentalidade similar, assim como a estrutura público-estatal. Dessa forma, seja no âmbito público, seja no privado, as relações regionais e internacionais do Japão estão ancoradas em preceitos identitários, em alinhamentos por interesses nacionais e em contextos construídos por constrangimentos estruturais, pautados na dualidade de amizade com o Ocidente e desconfiança com sua própria região.

2. A FORMAÇÃO DO COMPLEXO DE SEGURANÇA JAPONÊS

Antes de se chegar ao caso da segurança e da defesa cibernéticas do Japão *per se*, faz-se necessário entender como se formou o teatro de segurança no qual o país está inserido, visto que eu argumento que sua segurança cibernética é um reflexo direto da segurança do país nos moldes tradicionais. Ao final desta seção poderemos constatar como o xadrez de segurança do Leste Asiático foi sumariamente construído por elementos como identidade nacional e regional, legados coloniais, percepções de amizade e inimizade e mesmo cultura da memória, o que coloca os indivíduos como protagonistas da formação desse complexo de segurança através de fatores culturais.

Dessa forma, esse capítulo explora como o Japão, a partir da ideia de Pan-Asianismo, passou a delinear o teatro de segurança do Leste Asiático e, em menor medida, de outros países da região para além deste subcontinente. Nesse processo, o Pan-Asianismo foi submetido a duas reformulações, no pós-Primeira Guerra e no pós-Segunda Guerra, desempenhando distintos papéis a depender do momento histórico (RYŪHEI, 2007). Junto do Pan-Asianismo encontram-se as consequências da belicosidade japonesa ao longo da primeira metade do século XX, sendo essas primordiais na configuração das atuais relações regionais do Japão com seus vizinhos imediatos da Ásia. Como consequência, graças a esses acontecimentos novas camadas foram adicionadas ao teatro de segurança que encontramos hoje no Leste Asiático e que afetam a segurança cibernética do país.

2.1. O Pan-Asianismo na Era Meiji e a primeira metade do século XX

A ideia original de Pan-Asianismo surgiu no Japão como contraponto à política externa vigente da Era Meiji (1868–1912). Naquele período, conforme aponta Sven Saaler (2007), o governo Meiji tinha como objetivo se juntar ao "clube" das grandes potências da época após a abertura forçada do Japão e da China ao exterior por potências ocidentais, em meados do século XIX. Isso fez com que ambas as nações tivessem que se redefinir no cenário internacional, o que levou o Japão, neste caso, a buscar uma modernização e uma ocidentalização, o que ruiu o tradicional sistema sinocêntrico no Leste Asiático (SAALER, 2007). Devido a esse rearranjo político na região, o Governo Meiji passou a negar seu pertencimento à Ásia e se considerar uma nação ocidental, assim como as demais potências da época, dado que o modelo padrão de Estado desenvolvido incluía apenas nações ocidentais na ótica de soberania estatal, o que excluía nações não ocidentais desse jogo de soberania por serem tidas como inferiores

(RYŪHEI, 2007). Logo, fazer parte do Ocidente era a única forma, a partir dessa visão, de ser internacionalmente respeitado pelas potências dominantes do século XIX, e aqui se percebe uma alteração no comportamento japonês em face a uma mudança na estrutura na qual o país estava inserido.

Outra justificativa para esta mudança reside no fato de um dos traços mais marcantes da política externa japonesa ao longo da história é seu alinhamento à "potência do dia", como mencionado por Hook et al. (2012). Assim como ocorreu até o século XIX, o Japão gravitava ao redor da China por essa ser a maior potência da região, o que permitia que o Japão importasse uma série de habilidades administrativas e *know-how* na produção de armamentos, por exemplo, responsável pela unificação do Japão no século XVI. A partir do momento que a ordem sinocêntrica foi derrubada, portanto, o governo japonês deu continuidade à sua política de alinhamento à potência do dia e passou a gravitar junto das grandes potências ocidentais, em especial dos Estados Unidos. Esse novo alinhamento aos EUA e ao Ocidente novamente propiciou ao Japão a importação de técnicas ocidentais de administração e tecnologia militar, traduzindo-se novamente em uma forma de nova unificação nacional pós-Restauração Meiji.

Nesse contexto, o Pan-Asianismo foi concebido com o intuito de estruturar uma nova identidade nacional no Japão contrária a esse *status quo*, a qual clamava por um retorno do Japão à Ásia e a seus valores e sua cultura tradicionais, criticando a modernização, ou ocidentalização, do país. Isso posto, a visão embrionária do Pan-Asianismo enfatizava traços comuns do Japão com as demais nações de seu entorno, o que justificaria a necessidade de os países asiáticos se unirem contra a invasão ocidental em vigor no continente que punha em risco a identidade histórica da região[6], sempre calcado em preceitos de integração, solidariedade e identidade regionais (SAALER, 2007). Devido ao Pan-Asianismo, portanto, o debate identitário no país ora indicava o Japão como país asiático, ora como país ocidental, dado o posicionamento do governo Meiji[7].

Saaler (2007) ainda aponta que, com a vitória do Japão na Guerra Russo-Japonesa (1904–1905), a visão Pan-Asianista do Japão começou a ganhar espaço na Ásia, em especial no Sul e no Oeste do continente, bem como no mundo árabe, visto que um país asiático havia conseguido derrotar uma potência considerada ocidental pela primeira vez. Nesse momento, os

[6] Considerando que ao final do século XIX e início do século XX uma quantia expressiva de países asiáticos era colônia de potências ocidentais e, portanto, haviam sido invadidos e dominados pelo Ocidente.

[7] A exemplo do posicionamento pró-Ocidente do governo Meiji estava o slogan "abandonar a Ásia, juntar-se à Europa", cunhado por Fukuzawa Yukichi (1834–1901), educador e formador de opinião japonês neste período, conforme aponta Hatsuse Ryūhei (2007). A política externa *mainstream* do Japão na Era Meiji, portanto, era "baseada no duplo padrão dos códigos de conduta de potência ocidentais configurado dentro do sistema de Estados ocidental" (RYŪHEI, 2007, p. 229).

ideais Pan-Asianistas japoneses não só começam a ser acatados por outras nações asiáticas, como o país passou a ocupar o posto de líder regional, haja vista sua distinta superioridade militar no continente e seu destaque na cena internacional[8]. Aponta-se aqui como a sucessão de vitórias do Japão na Guerra Sino-Japonesa e na Guerra Russo-Japonesa desencadeou reações distintas no Ocidente, grupo que o Japão tentava adentrar. Enquanto a vitória do Japão contra a China foi bem vista pelo Ocidente por significar uma derrota da China "amarela", a vitória contra a Rússia reverberou negativamente dentre as potências da época por ter sido um golpe contra uma "potência branca" (HOOK et al., 2012), primeira ocorrência do tipo até aquele momento.

É só em 1916, entretanto, que as bases do Pan-Asianismo são postas em palavras pela primeira vez, por Kodera Kenkishi[9], em um texto intitulado *Treatise on Greater Asianism*. Para ele, o que definia a unidade cultural dos povos do Leste Asiático era o uso de ideogramas chineses como sistema de escrita, o que está diretamente conectado à proximidade geográfica e ao legado histórico do Japão à ordem sinocêntrica, a qual representava, antes da Era Meiji, uma estrutura tradicional de relações interestatais no continente, tanto em matéria de política quanto de economia; da mesma forma, dentre os povos asiáticos existiria um senso de família, visto que todos pertenceriam à chamada raça amarela; por fim, o sentimento de destino comum na luta contra o imperialismo ocidental, ou mesmo contra a modernização do continente, seria um dos pontos de convergência das nações asiáticas (SAALER, 2007)[10].

É após a Primeira Guerra Mundial (1914–1918), no entanto, que o Pan-Asianismo começa a tomar novas formas no Japão e na Ásia e passa a ser uma possibilidade real de política externa. Neste momento, segundo Saaler (2007), a identidade Pan-Asianista alcança a política nipônica, muito por conta do claro potencial militar do Japão na cena internacional, visto que o

[8] Saaler (2007) ressalta, entretanto, que a despeito da adesão da Ásia ao movimento originado no Japão, os países do continente viam o Pan-Asianismo com suspeita, e um dos exemplos deste caso é o acadêmico chinês Li Dazhao, o qual advogava favoravelmente à união de nações asiáticas mais fracas para combater o Pan-Asianismo japonês. De mesmo modo, por parte de pensadores japoneses também havia críticas contra o movimento iniciado no país, mesmo que escassas. Miyazaki Torazō, por exemplo, rejeitava que o Japão deveria ser o líder do continente, visto que para ele apenas a China tinha o prestígio, os recursos, o capital humano e o tamanho geográfico para ocupar tal posto na Ásia.

[9] Ávido pesquisador de política externa e, à época de sua declaração, pertencente à câmara baixa, ou câmara dos deputados, do parlamento japonês. Ocupou o cargo por seis mandatos, de 1908 a 1930, e foi um dos expoentes na disseminação das ideias Pan-Asianistas na primeira metade do século XX.

[10] Apesar de a definição de Pan-Asianismo ter surgido nesses moldes apenas em 1916, Itagaki Taisuke, outro figurão japonês, já havia feito discursos na *Taiwan Assimilation Society*, em 1914, assinalando que o Japão e a China não tem basicamente nenhuma diferença em termos de modos e de costumes, sendo que os dois países têm a mesma cultura e pertencem à mesma raça (*dōbun dōshu*, 同文同種), convergindo com os pressupostos de Kenkishi. A nível de observação, a *Taiwan Association Society* foi um Movimento cujo objetivo era promover relações harmoniosas entre japoneses e taiwaneses baseado no preceito de igualdade racial, e Taisuke era um de seus fundadores.

país havia sido parte do grupo de vitoriosos da Primeira Guerra, mas também pela influência de grandes jornais da época através de publicações com teor Pan-Asianista que acabaram por alcançar e influenciar o pensamento de elites e políticos japoneses. Dado seu crescente poder nacional, desse modo, o Japão passa a reivindicar uma liderança na região e desvirtua os aspectos fundantes do Pan-Asianismo na nação, passando a focar agora em como o país tinha a "missão sagrada" de libertar a Ásia e unir a humanidade. Nesse sentido, o Pan-Asianismo começa até mesmo a adotar um tom religioso, identificando o Japão como sendo uma "terra dos deuses" e, portanto, o verdadeiro Reino do Meio em detrimento da China, país que passava por constantes trocas dinásticas e por governanças tártaras que manchavam a política chinesa.

A partir dessa mudança de interpretação do Pan-Asianismo e de sua incorporação à política japonesa, essa identidade transicionou de um tipo de oposição política, no período Meiji, para uma forma mutada de posicionamento político dentro das próprias estruturas governamentais, ao final da década de 1930, na chamada "Nova Ordem" asiática (SAALER, 2007). Devido a essa nova faceta do Pan-Asianismo no Japão e através do entendimento de que o Japão era superior e, portanto, um líder nato na Ásia, as nações asiáticas começaram a rechaçar por completo a identidade Pan-Asianista, a qual estava sendo usado para legitimar a autoridade colonial japonesa e disfarçar o expansionismo nipônico sobre o continente. Foi nesse período que ocorreu o Massacre de Nanquim[11], por exemplo, uma das maiores feridas do passado colonial japonês sobre a China, até hoje lembrado pelos chineses como um dos momentos mais nefastos do passado recente da nação, fruto de razões coloniais japonesas justificadas pelo Pan-Asianismo.

Desse modo, Ryūhei (2007) afirma que o Japão era a única exceção no continente asiático neste período, pois além de ser totalmente independente, já no século XIX havia iniciado suas empreitadas expansionistas e se juntado para mais ou para menos a esse clube das grandes potências ocidentais, colonizando vizinhos como Taiwan, Coreia, Sacalina do Sul,

[11] A 13 de dezembro de 1937, ao longo da Segunda Guerra Sino-Japonesa, o Império do Japão tomou a cidade de Nanquim, então capital da China, e causou a destruição da cidade e uma série de assassinatos e estupros em massa que vitimaram milhares de pessoas. Não existe consenso ou registros oficiais para o número de mortos, mas tanto a academia quanto o governo da China estimam que o número de perdas alcance a casa das 300 mil pessoas, entre militares e não-combatentes. Há autores que indicam um número de até 500 mil se considerarmos aqueles que fugiram e se tornaram deslocados internos por conta do ataque. O assalto foi anos mais tarde classificado como um crime de guerra em diversos escalões. Além do ocorrido em si, o que é carregado pela China até hoje como uma mágoa histórica contra o Japão, soma-se o fato de que muitos na sociedade japonesa, especialmente nacionalistas e figuras políticas, diminuem ou menosprezam esse ataque, ou mesmo negam completamente sua ocorrência através de revisionismos históricos contraditórios (WAKABAYASHI, 2007). Por fim, o governo japonês nunca adotou uma postura clara a respeito da atrocidade, deixando esta página em aberto na história de seu povo e do povo chinês, o que é recorrentemente utilizado pela China como justificativa para sua desconfiança e constante inimizade com o Japão, levantando inclusive a bandeira de que Tóquio é imprevisível e que a história pode voltar a se repetir se a China não se manter alerta quanto à atuação japonesa.

península de Liaotung, Micronésia e, indiretamente, a Manchúria. O autor menciona ainda que se analisarmos a Ásia pré-Segunda Guerra Mundial, praticamente todas as nações do continente eram colônias ou do Japão, ou de potências ocidentais, evidenciando como o Japão se destoava do restante das nações asiáticas por conta de seu poder e influência, muito embasados no Pan-Asianismo incorporado à política no pós-Primeira Guerra.

Nesse quesito, a invasão japonesa sobre a Ásia pode muito mais ser comparada às invasões nazistas sobre a Noruega e sobre o Cáucaso russo ao longo da Segunda Guerra Mundial que de fato com uma tentativa de libertar o continente do Ocidente, visto que, acima de tudo, a tomada de recursos naturais para a continuidade de seus esforços militares era o objetivo central do Japão Imperial[12]; o Pan-Asianismo distorcido pelo governo japonês, portanto, utilizou a libertação da Ásia como pano de fundo para justificar seu expansionismo no continente. Dessa maneira, ao invés de superar fronteiras nacionais, o Japão passou a criar outras divisões por motivos de guerra, e libertar a Ásia nunca havia sido um objetivo de fato do Império Japonês (SAALER, 2007). Assim, visto que o objetivo do Japão era se tornar uma das grandes potências da época e se juntar ao Ocidente, essa tomada de colônias na região, como Taiwan em 1895 e a Coreia em 1910, foi apenas uma cópia do comportamento ocidental na região. A colonização era interpretada como uma forma de o Japão sobreviver e prosperar naquele contexto e era tido como um movimento legítimo de uma potência, visto que era assim que as contrapartes ocidentais atuavam (HOOK et al., 2012). Esse esforço nipônico sobre a Ásia passou a ser chamado pela literatura especializada de *Greater East Asia Co-Prosperity Sphere*, aqui definido pelo nome em português "Esfera da Coprosperidade". No pós-Segunda Guerra, como será apresentado na seção seguinte, o Pan-Asianismo como um todo passou a ser um sinônimo da Esfera de Coprosperidade e, portanto, evitado no discurso político pós-1945.

É importante ressaltar, entretanto, que o relacionamento entre o Japão e as potências ocidentais era dotado de expectativas diferentes por ambas as partes. Enquanto o Japão tinha como objetivo ser absorvido pelo sistema de potências ocidental, o Ocidente não considerava o Japão como um membro pleno desse grupo de países, muito por conta de questões raciais. Apesar de o Japão ter sido parte dos Aliados na Primeira Guerra Mundial e ser dotado de todos os requisitos para se juntar definitivamente a esse grupo de potências, o país era segregado por não ser factualmente ocidental, e no exemplo do Tratado de Versalhes, não recebeu as mesmas recompensas que os países de fato ocidentais. Além disso, a cláusula de igualdade racial

[12] Nesse caso, as invasões japonesas não se assemelham às alemãs por motivos ideológicos próprios do sistema alemão, mas sim como forma de obtenção de recursos naturais em território estrangeiro para continuidade dos esforços de guerra japoneses.

proposta pelo Japão na Liga das Nações foi rejeitada pela organização, demonstrando como não havia interesse por parte do Ocidente em colocar Estados não-ocidentais em um mesmo pé de igualdade. Essa é a justificativa pela qual o Japão, anos mais tarde, alinhou-se à nova potência do dia, a Alemanha Nazista, como forma de se livrar desse estrangulamento ocidental e reivindicar seu espaço no xadrez das grandes potências, dado que os líderes políticos nipônicos passaram a enxergar o sistema ocidental como tendencioso contra o Japão (HOOK et al., 2012).

Saaler (2007) continua que, nesse momento de inflexão no movimento Pan-Asianista, seu ápice se deu em 1943, em meio à Segunda Guerra Mundial, quando Japão, Machukuo, China, Burma, Tailândia e Filipinas se reuniram em Tóquio, na *Assembly of Greater East Asiatic Nations*, para definir o futuro da Ásia. Nessa ocasião, chegou-se à conclusão de que "países asiáticos deveriam formar alianças com o intuito de serem permanentemente libertos da intervenção, do controle e da ocupação estrangeiras" (SAALER, 2007, p. 13), como contraponto à Carta do Atlântico, culpando os Estados Unidos e o Reino Unido pela agressão e exploração do continente, inclusive como sendo essas as razões para a guerra em vigência (IBID, 2007). Em cerca de dois anos após a conferência, entretanto, o Pan-Asianismo foi de seu ápice à sua falência por conta da derrota do Japão na Segunda Guerra, quase desaparecendo na Ásia. Dessa maneira, da criação do movimento na segunda metade do século XIX como uma forma de união dos povos asiáticos contra a invasão ocidental, até seu ponto alto e quase extinção na década de 1940, naquele momento interpretado como um movimento expansionista e colonizador, cerca de 80 anos se passaram. O Pan-Asianismo, ao final de 1945, foi cristalizado na ideia da Esfera de Coprosperidade e é até hoje lembrado como o momento em que o Império do Japão usou de sua brutalidade para subjugar os povos asiáticos.

2.2. O período da Guerra Fria e o século XXI

Ao final da Segunda Guerra Mundial, a inserção do Japão no sistema internacional foi modificada por completo devido à sua derrota no conflito e à subsequente ocupação americana no país até 1952. O governo de Tóquio cogitou neste período adotar um viés de neutralidade e não alinhamento, mas a despeito dos bombardeios nucleares sobre o Japão, a classe política japonesa optou por se alinhar à potência do dia e ter os Estados Unidos como principal aliado, bilateralismo cristalizado pela Doutrina Yoshida (HOOK et al., 2012)[13]. É neste período

[13] Hook et al. (2012) também apontam que essa relação bilateral com os EUA era plenamente suficiente a ponto de o Japão evitar debates de segurança com outras nações, dado que poderiam enfraquecer o arranjo de segurança com os Estados Unidos.

também que o Japão assina seu primeiro acordo de cooperação mútua com os EUA, em 1951, consolidando a presença americana no Leste Asiático de maneira permanente. Isso posto, observa-se que desde o fim da Segunda Guerra Mundial o Japão adotou ao menos dois grandes vieses em sua política externa. O primeiro, no contexto da Guerra Fria, caracterizava-se pelo alinhamento automático aos EUA e por meios diplomáticos quando outros atores eram envolvidos, sendo que toda e qualquer relação internacional securitária era canalizada pelo ANPO. Isso se deu não só pela desmilitarização do país conforme colocou sua nova Constituição, mas também pelo exercício de ruptura com seu passado colonial. Para além da própria Doutrina Yoshida, esse comportamento securitário do Japão pode ser visto como política em outros planejamentos estratégicos ao longo da Guerra Fria, como a Doutrina Fukuda; proposta em 1977 pelo então premiê Takeo Fukuda, seu pressuposto básico indicava que o Japão não pretendia se tornar uma potência militar na região, muito menos balancear o poder militar em declínio dos EUA sobre o continente. Pelo contrário, esforços diplomáticos e a expansão de sua Assistência Oficial ao Desenvolvimento (ODA) aos países do Leste e do Sudeste Asiáticos foi o que definiu as diretrizes securitárias do Japão nesse período (HOOK, et al., 2012).

No que tange às ameaças securitárias contra o Japão ao longo da Guerra Fria, a contenção da Coreia do Norte foi uma preocupação recorrente neste contexto e compartilhada entre o Japão, os Estados Unidos e a Coreia do Sul. Essa percepção comum de ameaça foi responsável tanto pelo estreitamento das relações bilaterais entre os japoneses e os sul-coreanos, como também entre o Japão e os próprios Estados Unidos, uma vez que com a renovação do ANPO, em 1960, ambos os países se comprometeram a repelir a Coreia do Norte na região. Apesar de ao longo da Guerra Fria existir esta espécie de triângulo securitário Coreia do Sul-EUA-Japão, as relações entre os japoneses e os sul-coreanos nunca se aprofundaram verdadeiramente. Como expõem Hook et al. (2012), a barreira colonial entre esses dois países assegurou que nenhuma conexão profunda fosse estabelecida entre ambos, ao passo que os EUA sempre seriam o país através do qual suas relações se dariam, como através da concessão de bases militares aos americanos em solo japonês para proteção da península coreana. Os dois fatores que possivelmente mais colaboraram com o estreitamento das relações entre o Japão e a Coreia do Sul foram (1) a pressão conjunta exercida pelos dois países sobre a administração Carter, em 1977, clamando pelo abandono do plano americano de retirar suas tropas da Coreia do Sul, o que poria em risco a segurança de todo o Leste Asiático haja vista uma possível invasão do Norte; e (2) a ODA japonesa que passou a ser destinada à Coreia do Sul, o que influenciou a estabilidade sul-coreana positivamente durante a Guerra Fria.

Nessa conjuntura, a situação da China era semelhante à da Coreia do Norte: o Japão e os EUA compartilhavam uma política securitária de contenção deste país, e assim como as bases americanas em solo japonês serviam para evitar uma invasão da Coreia do Norte sobre a do Sul, impediam também um eventual avanço chinês sobre Formosa. Nesse sentido, a Ilha de Taiwan também foi adicionada sob o escopo do ANPO em 1960. Hook et al. (2012) dizem que, da parte chinesa, imaginava-se que essas movimentações serviam para manter a China dividida e reviver o militarismo japonês em apoio à hegemonia americana no Leste Asiático. Na mentalidade política japonesa da época, por outro lado, o poder absoluto dos EUA no Leste da Ásia seria suficiente para dissuadir qualquer contenda envolvendo a China na região, e nem mesmo o desenvolvimento de armas nucleares pelos chineses a partir de 1964 colocaria em cheque o guarda-chuva securitário promovido pelos Estados Unidos. Ao fim e ao cabo, o saldo das relações sino-japonesas ao longo da Guerra Fria oscilou para mais ou para menos, mas manteve-se relativamente estável ao longo do período. As décadas de 1970 e 1980 são destaque, visto que nesses anos observou-se uma reaproximação entre os EUA e a China com o intuito de contrabalancear a ameaça soviética, bem como a normalização das relações sino-japonesas, demonstrando como os chineses tolerariam o ANPO em certa medida (HOOK et al., 2012).

No contexto pré-1991, portanto, David Welch (2011) aponta que sequer há concordância se o Japão tinha de fato uma estratégia nacional que focasse em segurança ao longo desse período, seja pela falta de mentalidade ou pela falta de necessidade em se pensar tal política, uma vez que os Estados Unidos se encarregavam quase que totalmente do assunto conforme proposto pela Doutrina Yoshida. Desse modo, com o término da Guerra Fria, o sentimento de que a nação estava desassistida frente a uma possível retirada dos EUA da região foi o que irrompeu o segundo viés da política externa nipônica desde o fim da Segunda Guerra, o qual está vigente até o presente, que se resume na proatividade internacional japonesa baseada no multilateralismo em seus debates políticos e securitários. Além desse fator, observa-se também que com a dissolução da União Soviética (URSS) muitas barreiras foram eliminadas na Ásia, como com a diminuição das tropas soviéticas (russas) no continente, ou mesmo a ausência do próprio tensionamento bipolar em si, visto que a Guerra Fria exigia dedicação total ao tema como pauta securitária do norte global.

Desse modo, após o cenário de bipolaridade e o desaparecimento de uma das figuras antagônicas globais, figurou-se no Leste e Sudeste Asiáticos a reemergência de conflitos regionais que se tornaram problemas de segurança notáveis. As disputas entre o Japão e a China sobre as Ilhas Senkaku, sobre as Ilhas Paracel e Spratly, neste caso entre a China e o Sudeste Asiático, ou mesmo questões de soberania entre a Coreia do Sul e a Coreia do Norte ou China

e Taiwan, são exemplos desse reacendimento de conflitos. Assim, o governo do Japão anunciou no pós-Guerra Fria que iria explorar novas oportunidades oferecidas pelo fim do conflito, tanto para começar a superar seu legado colonial sobre a Ásia, quanto para aumentar diálogos de segurança e confiança com Estados da região (HOOK et al., 2012)[14].

Posto isso, o governo japonês procurou expandir suas relações multilaterais nessas duas regiões como forma de alinhar o maior número de países possível quanto a esses novos problemas de segurança. Como resultado, tem-se dois cenários básicos: a adição de pautas securitárias em organizações que naturalmente não tratam desse assunto, como a Cooperação Econômica Ásia-Pacífico (APEC) e especialmente a Associação de Nações do Sudeste Asiático (ASEAN), de um lado, e a inserção da China no máximo possível de arranjos multilaterais de segurança, por outro lado, uma vez que os chineses estão envolvidos na maioria dos problemas securitários da região e busca-se controlá-los através desses arranjos multilaterais (HOOK et al., 2012). Nesse quesito, destaco a ASEAN+3 e o Fórum Regional da ASEAN (ARF) como as duas instituições securitários mais significativas do Leste e Sudeste Asiáticos[15].

Quanto à abordagem de segurança internacional na ASEAN, o Japão foi pioneiro na inserção desses debates no âmbito da organização. Logo em 1991, o então Ministro das Relações Exteriores do Japão Tarō Nakayama propôs na Reunião Ministerial da ASEAN daquele ano que a organização deveria se tornar um "fórum para diálogo político [...] designado a melhorar o senso de segurança mútua" na região. Dois anos depois, em 1993, o ARF já estava formado, com adesão inclusive dos EUA, propiciando encontros anuais desde então para tratar da segurança da Ásia Oriental (HOOK et al., 2012). Esse tipo de diálogo de segurança é bastante visado pelo Japão, visto que não fere os princípios de sua Constituição e não rivaliza com o ANPO, dado que não há nenhum comprometimento militar ao arranjo, com o bônus de

[14] Sobre este ponto, é necessário mencionar que desde os anos 1990 o Japão ampliou também seu entendimento de o que é segurança internacional *per se*, dado que a segurança humana, por exemplo, figura como um dos maiores problemas de segurança internacional na atualidade segundo o Ministério das Relações Exteriores japonês (MOFA). Por conta disso, o Japão ampliou sua ajuda humanitária através do ODA para outras regiões do globo como forma de reverter cenários de subdesenvolvimento e pobreza, de falta de acesso à água potável, medicamentos e alimentos, bem como para mitigar efeitos de desastres naturais e questões ambientais que põem em risco a segurança internacional.

[15] Há uma série de outros arranjos multilaterais nos subcontinentes asiáticos, como as "*Ocean Peacekeeping Operations*" propostas pelo Japão em 2001 na ASEAN+3, que promovem exercícios conjuntos anti-pirataria nas águas da região. Outra organização proposta pelo Japão e que também realiza encontros anuais é *a Asia's Security Conference*, vinculada ao *International Institute for Strategic Studies*, que serve como contraponto ao ARF por se tratar de um encontro multilateral dos Ministérios da Defesa dos países membros; o ARF, nesse caso, é um encontro dos Ministros das Relações Exteriores de cada país. Por fim, outro organismo proposto pelo Japão foi o Diálogo de Segurança Quadrilateral (QUAD), este extrapolando o Extremo Oriente visto que é composto por Japão, Estados Unidos, Índia e Austrália, mas que desempenha um papel chave no balanço securitário no Pacífico. A China, como contraponto, constantemente adota um tom taxativo contra esse tipo de multilateralismo por considerar que o Japão está expandindo a sua presença naval e a da ASEAN nos mares circundando a China (HOOK et al., 2012).

promover a diplomacia política intrarregional não coercitiva.

Essas propostas japonesas de multilateralismo na Ásia sempre procuram incluir os EUA nos debates, dado que assim não só se pode ter uma maior influência dos EUA na região, o que vai de encontro aos objetivos estratégicos japoneses, como as próprias políticas de segurança do Japão são mais facilmente disseminadas com os Estados Unidos ocupando um assento nesses organismos (SAHASHI, 2016). Sendo assim, a presença americana no multilateralismo securitário da Ásia Oriental serve tanto para conter o avanço da China como para rebalancear a região, como consequência. Outro ponto estratégico ao Japão quanto a essa nova forma de se fazer política multilateral na Ásia é o interesse em recuperar a identidade regional junto dos países vizinhos, em tentativa de se reconciliar com a região e redesenhar sua imagem. Quanto a isso, o ex-Primeiro-ministro Jun'ichirō Koizumi (2001–2006) foi o principal político a incentivar a criação de uma comunidade regional que não só reinseriria o Japão na Ásia Oriental como estabilizaria a região através desse sentimento de pertencimento mútuo propiciados pelo regionalismo (TOGO, 2008).

De outro modo, Hook et al. (2012) também apontam que há algumas limitações nesse tipo de multilateralismo, como a necessidade de servir apenas como complemento ao acordo de segurança mútua com os EUA, visto que esse é o pilar da política securitária do Japão até hoje, e a própria forma de funcionamento do multilateralismo, dado que cumpre apenas um papel de diálogo em vez de ação, o que não garante que medidas concretas em prol da paz no Leste e Sudeste Asiáticos de fato sejam tomadas. Dessa maneira, as próprias ameaças contra o Japão acabam não sendo endereçadas como deveriam pela falta de ações concretas que contornariam a disputa territorial com a China sobre as Ilhas Senkaku, por exemplo, ou mesmo que arrefeceriam demais contextos sob constante pressão como as Ilhas Paracel, Spratly e Taiwan.

Para além do multilateralismo como foco de sua proatividade pós-1991, o Japão também se mostrou proativo através de sua atuação doméstica quanto à segurança nacional. Nesse aspecto, observou-se uma série de institucionalizações do tema, como a partir da criação do *National Security Council* (NSC) e da *National Security Strategy* (NSS), ambos em 2013, sendo a primeira vez na história que o Japão de fato pôs em palavras uma estratégia de segurança nacional. Nesses documentos, assim como em diversos outros, o Japão continua definindo o militarismo chinês e norte-coreano como as principais ameaças à segurança do Japão; em 2022, entretanto, a NSS foi revisada pela primeira vez e a Rússia passou a ser o tema de boa parte do documento, haja vista a Guerra da Ucrânia, o que modificou a percepção securitária da Rússia por parte do Japão. A década de 2010 também foi importante por ser um dos momentos em que a segurança cibernética japonesa mais evoluiu em termos de política, como será apresentado

em detalhes no capítulo seguinte.

Vale ser mencionado que, apesar da constância da ameaça chinesa na percepção securitária do Japão nas últimas décadas, observou-se no pós-Guerra Fria uma mudança de tom de Tóquio quanto ao país vizinho. Em 1999, por exemplo, as diretrizes do ANPO foram modificadas e, abandonando o caráter geográfico adotado pelo tratado em 1960, o acordo passou a avaliar situações que poriam em risco a segurança da região. Sendo assim, a China foi removida do escopo explícito do tratado, visto que pelo antigo caráter geográfico do ANPO Taiwan estava sob proteção do documento, colocando a China em uma zona cinza de atuação do bilateralismo nipo-americano, o que Hook et al. (2012) indicam como um ponto positivo para esse tempo. Nas *National Defense Program Guidelines* (NDPG) de 2004, por conseguinte, o Japão se referiu à China como "uma área de segurança regional para a qual o Japão deve se manter atento", na medida que em 2010 a questão chinesa já era descrita como "um problema de interesse da sociedade regional e global" (HOOK et al., 2012). Hoje, por outro lado, a China não só é enquadrada nos documentos oficiais do Japão como um dos maiores desafios do país no ambiente de segurança ao redor do arquipélago, como é descrito em detalhes que tipo de atividades efetuadas pelo país são ameaças ao Japão. O Ministro da Defesa Nobuo Kishi, por exemplo, menciona no LBD de 2022 que a China tenta unilateralmente modificar o *status quo* por coerção nos Mares do Sul e do Leste da China, e que tem se aproximado da Rússia, uma nação agressora, através de exercícios aéreos e marítimos em locais circundando o Japão; da mesma forma, a China tem deixado claro como não pretende hesitar em unificar Taiwan pelo uso da força, aumentando ainda mais as tensões na região (MOD, 2022). Dessa maneira, a descrição oficial do governo japonês sobre a ameaça chinesa sofreu mudanças ao longo dos últimos anos, fluindo de um breve período de arrefecimento a partir de 1999 para uma exposição declarada de como a China é uma ameaça contra o arquipélago.

No que tange aos EUA, as relações nipo-americanas desde o fim da Guerra Fria passaram por momentos de turbulência e realinhamento diversas vezes. Essas turbulências estão normalmente conectadas aos constantes pedidos por parte dos EUA para que o Japão se torne mais militarmente ativo no bilateralismo securitário entre os países, o que entra em choque com o Artigo 9 da Constituição do Japão, ao passo que os momentos de reaproximação são justamente aqueles em que o comportamento japonês é reajustado para suprir essas necessidades americanas. A exemplo, o não envolvimento do Japão na Guerra do Golfo, em 1990[16], junto da negativa japonesa em se envolver em um possível conflito durante a crise

[16] Apesar de o Japão não ter participado da Guerra do Golfo, essa contenda deixou seu legado na segurança nacional japonesa. Em 1992 a Dieta japonesa aprovou o projeto de lei intitulado "Ato de Cooperação Internacional

nuclear norte-coreana de 1994, colocaram em xeque a visão dos EUA quanto à perceria com o Japão (HOOK et al., 2012). Contudo, os atentados de 11 de setembro serviram para reinserir o Japão na causa americana e realinhar o país aos Estados Unidos, já que as Forças de Autodefesa japonesas participaram tanto da Guerra do Afeganistão, em 2001, quanto da Guerra do Iraque, em 2003, como forma de apoiar a "guerra ao terror" do governo de George W. Bush. Nesse sentido, em 2014 o gabinete do Primeiro-ministro compartilhou uma decisão controversa dentre a opinião pública, a qual autoriza o uso da "autodefesa coletiva" em missões no exterior em ajuda a aliados, especialmente para fortalecer a cooperação mútua com os EUA (CABINET SECRETARIAT, 2014). Visto que isso figura como uma reinterpretação da Constituição no que tange ao uso mínimo de força, o Artigo 9 do documento em tese não está sendo infrigido, e essa tática é uma forma de expandir a atuação das forças militares japonesas junto a aliados, como os EUA.

Há de se mencionar, entretanto, que a Guerra ao Terror dos EUA preocupou o governo japonês na medida que o foco dos americanos não mais estava no extremo da Ásia, mas sim no Oriente Médio. Desse modo, assim como houve receio no pós-Guerra Fria de que os Estados Unidos se retirariam do Leste Asiático por conta do fim da bipolaridade, a mesma preocupação surgiu no início dos anos 2000, visto que o Oriente Médio passou a ser o foco das preocupações e da política externa americanas. Essas mudanças nas operações das Forças de Autodefesa indicam, portanto, uma tentativa de o Japão voltar a ser um Estado normal que consiga garantir sua segurança por conta própria, dado que não será possível contar com a ajuda americana *ad eternum*, mesmo que no momento o bilateralismo com os EUA seja a opção mais certeira para suas políticas de segurança. Apesar dessa proatividade japonesa quanto à sua segurança, iniciada na década de 1990, o Japão assiduamente menciona o fortalecimento da parceria com os EUA como política de segurança básica, indicando que o país pretende balancear sua proatividade com seu alinhamento aos americanos.

Tratando-se da Coreia do Norte no pós-Guerra Fria, as relações entre o Japão e esse país estão tensas desde então por conta da série de testes nucleares e de mísseis balísticos realizados pelos norte-coreanos, muitos dos quais sobrevoam o Mar do Japão e o próprio território japonês. Para além da já mencionada crise nuclear de 1994, em 2017 ocorreu uma nova crise envolvendo a Coreia do Norte, dessa vez por conta de seus constantes testes de mísseis balísticos. O número

em Operações de Paz das Nações Unidas", através do qual as Forças de Autodefesa do Japão foram autorizadas a participar de missões de paz e humanitárias, na supervisão de eleições e na provisão de recursos a terceiros Estados, por intermédio das Nações Unidos (OLIVEIRA, 2019). Essa reorientação das SDF não só ilustra a proatividade japonesa que se iniciou na década de 1990, como começa a dar indícios de que as Forças de Autodefesa japonesas não se encaixariam mais em seus moldes tradicionais de atuação conduzidos até então.

de testes em 2017, contudo, é menor se comparado à quantia de testes realizados em 2022, por exemplo, evidenciando que a crise de 2017 não era o cenário mais crítico possível que se podia alcançar, uma vez que a situação atual é deveras mais tensa por conta da atuação militar norte-coreana. Quanto a seus testes com mísseis, a Coreia do Norte já demonstrou publicamente sua insatisfação contra o Japão e seus LBDs atuais, uma vez que o Japão estaria exagerando a chamada "ameaça de mísseis norte-coreana", pondo as políticas defensivas do Japão em choque com o posicionamento de seu vizinho.

Em resumo, o Livro Branco de Defesa (LBD) de 2022 exemplifica como o Japão enxerga seus vizinhos e qual é o posicionamento atual do país quanto às suas ameaças. Nesse documento, o governo do Japão robusteceu seu tom contra ameaças advindas da China, da Coreia do Norte e especialmente da Rússia, tanto pela eclosão da Guerra da Ucrânia em si, como pela preocupação de como este país pode vir a formar uma aliança com a China, a qual poderá sentir-se legitimada a invadir Taiwan e criar um cenário de conflito no Leste Asiático de maneira direta. Quanto a Taiwan, o LBD de 2022 dobrou a quantia de páginas direcionadas ao tema em comparação ao Livro de 2021. Além disso, ainda quanto à Rússia, o Japão demonstra-se preocupado com possíveis cenários de guerra híbrida criados pelo país e que poderiam ameaçar a segurança japonesa, envolvendo diretamente o uso do ciberespaço, o que exigiria do Japão maiores capacidades defensivas (MOD, 2022). Nesse cenário, acrescenta-se ainda as ameaças cibernéticas advindas da Coreia do Norte e da China que, juntamente da Rússia, são os três únicos Estados mencionados pelo Japão dentre aqueles que utilizam o ciberespaço de maneira maliciosa e que ameaçam a integridade japonesa nesse domínio.

Ao fim e ao cabo, Hook et al. (2012) dizem que, após a Guerra Fria, de todas as regiões do mundo compostas por grandes potências o Leste Asiático é a menos integrada regionalmente; por parte da Europa, por exemplo, tem-se um continente altamente institucionalizado na figura da União Europeia; no que tange à América do Norte, por outro lado, tem-se uma regionalização marcada pelo NAFTA; o Leste Asiático, entretanto, é a região que menos se integrou entre si e apresenta uma regionalização mais branda se comparada às demais regiões, tendo praticamente nenhuma institucionalização, mesmo levando-se em consideração as parcerias existentes com a ASEAN[17]. Isso posto, ao mesmo tempo que o país

[17] A ASEAN, neste caso, tem ocupado um papel central nas políticas securitárias do Japão por conta da relevância econômica que a organização representa para o Japão. O Sudeste Asiático não só é uma das principais fontes de matérias-primas e, ao mesmo tempo, mercado consumidor ao Japão, como está geograficamente entalhado no meio das rotas marítimas advindas do Oriente Médio, principal fornecedor de petróleo ao Japão. Assim, desde o LBD de 1980 o Japão destaca que a segurança da ASEAN é a segurança do próprio Japão (HOOK et al., 2012). Dito isso, esse é o motivo pelo qual a ASEAN rotineiramente é o órgão multilateral priorizado pelo Japão para questões de segurança.

continua gravitando ao redor da potência do dia, o Japão não deixa de usar de sua proatividade para perseguir seus objetivos internacionais, mesmo que isso não resulte em uma profunda integração regional.

2.3. As relações russo-japonesas

O Japão e a Rússia têm tido relações galopantes em termos de segurança internacional desde meados do século XIX, quando o Japão passou por sua abertura ao exterior. A Rússia, não obstante, foi a primeira nação ocidental a assinar um tratado em pé de igualdade com o Japão, em 1875, envolvendo a cessão dos territórios da Sacalina para a Rússia por parte dos japoneses, em troca da soberania sobre as Ilhas Curilas, até o limite da Península de Kamchatka, que estavam sob domínio russo (GRISHACHEV, 2019). Como mencionado no início deste capítulo, um dos pontos de maior conflito com o Ocidente neste período era a desigualdade com a qual o Japão era tratado pelas potências ocidentais em seus tratados internacionais, e a Rússia foi o primeiro Estado ocidental a romper com esse padrão em relação ao Japão. Esse reconhecimento formal de igualdade expresso pela Rússia foi fundamental para alavancar o emergente governo Meiji, ao passo que ambos os países coexistiram pacificamente devido a essa igualdade de tratamentos até o início do século XX (IBID, 2019).

As relações russo-japonesas tiveram seu ponto de virada no ano de 1904, quando o Japão declarou guerra contra a Rússia por conta de seu estabelecimento permanente na Manchúria como resultado da cessão da península de Liaodong à Rússia em 1895 e da Guerra dos Boxers de 1900[18]. Além de a presença russa na Manchúria ter sido um sinal de expansão do país sobre a Ásia, o que vinha ocorrendo desde a construção da Ferrovia Transiberiana, também representou uma ameaça à dominação japonesa sobre a península coreana. Essa percepção japonesa era justificada devido ao apoio russo a uma Coreia independente, conforme indica Igor V. Lukoyanov (2019). O governo do Japão, entretanto, tentou resolver a situação por vias diplomáticas, já que desde a Restauração Meiji o pacifismo passou a ser central à política

[18] A Guerra dos Boxers foi iniciada na China no ano de 1900, quando o grupo de mesmo nome, apoiado pela dinastia chinesa Qing, levantou-se contra as ocupações estrangeiras na China que vinham ocorrendo há mais de trinta anos no país. Nesse conflito, o Japão teve papel fundamental na estabilização do levante por enviar cerca de 40% das tropas estrangeiras que participaram do conflito, muito por incapacidade britânica em enviar suas próprias tropas, visto que o Reino Unido já estava ocupado com a Guerra dos Bôeres, na África do Sul. Nesse contexto, o Reino Unido compensou o Japão com o pagamento de GBP 1 milhão para enviar sua força militar à guerra; a participação japonesa, além de ter sido decisiva, serviu para mostrar ao Ocidente que o Japão era um país militarmente ativo e estruturado e deveria ser respeitado. Além disso, a guerra também foi simbólica por ter sido a primeira vez que um país asiático lutou ao lado de potências ocidentais em uma aliança. A Rússia, por fim, foi um dos países a participar do conflito ao lado dos vitoriosos e acabou por se estabelecer de maneira definitiva na Manchúria, inclusive com o desenvolvimento de infraestrutura no local (DARÓZ, 2018).

externa do país, mas mesmo a Rússia já tendo indicado que não tinha interesse na Coreia e que gradualmente se moveria para longe do país, conforme as concessões exigidas por Tóquio, o Japão optou arbitrariamente pelo conflito (LUKOYANOV, 2019).

No próprio ano de 1904, quando a guerra foi iniciada, as relações diplomáticas com a Rússia foram cortadas (DARÓZ, 2018). Duas das razões principais que garantiram a vitória dos japoneses no conflito foi a distância da Manchúria do governo central russo, o que impossibilitou o envio imediato de reforços por Moscou e garantiu a superioridade numérica do Japão, bem como a doutrina tática ofensiva do Japão que, apesar de causar um número expressivo de baixas em seu exército, assegurou um avanço implacável sobre os soldados russos (DARÓZ, 2018). A nível de comparação, os duros avanços japoneses se assemelhavam em algum grau com a *blitzkrieg* alemã. A Rússia, portanto, acabou sendo simbólica ao Japão tanto por ter sido o primeiro país ocidental a assinar um tratado em igualdade com os japoneses quanto por ter sido o primeiro país ocidental a ser derrotado por uma nação asiática. A vitória dos japoneses sobre a Rússia em conjunção à participação do país na Guerra dos Boxers, portanto, serviu para solidificar a imagem do Japão enquanto uma potência militar internacional.

No entanto, as diferenças russo-japonesas pós-conflito foram superadas por vontade política de ambos os governos, os quais restabeleceram suas relações diplomáticas em 1925 enquanto promoviam cooperação bilateral nas esferas econômica, política, militar e inclusive cultural, a ponto de se tornarem potenciais aliados na década de 1920 (GRINYUK, SHULATOV e LOZHKINA, 2019; PESTUSHKO e SHULATOV, 2019). Essa reaproximação era desgastada, contudo, pela rivalidade que ainda existia quanto à dominação de certas partes do território chinês, uma vez que tanto o Japão quanto a Rússia (agora União Soviética) estavam presentes na região do Mar Amarelo. Da mesma forma, a vontade soviética de disseminar o comunismo no Japão era constantemente frustrada pelo fato de o Partido Comunista Japonês ser um partido pouco expressivo no país (GRINYUK, SHULATOV e LOZHKINA, 2019).

Para além do óbvio desalinhamento entre os dois países durante a Segunda Guerra Mundial, visto que compunham alianças inimigas no conflito, o período pós-Segunda Guerra foi um momento em que as relações russo-japonesas novamente se desgastaram por conta do comportamento agressivo do Império do Japão ao longo do conflito. O Tratado de Amizade, Aliança e Assistência Mútua Sino-Soviético assinado entre a China e a URSS em 1950, por exemplo, logo em seu primeiro artigo aborda que a premissa da segurança coletiva entre os soviéticos e os chineses servia para prevenir um restabelecimento do imperialismo japonês, mas também reconhecia que ambas as nações deveriam assinar um acordo de paz com o Japão em

conjunção com as demais potências aliadas. Um ano mais tarde, em 1951, era a vez dos EUA e do Japão estabelecerem seu primeiro tratado de segurança mútua que, assim como o tratado sino-soviético, também previa que agressões contra um significavam agressões contra o outro país. Como previa o tratado entre a URSS e a China, o Japão de fato melhorou suas relações com os chineses a partir da assinatura de seu tratado de paz, em 1952, formalmente pondo um fim à Segunda Guerra Sino-Japonesa que perdurou de 1937 a 1945. Apenas em 1972, entretanto, as relações diplomáticas entre a China e o Japão foram restabelecidas, oficialmente declaradas através do Tratado de Paz e Amizade de 1978 assinado pelas duas nações.

Desde a primeira versão do ANPO, portanto, a aproximação entre Tóquio e Washington pôs em um crescendo as preocupações soviéticas quanto ao Leste Asiático. O acordo nipo-americano não afetava diretamente as relações entre o Japão e a URSS, mas tensionava essas relações dada a presença constante e assegurada de tropas americanas no arquipélago (HARUKO, 2019; CHUGROV, 2019). Além disso, a renovação do acordo em 1960, junto do Tratado de Amizade sino-japonês, foi interpretado negativamente pelos soviéticos visto que essa movimentação parecia isolar a URSS do cenário internacional em prol do fortalecimento de um triângulo Japão-EUA-China (HARUKO, 2019).

Shimotomai Nobuo (2019) resume que as relações russo-japonesas desde o fim da Segunda Guerra Mundial até o final da Guerra Fria são bem ilustradas pelas visitas oficiais de altas figuras políticas de cada país. Do lado do Japão, nesses mais de 45 anos apenas duas visitas oficiais foram feitas por líderes políticos japoneses de alto escalão, ao passo que Gorbachev, do lado soviético, foi o único líder da URSS a visitar o Japão, uma única vez, ao longo de todo esse período. Isso demonstra como essa relação bilateral era ao menos limitada e escassa, e que desse obstáculo surgiam problemas para ambos os lados pela falta de proximidade política. Nobuo complementa também que ao momento da Perestroika houve uma possibilidade de avanço nas relações nipo-soviéticas, mas que para as lideranças políticas japonesas essa reconstrução foi oferecida tardiamente.

Adentrando o século XXI, Kawaraji Hidetake (2019) aponta que o Japão tem tido dificuldades neste período para estabelecer relações mais saudáveis com seus vizinhos (incluindo a Rússia, mas não só), devido às disputas territoriais em andamento hoje. No caso específico da Rússia, a contestação de posse sobre os Territórios do Norte, assim como o fortalecimento do militarismo russo sobre a região, era um dos principais problemas no relacionamento russo-japonês ao menos até fevereiro de 2022[19]. Essa disputa territorial datada

[19] Hidetake igualmente menciona que a própria presença dos Estados Unidos em solo japonês também é, sob certos pontos de vista, uma disputa territorial contemporânea no Japão. Isso se dá, pois, não só a população japonesa

especificamente de 1945, meses antes do fim da Segunda Guerra Mundial, quando a União Soviética concordou em entrar em guerra contra o Japão, após a Conferência de Ialta, sob a condição de retomar a posse das Ilhas Curilas que estavam sob controle japonês[20], para além de outras recompensas.

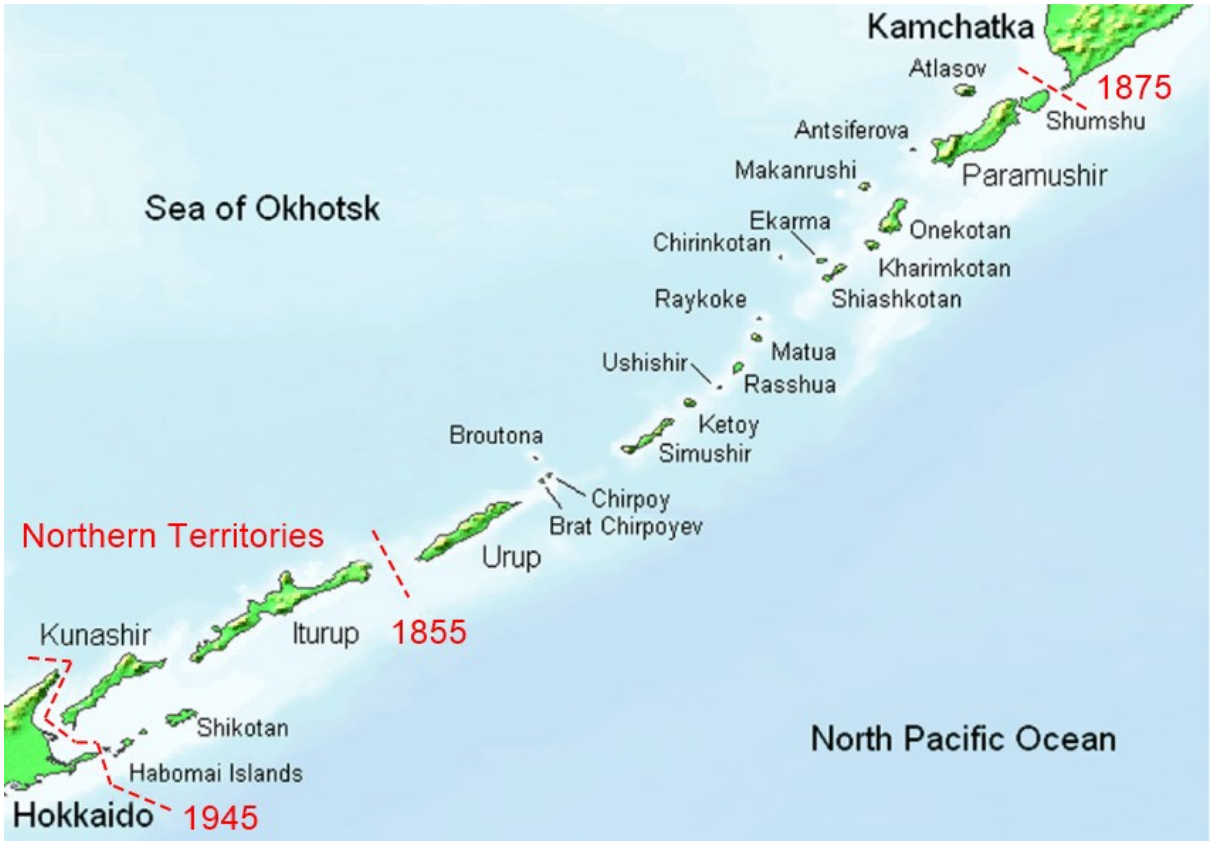
Entretanto, essa reconfiguração no controle das ilhas ocorreu de maneira unilateral e em violação ao pacto de não-agressão assinado entre os japoneses e os russos durante a Segunda Guerra, sem que o Japão pudesse negociar sua própria soberania sobre as ilhas. A questão com o Japão, neste caso, é que a Rússia deve devolver parte das Ilhas Curilas ao Japão, as que configuram os Territórios do Norte, visto que desde 1855 elas pertenciam ao Japão e não tinham sido negociadas no Tratado de 1875, então não seria legítimo que a URSS controlasse essa porção das ilhas. A partir da visão de 1855, portanto, as Ilhas de Habomai, Shikotan, Kunashiri e Etorofu são reivindicadas pelo Japão como parte integrante de seu território, já que a passagem dessas ilhas à URSS em 1945 ocorreu de maneira ilegítima. Assim, o problema maior nessa disputa territorial é a própria interpretação de o que são as Ilhas Curilas. Aos japoneses, as Ilhas Curilas começam a partir dos Territórios do Norte, então quando as Curilas foram passadas aos soviéticos em 1945, os Territórios do Norte não deveriam ter sido incluídos. Pelo lado russo-soviético, entretanto, as Curilas representam a totalidade do cinturão de Ilhas desde Hokkaidō até Kamchatka, o que inclui os Territórios do Norte nessa ótica e, portanto, pertencem legitimamente aos russos.

Andrey Kravtsevich (2019) menciona, no entanto, que a ilegitimidade e ilegalidade levantadas pelo Japão quanto ao controle russo sobre os Territórios do Norte não estão de fato amparadas pelo direito internacional, enredando a prerrogativa japonesa. Até a data, nenhum acordo foi alcançado entre os dois países apesar dos constantes diálogos bilaterais para a resolução desta disputa territorial, os quais perfuram a década de 2020. O posicionamento oficial do Japão, entretanto, continua sendo de que a Rússia está ocupando ilegalmente as ilhas, as quais são parte inerente do território japonês (MOFA, s.d.).

protesta contra o estabelecimento de bases militares americanas no país, em especial os okinawanos, como os países de seu entorno claramente tensionam suas relações com o Japão por conta dos contingentes militares mobilizados permanentemente no país.

[20] A configuração territorial neste momento se dava pelo Tratado de 1875 citado no início desta seção, quando pela primeira vez o Japão assinou um acordo em pé de igualdade com uma potência ocidental. Dessa maneira, a troca bilateral de territórios havia destinado a totalidade das Ilhas Curilas ao Japão, expandindo o controle japonês para além dos Territórios do Norte.

Figura 1 – Reivindicações sobre os Territórios do Norte entre o Japão e a Rússia



FONTE: RESEARCH GATE, edição própria.

Do mesmo modo, Hidetake (2019) também cita que o livre mercado e a integração militar que ocorre entre países normalmente estão conectados a reduções de antagonismos militares, mas que na Ásia-Pacífico ambos os fatores são causadores de conflitos entre o Japão e seus vizinhos. Isso se dá não só pelas diferenças políticas e econômicas russas, chinesas e norte-coreanas em relação ao Japão, como também pela conexão dos japoneses com os Estados Unidos, o que de certa forma perpetua uma batalha por hegemonia no Leste Asiático entre os EUA e a China. Desse modo, levando em consideração que a mentalidade russa ainda parece funcionar sob uma ótica de Guerra Fria moderna, a presença americana limita em grande medida um relacionamento mais profundo entre a Rússia e o Japão, assim como ocorre com a China e a Coreia do Norte, tendo em vista que os Estados Unidos estão estacionados no meio da estrada que conecta essas nações.

Como forma de superar esse antagonismo contra a Rússia, Hidetake finaliza dizendo que o Japão deveria se juntar à esfera econômica do nordeste asiático junto da China e das duas Coreias, como planejado por Moscou. Nesse caso, em 2011 os russos inauguraram um gasoduto que conecta as Ilhas Sacalinas com Vladivostok, o qual pretender ser expandido para a China e

as Coreias, juntamente de uma linha férrea que conectaria essas quatro nações. Isso posto, se o Japão fosse adicionado a esse rearranjo econômico da região, o país não só se beneficiaria economicamente como poderia reduzir as tensões militares que rodeiam o Leste Asiático. Entretanto, conforme apontam Hook et al. (2019), o Japão já rejeitou ao menos três propostas de reconfiguração securitária do Leste Asiático postas em discussão ao longo da Guerra Fria. A primeira foi sugerida pela União Soviética, em 1969, na forma de um arranjo de segurança coletiva no Leste Asiático, enquanto a segunda, proposta em 1988 também pela URSS, envolvia a criação de uma comunidade de segurança ampla para a região. Em ambas as ocasiões, o governo japonês interpretou as sugestões soviéticas como tentativas de barrar as parcerias bilaterais dos Estados Unidos, especialmente com o Japão e a Coreia do Sul, e que portanto não foram consideradas pelo parlamento japonês. Por fim, a proposição da ASEAN de Zona de Paz, Liberdade e Neutralidade, em 1971, tampouco foi bem recebida pelos japoneses, visto que esse arranjo parecia excluir a influência americana na região, o que não era interessante ao Japão naquele momento. Apesar de hoje o Japão ter uma política externa mais multilateralizada que no período da Guerra Fria, os japoneses ainda enxergam os EUA como seu principal aliado na região e não planejam abandonar esse bilateralismo para arriscar suas chances ao lado de uma eventual nova aliança.

Quanto a isso, Hook et al. (2019) também mencionam que, após a Guerra Fria, o Japão de fato iniciou conexões bi e multilaterais sobre segurança no Leste Asiático, mas sempre para complementar e nunca suplantar suas relações com os Estados Unidos. Nesse sentido, os EUA normalmente são parte integrante desses diálogos de segurança entre o Japão e outras nações da região, sendo responsável inclusive por iniciar muitas dessas aproximações. Dessa maneira, um rearranjo moderno do teatro de segurança no Leste Asiático como sugerido por Hidetake parece improvável dado o engajamento histórico do Japão com os EUA e a rejeição de outras formas de alinhamento securitário na região sem a presença americana.

Com isso quero dizer que é impossível desvincular a Rússia da segurança internacional do Japão, apesar de nas últimas décadas a China e a Coreia do Norte ocuparem o posto de principais ameaças contra o Japão de maneira mais marcada. Nesse contexto, com o início da Guerra da Ucrânia, a Rússia começou a se tornar uma ameaça mais proeminente contra o Japão na atualidade, em especial pelo tipo de influência que o conflito pode ter sobre a China. Isso tanto é verdade que a Rússia não era mencionada pelo MOFA, por exemplo, como uma das maiores ameaças contra o Japão quando o assunto eram Estados securitizados, indicando como ocupantes desse posto única e exclusivamente a China e a Coreia do Norte. Essa reorientação após a Guerra da Ucrânia é observável em documentos oficiais japoneses lançados após o início

do conflito, em especial sua *National Security Strategy* atualizada em 2022. Na primeira versão da NSS, em 2013, a Rússia foi brevemente mencionada em um único parágrafo de um documento de 37 páginas, no momento em que o Japão reconhece que por conta do estado severo de segurança no Leste Asiático, seria crítico cooperar com a Rússia em todas as áreas para garantir uma maior segurança à região. Da mesma forma, essa cooperação deveria seguir para uma negociação pacífica das disputas sobre os Territórios do Norte, a questão pendente mais importante entre os dois países (MOFA, 2013). Contudo, a NSS de 2022 dá uma guinada no assunto quando passa a indicar a agressão russa à Ucrânia como um rompimento das fundações e das leis que moldam a ordem internacional. Nesse sentido, a tentativa de mudança da ordem internacional inicialmente conduzida pela Rússia é identificada como uma preocupação basilar à segurança do Japão, uma vez que o grau de militarismo nas proximidades do arquipélago aumentou consideravelmente e outros países, como a China, podem adotar posturas de rompimento internacional similares (MOFA, 2022).

Esse possível *spill-over* temido pelas autoridades japonesas poderia ocorrer sobre Taiwan, na medida que a China poderia usar da força para dominar o governo da Ilha, o que representaria uma segunda ruptura da ordem internacional semelhante à que ocorre hoje na Ucrânia. Caso isso se concretize, uma invasão a Taiwan significaria um provável conflito militar muito próximo do território japonês e que possivelmente exigiria uma resposta japonesa, haja vista o alinhamento estratégico do país a Taiwan e seu papel no acordo bilateral com os Estados Unidos. Desse modo, desde o início da Guerra da Ucrânia, em fevereiro de 2022, a Rússia tem ocupado um novo papel na segurança internacional do Japão não só por representar uma ameaça contra o *status quo* internacional, como também pelo tipo de frisson que isso poderia causar em outros países securitizados pelo Japão.

No domínio cibernético, contudo, a Rússia tem ganhado seu espaço de preocupação no governo do Japão mesmo antes da Guerra da Ucrânia, seja pelo número de ciberataques que eram rastreados como advindos de lá, seja pelo tipo de guerra híbrida que o país vinha imprimindo no mundo. Uma das inquietações mais latentes envolvendo a Rússia e o ciberespaço, como será apresentado mais adiante, dizia respeito a possíveis ataques cibernéticos contra os Jogos Olímpicos de Tóquio, os quais não foram observados ou, se observados, não foram efetivos como os efetuados contra os Jogos Olímpicos de Inverno de 2018. Isso posto, enquanto os ataques contra a MHI são um exemplo real da ameaça chinesa contra as estruturas cibernéticas do Japão, e que os ataques contra a Sony Pictures representam a ameaça materializada da Coreia do Norte no mesmo domínio, o Japão não tem um exemplo similar de ataque cibernético russo que de fato chacoalhou a segurança cibernética do Japão. Os Jogos de

Tóquio poderiam ter sido esse exemplo, mas não foram. Dessa forma, diretamente contra o Japão, a ameaça russa continua sendo expressa pela ideia do que pode vir a ocorrer, não do que já ocorreu contra o país como nos exemplos chinês e norte-coreano.

Mesmo assim, a CSS de 2021 foi o primeiro documento cibernético a apontar a Rússia como uma das principais ameaças contra o país no ciberespaço, ao menos nesse domínio, um ano antes da NSS fazer o mesmo, nesse último caso elevando o país ao patamar de principais ameaças contra o Japão de forma ampla independentemente do domínio. Entretanto, volto a mencionar como nesse momento a Rússia é elevada a uma das principais ameaças cibernéticas contra o Japão não porque de lá advêm ataques cibernéticos severos – como mencionado, não há exemplo histórico de grandes ciberataques russos contra o Japão –, mas sim pelo tipo de guerra de informação e guerra híbrida que vem sendo efetuada pela Rússia em outras regiões do mundo, o que presumidamente ameaça o Japão. Sendo assim, os russos estão recomeçando a ocupar um espaço de ameaça notável contra o Estado japonês apenas agora, haja vista a ruptura da ordem internacional como fruto da Guerra da Ucrânia, conforme indicado na NSS de 2022.

Esta contextualização histórica, portanto, permite mostrar que o Japão e a Rússia tiveram constantes relações de proximidade e distanciamento ao longo do último século e meio, inclusive com mudanças repentinas de alinhamento, como com a eclosão precipitada da Guerra Russo-Japonesa. A atual conjuntura representa perfeitamente essa tendência história de relacionamento errático entre os dois países: apesar de haver ranhuras no relacionamento da Rússia e do Japão no ciberespaço há mais tempo, até antes da Guerra da Ucrânia seu relacionamento num cenário mais amplo era interpretado como de possível cooperação, inclusive para maior estabilidade do Leste Asiático. Após a invasão da Ucrânia, entretanto, o governo japonês rapidamente levantou um muro entre os dois países e devido a essa ruptura da ordem internacional reescreveu sua NSS para comportar a atual postura russa de choque com o Ocidente. Diferentemente do início da Guerra Russo-Japonesa em 1904, fruto de decisões e ações mal tomadas por políticos nipônicos com visão fechada, citando as palavras de Lukoyanov (2019)[21], desta vez o posicionamento japonês contra a Rússia tem justificativas mais sólidas.

2.4. O resíduo social pós-colonização

[21] Muito conectado aos conceitos de "percepções e falsas percepções" propostos por Robert Jervis (1976).

Parto do pressuposto que existem ao menos três grandes testamentos do período colonial japonês no Leste Asiático que são responsáveis, ao fim e ao cabo, por moldar as bases do teatro de segurança moderno da região, o qual tem o Japão como foco central na interpretação de ameaça pelos seus vizinhos e vice-versa: (1) o quase desaparecimento do Pan-Asianismo no país e na Ásia e a percepção que disso restou; (2) a simbologia do Santuário Yasukuni e a reatividade das nações vizinhas; e (3) os legados diretos da Segunda Guerra Mundial nas relações intra-Leste Asiático. Em linhas gerais, isso se dá, pois, o Japão ainda tende a exaltar seu período imperial em detrimento de se retratar frente às nações afetadas no passado para superar esse seu tempo histórico. Além disso, o país tende a perpetuar seu alinhamento à potência do dia, colocando em choque os interesses e as expectativas das nações do Leste Asiático com o Japão, haja vista a estrutura em que estão inseridos.

Iniciando pelo Pan-Asianismo, essa identidade e posterior forma de política externa foi praticamente eliminada do Japão, em parte pela derrota do país no conflito, o que reduziu em muito o poderio militar e a capacidade de influência nipônicas, mas também devido à ocupação americana no país até 1952, como mencionado, a qual foi responsável por uma reconfiguração política e econômica do Japão. Foi após esse período que o Pan-Asianismo se tornou um tabu na sociedade asiática, tanto pelas atrocidades cometidas pelos japoneses no continente quanto pela falta de utilidade do movimento a partir da década de 1950, uma vez que os países asiáticos iniciaram seus processos de independência e o auxílio do Japão na "libertação da Ásia" já não era mais justificável; dessa forma, nesse contexto o Pan-Asianismo passou a ser confundido com a própria política expansionista da Esfera de Coprosperidade (RYŪHEI, 2007).

A partir dos processos de independência das nações asiáticas desde a década de 1950, portanto, o desenvolvimento econômico da Ásia substituiu a busca por independência como principal objetivo dos países da região (IBID, 2007). Foi nesse período que ocorreu a ascensão dos Novos Países Industrializados (NPI) Coreia do Sul, Taiwan, Hong Kong e Singapura, os chamados tigres asiáticos. Da mesma forma, desde a década de 1980 tem-se observado uma mudança do centro dinâmico da Ásia do Leste para o Sudeste Asiático, visto que os Estados-membros da ASEAN seguem esta mesma fórmula de desenvolvimento econômico como política primordial que tem logrado êxito (IBID, 2007).

À vista disso, Ryūhei (2007) indica como as ideias remanescentes de Pan-Asianismo no Japão passaram também a focar no desenvolvimento econômico do continente como forma de unir os países asiáticos sob um mesmo objetivo comum. O autor comenta como ONGs japonesas passaram a atuar no desenvolvimento de comunidades e zonas rurais em outros países asiáticos a partir da década de 1970, retomando o senso de cooperação transnacional com

caráter Pan-Asianista. ONGs com foco em ajuda humanitária também começaram a se encaixar em uma nova ótica Pan-Asianista, como a Peshawar-kai, fundada por Tetsu Nakamura, a qual presta serviços médicos em zonas necessitadas principalmente na Ásia, mas também em outros locais fora do continente.

Para além das ONGs apontadas por Ryūhei, indico como o governo japonês deu início à sua política de Assistência Oficial ao Desenvolvimento (ODA) na década de 1950, focada na ajuda econômica a países asiáticos, o que também pode ser enxergado como uma forma de cooperação transnacional "Neo-Asianista". Apenas no ano de 1978 a ODA japonesa passou a incluir outras regiões do globo para além da Ásia (MOFA, 2022c). Conforme apontado no *White Paper on Development Cooperation* de 2017, último a fazer uma listagem histórica dos desembolsos por parte do Japão ao longo das décadas no que tange à ODA, 94,4% de toda a ajuda japonesa se destinava à Ásia[22] na década de 1970, porcentagem que decresceu ao longo das décadas na medida que outras regiões do planeta foram adicionadas ao plano de doações do Japão. No ano de 2016, último divulgado no livro branco, a Ásia continuava sendo o continente com a maior alocação de recursos, totalizando 52,3% de toda a ODA japonesa[23].

Contudo, o Japão praticamente não inclui doações ao Leste Asiático em seu orçamento da ODA, seja pelo foco da ajuda ser a países subdesenvolvidos, seja por motivos políticos. Nessa ótica, a Coreia do Sul, a Coreia do Norte e a Rússia não estão incluídas no programa japonês, e a China recebe uma cifra diminuta do total do orçamento. Segundo dados da OCDE (s.d.a), a China recebeu apenas USD 2 milhões em doações no ano de 2020, enquanto os países que encabeçam a lista receberam montantes bilionários[24]. Isso posto, apesar de o Japão contar com um tipo de Neo-Asianismo que foca na economia como centro de sua integração com a Ásia, o Leste Asiático é praticamente removido dessa cooperação econômica. Isso pode ser outra peça no quebra-cabeça da má impressão que o Japão causa no Leste Asiático, perpetuando a rixa com esses países. Em adição, visto que outras regiões do globo foram também incluídas da ótima da ODA japonesa, a Ásia perdeu o foco exclusivo dessa ajuda, o que enfraquece o propósito Pan-Asianista das doações.

Em síntese, apesar de Ryūhei e Saaler concordarem que o Neo-Asianismo japonês é um fato observável no país, hoje em termos econômicos visando ajudar países subdesenvolvidos

[22] Excluindo o Oriente Médio, que está em uma categoria separada com o norte da África.

[23] Em caráter informativo, o Japão é o terceiro maior doador de ODA do mundo, tendo alcançado a cifra de USD 17,6 bilhões em doações em 2021, segundo os dados mais recentes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE, s.d.b).

[24] Considerando os três primeiros do ranking, Bangladesh recebeu USD 2,1 bilhões, Índia USD 1,8 bilhão e Indonésia USD 1,3 bilhão.

do continente a superarem esse *status*, Saaler entende que a visão Pan-Asianista tradicional está morta no país. Mesmo existindo um suposto Neo-Asianismo que remeteria à ideia original do movimento no que tange à integração e à cooperação no continente asiático, o Pan-Asianismo ficou de fato preso ao passado, atrelado à imagem do Império japonês enquanto um movimento expansionista e colonizador que causou uma série de desastres humanitários no continente e abriu feridas ainda não curadas entre os países do Leste Asiático. Dessa forma, mesmo que a ODA tenha esse viés Pan-Asianista que fortalece os laços do Japão com uma porção de países asiáticos, os Estados securitizados pelo país não recebem nenhum ou quase nenhum investimento deste programa, o que exclui uma aproximação mais profunda com os países que compõem ameaças contra o Japão nessa ótica econômica de ajuda.

O segundo ponto que traz à tona o passado imperial do Japão e, por conseguinte, as lembranças do Pan-Asianismo na forma da Esfera de Coprosperidade, são as visitas oficiais de altos políticos ao Santuário Yasukuni, em Tóquio. A partir da década de 1950, o Santuário Yasukuni foi transformado em um local de memória aos milhões de mortos durante a Segunda Guerra Mundial. Na década de 1950, não obstante, iniciaram-se também preparativos para a consagração e a homenagem de criminosos de guerra no Santuário, o que se concretizou na década de 1970. O então Imperador Shōwa (Hirohito) foi o último Imperador a visitar o local, em 1975, visitas as quais cessaram após o Imperador descobrir que tais criminosos de guerra estavam sendo homenageados, especialmente os de classe A, conforme documentos revelados a público apenas em 2007 (NYT, 2007). Entretanto, inúmeros Primeiros-ministros japoneses visitaram o Santuário a despeito das fricções e da percepção negativa dos países vizinhos de que tais visitas enalteciam o passado nacionalista e militarista do Japão pré-1945. No próprio ano de 1975, Takeo Miki foi o primeiro premiê a visitar o Santuário, a 15 de agosto, data que representa o fim da Segunda Guerra Mundial no Japão, seguido por diversos de seus sucessores, como Fukuda Takeo, Masayoshi Ōhira, Zenkō Suzuki, Yasuhiro Nakasone, Kiichi Miwazawa e Ryūtarō Hashimoto.

O ápice dessas visitas, entretanto, ocorreu durante o governo de Jun'ichirō Koizumi (1996–2009), quando o então chefe de governo fez seis visitas ao Santuário entre os anos de 2001 e 2006. Neste sentido, a relação do Japão com os vizinhos do Leste Asiático retrocedeu a um dos pontos mais baixos desde a Segunda Guerra, o que gerou até mesmo demonstrações estudantis na China (TOGO, 2008), dado que as visitas iniciadas na década de 1970 eram vistas pelos vizinhos como uma alusão à glória japonesa do pré-1945 e, como consequência, do Pan-Asianismo colonialista sobre o continente. Além de demonstrações estudantis, as visitas de Koizumi criaram principalmente dois tipos de reação com a China: de um lado, houve uma

queda da estima do Japão pela China, o que gerou revoltas no país e uma resposta ríspida da mídia chinesa; por outro, a opinião pública japonesa sobre a China igualmente atingiu um declínio histórico nas pesquisas de opinião conduzidas pelo *Cabinet Office* (SAALER, 2007). Junto disso se aponta como o governo de Koizumi não contava com uma política clara voltada para a Ásia, o que fez com que o Japão se isolasse do restante do continente, abrindo espaço para os Estados Unidos fortalecessem sua posição de única superpotência à época (IBID, 2007). Dessa maneira, o enfraquecimento das relações sino-japonesas observado no início da década de 2000 esteve diretamente ligado à alusão de exaltação do passado colonial do país e, como consequência, Pan-Asianista, consumado na figura do Santuário Yasukuni e nas visitas de Primeiros-ministros ao local, em especial de Koizumi.

Após os escândalos de Koizumi com o Santuário, Shinzō Abe foi o último premiê a visitá-lo ocupando o cargo mais alto da política japonesa, em dezembro de 2013, igualmente sob forte repreensão chinesa, sul-coreana e inclusive americana, fato que não voltou a se repetir até o momento. Membros do governo do Yoshihide Suga, entretanto, visitaram o Santuário em 2021, e o atual premiê Fumio Kishida, apesar de não haver feito uma visita *per se*, enviou oferendas a Yasukuni duas semanas após sua posse. As oferendas de Kishida foram interpretadas pela Coreia do Sul como sendo decepcionantes e lamentáveis, e que o Japão deveria encarar seus atos do passado (BOSCHI, 2022). As visitas a Yasukuni, dessa forma, continuam a promover fricções com os Estados vizinhos por trazer à tona o passado brutal e imperialista do Japão pré-1945. Em outras palavras, as ações conduzidas sob a então política externa Pan-Asianista reverberam até o momento no Leste Asiático, dificultando a proximidade dessas nações e consolida um *status quo* de desconfiança e inimizade na região.

Por fim, o historiador sul-coreano Gi-Wook Shin, em entrevista para Melissa de Witte (2020), faz uma série de apontamentos a fim de entender como os legados da Segunda Guerra Mundial afetam as relações atuais na Ásia e em especial no Leste Asiático. Em um primeiro momento, Shin afirma que o conflito nunca foi completamente resolvido na região. Nesse cenário, a Guerra da Coreia ainda não foi de fato finalizada, visto que apenas uma trégua foi assinada entre a Coreia do Norte e a China, sem assinatura sul-coreana, o que não pode ser considerado um acordo de paz. Além disso, a constante disputa por territórios entre as nações do Leste Asiático[25] perpetuam desavenças históricas, resultando em deformações diplomáticas na atualidade entre o Japão e seus vizinhos. Daniel Schumacher (2015) também adota uma linha de raciocínio similar, afirmando que o fim da Segunda Guerra não resultou em uma transição

[25] Como as disputas entre o Japão e a China sobre as Ilhas Senkaku (Diaoyu aos chineses) ou a disputa nipo-coreana sobre as Ilhas Takeshima (Dokdo aos coreanos).

suave para a auto-regência das nações dominadas, mas sim que guerras locais foram incorporadas ao conflito mundial, e que após sua conclusão voltaram a ser guerras locais. Schumacher finaliza esse entendimento reforçando que, neste contexto, as administrações desses países, em conjunto a grupos de interesse, rotineiramente citam esses legados e desavenças, e que a mídia constantemente incita essas controvérsias contra o Japão.

Shin ainda estabelece que um dos principais pontos de divergência entre a China, o Japão e a península coreana é o tipo de memória que cada país tem da Segunda Guerra Mundial. Por um lado, a China celebra sua vitória sobre o Japão enquanto ponto fulcral da Segunda Guerra[26]; para a Coreia, sua libertação da opressão japonesa ao longo do conflito é lembrada pela população; ao Japão, no entanto, a honra às vítimas dos ataques nucleares é a memória mais marcante da contenda. Há ainda o ponto de vista americano sobre o conflito, o qual se expressa pelo constante desconforto em tratar sobre os eventos transcorridos na Segunda Guerra, visto que o país foi responsável pelos bombardeios nucleares sobre o Japão e pelo aprisionamento de 120 mil japoneses em campos de concentração nos Estados Unidos (DE WITTE, 2020). Sendo assim, para Shin, os EUA são sempre reticentes quanto à guerra no Pacífico, ao passo que procuram enaltecer sua vitória contra o nazismo na Europa como ilustração da participação americana na guerra[27]. Além disso, por parte da China e da Coreia, fatos como o Massacre de Nanquim e as mulheres de conforto rodeiam a percepção desses povos quanto à ação japonesa na Guerra, ao passo que o Japão tem como foco de sua memória coletiva acontecimentos como Pearl Harbor e os bombardeios a Hiroshima e Nagasaki, colocando-se sempre num lugar de vítima e nunca de malfeitor no conflito[28]. Isso faz com que as expectativas do lado chinês e coreano sejam diferentes daquelas do lado japonês: enquanto a China e a Coreia sempre esperam algum tipo de retratação por parte do Japão, visto que esse é o país que marca a memória coletiva dessas nações quanto à Segunda Guerra, os Estados

[26] Na memória coletiva de Taiwan, a luta de resistência contra o Japão na China continental se tornou o ponto histórico de referência à população, fato que passou a definir a própria percepção de Estado em Taiwan em sua formação no período de Chiang Kai-shek (SCHUMACHER, 2015).

[27] Quanto a esse aspecto, Schumacher (2015) indica que a guerra na Ásia era virtualmente esquecida na historiografia *mainstream* global no passado, ao passo que os eventos transcorridos na parte europeia da guerra eram os que recebiam os holofotes. Em adição, vítimas asiáticas que tentavam falar sobre o sofrimento do continente ao longo da Segunda Guerra eram marginalizadas ou deslegitimadas. Foi apenas nas décadas de 1980 e 1990 que a guerra na Ásia começou a de fato ser explorada, e os estudos do tema acabaram se dividindo em duas grandes vertentes: (1) o antigo Império de guerra do Japão, que se estendia até Taiwan, China continental e Coreia, e (2) os acontecimentos na periferia do continente, especialmente o Sudeste Asiático e a península da Malásia. Essas memórias foram sobremaneira inflamadas no continente nos anos 2000 através de movimentos de liberalização política, o que gerou impactos positivos nessas sociedades, como a construção de memoriais e sítios de herança cultural.

[28] O historiador sul-coreano Jie-Hyun Lim chama isso de nacionalismo de vitimização, adotado tanto pelo Japão quanto pela China no que concerne ao passado de guerra desses países (SCHUMACHER, 2015).

Unidos são o país que compõem a memória coletiva japonesa, visto que seu sofrimento no conflito foi causado pelos americanos. Logo, o Japão moderno não dá a devida atenção às suas próprias atrocidades perpetradas no continente asiático, impedindo uma reconciliação plena com a Coreia e a China (DE WITTE, 2020)[29].

Apesar de o Japão ter sido um Império que se expandiu por diversas partes da Ásia, não somente ao lado Leste do continente, Schumacher (2015) completa que demais países, como Tailândia, Vietnã, Camboja, Laos e o subcontinente indiano, saíram praticamente ilesos do conflito. Isso faz com que a Segunda Guerra Mundial seja hoje virtualmente ausente nesses países em suas memórias históricas coletivas. Dessa forma, o Japão não é interpretado como um Estado rival nesses países, o que nos ajuda a entender como apenas no Leste Asiático o Japão é tido até hoje como um inimigo e que apenas lá essa memória de sofrimento pretérito é continuamente trazida à tona. Além disso, Schumacher pontua que mesmo todos esses países tendo lutado contra invasões japonesas, a figura do Japão enquanto inimigo foi substituída, após a Segunda Guerra Mundial, pelas figuras de outras potências, como o Reino Unido na Malásia, a França e os Estados Unidos na Indochina, a Holanda e o Reino Unido na Indonésia, os Estados Unidos no Vietnã, etc., o que fez com que a memória coletiva desses países substituísse o Japão por novos Estados inimigos.

Outro legado da Segunda Guerra mencionado por Shin e que acrescenta uma camada ao atual teatro de segurança do Leste Asiático é a percepção de injustiça advinda do Tribunal de Tóquio, visto que este não logrou êxito em endereçar as atrocidades cometidas pelos japoneses ao longo da guerra na Ásia. Isso se deu, pois, o tribunal *ad hoc* focou em ações perpetradas pelo Japão que efetivamente afetaram os Aliados, como Pearl Harbor ou o maltrato de prisioneiros Aliados na guerra, deixando de lado a brutalidade sofrida pelos chineses e pelos coreanos. Para completar, o Acordo de Paz de São Francisco eliminou as obrigações do Japão de pagar reparações por seus crimes de guerra, deixando a China e a Coreia sem nenhum tipo de assistência após o conflito; ambos os países sequer participaram do tratado e, portanto, não tiveram voz para reivindicar por reparações às perdas humanas e materiais da guerra (DE

[29] Shin cita como exemplo a Suprema Corte sul-coreana, a qual exigiu em 2018 que companhias japonesas pagassem compensações aos coreanos que foram mantidos como trabalhadores forçados ao longo da guerra. Isso fez com que o Japão removesse a Coreia do Sul de uma lista de parceiros comerciais favorecidos, o que foi respondido de igual maneira pela República da Coreia. Ao mesmo tempo, Shin menciona a pressão feita pelos japoneses sobre os Estados Unidos para que visitassem o local do bombardeio em Hiroshima, um dos memoriais mais importantes desses eventos no Japão, o que foi feito por Barack Obama em 2016. Nesse caso, o Japão não demonstra o mesmo interesse ou esforço em se reconciliar com seus vizinhos, como reconhecendo e se desculpando pelas mulheres de conforto ou pelo Massacre de Nanquim, o que nunca foi feito até hoje. Isso é dizer que o Japão é o país cujo posicionamento é cobrado no Leste Asiático, enquanto os Estados Unidos são o país cobrado pelo Japão quanto a acontecimentos no continente..

WITTE, 2020). Por conseguinte, em 1955 todos os sentenciados em Tóquio foram libertos, mesmo aqueles condenados à prisão perpétua, o que se fez perder o senso de justiça perante os malfeitos do Japão na Segunda Guerra (KUSHNER, 2015). Como consequência, Robert Farley (2015) acrescenta também que culpabilidade e punições ao Japão são reivindicações frequentes por parte da China e das Coreias.

Nesse contexto, Barak Kushner (2015) estabelece que o Tribunal de Tóquio ilustra como se dá o jogo identitário no Leste Asiático mesmo hoje, na medida que essas assimetrias na forma como as diferentes nações do Leste Asiático são tratadas acabam definindo o que é ser chinês, japonês ou coreano na região. Desse modo, o próprio entendimento da região sobre seu passado e suas atuais dinâmicas internas, como põe Kushner, estão enraizados na maneira como a Segunda Guerra Mundial terminou, e essa espécie de rancor guardado pelos países do Leste Asiático persiste desde então e afeta as relações intrarregionais no século XXI.

Farley (2015) menciona também como a influência americana no Japão pós-1945 similarmente moldou o imaginário coletivo do Japão frente ao continente como um dos legados da contenda. Uma vez que movimentos revolucionários se disseminaram na Ásia pós-Segunda Guerra, o que incluía uma predominância comunista no continente, os Estados Unidos à época eram constantemente interessados em um Japão desmilitarizado que servisse como baluarte contra o expansionismo comunista no Leste Asiático. Esses movimentos revolucionários, como os ocorridos na China, na Coreia, no Vietnã e na Indonésia, não tinham interesse em uma reabilitação da imagem japonesa, o que incentivava os EUA a apoiar um Japão conservador na região. Dessa forma, a conexão do Japão aos Estados Unidos enquanto contrário às revoluções na Ásia coroava as desconfianças dessas nações contra os japoneses. Esse ponto é bastante visível hoje quando observamos o tipo de relação que o Japão tem com a Coreia do Sul. Apesar de Seul compartilhar relações tensas com Tóquio por conta dessa cultura da memória do Japão do passado, ao fim e ao cabo a Coreia do Sul é um país semelhante ao Japão no que diz respeito a seu posicionamento internacional: ambos os países são democracias liberais, estão alinhados ao Ocidente em matéria política e tem acordos de segurança assinados com os Estados Unidos, o que reforça a imagem de aliados ao inimigo por uma visão chinesa, norte-coreana e mesmo russa. Dessa forma, a proximidade do Japão com os Estados Unidos desde o final da Segunda Guerra tem afetado diretamente a percepção e as relações do Japão com seus vizinhos securitizados. Como consequência, as relações com a Coreia do Sul são muito mais estáveis, haja vista o mesmo alinhamento do Japão no contexto internacional, mas Kushner (2015) aponta que para os países comunistas do Leste Asiático, nomeadamente a China e a Coreia do Norte, os Estados Unidos são tidos como o novo poder imperial na região do qual tentam se

proteger.

Com o intuito de finalizar o raciocínio deste trecho, usarei a Alemanha como exemplo de país que conseguiu reverter seu legado frente a países afetados por suas políticas, mesmo tendo sido responsável por um dos períodos mais sombrios da história. Nesse sentido, indico a Alemanha como um paralelo oposto ao Japão no que diz respeito a seu comportamento frente a crimes de guerra, pois o governo alemão adota o remorso e a retratação por suas atrocidades como pontos fulcrais da política pós-nazismo do país para evitar que tais erros se repitam, diferentemente do Japão que ignora seu passado imperial e todas as tragédias que disso surgiram ao passo que recorrentemente exalta esse período.

Como primeiro exemplo, retomo o contexto de injustiça sentido pelo Leste Asiático quanto à punição de seus agressores. Ainda na Alemanha atual, expressões (neo)nazistas costumam ser implacavelmente punidas pelas autoridades, e desde os julgamentos de Nuremberg tenta-se encontrar elementos nazistas na sociedade e trazê-los à justiça. Após a condenação de John Demjanjuk[30], a legislação alemã foi alterada para expandir ainda mais a forma que são julgados aqueles conectados à antiga máquina de guerra nazista. Hoje, qualquer pessoa ligada a esse passado está apta a ser levada a juízo, independentemente de vínculos com o assassinato direto de pessoas identificadas. A exemplo estão as condenações recentes de Reinhold H. em 2016, com então 94 anos, o qual fora guarda do Campo de Auschwitz e cúmplice de cerca de 170 mil assassinatos entre 1943 e 1944; Bruno D., condenado em 2020 com 93 anos também por ser ex-guarda do Campo de Sutthof; Yosef S., antigo guarda do Campo de Sachsenhausen, condenado em junho de 2022 por outro tribunal aos 101 anos; e a sentença contra Irmgard F. em dezembro de 2022, com 97 anos, por ter sido secretária também do Campo de Stutthof (DW BRASIL, 2023). Isso demonstra que, diferentemente do comportamento do Estado japonês, a Alemanha busca punir até hoje qualquer indivíduo que possa estar conectado ao nazismo. Enquanto na Alemanha nota-se uma tentativa constante de mudança em relação ao passado, no Japão inexiste qualquer intento de culpabilizar os que hoje estão vivos e foram responsáveis por crimes na Segunda Guerra. Além disso, muitos dos condenados pelo Tribunal de Tóquio foram isentos de punição após o julgamento, como já mencionado.

Outro exemplo na Alemanha atual que demonstra como o país permanentemente tenta

[30] Antigo guarda de um campo de concentração nazista na Polônia ocupada condenado em 2011, aos 91 anos, por ser cúmplice no assassinato de milhares de prisioneiros pelo posto que ocupava. O ponto de inflexão neste caso foi a justificativa para sua condenação, embasada apenas no fato de que o indivíduo era guarda de um campo de concentração. Até este caso, o julgamento de criminosos de guerra era feito apenas se fosse provado que o réu estava conectado diretamente à morte de algum indivíduo em particular.

superar sua imagem do passado é o tratamento dado ao Holocausto na educação da população. Entre seus 13 e 15 anos, adolescentes alemães tem acesso à história do Holocausto pela primeira vez em seu tempo escolar, sendo essa uma matéria obrigatória da grade curricular no país. Livros de história, filmes, documentários, excursões a museus, sinagogas e antigos campos de concentração são formas que os alunos têm de aprender sobre o tema, inclusive pelas perspectivas das vítimas. Isso ensina a juventude a não relativizar o nazismo e a truculência alemã na Segunda Guerra, e práticas nesse sentido vêm sendo aplicadas no país desde a década de 1970 (DW BRASIL, 2022). O Japão, por outro lado, adota uma narrativa de vitimização quanto à Segunda Guerra, como já elaborado, diminuindo os malfeitos do país. Tão cedo quanto 1950, os japoneses tiveram seus livros didáticos editados pelo governo de forma a suavizar o texto sobre as consequências de seu imperialismo na Ásia. Nesses livros não constava, por exemplo, o número de vítimas ou mortos em grandes massacres japoneses como o de Nanquim, ao passo que substituía palavras com teor negativo, como "invasão" por "avanço" sobre o continente. Mais recentemente, nos anos 2000, novos livros de história foram distribuídos em escolas com tom igualmente moderado sobre a natureza das agressões japonesas no passado, como a Primeira e a Segunda Guerras Sino-Japonesa, a anexação da península coreana e a Segunda Guerra Mundial. Desse modo, o negacionismo japonês se expressa mesmo no nível educacional da sociedade, e as crianças e jovens japoneses não crescem com uma mentalidade de arrependimento e empatia pelas pessoas que sofreram sob controle de seu povo.

A cultura da memória é o terceiro ponto de divergência entre a Alemanha e o Japão quanto aos seus erros do passado, o que também se conecta aos demais pontos. Na Alemanha procura-se aclarar como terceiros sofreram nas mãos dos alemães, ideia expressa através da construção de memoriais públicos como o Memorial do Holocausto, em Berlim, ou pela conversão dos antigos campos de concentração em pontos de visitação e aprendizado sobre o genocídio nazista, como Buchenwald, Dachau e Bergen-Belsen. Esse tipo de comportamento coloca as vítimas (terceiras) no centro do debate e como a população alemã causou sofrimento sobre outros seres humanos, a fim de gerar uma percepção de remorso e arrependimento na população. No Japão, por outro lado, a cultura da memória principal sobre o passado de guerra do país reflete os japoneses sofreram nas mãos de outrem, e não como o Japão provocou sofrimento. Assim, os memoriais que celebram as vítimas japonesas são aqueles que recebem destaque, como os em Hiroshima e Nagasaki, ou mesmo o Santuário Yasukuni, que celebra apenas os mortos do lado japonês, inclusive generais condenados por crimes de guerra. Dessa maneira, a cultura da memória alemã culpabiliza o país e procura esclarecer ao seu povo e ao mundo que a Alemanha não voltará a ocupar o mesmo posto do passado, enquanto a sociedade

japonesa vira-se para dentro e para o seu próprio sofrimento, sem procurar se retratar perante os Estados vítima e admitir sua parcela de protagonismo no sofrimento humano na primeira metade do século XX.

Em resumo, Schumacher (2015) destaca que as sociedades asiáticas, o que inclui outros países para além do Japão, costumam ter "culturas de honra" que dificultam o reconhecimento de erros do passado, o arrependimento e o remorso. Isso ilustra, portanto, como a Alemanha conseguiu reverter seu quadro de maior rival da Europa, ou mesmo de boa parte do tecido internacional ao longo das décadas de 1930 e 1940, para um dos principais aliados do Ocidente no tempo presente. O Japão, no entanto, tornou-se um dos principais inimigos das sociedades afetadas pelo seu expansionismo violento, efeito direto das constantes falhas e desvios propositais do Japão em reverter sua imagem colonial.

Para finalizar, trago como após a Segunda Guerra Mundial, mesmo com a humilhação do Japão devido aos bombardeios atômicos efetuados pelos Estados Unidos, o país opta por se alinhar aos americanos à luz de sua política centenária de alinhamento à potência do dia. Hook et al. (2012) mencionam que os líderes políticos do Japão consideraram optar por uma neutralidade ou um não-alinhamento a nenhuma potência em específico, mas ao fim e ao cabo o país alinhou-se aos Estados Unidos por ser a potência vigente, agora nuclearizada, para sobreviver e prosperar. Esse alinhamento se cristalizou na forma da Doutrina Yoshida no imediato pós-Segunda Guerra, na assinatura do Tratado de São Francisco, em 1951, e subsequente tratado de segurança assinado com os americanos, o que firmou o Japão como um bastião americano na Ásia. Apesar do alinhamento japonês aos EUA, o Japão nunca deixou de atuar de maneira proativa e condizente com seus objetivos internacionais. Exemplifico com a negação do Japão em participar da Guerra da Coreia e da Guerra do Vietnã, nas décadas de 1950 e 1960, ou mesmo o leve distanciamento dos EUA na década de 1970 em face ao declínio econômico do país e ao choque do petróleo de 1973, o que obrigou o Japão a buscar outras maneiras de se relacionar com o Oriente Médio, uma vez que o país era dependente dos recursos energéticos importados de lá.

2.5. Conclusões do capítulo

Em dezembro de 2022, quando uma nova versão da Estratégia de Segurança Nacional do Japão foi lançada, o então Ministro de Relações Exteriores Yoshimasa Hayashi verbalizou, em sua declaração de lançamento do documento, que o Japão está atualmente imerso no mais severo e mais complexo ambiente de segurança desde a Segunda Guerra Mundial, e que manter

e desenvolver uma ordem internacional aberta e livre, baseada no estado de direito, tem se tornado mais importante do que nunca (MOFA, 2022a). Na CSS de 2022 é mencionado, nesse sentido, como está havendo tentativas unilaterais de mudança do *status quo* internacional e que a acumulação militar está constantemente ocorrendo na vizinhança do Japão. Tóquio cita no documento como as agressões russas à Ucrânia têm balançado as fundações da ordem internacional, que o mesmo pode vir a ocorrer no Leste Asiático no futuro e que, portanto, o Japão reforçará fundamentalmente suas capacidades de defesa (MOFA, 2022b). O Ministro das Relações Exteriores finaliza dizendo que como forma de melhorar o ambiente de segurança ao redor do Japão, o país desenvolverá estratégias tal como o fortalecimento da aliança com os Estados Unidos, a coordenação com países *like-minded* perseguindo um "Indo-Pacífico livre e aberto", bem como se engajando diplomaticamente com regiões e países vizinhos (MOFA, 2022a).

Em meio a esse cenário preocupante em que se encontra o Japão, penso que valha a pena finalizar este capítulo tentando diferenciar, dentro do possível, o tipo de antagonismo identitário partilhado entre o Japão, a China e as Coreias, de um lado, e pelo Japão e a Rússia, do outro, e como isso molda profundamente o teatro de segurança da região, mesmo que de maneira imperceptível. Enquanto as Coreias e a China passaram por um processo de colonização e exploração predatória de seu povo e de maneira sistemática por parte do Império do Japão, a Rússia é um país com o qual o Japão, ao máximo, perpetua relações de altos e baixos como com qualquer outra potência internacional. Nesse sentido, as diferenças identitárias entre o Japão, as Coreias e a China tem uma toada de superação de uma dominação militar que punha em risco a sobrevivência real dos povos do continente sob o controle japonês, na medida que a Rússia, em relação direta ao Japão, historicamente mantém diferenças envolvendo disputas e controle sobre territórios, por exemplo, muito menos urgentes que um cenário de sobrevivência de um povo posta à prova.

Isso observado, a principal divergência identitária entre a Rússia e o Japão é sua proximidade aos EUA e tudo que isso acarreta, como uma presença constante de tropas americanas no arquipélago vizinho e toda a influência democrático-capitalista sobre o Leste Asiático que penetra na região, sobremaneira pelo Japão. Assim, o desencontro dos interesses nacionais russo-japoneses se dá muito mais pela figura dos Estados Unidos que por motivos naturalmente advindos dos japoneses contra os russos e vice-versa. Por conta disso, não foi construído no imaginário russo uma figura antagônica para o Japão como ocorreu no Leste Asiático. Apesar dos conflitos contra os russos, seja na figura da guerra do início do século XX, seja pelas disputas territoriais pelos Territórios do Norte, não existe na Rússia uma percepção

de Japão enquanto inimigo da nação, visto que os russos não foram, como os chineses e os coreanos, alvo de colonialismo por parte do Império japonês no passado. A maior diferença identitária entre essas nações, neste caso, não envolve casos de exploração e humilhação como sofridos pelas contrapartes do Leste Asiático, mas sim pelos seus próprios alinhamentos antagônicos nos campos econômico e político, visto que o Japão é o principal aliado estadunidense no Extremo Oriente e quiçá na Ásia, em adição ao fato de o país promover ideias democraticamente liberais, o que não ocorre na Rússia[31]. Inclusive, o crescendo na securitização da Rússia por parte do governo japonês não se dá por ameaças direcionadas ao Leste Asiático ou contra o Japão em si, mas sim porque a Rússia está sob processo de ruptura da ordem internacional pré-estabelecida e isso pode influenciar a atuação chinesa na região. Assim, a elevação da Rússia como ameaça ilumina a necessidade de manutenção da ordem internacional ocidental ao invés de factualmente representar um mecanismo de repulsão a ameaças russas miradas contra o Japão.

Dessa maneira, assim como as percepções de ameaça foram co-construídas no Leste Asiático como bem poria a teoria construtivista, as divergências identitárias entre os russos e os japoneses não ocorreram de maneira sistematicamente estabelecida pela violência e pela submissão, como ocorreu com os chineses e os coreanos. Em suma, a relação agente-estrutura envolvendo o Japão, a China e as Coreias ocorreu de maneira muito mais epidérmica entre essas nações, acarretando inimizades e preocupações mais palpáveis e latentes que se comparado ao tipo de desalinhamento identitário observado entre o Japão e a Rússia. Há de se mencionar, nesse contexto, que o mesmo motivo que afasta a Rússia do Japão é o que aproxima os japoneses dos sul-coreanos: os Estados Unidos. Nesse contexto, os sul-coreanos encabeçam as pautas de retratação histórica do Japão, como através dos protestos envolvendo as mulheres de conforto e que demonstram como o passado entre a Coreia e o Japão ainda está vivo no imaginário da península, mas, ao mesmo tempo, o alinhamento aos EUA coloca ambos os países sob o mesmo guarda-chuva identitário no Leste Asiático nesses termos. Seja pelos acordos de segurança mútua assinados pelos dois países com os Estados Unidos, seja pelos seus modelos de política e economia, a inimizade do Japão com a Coreia do Sul está mais desbotada no século XXI pela mentalidade comum que une os países. Para a China e a Coreia do Norte, em contrapartida, não há nada que hoje indique que a imagem do Império do Japão já não exista

[31] A própria disputa sobre as Ilhas Curilas, como apontado por Kravtsevich (2019), iniciou-se em 1945 por considerações puramente geoestratégicas, visto que a segurança soviética no Leste Asiático seria fortalecida com a dominação de novos territórios. Sendo assim, diferentemente de como ocorre contra a Coreia do Norte e a China, o principal tensionamento russo-japonês tem raízes políticas, exemplificando as relações de segurança entre esses dois Estados de maneira profícua.

mais no tabuleiro internacional; na montanha-russa que são as relações russo-japonesas, a primeira metade da década de 2020 marca uma nova ascensão da Rússia enquanto protagonista do teatro de segurança japonês, como já ocorreu em outras ocasiões décadas atrás, mas dessa vez com força total.

Por fim, menciono que a atual proatividade japonesa destacada desde o fim da Guerra Fria pode ser facilmente percebida de maneira negativa pelos seus vizinhos securitizados, em especial a China e a Coreia do Norte. Apesar de o Japão jogar dentro de suas linhas constitucionais e não se engajar em qualquer tipo de ofensiva internacional, há outras formas de militarização formal para além da aquisição de aparato de guerra, como a militarização da esfera política japonesa. O próprio estabelecimento do NSC e da NSS em 2013 representam isso, visto que, apesar de o Japão ainda respeitar sua abdicação à guerra, incessantemente debate e institucionaliza questões de segurança internacional e dá indícios de um militarismo aos moldes tradicionais através de suas tentativas de reforma constitucional e de expansão de seu orçamento militar, por exemplo. É relevante mencionar que o segundo mandato de Shinzō Abe (2012–2020) foi, desde o fim da Segunda Guerra Mundial, o mais próximo que o Japão chegou de reformar sua Constituição e possivelmente abandonar seus preceitos pacifistas impressos pelo Artigo 9, mesmo que de maneira parcial. Desse modo, a constante desconfiança compartilhada pelos seus vizinhos de que o Japão se remilitarizará formalmente não parece ser injustificada quando observamos sua atuação proativa: tem-se hoje um Japão com uma política de segurança consciente, delimitada e formulada por sua própria estrutura política; um multilateralismo em segurança em grande medida estabelecido por influência japonesa; uma realidade política doméstica alinhada a uma reforma constitucional que se aproxima da maioria; e Forças de Autodefesa que, a cada reinterpretação da Constituição, expandem sua atuação internacional e se veem presentes ao redor do mundo. Dessa forma, apesar de o Japão tentar se defender da melhor forma que pode, o país parece estar caindo em uma armadilha montada por si próprio na medida que busca expandir sua realidade militar sem restaurar sua imagem perante o Leste Asiático. Esse tipo de comportamento é justamente o que remonta ao colonialismo japonês e faz com que nações como a China e a Coreia do Norte se sintam ameaçadas e busquem escalar ainda mais seu militarismo, pois é inconcebível permitir que o Japão se torne uma ameaça militar semelhante ao que era no início do século XX. Esse pensamento, desse modo, está difundido no Leste Asiático a ponto de ter se tornado um medo constante e um dos vieses identitários dos rivais do Japão.

3. A EMERGÊNCIA DA SEGURANÇA CIBERNÉTICA NO JAPÃO

O advento do ciberespaço como um domínio de atuação internacional e de disseminação de poder ocorreu, em grande medida, a partir do final dos anos 1990 e início dos anos 2000, apesar de sua formação datar da década de 1960. Nesse período, a internet passou a ser mundialmente acessada por milhões de usuários e, como consequência, suas funções foram ampliadas extraordinariamente, o que desvirtuou a plataforma de seu propósito inicial de interação comunicacional e expôs as fragilidades desse sistema (PAGLIARI, AYRES PINTO e VIGGIANO, 2020). Conforme apontado por Joseph Nye (2010), em 1993 existiam cerca de 50 sites em todo o mundo, ao passo que, ao final da década, esse número já ultrapassava os cinco milhões. A quantia de informações digitais, nesse sentido, aumenta cerca de dez vezes a cada cinco anos, segundo Nye. Em vista de sua expansão e da exposição de suas fragilidades, portanto, precisou-se pensar em métodos para proteger a rede mundial de computadores e aperfeiçoar o novo ambiente virtual internacionalizado, o que culminou na eventual securitização do ciberespaço.

No Japão esse cenário não foi diferente, especialmente porque essa emergência do ciberespaço enquanto variável de segurança ocorreu na era de proatividade internacional do Japão, o que propiciou uma consolidação mais rápida da postura cibernética japonesa desde o princípio. A primeira medida de proteção nacional quanto ao universo cibernético foi a criação do *Japan Computer Emergency Response Team Coordination Center* (JPCERT/CC), em 1996 (HATHAWAY et al, 2016). A partir do começo do século XXI, entretanto, observa-se no país um intenso fluxo de securitização do ciberespaço através do estabelecimento de diversas instituições nacionais em resposta a crescentes ataques, cada vez mais sofisticados, contra sites de Ministérios e agências governamentais japonesas. No ano de 2005, por exemplo, foram criados o *Information Security Policy Council*[32] e o *National Information Security Center*[33], ao passo que em 2015 a primeira *Cybersecurity Strategy* do Japão foi lançada, tendo recebido revisões nos anos de 2018 e 2021 (GADY, 2017; KALLENDER e HUGHES, 2016; KSHETRI, 2014; SOESANTO, 2020).

Não obstante, tendo em vista o surgimento, a securitização e a institucionalização do ciberespaço por conta de ameaças em ascensão, faz-se necessário mencionar que um novo universo de segurança e defesa surgiu em concomitância. Dentro do jargão cibernético, conceitos como ciberespaço, cibersegurança, ciberdefesa, ciberataque, ciberespionagem e

[32] Hoje *Cyber Security Strategic Headquarters*.
[33] Hoje *National center of Incident readiness and Strategy for Cybersecurity*.

cibercrime passaram a ser utilizados nas Relações Internacionais para definir eventos cibernéticos; esses conceitos, entretanto, variam em definição e em utilidade a depender das circunstâncias. Sendo assim, para se entender o âmbito cibernético é necessário, inicialmente, definir esses conceitos para que se parta de uma base comum de análise aos eventos no ciberespaço.

Posto isso, nesta seção pretendo fazer um breve apanhado histórico focado nos aspectos que julgo como principais na evolução da cibersegurança na política japonesa, especificamente a ocorrência de ataques que mudaram o *status quo* do tema, a confecção de documentos e a formação de instituições voltadas à cibersegurança, bem como a "militarização" do ciberespaço pelo Japão. Pretendo também explorar como o governo japonês define o ciberespaço e os eventos a ele relacionados, já que isso em parte determina que tipo de respostas o governo adotará para robustecer o sistema e combater ameaças. Nessa segunda parte, farei uma breve revisão bibliográfica, expondo as definições dos conceitos trazidos acima segundo a academia especializada, para em seguida contrapor com a visão do governo japonês dessas concepções, por meio de uma revisão documental.

3.1. Dos anos 1990 aos anos 2000

Em 1988, um estudante de computação chamado Robert Morris criou um *software* capaz de identificar possíveis fragilidades em sistemas de computadores como senhas fracas. Esse programa, entretanto, acabou saindo do controle de Morris por conta de brechas em sua própria programação e começou a se multiplicar nas máquinas em que estava instalado, deixando-as lentas a ponto de se tornarem inúteis. Esse incidente é conhecido até hoje como o primeiro incidente *worm* do mundo, como é comumente chamado esse tipo de vírus que se multiplica e infecta outras máquinas. Para evitar que outros incidentes do tipo ocorressem, diversos núcleos de resposta a incidentes cibernéticos passaram a ser criados no mundo. No Japão, o primeiro Grupo de Resposta a Incidentes de Segurança em Computadores (CSIRT) foi criado em 1992 de maneira embrionária, atuando como um receptor de informações do exterior a fim de coordenar respostas a incidentes nos sistemas de computadores do país. Em 1996 este grupo inicial é oficializado na figura do *Japan Computer Emergency Response Team Coordination Center* (JPCERT/CC), ou Centro de Coordenação de Equipes de Resposta a Emergências de Computadores do Japão, em tradução livre. Dois anos mais tarde, em 1998, o JPCERT/CC foi o primeiro CSIRT japonês a se juntar ao *Forum of Incident Response and Security Teams* (FIRST), um fórum internacional de CSIRTs, e neste momento o grupo passou a investir na

formação de CSIRTs dentro de empresas e organizações japonesas (JPCERT/CC, 2022).

Até o final da década de 1990, portanto, os primeiros CSIRTs tinham sido criados para evitar a disseminação de *worms* nas redes de computadores, bem como para coordenar respostas a incidentes em escala internacional. Nesse sentido, o caso do *worm* Morris é mencionado pelo JPCERT/CC (2022) como o motivo pelo qual iniciaram no Japão movimentos de proteção da rede de computadores do país. Além disso, no final do século XX organizações e empresas japonesas começaram a ser inseridas nessa ótica de proteção, visto que também poderiam ser afetadas pela disseminação indiscriminada de vírus em suas máquinas. Na virada do século XXI, entretanto, as preocupações envolvendo os sistemas de computadores começaram a ocupar outro patamar no Japão; no início do próprio ano 2000 inúmeros sites de ministérios e agências do governo japonês foram hackeados e alterados pelos invasores, o que chocou a opinião pública japonesa e alertou o país sobre a importância da segurança também no ambiente virtual (KSHETRI, 2014; JPCERT/CC, 2022). Ainda em fevereiro de 2000, o governo japonês já havia estabelecido o *IT Security Office*, sob o controle do gabinete do Primeiro-ministro, primeiro órgão do gênero para tratar da segurança da informação, como era comumente referido na época. Conforme apontado na página do JPCERT/CC (2022), nesse período uma série de ameaças começaram a surgir de uma só vez, como o *worm* Code Red e o vírus Nimda, os quais infligiram grandes danos nos sistemas de computadores do mundo, bem como botnets e golpes por *phishing*; Franz-Stefan Gady (2017) assinala que, como consequência, há também uma maior sofisticação por trás dos ataques da época. Dessa maneira, o monitoramento da internet passou a ser uma constante dentro de organismos governamentais e não governamentais.

Menciono que tanto a criação do JPCERT/CC quanto do *IT Security Office* representam a institucionalização da questão ciber pela sociedade e pelo governo japoneses. De um lado tem-se a primeira organização sem fins lucrativos que serve para a promoção de informações relacionadas a incidentes cibernéticos (HATHAWAY et al., 2016), e do outro a primeira estrutura governamental que se dedicava ao tema no Japão. É no ano de 2005, entretanto, que as principais instituições ciber-relacionadas são estabelecidas no Japão; o *Information Security Policy Council* (ISPC) foi criado para formular as estratégias cibernéticas básicas da nação, coordenar políticas com agências de assuntos internos, estrangeiros, de indústria, comércio e defesa, sendo esse o órgão governamental consultivo de mais alto nível no país, ao passo que o *National Information Security Center* (NISC) foi estabelecido como o departamento administrativo permanente do ISPC, ou secretariado, substituindo o então *IT Security Office*, cujo objetivo era aplicar diretrizes, auditar agências governamentais e investigar falhas internas (KALLENDER, 2014; KATAGIRI, 2021). Logo no início dos anos 2000, a então *Japan*

Defense Agency (JDA), hoje Ministério da Defesa do Japão (MOD), incorporou à Força Aérea de Autodefesa a primeira unidade de cibervigilância e, posteriormente, também à Força Marítima de Autodefesa e à Força Terrestre de Autodefesa (KALLENDER, 2014). Sendo assim, a segurança cibernética não só havia recebido instituições próprias para tratar do tema como havia sido diretamente inserida nas Forças de Autodefesa do Japão através das ditas unidades de vigilância cibernética. Paul Kallender (2014) também aponta que, em 2006, o ISPC lançou a primeira *National Strategy on Information Security* (NSIS) do país, que pode ser comparada à atual *Cybersecurity Strategy*, cujo objetivo era endereçar problemas envolvendo segurança da informação. Nesse período, entretanto, o MOD se preocupava com a falta de conexão entre cada ramo das SDF para tratar da segurança cibernética nacional, uma vez que as unidades de cibervigilância operavam separadamente em cada setor militar.

Nos anos de 2007 e 2008, já sob a figura do Ministério da Defesa do Japão, que substituiu a JDA em junho de 2006, ocorre uma segunda onda de "militarização" do ciberespaço após a inserção das unidades de cibervigilância às SDF. Em um primeiro momento é inaugurada a *Defense Information Infrastructure*, uma rede de comunicação de alta capacidade que conecta bases e campos das SDF em alta velocidade, a partir de uma via interna e outra conectada à internet (IBID, 2014; PAGANINI, 2016). Um ano depois, o MOD e as SDF inauguram seu sistema C4 (Comando, Controle, Comunicações e Computadores) próprio, tipo de sistema responsável por criar uma doutrina conjunta aos braços das forças armadas para atuarem em sincronia. Nesse aspecto, o C4 também fica incumbido de analisar novas comunicações e tecnologias da informação aplicadas a guerras, reconhecendo como o âmbito cibernético também faz parte de cenários de conflito.

Por fim, a partir de 2009 observou-se uma série de ataques cibernéticos em escala internacional, contexto em que os serviços de internet da Coreia do Sul e dos Estados Unidos foram alvos visados para ataques de negação de serviço distribuída (DDoS). Esses ataques atingiram o Japão um ano mais tarde, em 2010, e perduraram ao menos até 2011, quando o país constatou uma série de vulnerabilidades em sua cibersegurança por conta das consequências dessas infrações. Como será exposto na próxima seção, essa onda de ataques internacionais foi um dos fatores responsáveis pela remodelação tanto da cibersegurança quanto da ciberdefesa do país. Indica-se que, devido a esses ataques, o Japão passou a adotar um tom muito mais proativo que nos anos anteriores em assuntos de segurança cibernética, o que culminou na criação de suas primeiras unidades de defesa cibernética com capacidades ofensivas no ciberespaço. Ao final dessa década, por fim, o ISPC lança a segunda versão da *National Strategy on Information Security*.

Isso posto, diferentemente das preocupações do país ao longo dos anos 1990, na década de 2000 observa-se a ocorrência de ataques cibernéticos mais sofisticados contra uma ampla variedade de alvos. No Japão, isso culminou na (1) institucionalização da questão cibernética a partir da criação de organismos governamentais e não governamentais que tratam do tema; na (2) criação dos primeiros documentos oficiais versando sobre cibersegurnaça; bem como no (3) envolvimento da antiga JDA, posterior MOD, e das Forças de Autodefesa na proteção à informação, indicando o início da militariação do campo cibernético no país.

3.2. A década de 2010

Como resultado dos ataques que atingiram os EUA e a Coreia do Sul em 2009, já no ano de 2010 observa-se uma mudança notável no comportamento do Japão quanto ao ciberespaço. Em maio daquele ano, o ISPC lançou um novo documento substituto para a então NSIS, intitulado *Information Security Strategy for Protecting the Nation* (ISSPN), onde o governo japonês enquadrou a ciberdefesa em termos de segurança nacional pela primeira vez e pediu para que os grandes atores do país se preparassem para ataques cibernéticos de larga escala (KALLENDER e HUGHES, 2016). Esses ataques não tardaram, e apenas quatro meses depois, em setembro de 2010, ataques *spear-phishing* sofisticados acometeram grandes corporações, institutos de pesquisa e o próprio governo japonês, como informado pelo *Ministry of Economy, Trade, and Industry* (METI), o que representou um aumento de seis vezes desse tipo de ataque e 1/3 de todos os ataques cibernéticos registrados no Japão naquele período (IBID, 2016). Um ano mais tarde, em 18 de setembro de 2011, o Japão foi alvo dos ciberataques mais graves registrados até o momento contra o país, atingindo embaixadas japonesas no exterior, o parlamento japonês e setores militares, como a Mitsubishi Heavy Industries[34], principal fabricante de armamentos do Japão. Nesse caso, foram acessados projetos e esquemas de produção do sistema de defesa antimísseis do Japão, bem como de aviões de combate e veículos de lançamento espacial japoneses, além de detalhes sobre outras armas estratégicas não divulgadas (IBID, 2016). Evidências indicam que esses ataques foram realizados pela China, visto que as máquinas invadidas mantiveram comunicação com um servidor chinês por um mês e os invasores incluíram ideogramas chineses em seus códigos (LEWIS, 2015). Ademais, as incursões coincidiram com o 80º aniversário do Incidente da Manchúria,

[34] Outras empresas de engenharia de defesa espacial como a IHI Corporation e a Kawasaki Heavy Industries, bem como a própria Agência Japonesa de Exploração Espacial (JAXA), também foram alvo dessa onda de ciberataques (KALLENDER, 2014).

responsável pela anexação da Manchúria pelo Japão em 18 de setembro de 1931 (KSHETRI, 2014), outro fator que indica uma possível conexão da China aos ataques como memória e retaliação.

Gady (2017) aponta que, inicialmente, o MOD passou a se envolver mais profundamente na questão cibernética por influência do que vinha sendo produzido pelo ISPC, visto que o ciberespaço era apresentado como um possível domínio de guerra por aquela instituição, evidenciando a necessidade de envolvimento deste Ministério. Nesse contexto, Paul Kallender e Christopher Hughes (2016) destacam que, como resultado dessa inquietude, o Ministério da Defesa japonês passou a pensar em uma maior "militarização" do ciberespaço, e naquele cenário foi incitado a estabelecer uma doutrina de cibersegurança no país a partir do que foi apresentado no *Mid-Term Defense Program* (MTDP) de 2011. No MTDP daquele ano, por exemplo, o MOD menciona a ciberdefesa da nação pela primeira vez em mais detalhes, e este é o primeiro documento a identificar o ciberespaço como um grande desafio securitário (KALLENDER, 2014).

O que ficou conhecido como o escândalo contra a MHI, no entanto, pode ser considerado o "ano zero" do Japão no que concerne ao tratamento de sua segurança e defesa cibernéticas (KALLENDER, 2014), na medida que já em 2012 o MOD passou a considerar respostas a ciberataques dentre suas dez prioridades (KALLENDER e HUGHES, 2016) e todo o aparato institucional e político moderno que hoje existe no país para tratar do tema surgiu a partir desses ataques. Como resultado desse cenário de vulnerabilidades e da doutrina de cibersegurança estabelecida pelo MOD a partir do MTDP de 2011, o governo japonês destinou JPY 1,2 bilhão para a criação do *Cyber Defense Command* (CDC)[35] japonês, o qual foi concluído em 2014 e ficou responsável por, dentre outros aspectos, unificar o controle sobre as unidades de cibervigilância fragmentadas nas Forças Aérea, Marítima e Terrestre de Autodefesa do Japão (IBID, 2016; KALLENDER, 2014). Barlett (2020) estabelece que a criação do CDC representa uma das primeiras medidas de defesa cibernética *per se* adotadas pelas Forças de Autodefesa do Japão, resultado direto dos ataques que acometeram o país em 2011[36].

Outro passo significativo dado pelo governo japonês na questão cibernética foi o

[35] Por vezes também chamado de *Cyber Defense Group* ou *Cyber Defense Unit* em documentos oficiais. Explorado com mais detalhes nos capítulos 3 e 4.

[36] Outras ocorrências menores também marcaram a evolução do tema ciber nas políticas de segurança do Japão. No ano de 2012, por exemplo, o Japão divulgou publicamente que compraria partes das Ilhas Senkaku, ocasionando uma leva de ciberataques a agências governamentais japonesas alegadamente advindos da China. Não por coincidência, o governo japonês passou a reconhecer o ciberespaço como um domínio amparado pelo direito internacional, o que garantiria o direito da autodefesa ao Japão. Quanto a esse aspecto, o ciberespaço foi reconhecido como parte dos "bens comuns globais" junto dos domínios terrestre, aéreo, marítimo e espacial e que, portanto, necessitava de defesa estatal.

lançamento do *Basic Act on Cybersecurity* (BAC), em novembro de 2014, até hoje um dos documentos basilares que regem a cibersegurança nipônica. Nesse texto, o governo expôs as políticas básicas relacionadas à cibersegurança do país, inclusive em termos de responsabilidade dos governos nacional e locais, a partir do qual se desenhou a reestruturação das instituições de cibersegurança do país. Em primeiro lugar, no próprio ano de 2014, o *Information Security Policy Council*, órgão responsável pela formulação das estratégias de cibersegurança, foi renomeado para *Cyber Security Strategic Headquarters* (CSSH) e movido para o gabinete do Primeiro-ministro do Japão. Isso fez com que essa instituição ficasse em um dos graus hierárquicos mais altos da política japonesa, acima dos Ministérios, por exemplo, agora capaz de monitorar planos orçamentários envolvendo cibersegurança tanto dos Ministérios quanto de demais instituições administrativas independentes (KALLENDER e HUGHES, 2016). Nesse sentido, o BAC e o CSSH foram pensados para diminuir a fragmentação na formulação das políticas e no controle do ciberespaço, uma vez que uma instituição governamental com poderes expandidos, como o CSSH, seria capaz de delinear mais assertivamente uma estratégia nacional única voltada ao ciberespaço. Dessa maneira, por ter sido alocado dentro do gabinete do Primeiro-ministro, o CSSH tem hoje autoridade para formular padrões de segurança comuns para todos os Ministérios, diferentemente do que acontecia antes, quando cada Ministério formulava suas diretrizes cibernéticas de maneira individual, bem como avaliar suas performances à luz de possíveis brechas e inadequações no sistema (IBID, 2016).

Um ano mais tarde, em 2015, o CSSH lançou a primeira *Cybersecurity Strategy* do Japão, conforme previsto no BAC; a CSS, portanto, substituiu os textos anteriores do NSIS e do ISSPN. Uma das principais diferenças entre esses documentos é que a CSS passou a identificar o ciberespaço como elemento chave na segurança (inter)nacional do Japão, ao passo que o tema foi encaixado na tradicional estratégia securitária de "contribuição proativa para a paz internacional", segundo Kallender e Hughes (2016), para demonstrar a determinação do então governo de Shinzō Abe em securitizar o domínio cibernético. A CSS de 2015 também serviu para começar a atrair atenção aos Jogos Olímpicos que aconteceriam em 2020 em Tóquio, visto que do ponto de vista das autoridades japonesas este seria um evento suscetível a inúmeros ataques cibernéticos que poderiam pôr em risco a integridade de infraestruturas críticas do Japão[37].

[37] Conforme apontado por Mihoko Matsubara (2021), o anúncio de Tóquio enquanto sede dos Jogos Olímpicos de 2020 ocorreu no ano de 2013. Desde aquele momento, portanto, o governo japonês vinha fortalecendo sua segurança cibernética para promover um ambiente seguro aos jogos. Nesse sentido, Matsubara indica que o Japão

Também no ano de 2015, o NISC foi renomeado para *National center of Incident readiness and Strategy for Cybersecurity* (ainda sob a sigla NISC), dando continuidade ao seu papel de secretariado do agora CSSH. Gady (2017) ainda menciona que nesse ano, em meio a essa reestruturação em curso no Japão, o sistema de aposentadorias japonês foi hackeado e os dados de cerca de 1,25 milhão de pessoas foram vazados. Esse foi possivelmente o último ataque de grandes proporções a atingir uma instituição governamental até o momento. Por conta desses ataques, em 2015 o *Cyber Defense Exercise with Recurrence* (CYDER), criado em 2013, passou a treinar oficiais do governo central para responder a incidentes cibernéticos, abrangendo também governos municipais e agências governamentais afiliadas de todo o Japão (MATSUBARA, 2021).

Nos últimos anos da década de 2010, no entanto, não se observou a incidência de ataques cibernéticos significativos como os que ocorreram no início da década. Entretanto, o governo japonês deu continuidade à institucionalização da questão, seja pela confecção de novos documentos, seja pela criação de novas instituições. Em 2017, por exemplo, foi criado o *Industrial Cyber Security Center of Excellence*, cujo objetivo é proteger infraestruturas críticas, especialmente as industriais, de ataques cibernéticos que possam infligir danos físicos nessas infraestruturas. A instituição expõe que esses ataques advêm do exterior e põem em risco infraestruturas estratégicas que sustentam a economia e a sociedade do Japão e que, portanto, faz-se necessário aumentar drasticamente a proteção desses locais contra ameaças cibernéticas (IPA, s.d.). Da mesma forma, no ano de 2018 a segunda versão da *Cybersecurity Strategy* japonesa foi lançada, com foco de três anos, assim como sua antecessora. Por fim, em 2019 o METI lançou a *Cyber/Physical Security Framework*, em linha à visão de Sociedade 5.0, como será abordado mais à frente, a qual apresenta uma revisão das medidas de (ciber)segurança que devem ser adotadas pela sociedade industrial japonesa.

3.2.1. Entendimentos iniciais de ciberespaço e cibersegurança no Japão

Por ser um ambiente de atuação internacional relativamente recente, definir os componentes do ciberespaço não é uma tarefa consensual na comunidade científica ou na cena política. Tratando-se inicialmente do ciberespaço, Daniel Kuehl (2009) propôs um conceito amplo baseado em 14 definições apresentadas por fontes diferentes como sendo

> [...] um domínio global no ambiente de informação cujo caráter distintivo e único é enquadrado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações através de redes interdependentes

teve este "prazo" para que sua cibersegurança se tornasse mais resiliente e robusta.

> e interconectadas usando tecnologias de informação e comunicação (KUEHL, 2009, p. 28, tradução minha)[38].

Kuehl deixa claro que as ações tomadas no ciberespaço não necessariamente ficam restritas ao âmbito digital; podem também ter efeitos em outros domínios e elementos de poder (KUEHL, 2018). O mesmo foi feito por Breno Medeiros e Luiz Goldoni, em 2020, quando esses pesquisadores igualmente conceituaram ciberespaço a partir da junção de definições individuais expressas por especialistas. Nesse sentido, o ciberespaço

> [...] pode ser entendido como um domínio único de interação humana artificial, dissociado em parte dos elementos físicos, que permeia os domínios tradicionais. Existe através da conexão de diferentes camadas: tecnológica, técnica e pessoal. Possui peculiaridades únicas, possibilitadas por sua imaterialidade parcial e interconectividade expansiva. O ciberespaço está em constante evolução com o avanço da tecnologia, e em constante mudança à medida que diferentes atores o utilizam, moldando-o para atender às mais diversas necessidades (MEDEIROS e GOLDONI, p. 37, 2020, tradução minha).[39]

Sendo assim, ambos os conceitos apresentam o ciberespaço de formas um tanto diferentes, apesar de formados a partir da mesma estratégia (compilação de significados em um mais abrangente). Enquanto Kuehl o descreve focando nos objetivos e meios pelos quais se pode utilizá-lo, Medeiros e Goldoni destacam o caráter diverso do domínio cibernético e como esse está em constante transformação e adaptação. Dessa forma, mesmo aquelas definições mais amplas diferem em sua essência a depender da forma como se decide descrever o ciberespaço, como as propostas pelos pesquisadores mencionados.

As definições de cibersegurança e ciberdefesa na academia, por outro lado, aproximam-se da conceituação de segurança e defesa aos moldes tradicionais, mas com uma lógica cibernética aplicada. O conceito de cibersegurança proposto pela União Internacional de Telecomunicações (UIT), em 2008, é citado por Melissa Hathaway e Alexander Klimburg como sendo

> [a] coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gerenciamento de risco, ações, treinamento, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético e a organização e os ativos do usuário. [...] A cibersegurança se esforça para garantir a obtenção e a manutenção das propriedades de segurança da organização e dos ativos do usuário contra riscos de segurança relevantes no ambiente cibernético. Os objetivos gerais de segurança compreendem o seguinte: disponibilidade; integridade, que pode incluir autenticidade e não repúdio; e

[38] "[...] global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies".

[39] "[...] can be understood as a unique domain of artifcial human interaction, disassociated in part from physical elements, which permeates the traditional domains. It exists through the connection of different layers: technological, technical and personal. It has unique peculiarities, made possible by its partial immateriality and expansive interconnectivity. Cyberspace is constantly evolving as technology advances, and is constantly changing as different actors use it, shaping it to meet the most diverse needs".

> confidencialidade (HATHAWAY e KLIMBURG, p. 12, 2012, tradução minha)[40].

Os autores mencionam, entretanto, que o termo cibersegurança só foi de fato inserido nos debates sobre o espaço cibernético após o "bug do milênio", nos anos 2000, quando o assunto passou a ser tratado de maneira mais holística. Antes desse período, termos como "segurança da informação" e "segurança da internet" eram mais utilizados e setorizavam diferentes vieses da cibersegurança.

Diferentemente dos conceitos de ciberespaço e cibersegurança, entretanto, a definição de ciberdefesa é mais observada em documentos governamentais que na academia especializada. Tendo como exemplo o conceito do Brasil, a Doutrina Militar de defesa Cibernética brasileira, lançada em 2014, estabelece que a defesa cibernética é um

> [...] conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente (MINISTÉRIO DA DEFESA, p. 18, 2014).

Portugal, por outro lado, poupa palavras em sua Estratégia Nacional de Segurança do Ciberespaço, onde define ciberdefesa apenas como uma "[...] atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço" (CNCS, 2019).

Tal como as definições mais clássicas de segurança e defesa, portanto, a cibersegurança tem um caráter abrangente, voltando-se a políticas, práticas e valores que devem ser adotados para proteger o sistema e seus participantes como um todo, evitando a propagação de riscos, ao passo que a ciberdefesa foca no combate a ameaças específicas a partir do uso de ferramentas de defesa[41]. Como coloca Héctor Luis Saint-Pierre (2006), "a segurança de um país corresponde à ausência de ameaças e a defesa é o conjunto de esforços adotados para neutralizar ameaças". Em adição, a cibersegurança, assim como a segurança tradicional, volta-se mais marcadamente à vida privada da sociedade, ao passo que a ciberdefesa ocupa-se com o ente público e com

---

[40] "[T]he collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality".

[41] Tratando-se de ferramentas ou armas cibernéticas usadas no ciberespaço com propósito de defesa, são tradicionalmente mencionados vírus com algum potencial danoso, como formas variadas de *malwares* e *worms*, assim como *backdoors*, programas de manipulação digital e de negação de serviço, e mais recentemente drones e inteligência artificial. Nesse sentido, dado o atual uso em ascensão de drones e inteligência artificial em cenários de conflito, pesquisadores indicam que em um futuro próximo esses aparatos poderão alcançar um estágio completamente autônomo e livre de interferência humana em sua operação, distinguindo-se como *Lethal Autonomous Weapons Systems* (LAWS); questiona-se, contudo, até que ponto esse tipo de tecnologia é de fato segura e em harmonia com o Direito Internacional Humanitário (CAVELTY, FISCHER e BALZACQ, 2017).

aquilo que possa vir a ameaçar a sobrevivência ou a ordem de um país, como interferências em infraestruturas críticas, por exemplo.

Por outro lado, no que diz respeito ao governo japonês propriamente, este passou a definir suas concepções de ciberespaço como conhecemos hoje a partir do lançamento do *Basic Act on Cybersecurity*, em novembro de 2014. Logo no segundo artigo do documento se pode encontrar o conceito de cibersegurança para o Japão.

> O termo 'cibersegurança' como usado neste Ato significa que as medidas necessárias foram tomadas para prevenir o vazamento, a perda ou o dano de informações gravadas, enviadas, transmitidas ou recebidas de maneira eletrônica, magnética ou qualquer outra forma que não possa ser percebida por sentidos humanos [...], e seguramente manusear aquela informação em outras maneiras; que as medidas necessárias foram tomadas para garantir a segurança e confiabilidade de sistemas de informação e de redes de comunicação e informação [...]; e que este *status* está sendo mantido e gerenciado propriamente (MOJ, 2014, tradução minha)[42].

Diferentemente de suas contrapartes acadêmicas, a definição de cibersegurança do governo japonês é muito mais preocupada em delimitar o que precisa ser protegido no ciberespaço e de que tipo de ações. Em conformidade aos conceitos anteriormente trazidos, no entanto, a conceituação de cibersegurança a nível governamental adota um tom generalista, no sentido de incluir sob sua responsabilidade qualquer camada social que tenha acesso a sistemas pertencentes ao ciberespaço para além do ente público-estatal. Nesse sentido, o BAC inaugura a tradição de "garantir um ciberespaço livre, justo e seguro" como princípio basilar da cibersegurança japonesa, ainda em vigor.

Dez meses após o lançamento do BAC, o governo do Japão promulgou a primeira *Cybersecurity Strategy* do país, em setembro de 2015, a qual foi atualizada em 2018 e em 2021. Apesar de o conceito de ciberespaço aparecer brevemente na *National Security Strategy* de 2013, como sendo "[...] um domínio global composto por sistemas de informação, redes de telecomunicações e outras, que provê uma fundação para atividades sociais, econômicas, militares e outras" (MOFA, 2013)[43], é apenas nas CSS que o termo é elaborado com mais precisão. Pegando um trecho da CSS de 2021, vê-se que atualmente o ciberespaço é descrito de uma maneira mais ampla que na NSS de 2013:

> A expansão global e o desenvolvimento do ciberespaço o transformaram em um lugar onde uma ampla variedade de informação, dados, tanto em termos de qualidade

[42] "The term "cybersecurity" as used in this Act means that the necessary measures have been taken to prevent the leakage, loss, or damage of information that is recorded, sent, transmitted, or received in electronic form, magnetic form, or any other form that cannot be perceived by the human senses, [...] and to securely manage that information in other such ways; that the necessary measures have been taken to ensure the security and reliability of information systems and of information and communications networks; and that this status is being properly maintained and managed".

[43] "[...] a global domain comprised of information systems, telecommunications networks and others, provides a foundation for social, economic, military and other activities".

> quanto de quantidade, podem ser gerados, compartilhados, analisados e distribuídos livremente por entre fronteiras nacionais, independentemente de tempo e lugar. Equipado com essas características, o ciberespaço oferece um lugar onde pessoas podem enriquecer suas vidas e perceber valores diversos através da criação de ativos intelectuais como inovações tecnológicas e novos modelos de negócios. Como tal, serve de fundação ao desenvolvimento sustentável da economia e da sociedade no futuro enquanto sustenta o liberalismo, a democracia e o desenvolvimento cultural (NISC, 2021, p. 17, tradução minha)[44].

Para além da definição padrão acima, um aspecto a ser mencionado é a inserção da ideia de Sociedade 5.0 ao ciberespaço, a partir da CSS de 2018. Como posto em decisão do Gabinete do Primeiro-ministro, "Sociedade 5.0 é o quinto estágio da história humana, seguindo as sociedades de caça, agrícola, industrial e de informação. É uma sociedade na qual novos valores e serviços são criados continuamente trazendo riqueza às pessoas da sociedade" (NISC, 2018, p. 1, tradução minha)[45]. Dentre esses valores e serviços, são mencionadas tecnologias como Inteligência Artificial (IA), *Internet of Things* (IoT), robótica, realidade virtual, *fintech*, e mesmo produtos eletrônicos como impressoras 3D. Essas evoluções tecnológicas, cujos impactos resultam na transformação das estruturas socioeconômicas existentes, seriam responsáveis pela unificação do ciberespaço ao mundo real (IBID, 2018). Da mesma forma, na CSS de 2021 o governo japonês volta a mencionar esse ponto, indicando como a década de 2020 provavelmente será uma "década digital" em que a sociedade e a economia japonesas terão um grande salto em direção à Sociedade 5.0, quando o ciberespaço, portanto, estará integrado ao mundo físico em um alto nível (NISC, 2021)[46].

Isso posto, há de se observar que o ciberespaço, no entendimento japonês, conta com uma retórica muito voltada à integração paulatina com o mundo físico, deixando de ser um espaço restrito apenas à internet ou ao espectro eletromagnético. Assim, ao invés de ser tratado

---

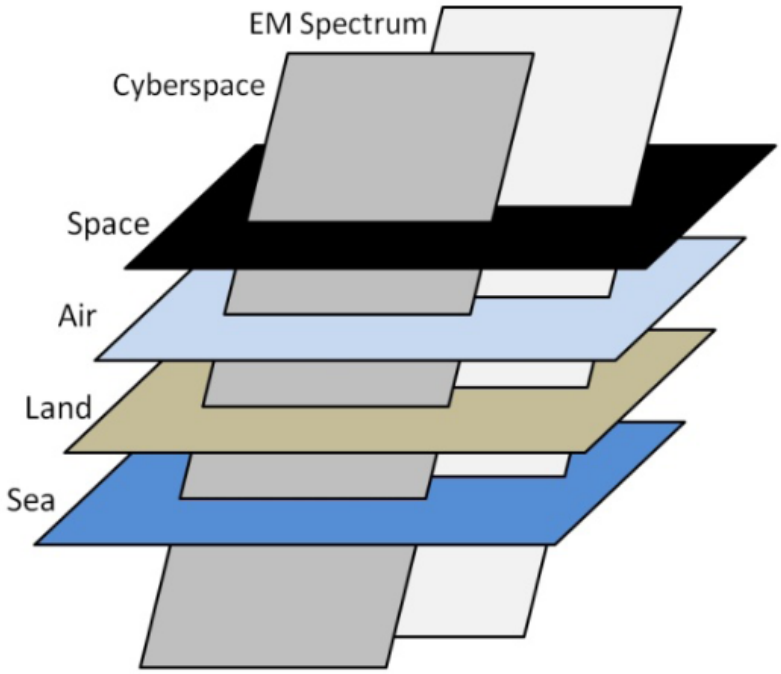
[44] "The global expansion and development of cyberspace has turned it into a place where a wide range of information and data, both in terms of quality and quantity, can be freely generated, shared, analyzed and distributed across national borders regardless of time and place. Equipped with these characteristics, cyberspace offers a place where people can enrich their lives and realize diverse values by creating intellectual assets such as technological innovations and new business models. As such, it serves as a foundation for the sustainable development of the economy and society in the future while underpinning liberalism, democracy, and cultural development".

[45] "Society 5.0 is the 5th stage of human history, following the hunting society, agricultural society, industrial society, and information society. It is a society in which new value and new services are created continuously bringing wealth to the people of society".

[46] Nesse processo de chegada a uma Sociedade 5.0, o governo japonês deixa claro como os processos de digitalização serão fundamentais à evolução da sociedade. Nesse sentido, a *Digital Agency* foi estabelecida em setembro de 2021 como um esforço para se criar essa sociedade digitalizada, promovendo com vigor uma transformação digital sob a visão de criar "uma sociedade onde as pessoas possam escolher serviços que se adequem às suas necessidades, bem como realizar diversas formas de felicidade através do uso de tecnologias digitais", visando alcançar uma digitalização amigável às pessoas e com ninguém sendo deixado para trás (NISC, 2021). Isso posto, a *Digital Agency* japonesa é uma espécie de bastião da Sociedade 5.0, visto que a digitalização é imprescindível para que o país alcance esse modelo social desejado.

como um domínio independente, o ciberespaço perpassa o mundo físico e o compõe juntamente das tecnologias e dos domínios tradicionais[47].

Figura 2 – Ciberespaço e espectro eletromagnético atravessando os domínios físicos como dimensões transversais de operação



FONTE: CONTI, NELSON e RAYMOND, 2013.

Da mesma forma, o ciberespaço é descrito repetidas vezes como um ambiente essencial às atividades socioeconômicas do país na contemporaneidade; logo, precisa ser protegido de ameaças que ponham em risco os livres fluxos de informação, a segurança dos ambientes humanos, a prosperidade econômica e social e a paz, conforme os preceitos democráticos da nação (NISC, 2015). Essa característica do ciberespaço é comum nas três Estratégias lançadas até então. Nesse sentido, o primeiro dos três eixos de direcionamento da CSS mais recente diz respeito a realçar a vitalidade socioeconômica e o desenvolvimento sustentável do Japão, avançando com temas como a transformação digital, através da digitalização em escalada de operações, produtos e serviços. Assim, tanto o ciberespaço quanto a cibersegurança, conforme apontado pelo governo japonês, estão conectados a valores corporativos (NISC, 2021).

Por fim, no que diz respeito à ciberdefesa, o Japão nunca definiu precisamente o que

[47] Autores como Nori Katagiri (2021) vão mais direto ao ponto descrevendo a ideia de Sociedade 5.0 como uma iniciativa governamental para criar um novo contrato social e modelo econômico por meio de inovações tecnológicas. Nesse contexto, o governo japonês tem sistematicamente integrado tecnologias digitais para realçar seu crescimento econômico e impulsionar soluções para desafios sociais.

entende por sua defesa cibernética. No entanto, analisando os Livros Branco de Defesa (LBD) mais recentes do país, o governo nipônico menciona em diversos trechos características de suas "capacidades de ciberdefesa". Nos documentos, isso se refere a capacidades de (1) identificação e análise de ameaças cibernéticas; (2) monitoramento de ataques para prevenção; (3) limitação e recuperação de danos em caso de ataque; e (4) interrupção do uso do ciberespaço por oponentes durante ataques contra o Japão (MOD, 2022). Este último ponto merece atenção, pois, a reestruturação do *Cyber Defense Command* japonês, em março de 2022, propiciou a esta unidade tal capacidade pela primeira vez, apesar de ainda ser questionável se esse tipo de ação é legítima tendo em vista a Constituição pacifista do país.

Além disso, em suas CSSs o Japão define duas outras características de sua ciberdefesa: a primeira, chamada de "ciberdefesa proativa" na Estratégia de 2018 e apenas de "ciberdefesa ativa", na de 2021, "[...] envolve cooperação com empresas ciber- relacionadas e a implementação de medidas ativas de prevenção contra ameaças antecipadamente" (NISC, 2021, p. 38, tradução minha)[48]. Em segundo lugar, a CSS de 2021 expõe que uma das medidas específicas do segundo eixo de direcionamento da Estratégia[49] é implantar uma "defesa cibernética compreensiva" no Japão. Esta faceta da ciberdefesa nipônica se refere a uma série de ações que serão adotadas pelo governo, como "[...] coleta e análise de informações para investigação, avaliação, emissão de alerta, resposta a ataques e subsequente planejamento de medidas políticas para prevenir recorrência [...]" (NISC, 2021, p. 36, tradução minha)[50].

Assim como a ciberdefesa ativa, a ciberdefesa compreensiva também prevê uma maior integração e colaboração com empresas ciber-relacionadas, o que possibilitará uma resposta geral muito maior a partir de rápidas coletas de informação tanto por partes públicas quanto privadas. Desse modo, observa-se como a ciberdefesa japonesa engloba mais que meios de ataque e defesa contra ameaças de maneira direta, abrangendo também logísticas de coleta de informações e cooperação entre setores para fortalecer a defesa japonesa no ciberespaço. A ciberdefesa ativa também é mencionada diversas vezes na NSS de dezembro de 2022, aparecendo igualmente neste documento como um tipo de defesa cibernética central do governo. Em contrapartida, a ciberdefesa compreensiva não aparece descrita nesses termos no documento de 2022; o que se tem, entretanto, é a definição de que todo o aparato de defesa do

[48] "[...] involves cooperating with cyber-related enterprises and implementing active preventive measures against threats in advance".
[49] Qual seja "Concretizar uma Sociedade Digital onde o Povo possa Viver com um Senso de Segurança e Proteção" (NISC, 2021, p. 6). Do original, "Realizing a Digital Society where the People can Live with a Sense of Safety and Security".
[50] "[...] collection and analysis to investigation, evaluation, issuing alerts, responding to the attack, and subsequent planning of policy measures to prevent recurrence [...]".

Japão é "compreensivo", através de termos como "poder nacional compreensivo"[51] e "arquitetura de defesa compreensiva"[52]. Sendo assim, a defesa cibernética também está incluída nessa característica de sua política.

De maneira geral, portanto, o governo japonês quebra com a lógica de que a ciberdefesa deveria se restringir a ações tomadas para proteger apenas o ente público contra ameaças que ponham em risco a sobrevivência do Estado. Isso se justifica, pois, no entendimento do governo nipônico, são limitadas as respostas contra ciberataques sérios que podem ser dadas pelos entes privados individualmente, seja através da autoajuda, seja por ajuda mútua, exigindo apoio governamental para lidar com esses casos (NISC, 2021), uma vez que entes privados estão sendo visados por governos estrangeiros e apenas outros governos têm recursos e capacidades para combater ataques governamentais. Entretanto, haja vista que o ciberespaço é reconhecido pelo Japão como um domínio com forte movimentação econômica e com tendências corporativas, a necessidade de o Estado colaborar com o setor privado não destoa completamente do escopo de sobrevivência estatal, já que nessa lógica a economia e determinados ramos privados, como o de infraestruturas críticas, estão intrinsecamente ligados à manutenção do Estado japonês enquanto tal.

3.3. Os primeiros anos de 2020

Logo no primeiro ano da década de 2020 o mundo se viu em meio à pandemia de Covid-19 e, por motivos sanitários, os Jogos Olímpicos de Tóquio de 2020 tiveram de ser adiados. Entretanto, o desenvolvimento do cenário cibersecuritário do Japão desde a primeira CSS de 2015, voltado à segurança do evento, não foi desperdiçado. Ao final dos jogos, em 2021, o Japão saiu praticamente ileso dos cerca de 450 milhões de ciberataques direcionados ao evento durante sua ocorrência, como informado pela *Nippon Telegraph and Telephone Corporation* e pelo comitê organizador dos jogos de Tóquio. Indica-se que o sucesso da estratégia japonesa foi sua ação preventiva para evitar o êxito de ataques cibernéticos, especialmente através da cooperação dos setores público e privado na segurança dos jogos[53]. A exemplo, o NISC

[51] O poder nacional do Japão é descrito como compreensivo na NSS de 2022, pois deve focar em cinco diferentes frentes para o sucesso de sua segurança nacional: o desenvolvimento de capacidades diplomáticas, capacidades de defesa, capacidades econômicas, capacidades tecnológicas e capacidades de inteligência (MOFA, 2022b).

[52] A arquitetura de defesa compreensiva do Japão envolve quatro áreas identificadas por Tóquio como complementares e inseparáveis do reforço das capacidades defensivas do país, quais sejam (1) pesquisa e desenvolvimento, (2) desenvolvimento de infraestrutura pública, (3) cibersegurança e (4) cooperação internacional (MOFA, 2022b).

[53] Nesse quesito, percebe-se um aumento na cooperação entre instituições governamentais com empresas privadas de tecnologia, tanto japonesas quanto estrangeiras. No caso do Japão, Toyota e Panasonic foram empresas-chave

requisitou que todas as companhias de infraestrutura crítica que proviam serviços aos Jogos Olímpicos de Tóquio passassem por avaliações de risco por seis vezes desde 2016, e organizou também cinco exercícios coletivos com as técnicas mais recentes de ciberataques, onde milhares de pessoas foram convidadas a participar.

Isso observado, a postura preventiva e defensiva do Japão no ciberespaço e ao longo dos Jogos Olímpicos de Tóquio exemplifica como esse tipo de defesa é vantajosa em algum nível, dado que medidas para correção de acidentes cibernéticos após a sua ocorrência tendem a ser mais custosas e desafiadoras. O Comitê Olímpico Internacional, inclusive, identificou a cibersegurança como uma área prioritária a ser melhorada em todas as edições futuras das Olimpíadas, muito tendo em vista os ataques realizados contra as Olimpíadas de Inverno de PyeongChang, na Coreia do Sul, em 2018[54].

Além disso, em 2021 a terceira versão da *Cybersecurity Strategy* do Japão foi lançada, a qual está em vigor no momento de escrita deste trabalho. Como será observado também nas próximas seções, esta versão do documento amplia o foco dado a alguns tópicos tidos como basilares à cibersegurança do Japão e ao ciberespaço como um todo. O ponto fulcral deste documento é, para fins desta pesquisa, a identificação da China, da Rússia e da Coreia do Norte pela primeira vez como as principais ameaças do Japão no ciberespaço, haja vista as pretensões maliciosas desses países quanto ao uso deste domínio. Isso representa um ponto de virada inicial na postura que o Japão vinha adotando até então; antes da CSS de 2021, o governo nipônico era reticente quanto aos que cometiam infrações no ciberespaço, seja pela não nomeação e não culpabilização de organizações e países financiadores de ciberataques, seja pela falta de adoção de sanções contra os infratores. Sendo assim, a nomeação da China, da Coreia do Norte e da Rússia como as principais ameaças contra o Japão no ciberespaço simboliza uma mudança não

em inovações para a proteção dos Jogos Olímpicos de Tóquio. Em uma contrapartida internacional, a parceria estabelecida entre o Japão e a *Israel Electric Corporation*, bem como com o *US Department of Homeland Security*, foram importantes respectivamente para a proteção de infraestruturas críticas e para o robustecimento da cibersegurança do país ao longo dos jogos.

[54] Na abertura dos jogos de inverno de 2018, a internet no local do evento foi cortada no início da abertura e o site dos jogos foi derrubado, o que impediu que muitos visitantes imprimissem seus ingressos e acessassem o espaço. Além disso, televisores alimentados pela internet tiveram seu funcionamento interrompido nessas dependências. Naquele cenário, os ataques alegadamente vieram da Rússia, sendo que seis oficiais de inteligência russos foram multados nos Estados Unidos como consequência. Devido a isso, o governo do Japão temia que a Rússia pudesse igualmente interferir nos jogos de Tóquio, tendo em vista que nos últimos anos foram apontados escândalos de doping financiados pelo Estado russo e o país foi banido temporariamente dos jogos, sendo que esses ataques presumidamente advindos da Rússia teriam caráter retaliativo por conta desse boicote. Ao longo do evento japonês, de fato foram observadas tentativas de ataques às agências que conduziam esses inquéritos de doping, mas não houve ocorrências graves. Em adição, à vista dos ataques na Coreia do Sul em 2018, o governo japonês se preocupou com as tecnologias IoTs utilizadas no evento, dado que muitos dispositivos estavam conectados em rede como tradutores ao vivo entre pessoas, reconhecimentos faciais e mesmo táxis sem motoristas, o que poderia envolver acidentes caso hackeados. Para essas preocupações tampouco houve incidentes dignos de menção.

só na securitização desse domínio, como também na atribuição declarada de ameaças cibernéticas pelo governo nipônico.

Por fim, no ano de 2022 a *National Security Strategy* japonesa também foi revisada, pela primeira vez desde seu lançamento em 2013. De maneira comparativa, a NSS de 2013 começou a introduzir o tema da cibersegurança na agenda de segurança (inter)nacional do Japão; nesta primeira versão, o ciberespaço é identificado como vital para a segurança japonesa e o país estabelece as regras básicas da segurança cibernética da nação, como a promoção de um ciberespaço livre e seguro, bem como o compartilhamento de informações inter-agências governamentais e cooperação entre países *like-minded* para a formulação de regras internacionais para o ciberespaço, visto que até então não se existia legislação concernente ao domínio cibernético por diferenças entre os países relevantes envolvidos.

A NSS de 2022, por outro lado, já trata da segurança cibernética com muito mais propriedade que o documento anterior, visto que nesse meio tempo ocorreram diversas institucionalizações do tema, seja pelas mudanças ocorridas no ISPC e no NISC e pelo lançamento de três *Cybersecurity Strategies*, seja pela experiência adquirida pelo país através das Olimpíadas de Tóquio. Dessa maneira, o documento de 2022 traz objetivos e posicionamentos nacionais bem mais claros quanto ao ciberespaço e à cibersegurança japonesa. A exemplo, a segurança cibernética é mencionada em particular como sendo uma área com riscos em escalada, visto que ciberataques têm sido constantemente usados para desabilitar ou destruir infraestruturas críticas, interferir em eleições e roubar informações sensíveis, por exemplo, inclusive com ataques financiados por Estados. Ainda, é altamente provável que cenários de guerra híbrida serão conduzidos de formas ainda mais sofisticadas num futuro próximo. Por conta disso, o governo nipônico aponta que suas capacidades de resposta no campo da cibersegurança precisam ser reforçadas em nível igual ou superior aos de países ocidentais.

Além disso, a NSS de 2022 menciona que o NISC ficará incumbido de construir uma nova organização que trate da segurança cibernética de maneira compreensiva e centralizada. Por fim, vale indicar que o governo japonês delineou como objetivo do documento introduzir capacidades de ciberdefesa ativas no país para eliminar de antemão a possibilidade de ciberataques sérios contra o país. Podemos conectar esse ponto ao sucesso das medidas de cibersegurança e ciberdefesa adotadas pelo país em face aos Jogos Olímpicos de Tóquio; como mencionei anteriormente, um dos sucessos para a ausência de incidentes cibernéticos graves ao longo do evento em Tóquio foi a série de medidas preventivas adotadas pelo país, e na NSS de 2022 o Japão deixa claro que pretende continuar nessa linha de atuação cibernética exitosa.

3.4. Sobre ameaças cibernéticas

O NISC estabeleceu na CSS de 2021 uma série de riscos e ameaças enfrentadas pelo Japão quanto à sua cibersegurança. A nível doméstico, por exemplo, o governo nipônico se preocupa com a maior digitalização da sociedade, seja pela maior exposição de sua população em redes sociais, o que abriria brechas para roubo de informações pessoais, seja pela expansão da IoT, o que propiciaria uma maior diversidade de alvos a serem atacados, especialmente no ramo industrial (BARLETT, 2020; NISC, 2021). Da mesma forma, o governo japonês sinalizou que a falta de instrução por parte da população sobre como usar o ciberespaço de maneira segura cria novas vulnerabilidades no sistema, tanto para a sociedade quanto para a economia, apontando como a "higiene cibernética" faz parte dos projetos do país, estratégia que vem sendo aplicada na Europa hoje. Por fim, outro exemplo de vulnerabilidade doméstica é a indicação de falta de recursos humanos no setor empresarial e no campo da tecnologia para atuar no ciberespaço, o que acaba criando uma dependência de recursos estrangeiros, desde produtos e serviços até novas tecnologias *per se*.

Por outro lado, no que tange a riscos e ameaças internacionais, o Japão menciona pela primeira vez em um documento estratégico oficial, na CSS de 2021, que a China, a Rússia e a Coreia do Norte são as principais origens das infrações cometidas contra a cibersegurança japonesa. Neste cenário, indica-se que a China presumidamente volta seus ataques ao roubo de informações de companhias relacionadas à indústria militar para assim impulsionar sua posse de tecnologias avançadas; a Rússia, por outro lado, comete infrações no ciberespaço para exercer influência com o intuito de atingir objetivos políticos e militares; e a Coreia do Norte, por fim, para além de conduzir ataques para alcançar objetivos políticos, tal como a Rússia, também tenta obter moedas estrangeiras com seus ataques, uma vez que este país mantém relações comerciais com pouquíssimos Estados mundo afora e seu acesso a moedas estrangeiras é bastante limitado. Além desses três países, o Japão também reconhece o envolvimento de organizações criminosas por trás de ciberataques que atingem a nação (NISC, 2021).

À vista disso, apesar de o Japão fazer menção a atividades como ciberespionagem e cibersabotagem no LBD de 2021, o país divide as infrações cibernéticas em duas grandes categorias: ciberataques e cibercrimes. Em sua definição de ciberataque, o Japão inclui atividades como "intrusão ilegal, roubo, alteração ou destruição de informações, parada ou mau funcionamento de sistemas de informação, execução de programas não autorizados, ataques

DDoS" (MOD, 2021, p. 284, tradução minha)[55], bem como APT, ataques contra sistemas de controle industriais e outras infraestruturas críticas que impactariam uma variedade de atividades econômicas e sociais, e mesmo aqueles ataques contra processos democráticos, visando e interferindo em eleições (NISC, 2021).

Em contrapartida, os cibercrimes são definidos pela *National Police Agency* (NPA) do Japão como sendo crimes de violação da *Unauthorized Computer Access Law*[56], crimes contra computadores/dados[57] e crimes relacionados à internet[58] (NPA, s.d.). Embora o Japão tenha assinado a Convenção de Budapeste sobre o Cibercrime, em 2001, a qual foi ratificada apenas em 2016, o que expande em grande medida as definições de cibercrime ao país, a NPA continua utilizando os mesmos balizadores acima mencionados em seus relatórios como métrica aos crimes cibernéticos no Japão. Nesse sentido, a agência de polícia japonesa mostrou, em um relatório lançado em 2022, que a quantia de presos por crimes cibernéticos no Japão ultrapassou o número do ano anterior – 6.933 em 2022 contra 6.690 em 2021. Das três categorias, crimes relacionados à internet são os mais recorrentes, totalizando 5.199 até então do total apresentado em 2022, contra 3.961 em 2021 (NPA, 2022). É importante mencionar, entretanto, que esses números representam apenas a quantidade de prisões efetuadas por cibercrimes, não retratando, portanto, o número real de infrações cometidas.

Dito isso, investidas tais como ciberespionagem e cibersabotagem já estão de maneira geral incluídas nas categorias de ciberataques ou cibercrimes propostas pelo governo japonês. Além disso, destaco como ciberespionagem é, a nível governamental, o maior risco à segurança cibernética nipônica, dado que esse é o tipo de manobra mais comum a afetar estruturas governamentais no tempo presente (SOESANTO, 2020; LEWIS, 2015). De outro modo, cibercrimes são a principal ameaça contra a sociedade civil japonesa, especialmente empresas e grandes corporações rotineiramente alvos de *ransomware*. No ano de 2020, por exemplo, mais de 100 empresas japonesas sofreram com tentativas de extorsão, das quais 33 pagaram uma quantia equivalente a JPY 123 milhões, ou cerca de USD 1,1 milhão, por conta de vírus do tipo *ransomware* (SIRIPALA, 2020).

[55] "Illegal intrusion, information theft, alteration or destruction, operation stop/malfunction of information system, execution of unauthorized program, DDoS".
[56] Promulgada em agosto de 1999, tendo recebido sua última emenda em 2013. Este tipo de crime faz menção a qualquer tipo de invasão não autorizada a computadores, seja por atividades hackers, seja através de credenciais oficiais (NPA, s.d.).
[57] Nesta categoria encontram-se crimes como fraude, destruição ou produção ilegal de dados eletromagnéticos e obstrução de atividades empresariais pela destruição de computadores (NPA, s.d.).
[58] Incluem-se atos como difamação, intimidação, infração contra direitos autorais, pornografia e prostituição infantil e distribuição de materiais obscenos (NPA, s.d.).

Contrariamente ao governo japonês, a academia especializada tende a expor as infrações cometidas no ciberespaço de maneira mais segregada. Thomas Rid, por exemplo, identifica que sabotagem, espionagem e subversão são as principais ameaças no ciberespaço. Respectivamente, o autor faz referência à "[...] tentativa deliberada de enfraquecer ou destruir um sistema militar um econômico", sendo coisas os alvos primários em detrimentos de indivíduos; "[...] tentativa de penetrar um sistema adversário com o objetivo de extrair informações sensíveis ou protegidas. Pode ser tanto de natureza social quanto técnica"; e à "[...] tentativa deliberada de prejudicar a autoridade, a integridade e a constituição de uma autoridade ou ordem estabelecida" (RID, 2012, pp. 16, 20 e 22, traduções minhas)[59]. Nye (2010), por outro lado, expõe que espionagem econômica, crime, ciberguerra e ciberterrorismo são as principais ameaças contra a segurança nacional de um Estado no ciberespaço. O autor também toma a iniciativa de inserir infrações cibernéticas numa ótica de *hard* e *soft power*, em categorias tanto intra quanto extraciberespaço envolvendo atividades cinéticas e não cinéticas. Sendo assim, o governo japonês adota um posicionamento mais genérico quando define suas ameaças majoritariamente como ciberataques ou cibercrimes. De qualquer forma, as diferentes categorias trazidas pela academia estão presentes no escopo estratégico japonês, mas sob guarda-chuvas mais amplos de classificação.

3.4.1. O estado atual das ciberameaças contra o Japão

Mesmo o governo japonês identificando outros atores internacionais como parte do *hall* de ameaças cibernéticas contra o país, especialmente aqueles não estatais, a China, a Coreia do Norte e a Rússia continuam representando as maiores hostilidades ao Japão. Esse ponto de vista já é endossado por muitos documentos oficiais do país, desde seus Livros Brancos de Defesa e da *Cybersecurity Strategy* mais recente até suas *National Security Strategy* e *National Defense Strategy* de 2022. Dessa maneira, serão exploradas nesta subseção apenas as hostilidades desses três países como ponto central de análise das respostas japonesas no ciberespaço.

Quanto às ameaças advindas da China, Adam Segal (2020) indica que o país é um dos atores mais ativos no ciberespaço da Ásia-Pacífico e vem desenvolvendo e movendo suas capacidades cibernéticas em busca de objetivos econômicos, políticos e estratégicos. Nesse sentido, tanto Segal quanto Robert Work e Greg Grant (2019) concordam que a China também

[59] "[...] deliberate attempt to weaken or destroy an economic or military system"; "[...] attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information. It may be either social or technical in nature"; e "[...] deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order".

vem elaborando uma política de compensação contra os Estados Unidos, baseada na aquisição de altas tecnologias, como 5G, IA e sistemas de informação quânticos, os quais não só robustecem a competitividade econômica do país como serve para modernizar o Exército de Libertação Popular (ELP) e ultrapassar o poderio ocidental, em especial dos EUA.

Além disso, o presidente chinês Xi Jinping declarou em 2014 que não há segurança nacional sem cibersegurança (ALSABAH, 2017), pensamento responsável por mover a cibersegurança ao topo das prioridades nacionais chinesas. Desde então, a cibersegurança tem ocupado um papel de fato central no pensamento militar moderno da China, a ponto de ser identificado como um dos pilares na "iniciativa de confrontação militar" entre Estados. Isso é dizer que aquele lado que detiver uma superioridade cibernética será capaz de realizar uma guerra de sistemas contra rivais, acarretando mau funcionamento e perda de controle sobre as operações inimigas a ponto de incapacitar suas armas e seus equipamentos, impedindo, portanto, o início de uma confrontação militar cinética.

Isso posto, apesar de a China ter uma postura bastante voltada à incrementação tecnológica do país, as autoridades chinesas de fato enxergam a China como fraca se comparada ao grau de ameaças de outras nações e, portanto, acaba adotando uma retórica vitimista no ciberespaço (SEGAL, 2020). Nesse sentido, Schumacher (2015) aponta que esta é uma das características atuais do nacionalismo chinês. Para o autor, o Partido Comunista Chinês vem desenvolvendo uma narrativa doméstica de vitimização internacional em face à humilhação provocada por potências estrangeiras sobre a China no passado, desde as guerras do ópio contra o Reino Unido até o Japão na Segunda Guerra Mundial. Essa postura é adotada pelo país tanto para angariar legitimidade doméstica ao Partido quanto para de fato tentar "superar" esse caráter de vítima.

No que diz respeito à postura ofensiva da China no ciberespaço, os chineses focam seus ataques contra o setor privado e manufatureiro envolvido com alta tecnologia, de lugares como Estados Unidos, Japão, Europa e Sudeste Asiático, como forma de roubar propriedade intelectual, segredos de negócios e outras informações que poderiam tornar o país mais competitivo e modernizar o ELP (IBID, 2020). Quanto a isso, os ataques sofridos pelo Japão em 2011, como mencionados anteriormente, foram rastreados como advindos da China e fazem jus à postura ofensiva do país, uma vez que o maior alvo dos ciberataques, a Mitsubishi Heavy Industries, não só é uma empresa de alta tecnologia como é responsável pela produção militar do Japão. Dessa maneira, a China não só teria a possibilidade de roubar tecnologia para ampliar sua competitividade econômica, como poderia modernizar o ELP, na medida do possível, como fruto dessas invasões cibernéticas. Entretanto, argumenta-se que mesmo a China conseguindo

roubar informações sigilosas, o país não conseguirá se modernizar por completo através de ciberespionagem.

Não obstante, a China também enfrenta contratempos quanto à sua segurança cibernética. Mesmo o país tendo investido cerca de USD 7,3 bilhões nesse ramo em 2019, isso é cerca de nove vezes menos que o montante investido apenas pelas companhias privadas dos EUA. Há também uma falta generalizada de profissionais para atuar na área; enquanto que em 2019 cerca de 700 mil postos de trabalho envolvendo cibernética estavam vagos na China, este número alcançou 1,4 milhão em 2020, segundo Segal. Junto disso, observa-se como desde 2010 a China vem sendo exposta a ciberataques a níveis periodicamente mais altos, e que suas redes militares, de inteligência e de monitoramento estão se tornando alvos óbvios de operações cibernéticas estrangeiras (IBID, 2020). Nesse ponto, o autor lembra do decreto de 2019 do Partido Comunista Chinês, o qual determinou a substituição em massa de todos os softwares e hardwares estrangeiros em uso no país como forma de contornar a ciberespionagem em solo chinês. Contudo, a dependência generalizada de tecnologias estrangeiras em redes críticas continua sendo uma das maiores fraquezas da China, segundo o autor.

Tratando-se da Coreia do Norte, este país vem desenvolvendo suas capacidades cibernéticas desde a década de 1990, anos antes de muitos países, inclusive do Japão. Essa proatividade norte-coreana foi parte da reestruturação do Estado conduzida por Kim Jong-il, e desde então a Coreia do Norte tem recrutado e treinado recursos humanos e criado instituições para desenvolvimento e sustento do país no ciberespaço. Devido a essa conjuntura, Daniel Pinkston (2020) aponta como a Coreia do Norte tem se tornado uma ameaça persistente, com notória atividade hacker, principalmente envolvendo ataques a bancos, ataques voltados ao roubo de criptomoedas e ataques *ransomware*. Além disso, o autor ressalta que os hackers norte-coreanos são altamente especializados e dificilmente dissuadidos a usarem ciberataques agressivos.

Esse tipo de ataque voltado à captação de moedas estrangeiras se justifica em parte pela falta de modernização econômica na Coreia do Norte, dado que desde a fome da década de 1990 tem-se observado uma revitalização econômica nula a despeito do rearranjo do país nessa mesma década. Assim, roubo de moedas estrangeiras é uma das únicas formas de consegui-las, o que também ajuda o país a contornar seu déficit comercial e as sanções impostas pela comunidade internacional. Pinkston ressalta ainda que essa captação de moedas serve inclusive para garantir a integridade do sistema norte-coreano, uma vez que o governo provê benefícios materiais aos aliados do regime em troca de lealdade com esses montantes captados ilegalmente. Aponta-se que através desses ciberataques a Coreia do Norte já tenha capturado

cerca de USD 2 milhões em moedas físicas e USD 500 milhões em criptomoedas aos cofres norte-coreanos (PINKSTON, 2020).

Como a CSS de 2021 indica, entretanto, a Coreia do Norte também realiza ciberataques com propósitos políticos contra rivais, assim como a Rússia. Contra o Japão, um dos exemplos mais marcantes desse tipo de ataque ocorreu em 2014, quando a Coreia do Norte lançou uma série de ciberataques contra a Sony Pictures Entertainment em retaliação ao filme *The Interview*, o qual satiriza o assassinato do líder norte-coreano Kim Jong-un. Através desses ataques, uma série de informações internas da empresa foram reveladas, desde dados de funcionários até filmes não anunciados, o que fez com que a Sony cancelasse o lançamento do filme nos cinemas e diminuísse sua divulgação. Tempo depois, a *National Security Agency* (NSA) conseguiu invadir sistemas norte-coreanos e comprovar que esses ataques advieram de lá. Aponta-se como esses ataques representaram uma certa mudança no ritmo norte-coreano no ciberespaço, haja vista o aparente sucesso do país em retaliar o filme da produtora, sendo que a partir daí o país passou a focar em ciberataques maiores como os voltados ao roubo de moedas (PINKSTON, 2020).

Mudando o foco para a Rússia, Valeriy Akimenko e Keir Giles (2020) indicam que para a segurança nacional russa não existe diferença entre o mundo físico e o mundo digital, a ponto de termos como "ciber" não serem utilizados em nenhum escalão. Isso se justifica, pois, a informação é a principal arma deste país no cenário internacional, e informações percorrem todos os espaços, sem distinção de concretude ou virtualidade. Sendo assim, o ciberespaço é comumente referido na Rússia como espaço da informação, compreendendo tanto a rede de computadores quanto a rede humana de processamento de informações. Essa postura rígida quanto aos fluxos de informação é observada também domesticamente; qualquer circulação de informações que possa pôr em risco a soberania estatal ou a sociedade é considerada preocupação-chave de segurança, incluindo protestos políticos que se opunham ao governo, já que a narrativa de informações poderia eventualmente derrubar o regime, por exemplo.

Esse tipo de configuração se assemelha, de sua própria maneira, aos pressupostos da Sociedade 5.0, considerada nas estratégias do Japão como base do espaço cibernético atual, dado o entendimento de que o mundo virtual e o mundo real estão se tornando indistinguíveis entre si. Do lado russo, entretanto, o objeto que leva o país a considerar essa configuração são os fluxos de informações na sociedade, enquanto para o Japão a IoT e as trocas comerciais que ocorrem no ciberespaço compõem suas justificativas centrais.

A forma como a Rússia não separa o mundo virtual do real é uma das razões pela qual o país é precursor das novas guerras híbridas e guerras de informação que têm sido observadas

no palco internacional, recorrentemente mencionadas pelo governo japonês como ameaças advindas daquele país. Uma vez que a transformação das informações em arma ocorre independentemente da forma que tenham, as capacidades russas são utilizadas de maneira holística em cenários de conflito, sejam essas capacidades tradicionais, sejam elas eletrônicas. O Ocidente, em contrapartida, costuma adotar respostas mais técnicas para atividades hostis puramente cibernéticas, sendo insuficientes para contornar as ameaças abrangentes da Rússia que compreendem desinformação, subversão, ambições que flertam com mudanças de regimes e efeitos de guerras eletrônicas e cinéticas (AKIMENKO e GILES, 2020).

Quanto a esse caráter holístico, Akimenko e Giles (2020) complementam dizendo que a Rússia atinge o ponto de contratar hackers externos, inclusive membros de organizações criminosas, como forma de complementar suas forças cibernéticas nacionais. Esse tipo de postura sempre põe a Rússia sob constante escrutínio público, o que, segundo os autores, não é fator suficientemente dissuasivo na condução das atividades cibernéticas assertivas da Rússia ou em suas campanhas de desinformação ofensivas. Dessa maneira, aquelas nações que constroem defesas cibernéticas que não acompanhem a complexidade do pensamento russo automaticamente estarão despreparadas para as diversas formas de ataques e campanhas da Rússia no ciberespaço.

Nesse quesito, o objetivo primeiro da Rússia com sua manipulação de informações é influenciar o comportamento e a percepção do inimigo, da população e da comunidade internacional. Isso se dá através de inteligência, influência e operações em redes de computadores, sendo que essas três atividades podem abranger propagação de desinformação, guerra eletrônica, desabilitação de comunicações, degradação de navegação e destruição das capacidades computacionais inimigas (AKIMENKO e GILES, 2020). Apesar de o Japão nunca ter sido alvo de ataques severos advindos da Rússia, existia um grande receio no Japão que os Jogos Olímpicos de Tóquio pudessem ser alvo de ciberataques russos similares ao que ocorreram na Coreia do Sul em 2018, como mencionado na subseção 3.3. Sendo assim, as preocupações japonesas atuais envolvendo a Rússia e o ciberespaço dizem respeito mais a cenários que poderiam vir a acontecer, diferentemente das preocupações concernente à Coreia do Norte e a China, já que esses países apresentam ameaças reais por conta de ataques reais já efetuados contra o país e que afetaram suas estruturas público-privadas.

Finalizo dizendo que os comportamentos das três nações que ameaçam o Japão são bastante diferentes em sua essência, e essas diferenças são bem apontadas nos documentos estratégicos do Japão. Dessa maneira, o governo nipônico está ciente que é alvo de ciberataques de naturezas distintas, como roubo de tecnologias por parte da China, extorsões milionárias

através de ataques cibernéticos norte-coreanos, bem como manipulação e guerra de informações pela Rússia. A partir desse cenário, o governo japonês sofre constantes modernizações em seu aparato cibernético para contornar essas ameaças pelas mais variadas frentes de atuação, desde pela dissuasão por seu sistema defensivo até por sua parceria com países *like-minded* e com o setor privado no compartilhamento de informações e tecnologias.

3.4.2. Sobre ciberguerra

Nos debates de cibersegurança também se discute como o ciberespaço pode, eventualmente, tornar-se palco de guerras cibernéticas entre Estados ou diferentes agentes do sistema internacional. Entretanto, como uma guerra cibernética nunca ocorreu de fato, a própria possibilidade de existência desse tipo de conflito é examinada pela academia. Nessa ótica, Rid (2012) indica que ciberguerras não se tornarão uma realidade, já que não contariam com as três características básicas de uma guerra, conforme definição de Carl von Clausewitz: ciberguerras não cumpririam com o requisito de ter um caráter violento com potencialidade letal; não teriam um caráter instrumental, como forçar inimigos a cumprirem com a vontade do atacante; e não teriam uma natureza claramente política.

Alguns exemplos são dados por Rid para elucidar como, até o momento, nenhuma ocorrência cibernética conseguiu englobar os três aspectos necessários para que uma ciberguerra estivesse em curso: os ataques contra a Estônia, em 2007; a operação Orchard, no mesmo ano, de Israel contra a Síria; os casos de DDoS ao longo da Guerra Russo-Georgiana, em 2008; e os ataques contra as usinas iranianas de enriquecimento de urânio, entre 2007 e 2010. Em todos esses casos, os artifícios cibernéticos não podem ser caracterizados como uma guerra *per se*, mas serviram como importantes complementos a interferências, inclusive por danos materiais, como nos casos da Síria e especialmente do Irã (NYE, 2010; RID, 2012).

Nesse sentido, apesar de o Japão caracterizar o ciberespaço como um "domínio artificial" na primeira CSS, o mesmo não ocorre nos documentos de 2018 e 2021. Isso inicialmente poria em dúvida se o NISC acredita que o ciberespaço é um local onde se pode realizar uma guerra, já que "domínio" é o termo formalmente utilizado no campo da segurança para se referir a espaços onde guerras podem ser travadas e, portanto, onde as forças armadas atuariam. Todavia, o Ministério da Defesa do Japão, através de seus LBDs, continua a definir o ciberespaço como um dos novos domínios internacionais, junto do espaço sideral e do espectro eletromagnético. Sendo assim, ao menos em um nível conceitual, a possibilidade de guerra cibernética não é nula ao governo nipônico; podemos observar nesse caso, entretanto,

como diferentes instâncias do governo japonês não estão totalmente articuladas, já que as definições do MOD e do NISC divergem em alguma medida nesse aspecto.

Por outro lado, três são os pontos dissonantes dessa possibilidade. Em primeiro lugar, o principal aparato cibernético atualmente compondo as Forças de Autodefesa do Japão é seu *Cyber Defense Command*. Apesar de esse comando de defesa ter passado por uma reestruturação, em março de 2022, responsável por unificar departamentos cibernéticos dispersos dentre as SDF, ainda não é considerado um braço independente das Forças de Autodefesa do Japão; países como a Alemanha, em contraponto, já consideram seu núcleo de defesa cibernética como um ramo de suas forças armadas. Todavia, há de se questionar se essa reestruturação não dá indícios da formação de um possível novo ramo às SDF nipônicas no futuro, especialmente tendo em vista que o CDC passou a contar com capacidades ofensivas após sua reestruturação. Até que isso não seja observado, contudo, o CDC não está configurado, aos moldes tradicionais, para atuar em uma possível guerra cibernética.

Em segundo lugar, o termo "ciberguerra" não é mencionado nas CSSs do Japão, o que nos diz que, de um ponto de vista estratégico, guerras cibernéticas não são até então uma preocupação declarada nesses documentos em específico. Nos LBDs do Japão mais recentes, no entanto, o MOD elabora sobre ciberguerras em dois contextos. O primeiro diz respeito à atuação da China no ciberespaço; conforme autoridades japonesas apontam, o governo chinês tem alegadamente desenvolvido capacidades para realização de uma guerra cibernética. Por conseguinte, o Japão menciona que desde 2019 tem enviado membros de suas Forças de Autodefesa ao *National War College*, nos Estados Unidos, para cursos voltados a comandantes de ciberguerra, para que assim aprendam sobre processos de tomada de decisão com autoridades americanas (MOD, 2022). Esse segundo aspecto pode nos dizer que, apesar de não estar oficialmente reconhecido em suas Estratégias de Cibersegurança, o tópico está no radar de preocupações do Ministério da Defesa japonês, já que o país envia seus comandantes para cursos voltados à ciberguerra e se preocupa que a China possa vir a iniciar uma guerra cibernética.

Por fim, o ministro da Defesa japonês, Nobuo Kishi, mencionou no último LBD do Japão, lançado em julho de 2022, que o país abordará de maneira criativa e ousada temas como guerra de informações e ciberguerra na *National Security Strategy* (NSS) japonesa que seria revisada ao final do ano fiscal de 2022 (MOD, 2022). Contudo, a nova NSS mencionada por Kishi, agora já lançada, não fala sobre ciberguerra em suas passagens. O único aspecto que continua a ser destacado no texto é o envolvimento do domínio cibernético em possíveis guerras híbridas, visto que meios militares e não-militares podem ser combinados para que se atinja

"objetivos militares, tais como guerra de informação, que utiliza a disseminação de desinformação anteriormente a um ataque armado" (MOFA, 2022b), e que esse tipo de conflito estará cada vez mais sofisticado no futuro.

A partir desses fatos, portanto, ainda que o Japão não considere guerras cibernéticas como parte de seu escopo estratégico mais duro – já que não são mencionadas nas CSSs e são repassadas brevemente nos LBDs –, o MOD aborda tal questão dentre suas pautas. Por conta disso, não se pode especificar com clareza como o governo japonês enxerga uma possível guerra cibernética, dado que esse tópico é até então tratado de maneira furtiva pelo governo em seus documentos oficiais. Em contrapartida, o MOD expõe com muito mais evidência como guerras híbridas são uma ameaça ao ambiente de segurança atual, especialmente para os países localizados em "zonas cinzas"[60]. Neste caso, o governo japonês aponta como ciberataques contra comunicações e outras infraestruturas críticas, operações que usam unidades militares sem especificação de nacionalidade, bem como disseminação de informações falsas na internet, fariam parte do escopo das guerras híbridas, cuja combinação dificultaria respostas por parte do Estado atacado (MOD, 2022). Dessa maneira, dado o posicionamento político japonês, guerras híbridas são uma preocupação governamental mais latente em detrimento de ciberguerras.

3.5. Conclusões do capítulo

Conclui-se, portanto, que apesar de preocupações com cibersegurança terem surgido na década de 1990, apenas nos anos 2010 essa vertente de segurança atingiu altos patamares estratégicos nas políticas japonesas. Indica-se também que o governo do Japão, por meio de seus documentos oficiais e de suas estratégias, está em constante evolução e mudança no campo cibernético.

Quanto às definições do governo japonês para o ciberespaço e a eventos correlatos, aponta-se como essas se diferenciam consideravelmente das proposições acadêmicas da área. Sobre o ciberespaço, o Japão foca em como este ambiente está em vias de se fundir com o mundo físico a ponto de não ser possível dissociar este do espaço cibernético, tendo em vista o entendimento de Sociedade 5.0, descrição destoante de certas narrativas que apontam o

[60] Conforme própria definição do MOD, zonas cinzas são aquelas regiões onde uma série de situações ocorrem, nem de paz, nem de guerra. Nas zonas cinzas, Estados usam da força para tentar modificar o *status quo* ou forçar rivais a aceitarem suas demandas ou afirmações (MOD, 2022). Nesse sentido, Neil Owens afirma que o Leste Asiático é uma zona cinza, e que os Estados da região precisam "adotar níveis cuidadosamente calibrados de força para avançar seus interesses lentamente, enquanto são cuidadosos para permanecer abaixo do limite que engatilharia uma resposta militar" (2018, p. 109, tradução minha).

ciberespaço como um quinto domínio independente de atuação internacional. Ainda, a retórica de que o ciberespaço é um ambiente corporativo e de suma importância à realidade econômica do Japão agrega um viés adicional ao ambiente cibernético como sendo basilar à evolução tanto da sociedade quanto da economia globais.

Em suas definições de segurança e defesa cibernéticas, por outro lado, o conceito amplo de ciberdefesa é o que se sobressai por ampliar o escopo de atuação governamental para além do ente público-estatal. Dessa maneira, por defesa cibernética o governo japonês também advoga favoravelmente a uma integração com o setor privado para expandir a troca de informações e os mecanismos de resposta a ciberataques, especialmente no ambiente empresarial, evidenciados pela ciberdefesa ativa e pela defesa cibernética compreensiva.

Por fim, no que diz respeito a ciberguerras, o governo japonês não apresenta em seus documentos oficiais um posicionamento claro quanto à possibilidade de realização desse tipo de conflito. É evidente, entretanto, que o governo japonês, em especial o Ministério da Defesa do país, preocupa-se com guerras híbridas e com o uso de ciberataques nesse cenário. Sendo assim, ciberataques seriam utilizados conjuntamente a meios cinéticos para o atingimento de objetivos militares. Isso posto, o governo nipônico tem preocupações mais reais relacionadas a ciberataques e cibercrimes que a uma eventual guerra cibernética. Nesse ponto, infrações como fraude, destruição de computadores, invasões não autorizadas a sistemas, negação de serviços e espionagem estariam no *hall* das ameaças latentes contra o país.

Creio que também seja importante destacar como a segurança cibernética não foi um tópico que evoluiu apenas em si, com seus próprios documentos e suas próprias instituições. Como vem sendo mencionado, o tema cibernético faz parte, inclusive com destaque, de inúmeros outros documentos que não focam necessariamente na segurança cibernética, como a Estratégia de Segurança Nacional do Japão e os Livros Brancos de Defesa do país. Esses textos, apesar de obviamente conectados à cibersegurança, tratam de todo o universo de segurança e defesa do Japão em caráter internacional, e neles o aspecto ciber tem sido amplamente reconhecido nos últimos anos. Meu intuito é dizer que a cibersegurança é um tópico atualmente abordado nos mais variados níveis políticos no Japão, desde o gabinete do Primeiro-ministro e individualmente nos Ministérios até a Polícia Nacional do Japão, a sociedade civil e o mundo corporativo, com temas como a *Internet of Things* e como isso afeta o cotidiano da sociedade.

Como um resumo desse contexto, alguns dos principais pontos trabalhados nas *Cybersecurity Strategies* do Japão definem os rumos que o país está tomando quanto ao tema nos últimos anos. Como aponta Matsubara (2021), desde a CSS de 2015 o governo japonês vem delineando o fortalecimento das parcerias público-privadas para o robustecimento da

cibersegurança do país, assim como coloca em caráter de urgência que grandes empresas adotem estratégias de cibersegurança em suas políticas internas. Na Estratégia de 2015, portanto, parte da responsabilidade de melhoria dos níveis de cibersegurança nacional foi depositada pelo governo nas mãos dos grandes executivos de empresas japonesas, sendo esse o primeiro documento estratégico do país a incluir o gerenciamento de empresas como um dos focos de segurança da nação. Isso se deu, pois, conforme apontam dados de uma pesquisa efetuada pela KPMG, apenas 13% das diretorias de empresas do Japão acreditava que a cibersegurança deveria ser discutida nesse grau hierárquico, em comparação à média global de 56% (MATSUBARA, 2021). Desse modo, o governo japonês estava pondo em pauta como o setor privado deve ser tão proativo quanto o governo no tratamento da questão cibernética, caso contrário o país não atingirá níveis adequados de cibersegurança.

Por conseguinte, a CSS de 2018 adicionou ao tópico o conceito de Sociedade 5.0, o qual lança luz à ideia de que não será mais possível separar o mundo físico do mundo digital num futuro próximo, sendo que na década de 2020 começaremos a observar mais marcadamente essa característica da sociedade. Isso acrescenta ao debate o entendimento de que a segurança cibernética deve ser tratada pelo governo como um ponto fundamental da segurança do país, uma vez que o mundo cibernético será parte integrante da vida em sociedade, das relações comerciais internacionais entre os países e as populações do globo. O traço marcante da CSS de 2021, por fim, é o rompimento com o comportamento histórico do Japão de não nomear perpetradores de ciberataques. No texto, o governo japonês identifica a China, a Coreia do Norte e a Rússia como as principais ameaças contra o Japão no ciberespaço, primeira vez que isso ocorre em um documento exclusivamente voltado à cibernética. Entretanto, o Japão continua relutante em adotar possíveis retaliações ou sanções a esses Estados, restringindo-se apenas à sua defesa passiva e a identificar essas ameaças e descrever que tais nações vêm desenvolvendo capacidades cibernéticas, inclusive em suas esferas militares, a serem usadas de maneiras maliciosas para roubo de informações sigilosas e expansão de influência.

4. A PERCEPÇÃO JAPONESA DE CIBERDEFESA

A essa altura já se faz claro alguns dos entendimentos basilares de ciberdefesa para o Japão no cenário atual. Em primeiro lugar, a cibersegurança vem ocupando um papel central nos debates de segurança internacional do Japão, especialmente desde os anos 2010. Além disso, o ciberespaço está se fundindo ao mundo físico, e em alguns anos já não será possível dissociar um do outro, sendo a década de 2020 o provável ponto de virada desse cenário; dentro dessa estrutura, existem três agentes que representam ameaças latentes contra o Japão, os quais efetuam ciberataques sofisticados com sua tecnologia. Por fim, como resposta, o governo japonês vem adotando uma postura mais proativa quanto à sua cibersegurança, como através da cooperação com o setor público e com países *like-minded* para que se garanta um ciberespaço livre, justo e aberto, bem como através da reforma de seu "exército" cibernético com a aquisição de novas capacidades, por exemplo. Por ser um dos domínios mais recentes do sistema internacional, dessa forma, a defesa cibernética dos Estados talvez seja a com maior potencialidade de exploração, incluindo a do Japão, uma vez que esta cena securitária está sob contínua construção.

Apesar de o governo japonês ser bastante aberto quanto a suas políticas e seus posicionamentos estratégicos, há algumas coisas que não são amplamente divulgadas pelo governo japonês, especialmente quanto aos seus aparatos de ciberdefesa. Diferentemente de alguns países como a Alemanha, que dispõe no site de suas forças armadas o número real de militares na ativa, o que inclui informações de suas forças de defesa cibernéticas[61], o governo japonês não apresenta números concretos sobre o pessoal empregado no CDC ou nas unidades de cibervigilância do país. Quanto a isso, a quantia de pessoas que atua na defesa cibernética do Japão é normalmente conhecida através de informações compartilhadas na mídia pelo Ministro da Defesa e pessoas relacionadas, por exemplo, em estimativas. Dessa forma, presume-se que ao momento de sua criação o CDC contava com 90 pessoas (BARLETT, 2020), sendo que atualmente o Japão conta com cerca de 890 trabalhadores, desses 540 como parte do CDC e outros 350 complementando as unidades de cibervigilância das SDF. Em adição, foi sinalizado em 2022 pelo MOD que existe a pretensão de elevar esse número para cerca de 4.000 a 5.000 pessoas no ano fiscal de 2027, muito através de uma formação preparatória que está sendo implementada nas escolas das SDF em locais como Kanagawa (KYŌDŌ TSŪSHINSHA, 2022).

[61] O governo alemão indica que seu braço armado cibernético conta com 1.260 "soldados" *in loco*, ou cerca de 14.200 se considerarmos o pessoal civil empregado por Berlim (BUNDESWEHR, s.d.).

Em comparação aos Estados vizinhos, o LDB de 2022 indica como a China conta com cerca de 175.000 "soldados cibernéticos", sendo 30.000 desses especializados em ciberataques; quanto aos norte-coreanos, o governo japonês presume que haja cerca de 6.800 pessoas no Exército Popular da Coreia em suas unidades cibernéticas; a Rússia, por outro lado, contaria com cerca de 1.000 indivíduos em sua unidade cibernética de comando (MOD, 2022). Dessa forma, dentre os quatro países, o Japão é aquele que presumidamente conta com o menor número de empregados no ramo da defesa cibernética do país, e o aumento desse número é um objetivo urgente do governo nipônico, como apresentado em suas políticas.

A despeito da imprecisão nesse número de pessoal, como vem sendo apontado, o governo japonês estabelece com clareza suas políticas de segurança cibernética em seus documentos oficiais. Entrando em minha resposta de como o Japão enxerga o ciberespaço a partir de sua estrutura de defesa, abordarei o tema a partir de três vieses verificáveis de atuação do governo, aqui identificados como os três fundamentos da ciberdefesa japonesa: (1) a constante proatividade do Japão no tema e como o país tenta elevar seu status securitário sem desrespeitar seus limites constitucionais; (2) a gradual aproximação das esferas pública e privada para tratar da defesa cibernética da nação; e (3) a tentativa persistente do governo japonês em se alinhar a Estados com mentalidades afins para fortalecer a cibersegurança internacional e como consequência sua defesa cibernética. Nesse cenário, os preceitos de *Whole of Government* (WoG), *Whole of Nation* (WoN) e *Whole of System* (WoS)[62], trazidos por Alexander Klimburg e Jason Healey (2012), são observáveis na conjuntura cibersecuritária e ciberdefensiva do Japão.

Os autores delimitam esses preceitos tendo como base as três partes sempre interessadas em como as políticas são entregues à sociedade: a parte governamental, a parte social e a parte internacional. O WoG, nesse caso, foi concebido como forma de reunir recursos entre departamentos governamentais para aumentar sua eficiência, sincronizando suas redes e políticas para partirem do mesmo lugar-comum de análise dos fatos. No caso da cibersegurança, Klimburg e Healey (2012) indicam que é normal que em países iniciantes no tema cibernético cada ministério ou organismo governamental cuide de suas próprias redes e políticas cibernéticas, por exemplo. Entretanto, em nações mais ciberneticamente avançadas essa fragmentação e falta de coordenação política intragovernamental[63] é desproposital, ocasionando uma maior coesão política entre diferentes órgãos envolvidos. A palavra "coordenação" é

[62] Livremente traduzidos como Integridade de Governo, Integridade de Nação e Integridade de Sistema.
[63] Que pode envolver diferentes níveis governamentais como central, provincial e local.

escolhida pelos autores para definir este nível.

Já o WoN visa aprofundar a cooperação estatal e não estatal, o que inclui desde serviços públicos e universidades até empresas de tecnologia, normalmente usado como termo guarda-chuva para todas as atividades não estatais relevantes à segurança nacional. Dessa forma, a proteção de infraestruturas críticas costuma ser a demonstração mais clara de *Whole of Nation,* visto que é de interesse governamental protegê-las mesmo sendo posse do setor privado. No caso da defesa cibernética de um país, a cooperação público-privada também pode ocorrer por compartilhamento de tecnologia ou mesmo *know-how*, visto que é desse setor que sai a maioria dos *softwares*, *hardwares* e serviços explorados ciberneticamente, além de ser a porção da sociedade que controla a maioria da infraestrutura de rede, programando-a e executando-a, e que continuamente pesquisa e especula sobre esse espaço (KLIMBURG e HEALEY, 2012). Neste caso, "cooperação" seria o termo definidor do WoN.

Por fim, o WoS representa uma forma de engajamento entre atores *like-minded* na esfera internacional, sejam eles estatais ou não estatais. "Este campo em rápida evolução lida com questões como normas de comportamento do Estado no ciberespaço e discute medidas de construção de confiança entre os Estados"[64] (KLIMBURG e HEALEY, 2012, p. 100, tradução minha). Posto isso, diplomatas, grupos de trabalho técnico, científico e industrial, para além das partes interessadas na governança da internet, compõem o quadro de agentes que formam a estrutura internacional de cibersegurança. A palavra "colaboração" descreve essa categoria, segundo os autores. Esses três níveis de engajamento serão apresentados na sequência para elucidar como o Japão entende o ciberespaço a partir de sua estrutura de defesa, sendo que cada um desses níveis de integridade comporta um dos fundamentos da defesa cibernética japonesa.

4.1. Proatividade política e limitações legais para a autodefesa

Inicialmente, faz-se necessário entender que o Japão adota uma política de defesa baseada no princípio exclusivo da autodefesa, dado que o país foi desmilitarizado após a Segunda Guerra Mundial e, por impedimentos constitucionais (vide Artigo 9 da Constituição do Japão), não pode adotar qualquer tipo de conduta militarmente ofensiva no cenário internacional. Esse aspecto de sua defesa também se aplica ao ciberespaço, e o limite de atuação do Japão neste domínio vem sendo debatido com assiduidade pelas autoridades políticas japonesas nacionalmente. Nesse caso, para além do Artigo 9 de sua Constituição, Katagiri

[64] "This rapidly evolving field deals with issues such as norms of state behaviour in cyberspace, and discussing confidence building measures between states".

(2021) complementa que a preocupação do governo quanto à sua defesa cibernética deve se expandir ao seu vigésimo primeiro Artigo do documento. O Artigo 21 da Constituição do Japão estabelece que "nenhuma censura será mantida, nem o sigilo de qualquer meio de comunicação violado", o que, segundo o autor, poderia tornar ilegal operações de reconhecimento e de SIGINT[65] efetuadas pelas estruturas de defesa nipônicas. Dessa maneira, Katagiri define que o Artigo 21 pode ser considerado mais emblemático para a cibersegurança japonesa que o próprio Artigo 9 da Constituição, visto que o teor deste Artigo e o rigor da lei japonesa dificultam o monitoramento das comunicações do país tanto por empresas de telecomunicações quanto pelo próprio governo. A meu ver, entretanto, o Artigo 21 da Constituição do Japão não se equivale à barreira imposta pelo Artigo 9, uma vez que missões cibernéticas não necessariamente envolvem censura ou quebra de sigilo de meios de comunicação, uma vez que ataques como o Stuxnet, por exemplo, servem para provocar danos físicos a infraestruturas por intermédio do ciberespaço. Esse tipo de ataque, que é um dos mais sofisticados já criados, é impedido pelo Artigo 9, mas não infringe os pressupostos do Artigo 21 *per se*.

Ademais, a partir da autodefesa como política oficial e da renúncia ao direito da guerra por conta de sua Constituição, o aparato legislativo japonês foi sendo igualmente estabelecido em complementaridade a essas políticas. Assim, hoje se observa no país um sistema judiciário que criminaliza e condena práticas ofensivas tanto por parte do governo quanto da esfera privada da sociedade, impondo constrangimentos sobre essas partes também no domínio cibernético. Segundo Katagiri (2021), para além de leis esparsas como a *Personal Information Protection Law* de 2003[66], o próprio código penal japonês prevê que certos atos normalmente efetuados como contramedida ofensiva podem ser considerados crimes, como a produção de vírus cibernéticos (Art. 168), o dano ao crédito de empresas privadas ou sua obstrução pela disseminação de rumores falsos na internet (Art. 233), ou mesmo interferências em computadores operacionais de negócios comerciais (Art. 234). Como o Japão provavelmente utilizaria ataques relacionados em um cenário de ciberataque, suas ações poderiam ser consideradas ilegais e, portanto, passíveis de punição (KATAGIRI, 2021).

Dada tal conjuntura doméstica, há uma variedade de pressupostos que delimitam o escopo de atuação das forças ciberdefensivas do Japão, abordando o que essas forças devem

[65] SIGINT, sigla para "*signal intelligence*", refere-se à coleta de informações ou inteligência por intermédio de sinais interceptados de comunicação entre pessoas ou entre máquinas.

[66] Estabelece que toda firma de telecomunicações deve claramente descrever e tornar públicos os propósitos de uso de dados pessoais, ao mesmo tempo que proíbe a coleta, o uso fraudulento e a transferência de dados a terceiros sem consentimento. Operações ciberdefensivas que planejam utilizar empresas de comunicação para coleta de inteligência, por exemplo, seriam criminalizadas sob o escopo dessa lei, enredando a atuação governamental (KATAGIRI, 2021).

proteger e como devem proteger. Nesse caso, Katagiri (2021) elabora a atuação das forças de defesa cibernética do Japão tendo como base os pressupostos de defesa ativa e defesa passiva. A defesa cibernética ativa consiste basicamente na capacidade de contra-atacar inimigos, causando algum tipo de dano direto ou destruição como forma de retaliação, para além de anular ou reduzir a efetividade de empreitadas cibernéticas de rivais. Por conseguinte, a defesa cibernética passiva se restringe a deter ações hostis por meios estáticos, como o fortalecimento de redes e de controles preventivos, instalação de *firewalls*, atualizações de *software*, monitoramento constante, bloqueio e redirecionamento de intrusões, assim como a utilização de *hackers* "éticos" para encontrar vulnerabilidades de dia zero, etc, impossibilitando que agressores atinjam seus objetivos. O próprio Manual de Tallin aborda os conceitos de defesa cibernética passiva e ativa, onde se aponta que uma defesa ativa, também chamada de ofensiva, é aceita por inúmeros atores como legítima, uma vez que uma defesa passiva é muito cara para ser mantida e requer muitos recursos humanos e financeiros para adaptação de todo o sistema. Dessa forma, a defesa ativa pode ser usada especificamente para deter potenciais ataques iminentes e específicos, sendo um método mais barato em contraposição à defesa passiva, que precisa estar ininterruptamente em operação (KLIMBURG e HEALEY, 2012)[67].

Katarigi (2021) argumenta que mesmo a defesa passiva sendo mais cara, esse é o tipo de defesa cibernética adotada pelo Japão, a qual foca no robustecimento de suas redes e na minimização de danos como forma de se proteger no ciberespaço. O autor menciona também que a ciberdefesa passiva do Japão é mais eficaz em conter a disseminação de *malwares* uma vez atingido pela ameaça, por exemplo, do que prevenir esse tipo de ataque, dado que esse posicionamento defensivo objetiva impedir um aumento no número de brechas em seus sistemas, sem dissuadir novos ataques *per se*. Contudo, para além de respeitar os limites constitucionais do país, a defesa passiva do Japão é a estratégia política mais viável para a situação política interna que o Japão está inserido; esse tipo de defesa não só gera apoio popular doméstico, dado que a população japonesa é incerta quanto a uma remilitarização do país, pendendo mais a uma continuidade de seu *status quo* securitário, ao passo que esse comportamento promove princípios do direito internacional e as regras de engajamento no ciberespaço que o Japão tanto tenta disseminar internacionalmente. Da mesma forma, o autor

[67] Em conformidade a esse entendimento, Lewis (2015) argumenta que o Japão teoricamente tem a liberdade de adotar uma postura ofensiva no ciberespaço, visto que muitos comportamentos de alguma forma ofensivos podem ser enquadrados em um propósito de defesa. Todavia, o problema neste caso reside na legitimidade e na autorização legal para que isso aconteça, o que poderia vir inclusive sob forma de uma reinterpretação constitucional, saída comumente utilizada pelo Japão para contornar seus limites de atuação internacional quando o assunto é segurança e defesa.

aponta que a defesa cibernética passiva do Japão funciona bem com o bilateralismo americano, visto que a autodefesa coletiva pode ser autorizada em casos cibernéticos, haja vista os resultados do encontro 2+2 entre EUA e Japão em 2019, por exemplo.

Keiji Takeda (2019), por outro lado, indica que há quatro categorias atualmente propostas para a atuação de forças de defesa cibernéticas. A primeira se refere à preservação da cibersegurança de organizações militares, o tipo mais comum de atuação em ciberdefesa. Essa categoria considera organizações militares os atores mais seguros do sistema e que, portanto, trabalham para produzir expertise e manter sua própria segurança interna. Sob este escopo estariam incluídas atividades como preservação de confidencialidade, integridade e disponibilidade de informações. A segunda categoria se destina à preservação da cibersegurança de infraestruturas críticas de um país, sendo esse um dos maiores objetivos dos Estados no presente. O terceiro tipo de atuação de forças ciberdefensivas se refere a operações cibernéticas em suporte a forças militares convencionais, em especial para a exploração de fraquezas de novas tecnologias usadas em guerra. Esse tipo de apoio se dá ciberneticamente pela invasão de sistemas, implantação de desinformação e destruição de conexões e funcionalidades, por exemplo, como forma de apoiar aqueles ataques e aquelas armas tradicionais de guerra. A quarta e última categoria proposta pelo autor concerne às operações cibernéticas totalmente desvinculadas das forças militares convencionais. Esse aspecto é o mais recente dentro de instituições de defesa, onde operações virtuais ocorrem em completa desconexão do plano militar tradicional e envolvem comportamentos mais ofensivos e mesmo destrutivos, como a neutralização de operações inimigas e táticas como o Stuxnet, que causam danos físicos por intermédio do ciberespaço.

Segundo Takeda (2019), as forças de defesa cibernética do Japão, dentro de suas limitações, operam nas primeiras três categorias de ciberdefesa apresentadas, sendo a primeira categoria a mais comumente conduzida pelas SDF. A quarta dimensão é a que está constantemente sob debate de um ponto de vista legal, uma vez que a Constituição do país proíbe o Japão de agir de forma militarmente ofensiva conforme Artigo 9 do documento, ao passo que há diferentes interpretações sobre que tipo de postura de fato ultrapassa a linha vermelha da Constituição, especialmente no ciberespaço; nesse caso, mesmo a terceira categoria contendo traços de comportamentos ofensivos, Takeda aponta que não ferem a Constituição do Japão por serem previstos em cenários de guerra e sob o escopo de operações de defesa.

Independentemente das categorias utilizadas para analisar a postura ciberdefensiva do Japão, autores como James Lewis (2015) e Benjamin Barlett (2020) concordam que seus atuais

aparatos ciberdefensivos de fato respeitam os limites constitucionais do país, na medida que se restringem ao propósito único de autodefesa; mesmo as capacidades ofensivas adquiridas pelo Japão com a reforma do CDC, em 2022, serão utilizadas exclusivamente para se defender de ataques cibernéticos. Sendo assim, qualquer medida de defesa ativa precisa ser expressamente autorizada, caso contrário está apta a ser interpretada como infração e submetida a julgamento, seja o ato executado por estruturas governamentais de defesa, seja pelo setor privado (KATAGIRI, 2021). Katagiri (2021) finaliza dizendo que, apesar de o sistema legislativo japonês ser eficaz para impedir um mal uso doméstico do ciberespaço, tem poucos efeitos sobre infratores estrangeiros, o que acaba minando a capacidade doméstica de atuação do Japão no ciberespaço, dado que o país é obrigado a se ater apenas a uma postura de defesa passiva, sem interromper a capacidade estrangeira de atacar o arquipélago ciberneticamente. Quanto a esse aspecto tendo a discordar do autor, uma vez que as Olimpíadas de Tóquio se converteram em um *case* de sucesso na história da defesa cibernética do Japão, onde os Jogos foram completamente protegidos por suas estratégias de defesa passiva e nenhum ataque significativo foi identificado. Como mencionado, neste momento esperava-se que a Rússia conduzisse ataques danosos contra o Japão em retaliação às sanções recebidas pelo Comitê Olímpico, o que não foi observado.

Nesse contexto, quanto às suas estruturas governamentais especificamente, a proatividade política japonesa entra em cena para tirar proveito da situação legal e constitucional sob a qual o país está submetido, encontrando as melhores alternativas para que o Japão consiga se proteger no ciberespaço, ao mesmo tempo que tenta flexibilizar, dentro do possível, esses mesmos limites legais e constitucionais. Como abordado anteriormente, até 2011 a cibersegurança japonesa era tratada de maneira fragmentada por Ministérios conectados ao assunto e por outras agências governamentais, como a NPA. Klimburg e Healey (2012) indicam que é normal que países iniciantes em suas políticas de cibersegurança deixem o assunto sob responsabilidade de cada Ministério ou departamento relacionado, mas que nações ciberneticamente avançadas entendem que essa fragmentação é desproposital no longo prazo. Nesse sentido, o Japão se torna uma nação ciberneticamente avançada, como poriam os autores, apenas após 2011, ano considerado um divisor de águas ao país quanto ao tema cibernético, quando o viés WoG da ciberdefesa japonesa começa então a aflorar. Naquele momento, começou a ser criada uma doutrina em segurança cibernética no Japão que resultou na centralização da proteção de infraestruturas críticas nas mãos do IPSC e, posteriormente, na formação de um comando cibernético que unisse os três ramos das SDF japonesas, o CDC, até então também fragmentados.

Para além da centralização de suas políticas e da criação do CDC como resposta direta aos eventos de 2011, todas as institucionalizações recentes da segurança japonesa, como a formação do NSC e o lançamento da NSS em 2013, a divulgação do BAC em 2014 junto da reinterpretação constitucional que autorizou as SDF a participar de missões de autodefesa coletiva no exterior, ou mesmo a confecção da primeira CSS do Japão em 2015, seguida de versões atualizadas em 2018 e 2021, ilustram a proatividade japonesa no tema e exemplificam seu plano de integridade governamental para tratar da segurança e defesa cibernéticas nacionais.

Mais recentemente, em outubro de 2021, após a eleição de Kishida e a continuidade do Partido Liberal Democrata (LDP) no poder, o partido começou a inserir nas pautas políticas do país sua vontade de aumentar os gastos no setor militar de 1% para 2% do PIB japonês, tópico mencionado também no mais recente Livro Branco de Defesa do MOD, lançado em julho de 2022. Barlett (2020) aponta que essa restrição dos investimentos em defesa a 1% do PIB é outro motivo pelo qual o Japão investe em uma defesa passiva, uma vez que o baixo orçamento faz com que o governo japonês tenha que tomar decisões difíceis sobre que capacidades investir no ciberespaço[68]. Assim, como forma de se manter dentro das linhas constitucionais e em respeito à sua política de autodefesa, o país opta por investir em capacidades defensivas em detrimento de ofensivas, muito por ser o que o orçamento permite. Uma eventual expansão desse investimento em defesa a 2% do PIB japonês, portanto, daria maior liberdade ao país para fortalecer seu aparato de defesa cibernético, podendo impulsionar suas capacidades ofensivas no ciberespaço como ocorreu recentemente, a partir da reformulação do CDC em março de 2022. A reestruturação do CDC, inclusive, é um bom exemplo de como o Japão respeita sua Constituição e seu princípio de autodefesa, uma vez que essa unidade de defesa alegadamente passou a contar com capacidades ofensivas, mas que são usadas apenas para defesa.

Não obstante, os limites constitucionais que interferem na atuação securitária do Japão são constantemente trazidos à mesa pelo LDP e seus apoiadores. Em sua proposta para segurança da informação confeccionada em fevereiro de 2012, por exemplo, o partido aponta que as Forças de Autodefesa japonesas deveriam se tornar forças de defesa dinâmicas que pudessem contornar ameaças de segurança proativamente e para além do território imediato do Japão (KALLENDER e HUGHES 2016). Nesse caso, fica ambíguo se o partido se refere a uma participação em arranjos de defesa coletiva, por exemplo, ou se o LDP se refere a uma possível

[68] A cibersegurança está tomando seu espaço dentro do orçamento de defesa do Japão, mas ainda de maneira tímida. Se compararmos os anos de 2018 e 2019, o saldo investido pelo Japão em defesa cibernética saltou de JPY 11 bilhões para JPY 25,6 bilhões, mas essa cifra continua representando menos de 0,5% de todo o orçamento de defesa do Japão, que se restringe a esse 1% do PIB (KOSHINO e GADY, 2020).

mudança na atuação sumariamente defensiva do Japão conforme prevê sua Constituição; é certo, no entanto, que essa interpretação do partido estica a possibilidade de atuação ofensiva do Japão como algo dentro da lei, seja no ciberespaço, seja no mundo físico, e isso expõe o viés de mudança adotado pelo partido. Da mesma forma, em abril de 2022, após a eleição da câmara alta, observou-se na Dieta um aumento nas cadeiras ocupadas por partidos de direita – tradicionalmente defensores de uma reforma constitucional – o que resultou em 62% de parlamentares favoráveis a uma revisão, porcentagem atingida pela primeira vez na história do Japão e se aproximando dos 2/3 exigidos para se iniciar debates de revisão da Constituição. Um dia após as eleições da câmara alta, em 11 de julho de 2022, Kishida reforçou em discurso sua vontade de alterar a Constituição do Japão para modificar o Artigo 9 do documento, em conformidade ao que vinha sendo trazido por Abe, um dos grandes símbolos do LDP.

Apesar de Abe não ter logrado êxito em seu plano de reformar a Constituição pacifista até 2020[69], o que poderia ter revisto a capacidade de o Japão portar forças de ataque tradicionais se o plano de reformular o Artigo 9 fosse completado, o ex-premiê deu passos importantes para a remilitarização formal do Japão. A atuação política de Abe, em um primeiro momento, abriu espaço para uma militarização política do país a partir da criação de instituições e de documentos oficiais regendo a segurança e a defesa do país, tanto em termos tradicionais quanto em termos cibernéticos, como mencionado. Em segundo lugar, Abe se tornou a figura política a partir da qual outros parlamentares, como o atual Primeiro-ministro Fumio Kishida, baseiam seus objetivos políticos para seus mandatos. Nesse sentido, Abe por si só é uma representação do viés WoG da política japonesa, uma vez que o ex-premiê foi responsável por unir uma legião de parlamentares em sua espécie de doutrina de "pacifismo proativo", como era chamada a proatividade militar de Abe, ao passo que sua atuação como chefe de governo gerou uma série de reestruturações institucionais alinhadas a um princípio de integridade governamental, tendo como exemplo na esfera de cibersegurança o remodelação do ISPC (agora CSSH) e do NISC na década de 2010.

[69] Katagiri (2021) indica que há ao menos três grandes problemas enfrentados pelo Japão em um cenário de reforma constitucional. Inicialmente, para que uma lei autorize o uso de ciberdefesa ativa, o tipo de cenário sob o qual usá-la teria de ser estritamente detalhado, o que é difícil de estabelecer tendo em vista a constante flexibilidade do ciberespaço. Em segundo lugar, revisar a constituição japonesa seria um pesadelo burocrático, segundo o autor, visto que teria de haver uma grandiosa sincronia entre diferentes agências governamentais como a NPA, o METI e o *Ministry of Internal Affairs and Communication* (MIC), já que diferentes leis estão sob o controle de distintos corpos políticos. Por fim, apesar de se notar um aumento no número de debates para reforma constitucional, bem como um certo apoio em ascensão por parte da elite política japonesa, ainda falta apetite sociopolítico para modificar o *status quo* constitucional em direção a uma política de defesa nacional ofensiva. O fracasso de Abe em sua meta de governo é um exemplo real disso, e mesmo que o ex-premiê tivesse logrado êxito em aprovar sua proposta no parlamento, o pleito teria de passar sob escrutínio popular e, neste caso, a população japonesa tende a ser ainda menos interessada nesse tipo de reforma que a classe política dominante.

Katagiri (2021) aponta o NDPG de 2018 como um segundo exemplo de possível reforma, neste caso legislativa, que expandiria o escopo de atuação passiva das SDF japonesas. Nesse documento, o MOD demonstra que o país está caminhando em direção a operações militares multi-domínio, as quais garantiriam o uso de meios cinéticos, espaciais e ciberespaciais em resposta a ataques. Dessa forma, o Ministério da Defesa do Japão aventa a possibilidade de expandir a utilização de respostas cibernéticas em face a ataques estrangeiros. Contudo, presume-se que esse tipo de resposta seja adotada para contornar ataques inicialmente cinéticos em vez de cibernéticos e, por se tratar de autodefesa, o Japão precisaria absorver o primeiro ataque antes de acionar sua autodefesa. Dessa forma, sua própria capacidade de resposta cibernética estaria em risco pela obrigatoriedade de absorção do primeiro ataque, haja vista a possibilidade de DDoS, por exemplo. Para que isso ocorra, entretanto, a lei das SDF precisaria ser novamente revisada para estabelecer um comando de operações conjuntas, dado que esse tipo de resposta só pode ser utilizada em missões específicas e não de maneira permanente.

Quanto a esses possíveis meios cinéticos, entretanto, a atual legislação voltada à autodefesa do Japão prevê que esse direito pode ser acionado quando três condições são cumpridas: (1) quando há um ato de agressão ilegítimo e iminente contra o Japão; (2) quando não há nenhuma outra maneira de lidar com tal agressão a não ser recorrendo ao direito da autodefesa; e (3) quando o uso da força for limitado ao nível mínimo necessário. Nesse caso, assim como está apontado no documento de 2012 intitulado *Toward Stable and Effective Use of Cyberspace*, há um impasse logo na primeira condição exigida pela legislação das SDF, uma vez que é difícil determinar a relação direta entre um ataque cibernético e um ato de agressão (MOD, 2012). Por conta disso, o documento estabelece que cada ataque cibernético será avaliado individualmente para que se verifique o cumprimento desses requisitos à autodefesa.

Como resumo de sua situação constitucional envolvendo o ciberespaço, a tendência que se tem é que o país continue a respeitar seus limites constitucionais, visto que seria imprudente deixar de investir em sua defesa cibernética por conta do Artigo 9, por exemplo, adaptando-se à realidade legal sob a qual o país está submetido. Isso é dizer que o Japão tira proveito de sua situação para focar naquilo que está constitucionalmente permitido à estrutura governamental, atuando de dentro para fora em sua proteção cibernética por uma postura de defesa passiva. Mesmo esse tipo de defesa cibernética sendo o mais custoso de maneira geral, é o que pode ser feito para que Tóquio não fique à mercê de suas ameaças cibernéticas. Entretanto, como legado de Shinzō Abe, o atual governo japonês não descarta a hipótese de reforma de sua Constituição, o que poderia alterar partes dessa postura sumariamente defensiva do país no ciberespaço e

expandir seu leque de armas cibernéticas para contornar ameaças específicas de seus rivais tradicionais na região.

4.2. A público-privatização da ciberdefesa do Japão

Apesar de muitas empresas privadas fabricarem aparatos militares utilizados em países mundo afora, como a própria Mitsubishi Heavy Industries no Japão, o monopólio do uso da força e de posse de material militar se restringe majoritariamente ao Estado; para além desse cenário, portanto, a participação da esfera privada em um cenário militar tradicional é baixa. A atuação do setor privado no domínio cibernético, por outro lado, é muito mais definitiva que sua participação nos domínios tradicionais de poder, uma vez que o ciberespaço não só é possuído em sua maior parte pelo setor privado, tanto em termos de *hardware* quanto de *software*, mas também pelo fato de a sociedade global participar ativamente desse novo domínio de disseminação de poder[70]. Quando analisamos a própria concepção da ideia de cibersegurança no contexto japonês, precisamente na década de 1990, como comentado no início do capítulo anterior, notamos que as ONGs CSIRT foram os primeiros núcleos de uma espécie de ciberdefesa no Japão, mesmo que de maneira muito embrionária. Dessa forma, tendo em vista que as primeiras unidades governamentais a tratar da cibersegurança nacional foram criados uma década depois da formação dos CSIRTs japoneses, nota-se que a participação da esfera privada foi fundamental nas tratativas de cibersegurança do Japão, observáveis mesmo antes do início da atuação governamental no tema.

Nesse sentido, a cooperação público-privada está no cerne da cibersegurança japonesa, e inicialmente podemos pensar em duas possíveis vertentes de atuação dessa cooperação. A primeira, voltada à proteção empresarial de maneira geral, procura estabelecer laços entre o governo e a esfera privada tanto para fins de transferência tecnológica entre setores quanto para disseminar conscientização quanto ao tema cibernético e a necessidade de se proteger no ciberespaço. A segunda, por outro lado, estipula uma maior cooperação especificamente com empresas consideradas infraestrutura crítica, como aquelas provedoras de energia, água e transporte, visto que são estratégicas à sobrevivência da nação como tal e, como consequência, são fundamentais para a segurança nacional e precisam ser protegidas também pelo governo. Independentemente do caso, o Japão se encontra mergulhado em uma estratégia de integridade

[70] Para se ter uma ideia, cerca de 90% de todos os ativos tecnológicos envolvendo comunicação e informação pertencem à indústria privada, sendo a maioria restante dispositivos domésticos ou de consumidores (YOKOHAMA, 2019).

nacional, ou *Whole of Nation*, na medida que busca convergir políticas e comportamentos público-privados, estatais e não estatais, no ciberespaço.

Conforme aponta Shin'ichi Yokohama (2019), o padrão de comportamento do setor privado japonês quanto a políticas de cibersegurança se resume a aguardar instruções de órgãos governamentais regulatórios. Esse padrão diverge bastante de contextos como o dos Estados Unidos, onde o setor privado proativamente se engaja com o governo através de seus próprios times políticos ou de associações de comércio, por exemplo, como forma de se tornar parte integrante do processo tomador de decisões e formulador de políticas, trazendo consigo conhecimento operacional e técnico a ser compartilhado com o governo. No caso do Japão, é raro que companhias privadas tenham suas próprias equipes para debate com a cena política, e como a formulação de políticas acaba se concentrando exclusivamente na mão do governo, o *know-how* técnico e operacional do setor privado fica em falta. Assim, mesmo que o objetivo do governo seja produzir políticas para a sociedade e para a economia na totalidade, a ausência do setor privado no debate solapa essas políticas em contraste ao que acontece em países como os Estados Unidos.

Dessa maneira, parte significativa das novas remessas de políticas governamentais voltadas ao setor privado se traduz no incentivo à participação ativa de empresas privadas na formulação, implementação e defesa do ciberespaço japonês junto do governo. Isso se daria, pois, há lacunas no compartilhamento de informações entre o governo e entes privados, engessando a formulação de políticas e a atuação governamental no tema. Para além do caso dos EUA, Schuetze (2020) exemplifica como essa troca de informações entre os dois setores difere também entre o Japão e a União Europeia, na medida que na UE as empresas de infraestruturas críticas, por exemplo, são obrigadas a compartilhar incidentes com seus respectivos governos, enquanto no Japão essas empresas o fazem de maneira voluntária. Sendo assim, um dos vieses de atuação do governo envolvendo esse cenário é orçar plataformas de compartilhamento de informação público-privada, como o *Japan Electricity Information Sharing and Analysis Center*, que não só servem para compartilhamento de informações relacionadas a vulnerabilidades, ameaças e melhores práticas cibernéticas, como impulsionam cooperação com partes equivalentes no exterior.

Ademais, a cooperação público-privada para fins de segurança nacional é mencionada à larga em documentos estratégicos do governo, inclusive em seus documentos mais significativos ao tema, como a *Cybersecurity Strategy* de 2021 e a *National Security Strategy* de 2022. A NSS é bastante clara nesse sentido, indicando alguns pontos de prioridade no relacionamento público-privado em questões de segurança. A exemplo, menciona-se como o

Japão alavancará ativamente os resultados de pesquisas tecnológicas nos setores público e privado para desenvolver equipamentos de defesa; como o país pretende continuar com sua transferência de equipamentos e de tecnologia entre setores, implementando medidas que incluam formas de fazer tais transferências de maneira tranquila; como se planeja dar vazão a toda essa inovação e tecnologia desenvolvidas através da inserção de uma variedade de pesquisadores de ponta também da academia especializada, impulsionando cooperação entre todas as partes envolvidas e compartilhamento de saber; e como o governo promoverá um ambiente no qual a indústria de defesa possa aproveitar totalmente as oportunidades oferecidas por outras inovações do setor privado (MOFA, 2022b). O pináculo desse pensamento são as políticas de ciberdefesa ativa[71] e ciberdefesa compreensiva trazidas na CSS de 2021, cujos pressupostos são a cooperação governamental com empresas ciberrelacionadas e a implementação de medidas preventivas para antecipadamente combater ameaças (NISC, 2021).

Nessa conjuntura, eventos como a *Singapore International Cyber Week* mais recente, realizada em outubro de 2022, encaixam-se tanto nesta categoria de cooperação público-privada quanto no próximo fundamento que será apresentado envolvendo o multilateralismo internacional do Japão. Nesse encontro marcaram presença figuras políticas, líderes empresariais e industriais, bem como representantes acadêmicos de todas as partes do mundo, visando enfatizar a importância de parcerias público-privadas internacionais para compartilhamento de informação e para a construção de capacidades conjuntas em face a um cenário de ciberameaças sofisticadas em escalada. A *Cyber Storm* americana, o mais extenso exercício de segurança cibernética de seu tipo financiado por um governo, também conta com participação japonesa e une os setores público e privado internacionais para simulações contra ataques a infraestruturas críticas.

De outro modo, o empenho governamental para a proteção de infraestruturas críticas começou mais marcadamente em 2010, quando o governo japonês reconheceu pela primeira vez a importância de o país estar preparado para responder a ciberataques em larga escala contra essas empresas. Conforme aponta Kallender (2014), isso se deu em face aos ataques contra a Coreia do Sul e os EUA um ano antes; a partir desse momento, portanto, o governo japonês compartilhou a responsabilidade de proteção das infraestruturas críticas com a NPA, o MIC, o MOD e o MOFA, cada um com seus processos orçamentários e relacionamento independente com o setor privado, o que criou uma confusão de políticas e de arranjos cooperativos. Com a ineficiência desse emaranhado de relações em face aos acontecimentos de 2011, todo o corpo

[71] Nesse caso, não confundir a ciberdefesa ativa implementada pelo governo japonês com o conceito de ciberdefesa ativa enquanto política de comportamento ofensivo no ciberespaço.

cibernético japonês passou por reanálise e duas grandes questões surgiram no Japão após os ataques, segundo Kallender (2014): como uma das maiores empresas de defesa da Ásia não havia implementado o que se considera medidas básicas de cibersegurança, o que poderia ter evitado o incidente, e qual seria o grau de preparo institucional do país para contornar esse tipo de ciberataque APT sofisticado.

Desse modo, a primeira medida governamental adotada foi a modificação por completo de seus contratos com os produtores militares do país, como a MHI, através da inserção de cláusulas como prestação de contas constante sobre as falhas de segurança detectadas, escaneamentos gerais semanais usando antivírus, fortalecimento de criptografia e auditorias quanto ao treinamento sobre cibersegurança destinado a funcionários. Nesse caso, todos os CSIRTs foram convocados pelo ISPC a superar a falta de integração entre diferentes agências governamentais e o setor privado. De outro modo, no próprio ano de 2011 a proteção de infraestruturas críticas foi centralizada no NISC, neste caso com mais coordenação e autoridade, visto que a divisão desse cuidado dentre os Ministérios apontados foi insuficiente para que se evitassem os ataques. Essa mudança no NISC trabalha favoravelmente tanto ao objetivo de integridade governamental do primeiro fundamento da ciberdefesa japonesa, quanto ao objetivo de integridade nacional do país, dado que a partir disso o relacionamento com as empresas de infraestruturas críticas foi canalizado em uma única instituição especialiada.

Ressalto que apesar de o ano de 2010 ser o ponto de partida "oficial" de proteção a infraestruturas críticas no Japão pelo governo, desde 2005 Tóquio periodicamente relança sua *Cyber Policy for Critical Infrastructure Protection*, com última versão divulgada em junho de 2022 pelo CSSH. Essa política define planos de ação comum compartilhados entre o governo e operadores de infraestruturas críticas, sendo que a parte governamental tem a responsabilidade de promover a adoção de medidas independentes estabelecidas pelos próprios operadores dessas estruturas, ao passo que a parte privada se atém a elaborar medidas protetivas relevantes. É nessa política que o governo japonês identifica quais são os 14 setores considerados infraestruturas críticas no país[72], ao passo que estabelece cinco expectativas em relação às partes interessadas: (1) aprimoramento da capacidade de resposta a incidentes; (2) manutenção e promoção de princípios de segurança; (3) aprimoramento de sistemas de compartilhamento de informação; (4) utilização de gerenciamentos de riscos; e (5) aprimoramento das bases para a

[72] Serviços de informação e comunicação, serviços financeiros, serviços de aviação, aeroportos, serviços ferroviários, serviços de fornecimento de energia elétrica, serviços de fornecimento de gás, serviços governamentais e administrativos, serviços médicos, serviços de água, serviços logísticos, indústrias químicas, serviços de cartão de crédito e indústrias de petróleo (CSSH, 2022).

proteção de infraestruturas críticas.

Também mais recentemente, em abril de 2019, outros dois documentos foram lançados em concomitância: a quinta versão da *Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure* e a primeira edição do *Risk Assessment Guide Based on the Concept of Mission Assurance in Critical Infrastructure*, ambos bastante complementares em suas premissas e temas abordados, os quais ainda estão em vigor neste momento. O primeiro documento começa estabelecendo que a vida de modo geral e as atividades socioeconômicas estão ancoradas em múltiplos serviços providos por infraestruturas críticas, sendo que sistemas da informação são amplamente usados nesses serviços. Desse modo, dada sua própria natureza, espera-se que infraestruturas críticas provenham serviços seguros e sustentáveis, e as diretrizes em questão apontam como esses provedores, para além de entidades privadas e de negócios, são entidades socialmente responsáveis pelo seu modo de negócio. Sendo assim, com a ajuda necessária do governo, é desejado que operadores de infraestruturas críticas se envolvam ativamente no gerenciamento de riscos cibernéticos, estejam prontamente preparados para atuar nesses riscos e estabeleçam medidas estratégicas para reduzi-los mediante avaliações de risco. Através dessas premissas, portanto, serviços de infraestruturas críticas serão providos sem qualquer deterioração em qualidade ou sua suspensão, o que é inaceitável tanto para as próprias empresas quanto para as demais partes interessadas envolvidas (CSSH, 2019a).

O segundo documento inicia reconhecendo como as tecnologias da informação e comunicação se tornaram um fenômeno no modo de vida das pessoas e que gradativamente se convertem em um elemento indispensável na provisão de serviços e atividades sociais. No guia é mencionado que a qualidade e a produtividade neste setor têm avançado, ao mesmo tempo que vulnerabilidades e riscos em escalada surgem em meio a essa evolução. Neste cenário, operadores de infraestruturas críticas, a fundação das atividades econômicas e do modo de vida das pessoas, têm sido ameaçados por riscos cibernéticos. O documento, portanto, procura prover um panorama de engajamento quanto à avaliação de risco à segurança da informação, bem como medidas concretas de trabalho no tema, aprofundando o entendimento, a precisão e a padronização de avaliações de risco dentre operadores de infraestruturas críticas através da implementação de medidas próprias. Ao longo do texto, portanto, citam-se tópicos como o propósito da condução de avaliações de risco, a implementação de políticas e sistemas, cronogramas detalhados de atuação e planos para pessoal envolvido, bem como a validação das avaliações em execução e a continuidade desses exercícios (CSSH, 2019b). Em suma, é um passo a passo de como o setor privado, mais especificamente os operadores de infraestruturas

críticas, deve se comportar para estar à frente dos riscos enfrentados no ciberespaço e saber contorná-los com antecipação.

Takeda (2019) estabelece que um dos motivos da grande sensibilidade deste viés da ciberdefesa reside no fato de que os ciberatacantes sempre saem na dianteira contra infraestruturas críticas, uma vez que podem escolher seus alvos criteriosamente, enquanto as empresas atacadas conseguem proteger apenas um número limitado desses alvos. Nesse sentido, visto que os alvos normalmente são entes privados, como provedores de energia, água, transportes e comunicações, tais ataques cibernéticos seriam inicialmente categorizados como crimes ou mesmo terrorismo, ficando fora do escopo de atuação direta das forças nacionais. Assim, para que essas estruturas sejam mais bem protegidas, há de se ter grandes esforços cooperativos público-privados, compromisso constante com a causa e coordenação com a lei para que organizações de defesa nacional conduzam operações deste tipo.

O principal ponto de debate quanto à proteção de infraestruturas críticas, no entanto, concentra-se no envolvimento dúbio das forças nacionais neste tipo de defesa. Kallender (2014) aponta como as Forças de Autodefesa do Japão precisariam passar por mudanças legais para conseguirem proteger essa esfera do setor privado em caso de emergências envolvendo ciberataques, assim como seu quadro legal precisou ser alterado quando as SDF estenderam sua atuação para desastres nucleares e no transporte de cidadãos japoneses no exterior, por exemplo[73]. Esse desejo por parte do governo, contudo, já vem sendo expresso em documentos oficiais, como na recente NSS de dezembro de 2022, onde o governo japonês se comprometeu a estabelecer um arranjo cooperativo entre as SDF, a polícia e a Guarda Costeira para a proteção de plantas nucleares, de energia elétrica, bem como instalações de telecomunicações e outras infraestruturas. Estima-se que no outono japonês de 2023 o governo inicie debates para mudança das leis que regem a atuação das SDF, para assim ampliar sua proteção a infraestruturas críticas. Apesar de ainda não sabermos sobre este ponto, é bastante possível que esta mudança na lei ocorra de fato, dado o histórico de atuação do Japão.

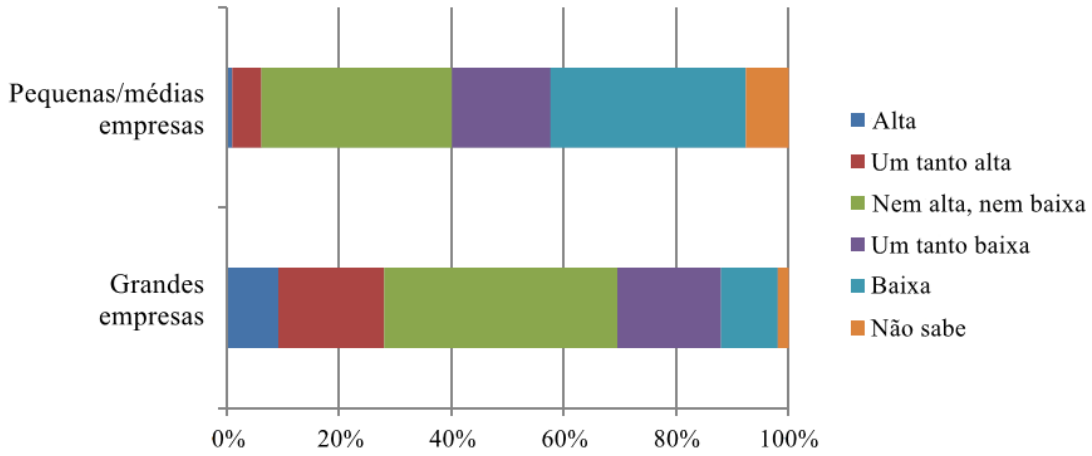
Tanaka Tatsuhiro, ex-general das Forças Terrestres de Autodefesa do Japão e agora pesquisador do Instituto de Segurança Nacional da Fujitsu, vai mais além e entende que a melhor estratégia para uma maior integração ciberdefensiva entre o governo e infraestruturas críticas é o estabelecimento de um "Ministério Cibernético" no país. Em entrevista ao *The*

[73] Como apontam Yuka Koshina e Franz-Stefan Gady (2020), o CDC, arranjo cibernético mais bem estruturado das SDF do Japão no momento, coordena a ciberdefesa apenas dos três ramos das Forças de Autodefesa japonesas e está encarregado de proteger a infraestrutura de informações críticas e redes militares do Ministério da Defesa em caso de ameaças estatais externas.

Diplomat, Tanaka entende que se faz necessário fortalecer a infraestrutura cibernética governamental a ponto de torná-la uma organização ao mesmo nível de outros Ministérios ou mesmo acima deles (KOSUKE, 2022). Em comparação, o NISC não é um centro de comando em ciberdefesa voltado para o manejo de crises, mas sim uma organização para coordenar respostas a situações cibernéticas; todos os documentos e diretrizes lançados pelo NISC ou pelas demais agências governamentais que lidam com cibersegurança, nesse sentido, funcionam em caráter coordenador. Dessa forma, na visão de Tanaka seria fundamental ter um Ministério amplo com mais poderes e responsabilidades, para que quando uma rede elétrica seja posta abaixo por ciberataques, por exemplo, alguma instância consiga utilizar de comando e controle para resolver a situação, o que não é alcançado pela coordenação impulsionada pelo NISC ou órgãos correlatos.

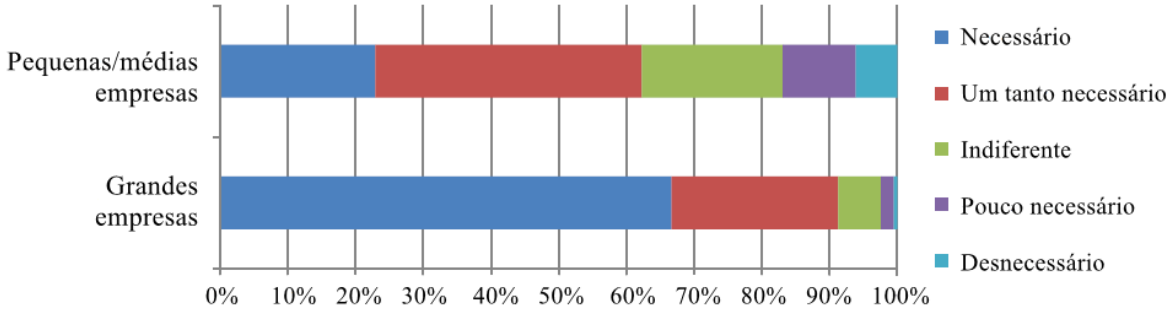
A despeito dos esforços governamentais até o momento e mesmo do próprio pioneirismo do setor privado na promoção da cibersegurança japonesa, Katagiri (2021) indica como a opinião da esfera privada ainda está dividida sobre políticas cibernéticas. A maioria das firmas japonesas, pequenas, médias ou grandes, permanece neutra ou sequer considera ameaças cibernéticas um provável problema, por exemplo. Contudo, a maioria das empresas japonesas parece concordar que há sim necessidade em robustecer seus sistemas de segurança; esse apoio chega a 90% dentre as grandes empresas se considerarmos a porcentagem de quem respondeu que é "necessário" ou "um tanto necessário" fortalecer suas ciberdefesas.

Gráfico 1 – Empresas japonesas respondem: qual a probabilidade de sua companhia ser ciberatacada?



FONTE: KATAGIRI, Nori (2021); edição e tradução minhas.

Gráfico 2 – Empresas japonesas respondem: é necessário fortalecer a defesa cibernética de sua companhia?



FONTE: KATAGIRI, Nori (2021); edição e tradução minhas.

De outro modo, cerca de 63% das empresas japonesas contam com o cargo de diretor de segurança da informação (CISO), contra 95% nos EUA e 85% na Europa, ao passo que em 36% das empresas japonesas onde o cargo de CISO existe, este papel é normalmente compartilhado com outras atividades ou responsabilidades por quem o desempenha; 17% e 18% dos CISOs americanos e europeus, respectivamente, desempenham outras atividades em conjunto a esse cargo (MATSUBARA, 2018). Esses dados são alguns exemplos que evidenciam tanto a necessidade da participação do setor privado na manutenção da cibersegurança japonesa, quanto a urgência de uma maior proatividade do setor na questão cibernética, dado que o Japão fica atrás de suas contrapartes ocidentais nesse quesito (YOKOHAMA, 2019). Isso indica, portanto, que a troca política tanto internamente ao setor privado quanto entre esse e a esfera pública ainda precisa avançar para se equiparar ao contexto de parceiros estratégicos do Japão.

Ainda, aponto como infraestruturas críticas têm sido alvos constantes de vazamentos de dados ou rupturas de sistema, mesmo que de maneira menos grave se comparado aos ataques de 2011. Em 2014, por exemplo, informações de carca de 190 mil membros do programa de passageiros frequentes da Japan Airlines foram acessadas. Apesar de nenhum vazamento de números de cartão de crédito ou senhas ter sido detectado, cerca de 21 mil peças de dados pessoais foram transferidos para servidores remotos não identificados. Mais recentemente, em 2021, o aplicativo de mensagens Line teve dados vazados de cerca de 86 milhões de usuários no Japão, e no mesmo ano a empresa de telecomunicações japonesa NTT revelou uma brecha em seus sistemas onde dados de 621 clientes, não especificados se usuários individuais ou outras companhias, foram enviados para servidores remotos sob o controle dos atacantes. Apesar de nesses casos informações pessoais de usuários terem sido acessadas e transferidas ilegalmente, esses ataques não resultaram na interrupção de serviços ou em preocupações físicas advindas dos ciberataques. Contudo, essas invasões confirmam como infraestruturas

críticas precisam continuar a aprimorar seus sistemas de defesa cibernética, uma vez que ainda apresentam brechas que põem em risco a segurança da informação das próprias companhias e de seus usuários.

Para finalizar, Matsubara (2018b) aponta ainda que uma das maiores dificuldades nas trocas entre o setor público e o privado se concentra no sistema de trabalho do Japão, onde resiste ao tempo a ideia de emprego vitalício. Nesse caso, os japoneses iniciam e finalizam sua carreira profissional em uma mesma empresa, e aqueles que começam suas carreiras no setor governamental ou em comunidades de inteligência raramente se mudam ao setor privado. Segundo relatório divulgado pelo *Japan Institute for Labour Policy and Training*, 87,9% dos entrevistados em pesquisa realizada responderam que preferem ter o mesmo emprego para toda a vida (JILPT, 2019). Essa falta de polinização entre o setor público e o privado, portanto, dificulta a tarefa de governos quando se trata de entender as ciberameaças reais enfrentadas pelo mundo empresarial e como protegê-lo. Essa realidade trabalhista difere muito dos Estados Unidos e do Reino Unido, por exemplo, indicando como esses países tendem a estar mais ciberneticamente preparados que o Japão, haja vista essa maior permutação de profissionais ora na esfera privada, ora na esfera governamental.

Takeda (2019) também menciona que o recrutamento e a retenção de pessoal especializado tem se tornado crítico no país. Nesse aspecto, trabalhadores do setor privado vem sendo contratados com salários muito mais altos se comparados aos de outros empregados das SDF japonesas, por exemplo, visto que os planos das carreiras militar e de segurança da informação na esfera privada costumam ser muito diferentes, e servir a uma força militar como o CDC não é o caminho mais atrativo. O autor contrapõe, contudo, que os profissionais do setor privado costumam ser muito bem treinados em cibersegurança genérica e, portanto, devem ser reinstruídos a lidar com ameaças muito mais sofisticadas se migrarem à segurança cibernética estatal. Yokohama (2018) parte desta mesma visão, alegando que diferentemente do que ocorre em companhias americanas e europeias, onde o conjunto de habilidades de seus empregados individualmente se complementam e criam um time corporativo de sucesso, as empresas japonesas preferem empregados mais generalistas e que foquem na organização como um todo, faltando este viés mais detalhado na atuação de seus agentes.

4.3. O multilateralismo japonês na questão cibernética

Kallender (2014) aponta que ao menos até 2010 as políticas de segurança da informação do Japão eram fruto direto de pressões americanas. Segundo Gady (2017), essas pressões eram

feitas para que o Japão melhorasse suas defesas cibernéticas para blindar as transferências informacionais e tecnológicas entre as duas nações, bem como para garantir a segurança do sistema de defesa antimísseis balísticos japonês, por exemplo. Dado o bilateralismo nipo-americano em assuntos de segurança, muitas informações militares americanas estão disponíveis em redes japonesas, logo, pressionar o Japão a melhorar sua infraestrutura cibernética reflete diretamente na integridade securitária dos EUA. No entanto, apenas em 2014 o Japão começou a adotar uma postura mais alinhada às expectativas americanas devido ao estabelecimento do CDC. Há de se apontar que nesse contexto o Ministério da Defesa japonês foi o principal ator a levar adiante a cooperação ciberdefensiva entre os Estados Unidos e o Japão (GADY, 2017). Kallender (2014) complementa dizendo que o encontro 2+2 de 2010 entre Japão e EUA foi o primeiro momento em que se propôs que o ciberespaço fosse tratado como agenda importante e que o tema fosse impulsionado nas cooperações trilaterais Coreia do Sul–EUA–Japão e Austrália–EUA–Japão.

Mais recentemente, no encontro Japão-EUA 2+2, de abril de 2019, os dois países concordaram em fortalecer cooperação em operações entre domínios, incluindo o espaço sideral, o ciberespaço e o espectro eletromagnético. Ainda, os ministros americanos e japoneses presentes no encontro afirmaram que leis internacionais se aplicam ao ciberespaço e que ataques cibernéticos poderiam, sob certas circunstâncias, constituir ataques armados para os propósitos do Artigo V do ANPO (MOFA, 2019). Dessa forma, o acordo de segurança assinado entre o Japão e os Estados Unidos paulatinamente passa a ser incorporado de maneira definitiva na segurança cibernética japonesa, como resultado dessa busca por alinhamento internacional quanto ao ciberespaço efetuada por Tóquio. Assim como vem acontecendo desde a década de 1950 com os domínios tradicionais de poder, portanto, o bilateralismo securitário entre Estados Unidos e Japão também constitui as bases da atuação internacional japonesa em termos de cibersegurança. Stefan Soesanto (2021) menciona, por exemplo, que o bilateralismo Japão-EUA em ciberdefesa é central para o esforço cibernético do Japão e é responsável por grande parte da cooperação em inteligência, da construção de capacidades e dos exercícios militares conjuntos entre os dois países.

Entretanto, Sonoko Kuhara (2020) argumenta que, mesmo chegando-se a esse consenso, os dois países enfrentam uma série de problemas no acionamento do tratado em caso de ataques cibernéticos. Em primeiro lugar, há uma falta de normas internacionais para endereçar esse tipo de problema e suas possíveis contramedidas; segundo Kuhara, nem mesmo o Manual de Tallinn, possivelmente o documento cibernético mais internacionalizado, tem *status* de norma internacional, e mesmo membros da OTAN adotam diferentes limites para o acionamento da

autodefesa ou defesa coletiva em ocorrências cibernéticas. Para o governo japonês, por exemplo, cada caso deve ser analisado individualmente, o que indica como não existe uniformidade quanto à defesa (coletiva) no ciberespaço nem mesmo para o próprio Japão. Em segundo lugar, é difícil decidir que tipo de contramedida adotar frente a ataques cibernéticos, dado que a atribuição no ciberespaço é muito difícil. Em relação ao ANPO, é desafiador estabelecer uma linha vermelha que justifique o acionamento da defesa coletiva e uma contra ação militar. Por fim, Kuhara aponta que ciberataques podem ser realizados em momentos de guerra, situações de "zona cinza" ou mesmo em tempos de paz e que, portanto, é difícil determinar se respostas tanto cibernéticas quanto cinéticas são apropriadas, dado que podem ser vistas como um escalonamento desnecessário em um conflito ou tensão.

Apesar dessa conjuntura de profunda cooperação bilateral com os Estados Unidos, o Japão também tem adotado uma política externa mais proativa e focada no multilateralismo ao menos desde o final da Guerra Fria, como mencionado; essa característica se repete no caso da cibersegurança japonesa. Nesse sentido, o terceiro fundamento da política de ciberdefesa nipônica se concentra em uma abordagem *Whole of System*, através da qual o Japão tenta integrar-se profundamente à cena internacional em que está inserido. Kallender (2014) aponta que os laços cibersecuritários do Japão com parceiros com importância elevada, como a Austrália, a Europa e a ASEAN, vem se expandindo verdadeiramente desde os ataques de 2011. Naquele momento, o MOFA passou a encabeçar o processo de coordenação internacional jurídica e política com os atores supracitados, como forma de fortalecer as normas internacionais de comportamento no ciberespaço, protagonizando este lado da cibersegurança japonesa. O autor também aponta como a atuação diplomática do MOFA vai de encontro com as políticas de defesa do MOD, na medida que a cibersegurança como conhecemos hoje não concerne mais apenas aqueles princípios básicos do ciberespaço; isto é, planejamento e produção militares, dados sobre o sistema anti mísseis balísticos do Japão e informações sobre defesa militar tradicional e de infraestruturas críticas, por exemplo, estão sendo acessados via ciberespionagem. Isso põe em risco não só a segurança cibernética japonesa como o próprio setor militar como um todo, uma vez que parte significativa dele está hoje conectado em rede, e a ação protagonista do MOFA no tema tem sido complementar aos interesses do MOD e da estrutura militar japonesa.

Outro resultado desse reposicionamento japonês foi demonstrado em seu LBD de 2011 (lançado um mês antes dos ataques de 2011), quanto o MOD classificou ameaças cibernéticas acima de ameaças de armas de destruição em massa e terrorismo em seu ranking de prioridades. Este LBD foi importante também por ser o primeiro a citar ameaças específicas como o Stuxnet

e mencionar que deveria existir uma integração entre governos nacionais *like-minded*, uma expansão dos poderes e do orçamento de agências de segurança em países *like-minded*, um aumento no número de institutos mundo afora que pesquisem sobre o tema, bem como um aumento na cooperação internacional em cibersegurança (KALLENDER, 2014). Essas medidas já proativas vieram a calhar, visto que um mês mais tarde o país seria vítima dos maiores ataques cibernéticos até a data; além disso, a política de alinhamento internacional a países de pensamento similar expõe como o Japão está disposto, a partir de então, a colocar outras nações no centro de seu debate para robustecer sua cibersegurança.

Essa ideia vai de encontro à reinterpretação do Artigo 9 da Constituição japonesa efetuada em 2014, a qual autorizou as SDF a participarem das chamadas missões de autodefesa coletiva[74]; nesse sentido, começa-se a inserir a ideia de autodefesa coletiva também no ciberespaço. Quanto a essa aproximação com múltiplos parceiros em termos de segurança cibernética, certamente se destacam os encontros regulares do Fórum Regional da ASEAN que tratam especificamente de cibersegurança, como o *ARF-ISM on ICTs Security 6th OESG*, de janeiro de 2021; os debates no âmbito da ONU, como o *UN Security Council Open Debate on Cyber Security*, de junho de 2021; as inúmeras consultas bilaterais entre o Japão e países estratégicos, como o Reino Unido, a França, a Austrália e a Índia; ou também os encontros do QUAD sobre o tema, sendo a divulgação mais recente do grupo o *Quad Joint Statement on Cooperation to Promote Responsible Cyber Habits*, um curto texto que faz parte do programa *QUAD Cyber Challenges* e que procura impulsionar as melhores práticas para usuários e provedores de internet na criação de um ambiente cibernético mais seguro. De todo modo, a OTAN é o arranjo multilateral de preferência do Japão para aprofundar sua cooperação internacional em cibersegurança. Só em 2022, por exemplo, o Japão se juntou oficialmente à *Cyber Coalition*, grupo da OTAN que através de jogos de guerra simula situações de

[74] Nesse momento foi quebrado o paradigma de que o Japão não poderia colocar em ação suas Forças de Autodefesa no exterior; até aquele momento, as SDF tinham autorização para proteger o Japão única e exclusivamente dentro de suas fronteiras. Dessa maneira, a decisão do gabinete ministerial de 2014 permitiu que as forças japonesas fossem usadas no exterior em ajuda a um país com relações próximas com o Japão e que estivesse sob uma condição de ataque que ameace claramente a sobrevivência do Japão e o direito à vida, à liberdade e à felicidade de seu povo. Neste caso, em conformidade à Constituição e ao princípio de autodefesa do Japão, o uso da força deve ser empregado em um nível mínimo necessário para apenas repelir tal ataque contra o Estado aliado (CABINET SECRETARIAT, 2014). O Manual de Tallinn é um tanto emblemático neste ponto, visto que no documento cita-se que a defesa cibernética é naturalmente coletiva, dado que os atores envolvidos dependem de uma série de provedores, organizações e outros países para auxiliar na suspensão de ciberataques. Essa defesa coletiva, portanto, existiria tanto no nível de detecção e resposta a ataques cibernéticos quanto de defesa ativa (KLIMBURG e HEALEY, 2012). Assim, para além da certa aceitação internacional de um arranjo de defesa coletiva no ciberespaço, o Japão não só indica essa possibilidade como chave em suas políticas como já tem autorização legal para tal a partir desta reinterpretação de 2014. Nas palavras do ex-Primeiro-ministro Yoshihide Suga, não se pode agir apropriadamente e com a agilidade necessária contra ciberataques sem cooperação estreita com outros países.

ciberataques, sistemas de computadores comprometidos e como contornar cenários afins que ponham em risco infraestruturas cibernéticas, e, em dezembro do mesmo ano, o país se tornou membro pleno do CCDCOE, o *hub* de ciberdefesa da OTAN sediado em Tallinn, na Estônia, que foca em pesquisa, treinamento e exercícios cibernéticos.

Essa integração do Japão ao sistema OTAN é oportuna não só para o Japão, dado que o país cumpre com seu objetivo de cooperar com nações *like-minded* e robustecer suas técnicas de ciberdefesa, como também serve ao propósito da organização de reforçar a cibersegurança japonesa para proteger seus próprios dados. Como mencionado anteriormente, os EUA impuseram as maiores pressões sobre o Japão para que o país passasse a adotar medidas cabíveis de proteção do ciberespaço para assim proteger as informações americanas que circulam nas redes japonesas, e essa preocupação é também compartilhada pelos países europeus, na medida que a cooperação com o Japão, especialmente cibernética, vem em escalada nos últimos anos.

Para além do já sabido viés colonial que torna o Leste Asiático uma região reconhecidamente anti-nipônica, o alinhamento do Japão a esta contraparte ocidental é motivo de atrito com seus vizinhos comunistas. Assim como ocorreu com a União Soviética, essa aproximação do Japão com as antíteses ocidentais tensiona as já complicadas relações intrarregionais; no caso do ciberespaço, o Japão deixa bastante claro em seus documentos oficiais que as nações *like-minded* são o foco principal do país em termos de parcerias internacionais. Apesar dos pesares, orbitar a OTAN demonstra como o Japão está alinhado a um grupo de países específico e nesta posição pretende ficar. O pilar WoS da ciberdefesa japonesa, desse modo, conta com um caráter construtivista bastante forte por parte do Japão, uma vez que existe a sensação de pertencimento a um certo círculo internacional de países *like-minded*, como o governo japonês nomeia repetidamente, em detrimento de países alheios a essa cooperação.

Nessa ótica de colaboração internacional, entretanto, o Japão também estende sua participação à construção de normas internacionalmente válidas para o ciberespaço, dado que a dificuldade de atribuição, dissuasão e resposta da comunidade internacional a ciberataques cria lacunas nas normas de comportamento internacional, dificultando a aplicação da lei existente para julgar tais incursões (KALLENDER, 2014). Nesse tema, Katagiri (2021) cita a assinatura da Convenção de Budapeste pelo Japão, em 2001, a qual foi ratificada apenas em 2012[75], comprovando como o país está comprometido através do direito internacional a

[75] A assinatura da Convenção de Budapeste pelo Japão foi facilitada pela passagem de uma lei contra cibercrime um ano antes, em 2011, que institucionalizou uma série de penalidades a transgressões como distribuição e

incorporar cláusulas em seu sistema legal sobre assuntos relacionados a redes de computadores, interferências em dados e sistemas, bem como cooperação com terceiros Estados para investigação e judicialização de atos criminalizados pela convenção. Katagiri contrapõe, no entanto, que esse tipo de alinhamento político não garante uma eficácia notável na discussão de ciberataques, uma vez que não criam mecanismos efetivos de aplicação da lei, por exemplo. O autor completa dizendo que o governo japonês está ciente da limitada eficácia dessa cooperação, mas que prefere levar adiante a imagem do Japão como um país "campeão" da cooperação global a despeito da inércia na deterrência efetiva de ciberataques.

Outro exemplo dessa aproximação para além da Convenção de Budapeste são os encontros como o *United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace* e o *Open-Ended Working Group*, nos quais o Japão concordou com os demais países participantes que o direito internacional provê proibições gerais para o uso malicioso de forças cibernéticas; que o direito internacional proíbe Estados a intervir digitalmente em assuntos internos de outros; e que operações cibernéticas que interfiram na política doméstica de Estados podem ser classificadas como violações de soberania (KATAGIRI, 2021). Nesse sentido, tanto o governo quanto a indústria digital nipônica tem se juntado ao discurso global de que o direito internacional se estende ao ciberespaço, haja vista o fortalecimento dos diálogos e das medidas de construção de confiança estabelecidos com países da União Europeia, da OTAN e da ASEAN (KATAGIRI, 2021), firmando um corolário à abordagem WoS da defesa cibernética japonesa.

4.4. Conclusões do capítulo

Este capítulo objetivou traçar o que identifico ser os três fundamentos da ciberdefesa japonesa: a proatividade política dentro da Constituição; a público-privatização da defesa cibernética do Japão; e o multilateralismo nipônico em cibersegurança. Aponto, desse modo, como o Japão está sabendo fazer uso da estrutura em que está inserido para performar no ciberespaço, especialmente quando traz para o debate a responsabilidade do setor privado em fortalecer a cibersegurança do país. Como falado anteriormente, a *Cybersecurity Strategy* de 2015 foi o primeiro documento oficial do Japão a colocar em pauta o gerenciamento de grandes empresas como uma estratégia de segurança nacional. A partir disso, diferentemente das forças militares tradicionais, no domínio cibernético a responsabilidade de defesa do território está

armazenamento de vírus de computador e demais *malwares* (KALLENDER e HUGHES, 2016).

sendo dividida com o setor privado em alguma medida, e isso destoa da esfera securitária tradicional. Essa cooperação do governo com o âmbito privado, desse modo, ocorre tanto pela falta de profissionais capacitados na área que possam preencher vagas estratégicas a nível governamental, por exemplo, quanto pelo fato de que as grandes empresas de tecnologia japonesas são responsáveis pela produção do ciberespaço em si e, portanto, detêm *know-how* de como manuseá-lo. Em outras palavras, a esfera privada da sociedade japonesa passa a ganhar protagonismo em um tema tradicionalmente dominado pelo Estado, revelando como o âmbito doméstico japonês é inseparável da promoção e da garantia de um ciberespaço livre, justo e seguro, utilizando as palavras do governo japonês.

Visto que parte significativa do avanço japonês no ciberespaço é reflexo de influência norte-americana, pode-se dizer também que essa estratégia de público-privatização da ciberdefesa japonesa é quase uma mimetização do cenário doméstico americano. Visto que nos EUA o setor privado faz parte permanente da formulação de pensamento, conhecimento e mesmo da legislação americana envolvendo o ciberespaço, o governo japonês está na tentativa de tornar as empresas japonesas as novas protagonistas do tema a âmbito nacional. Isso se torna claro quando analisamos os documentos oficiais do Japão onde o governo não só estimula a participação do setor privado na formulação política cibersecuritária, como indica que grandes empresas devem trazer à mesa ideias e práticas próprias para o reforço da cibersegurança nacional.

Esse aspecto, entretanto, não é marca exclusiva das forças de defesa cibernéticas do Japão. A integração com o setor privado no domínio ciber ocorre em inúmeros países cujas atividades cibernéticas são significativas, inclusive nos Estados inimigos do Japão, mas a diferença entre a integração do setor público-privado no Japão e nesses países se dá em bases legais. Diferentemente da Rússia, que em muitas ocasiões utiliza meios coercitivos para capturar ajuda privada no campo cibernético (AKIMENKO e GILES, 2020), da China, que através de seu tipo de governo consegue em algum grau interferir no funcionamento de grandes empresas para que objetivos estatais sejam atingidos de maneira mais assertiva, ou mesmo da Coreia do Norte, cujo Estado patrimonialista das coisas impossibilita a dissociação completa dos entes público-privados em assuntos de natureza securitária, o Japão conta com uma Constituição e sistemas político e econômico que devem ser seguidos com prestação de contas. Nesse caso, o governo japonês precisa buscar formas de jogar dentro das linhas da Constituição e de sua legislação para angariar apoio legítimo do setor privado para a causa, o que torna seu objetivo ainda mais difícil quando as grandes empresas de tecnologia operam em uma lógica liberal de mercado.

Fechando este tópico, uma das passagens da NSS de 2022 ilustra como o Japão vem pensando em segurança proativamente, tanto em termos cibernéticos quanto em termos tradicionais. Falando de suas estratégias para aprofundamento da público-privatização da (ciber)segurança japonesa, o documento aponta que o Japão não se limitará ao seu modo de pensar convencional para capitalizar suas capacidades tecnológicas avançadas, as quais vêm sendo desenvolvidas ao longo dos anos nos setores público e privado no campo da segurança nacional (MOFA, 2022b). Dessa forma, o governo não só enraíza a ideia de que as capacidades tecnológicas japonesas surgem em paralelo e em complementaridade entre os setores público e privado, como se mostra aberto a abandonar sua atuação tradicional em prol de um comportamento proativo de suas políticas. Isso reforça como a proatividade política japonesa tem esticado os limites de atuação do governo na (ciber)segurança nacional, respeitando a Constituição, mas buscando uma mudança legal.

Vale mencionar, portanto, que os três fundamentos apresentados para a ciberdefesa japonesa estão atualmente sob constante evolução e debate na esfera política do país. A proteção de infraestruturas críticas, no pilar da público-privatização da ciberdefesa japonesa, por exemplo, pode mudar consideravelmente nos próximos anos, haja vista uma possível alteração da lei das SDF. O mesmo pode ocorrer com o primeiro fundamento apresentado, envolvendo a proatividade japonesa e seus limites constitucionais, mas visto que reformular a Constituição do Japão é uma tarefa mais difícil que alterar a lei das SDF, uma possível mudança na primeira linha de atuação da ciberdefesa japonesa ainda parece distante, a despeito da declarada vontade dos últimos Primeiros-ministros nipônicos em alterar o documento. Por fim, o multilateralismo japonês no ciberespaço igualmente é objeto de mudança constante, uma vez que constantemente novos arranjos são estabelecidos para proteção cibernética de países envolvidos e diferentes instituições e grupos internacionais são acessados pelo Japão. Se no futuro a comunidade internacional lograr êxito em inserir defesa e segurança cibernéticas no direito internacional de maneira plena, por exemplo, o Japão terá cumprido com seu objetivo de estabelecer o desejado *common ground* de comportamento, resposta e punição aos infratores em escala internacional.

Para finalizar, agora mencionando os vieses de integridade da conformação ciberdefensiva japonesa, o Manual de Tallinn aponta que essas frentes deveriam ser desenvolvidas em sequência – primeiro WoG, depois WoN e por fim WoS –, mas não exclui a possibilidade de um país investir nesses estágios da forma que preferir (GADY, 2017). Assim, Gady (2017) aponta que o Japão é um exemplo de Estado com um WoS muito forte, dado que o país participa ativamente de conferências internacionais e tem encontros bilaterais bastante sólidos com parceiros estratégicos, mas que, no entanto, conta com um WoG e um WoN

insuficientemente centralizados, com inúmeros setores governamentais atuando paralelamente no tema da cibersegurança e por vezes pouco integrados entre si, especialmente quanto a empresas privadas. Essas, por sua vez, são resistentes em adotar medidas de proteção cibernética, compartilhar informações com o governo e agir política e proativamente para fortalecer a segurança cibernética nacional.

CONSIDERAÇÕES FINAIS

Em linhas gerais, esta dissertação teve como objetivo apresentar o que identifico serem os três fundamentos da ciberdefesa japonesa, isto é, as três principais linhas de atuação governamental no tema da defesa cibernética do Japão. O primeiro desses fundamentos remete a uma postura de integridade governamental cujo pressuposto é a sincronização política entre agências e órgãos governamentais para se obter eficiência máxima no tema cibernético; o segundo fundamento se baseia na ideia de integridade nacional, ou de cooperação público-privada para fortalecimento da estrutura de defesa nacional, seja pelo compartilhamento tecnológico, seja pelo compartilhamento de práticas e informações; e o terceiro fundamento, por fim, se concentra no pressuposto de integridade sistêmica, a partir do qual o Japão tenta alinhar comportamentos e práticas internacionais no domínio cibernético, em especial com países *like-minded*, como forma de fortalecer sua ciberdefesa.

Nesse contexto, busquei expor como essa realidade cibersecuritária, apesar de ter suas particularidades e mesmo certos pontos de virada se comparada à segurança tradicional do Japão, segue a mesma lógica do teatro de segurança preestabelecido na Ásia Oriental. Dessa forma, esse teatro de segurança é composto por países separados por identidades históricas divergentes, sejam elas por motivos coloniais, como a China e a Coreia do Norte, sejam por motivos políticos, como a Rússia. Assim, parece que se completa um ciclo nas relações securitárias intrarregionais: na medida que no passado o Japão era o país que acuava as demais nações da região, hoje, acima de tudo, o Japão é acuado por esses mesmos países, agora independentes e com pretensões militares sobre a região, sendo um deles uma das maiores potências mundiais. Esse rancor antinipônico historicamente construído na região, portanto, também influencia a esfera cibernética japonesa na medida que o ciberespaço se tornou outro domínio onde essas ameaças tradicionais interferem na segurança nacional do Japão.

É com base nessas ameaças securitárias que o Japão estabeleceu seus fundamentos em defesa cibernética como forma de contornar ou mesmo conter o avanço de países inimigos como a Rússia, a China e a Coreia do Norte. Nesse aspecto, o objetivo da política externa e securitária do Japão durante a Guerra Fria se assemelha aos propósitos das políticas externa e de segurança japonesa atuais: contenção de seus vizinhos para impedir que ameaças crescentes ponham em risco a integridade territorial do Japão. No século XXI, no entanto, essa política de contenção foi repaginada e hoje se apresenta de maneira mais moderna que no século passado, visto que o Japão está expandindo sua forma de pensar, agir e se alinhar internacionalmente para impulsionar seu plano de contenção também no ciberespaço e de maneira proativa.

Feitas essas observações, é perceptível como o Japão mergulhou de vez na questão cibernética pós-2011. Em suma, a partir daquele momento houve a reformulação total do ISPC e do NISC, o *Cyber Defense Command* é criado pelo Ministério da Defesa, o MOFA insere a cibersegurança na política externa japonesa e se torna um dos bastiões da atuação internacional do país no tema com seu multilateralismo, há também a ratificação da Convenção de Budapeste que por sua vez influencia as leis domésticas do Japão e, como extensão, a atuação da NPA, e podemos apontar também a entrada do Japão no sistema CCDCOE da OTAN e o robustecimento da ciberdefesa japonesa junto do setor privado. Em outras palavras, os vieses de WoG, WoN e WoS passaram a se desenvolver marcadamente após 2011. Considero que a entrada do Japão à organização de Tallinn, inclusive, deixa claro quais são as prioridades estratégicas do Japão em termos de parcerias e como esses países são priorizados para garantia de sua defesa e segurança cibernéticas, mesmo que haja uma proximidade grande do Japão com outras nações como as da ASEAN, a Austrália e a Índia.

No entanto, indico que dentre todas as modificações e avanços observados no Japão quanto à defesa cibernética do país, seu segundo fundamento de integridade nacional calcado na público-privatização da ciberdefesa japonesa é o ponto mais emblemático do tema. Isso se dá, pois, diferentemente do primeiro e do terceiro fundamentos, os quais também podem ser impressos sobre a atuação militar tradicional do Japão, o segundo fundamento é naturalmente uma postura ciberdefensiva, pois o domínio cibernético é o único onde o setor privado prevalece em seus mais variados níveis. A bola de bilhar realista é desmanchada nesse momento, haja vista a impossibilidade de desvincular o lado doméstico do Japão de sua cibersegurança, uma vez que parte significativa da ciberdefesa japonesa advém do setor privado doméstico e depende da inserção e proatividade desse setor no tema.

Ao mesmo tempo que o segundo fundamento é naturalmente um tema cibersecuritário, contudo, aponto como esse é o pilar mais frágil da ciberdefesa japonesa dada a resistência do setor privado em cooperar com o governo ou mesmo implementar as práticas recomendadas por seus órgãos oficiais como o NISC. Assim, apesar de concordar com Gady quando o autor fala que o WoS japonês é mais robusto que seus WoG e WoN, acredito que a integridade nacional japonesa se sobressai nos pontos que o Japão deve melhorar em sua defesa cibernética, dado que, para mais ou para menos, a remodelação do NISC e do IPS e a própria criação do CDC fortaleceram a integridade governamental do país no campo cibernético. Dessa forma, trazer o setor privado para o debate cibernético, como ocorre em países aliados, em especial os Estados Unidos, é o maior desafio do Japão na consolidação de uma segurança e de uma defesa cibernéticas mais dinâmicas e adaptadas às realidades nacional e internacional.

Por fim, assim como 2011 representa um ponto de virada no comportamento ciberdefensivo japonês em face aos ataques sofridos naquele ano, o Japão parece estar em outro momento de virada desde 2022 por conta da Guerra da Ucrânia. Quanto a isso, contudo, ainda há de se esperar para entendermos as reais mudanças que ocorrerão na política japonesa envolvendo o ciberespaço, mas desde a eclosão do conflito o Japão passou a adotar um tom mais rigoroso em seus documentos e objetivos estratégicos, tanto em termos tradicionais quanto em termos cibernéticos. Esse temor não só envolve a atuação maliciosa da Rússia no ciberespaço com suas guerras híbridas e de informação, como também o tipo de influência que isso poderia ter sobre demais países securitizados pelo Japão, em especial a China. A próxima *Cybersecurity Strategy* japonesa, a ser lançada provavelmente no segundo semestre de 2024, certamente contará com um mesmo tom taxativo contra a Rússia, sua atuação internacional e o tipo de interferência que isso pode causar no Leste Asiático como vem sendo observado nas estratégias nacionais do Japão tais como a NSS e seus Livros Brancos de Defesa.

Nesse sentido, apesar da incerteza daquilo que está por vir, espera-se que o Japão leve adiante seu comportamento tradicional de alinhamento à potência do dia e se mantenha próximo dos Estados Unidos quanto a políticas (ciber)securitárias, bilateralismo o qual permanece constante e relevante desde a década de 1950. Em contrapartida, com ou sem reforma constitucional, calculo que a proatividade japonesa no tema securitário não tem previsão para acabar, visto que desde o fim da Guerra Fria o Japão tem explicitado seu novo comportamento proativo a fim de modernizar seu então frágil e dependente sistema de defesa nacional. Isso posto, o governo japonês continuará ampliando sua ciberdefesa a nível governamental, nacional e sistêmico para atingir seus objetivos cibernéticos.

REFERÊNCIAS

AKIMENKO, Valeriy; GILES, Keir. Russia's Cyber and Information Warfare. *Asia Policy*, vol. 15, n. 2, pp. 67– 75, 2020.

ALSABAH, Nabil. China's Quest for Cybersecurity Causes Headache for Foreign Companies. The Diplomat, 2017. Disponível em: <thediplomat.com/2017/03/chinas-quest-for-cybersecurity-causes-headache-for-foreign-companies/>. Acesso em 07 mar. 2023.

BARLETT, Benjamin. Japan: An Exclusively Defense-Oriented Cyber Policy. *Asia Policy*, vol. 15, n. 2, pp. 93– 100, 2020.

BOSCHI, Alysson Araldi. A Estratégia de Segurança Nacional do Japão entre 2013 e 2022: ponto de inflexão na segurança internacional japonesa? *Monções: Revista de Relações Internacionais da UFGD*, vol. 11, n. 22, pp. 1–28, 2022. Disponível em: <https://ojs.ufgd.edu.br/index.php/moncoes/article/view/14510/9255>. Acesso em: 04 mar. 2023.

BUNDESWEHR. *Kommando Cyber- und Informationsraum*. (s.d.). Disponível em: <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum>. Acesso em: 19 fev. 2023.

CABINET SECRETARIAT. *Cabinet Decision on Development of Seamless Security Legislation to Ensure Japan's Survival and Protect its People*. 2014. Disponível em: <https://www.cas.go.jp/jp/gaiyou/jimu/pdf/anpohosei_eng.pdf>. Acesso em 19 mar. 2023.

CAVELTY, Myriam Dunn; FISCHER, Sophie-Charlotte; BALZACQ, Thierry. 'Killer robots' and preventive arms control. In: CAVELTY, Myriam Dunn; BALZACQ, Thierry (eds.). *Routledge Handbook of Security Studies*. Abingdon: Routledge, 2017.

CENTRO NACIONAL DE CIBERSEGURANÇA (CNCS). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. 2019. Disponível em: <https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf >. Acesso em: 25 jul. 2022.

CONTI, Gregory; NELSON, John; RAYMOND, David. Towards a Cyber Common Operating Picture. In: PODINS, K.; STINISSEN, J.; MAYBAUM, M. (eds.). *5th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications, 2013.

CHUGROV, Sergey V. Postaw Rleations between the USSR and Japan from the Late 1940s to the 1950s. In: STRELTSOV, Dmitry; NOBUO, Shimotomai (eds.). *A History of Russo-Japanese Relations:* Over Two Centuries of Cooperation and Competition. Leiden; Boston: Brill, 2019.

CYBERSECURITY STRATEGIC HEADQUARTERS (CSSH). *Guideline for*

Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure. 2019a. Disponível em: <https://www.nisc.go.jp/eng/pdf/principles_ci_eng_v5_r1.pdf>. Acesso em: 07 abr. 2023.

CYBERSECURITY STRATEGIC HEADQUARTERS (CSSH). *Risk Assessment Guide Based on the Concept of Mission Assurance in Critical Infrastructure*. 2019b. Disponível em: <https://www.nisc.go.jp/eng/pdf/guide_ci_eng_r1.zip>. Acesso em: 07 abr. 2023.

CYBERSECURITY STRATEGIC HEADQUARTERS (CSSH). *The Cybersecurity Policy for Critical Infrastructure Protection*. 2022. Disponível em: <https://www.nisc.go.jp/eng/pdf/cip_policy_2022_eng.pdf>. Acesso em: 05 abr. 2023.

DARÓZ, Carlos Roberto Carvalho. Guerra Russo-Japonesa: a preparação das Forças Armadas Imperiais do Japão. *Revista do IGHMB*, ano 77, n. 105, 2018.

DE WITTE, Melissa. *War never really ended in Asia, says Stanford scholar*. Stanford News, 2020. Disponível em: <https://news.stanford.edu/2020/08/27/war-never-really-ended-asia/#:~:text=September%202%2C%201945%2C%20is%20recognized,strains%20in%20diplomatic%20relations%20today>. Acesso em 02 jan. 2023.

DW BRASIL. Como os alemães aprendem sobre o Holocausto? Youtube, 23 mai. 2022. Disponível em: <https://www.youtube.com/watch?v=JsiexlRNZ5E>. Acesso em 03 jan. 2023.

DW BRASIL. Os últimos julgamentos de nazistas na Alemanha. Youtube, 02 jan. 2023. Disponível em: <https://www.youtube.com/watch?v=Dt5ddHuo8Bg>. Acesso em 04 jan. 2023.

FARLEY, Robert. *Why Post-WWII Reconciliation Failed in East Asia: The legacy of the war endures, impacting modern regional relations*. The Diplomat, 2015. Disponível em: <https://thediplomat.com/2015/12/why-post-wwii-reconciliation-failed-in-east-asia/>. Acesso em 3 jan. 2023.

FIERKE, Karin Marie. *Critical Approaches to International Security*. 2ª ed. Cambridge: Polity Press, 2015.

GADY, Franz-Stefan. Japan: the Reluctant Cyberpower. *Asie. Visions*, n. 91, Ifri, 2017.

GRINYUK, Vladimir A.; SHULATOV, Yaroslav A.; LOZHKINA, Anastasia S. Soviet-Japanese Relations in the 1920s: from Hostility to Coexistence. In: STRELTSOV, Dmitry; NOBUO, Shimotomai (eds.). *A History of Russo-Japanese Relations:* Over Two Centuries of Cooperation and Competition. Leiden; Boston: Brill, 2019.

GRISHACHEV, Sergey V. Russo-Japanese Relations in the 18th and 19th Centuries: Exploration and Negotiation. In: STRELTSOV, Dmitry; NOBUO, Shimotomai (eds.). *A History of Russo-Japanese Relations:* Over Two Centuries of Cooperation and Competition.

Leiden; Boston: Brill, 2019.

HARUKO, Ozawa. Soviet-Japanese Relations and the Principle of the "Indivisibility of Politics and Economics". In: STRELTSOV, Dmitry; NOBUO, Shimotomai (eds.). *A History of Russo-Japanese Relations:* Over Two Centuries of Cooperation and Competition. Leiden; Boston: Brill, 2019.

HATHAWAY, Melissa et al. *Japan Cyber Readiness at a Glance*. Potomac Institute for Policy Studies, 2016.

HATHAWAY, Melissa; KLIMBURG, Alexander. Preliminary considerations: on national cyber security. In: KLIMBURG, Alexander (ed.). *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE Publication, 2012.

HIDETAKE, Kawaraji. Japanese-Russian Relations in the 21st Century. In: STRELTSOV, Dmitry; NOBUO, Shimotomai (eds.). *A History of Russo-Japanese Relations:* Over Two Centuries of Cooperation and Competition. Leiden; Boston: Brill, 2019.

HOOK, Glenn D.; GILSON, Julie; HUGHES, Christopher W.; DOBSON, Hugo. *Japan's International Relations: Politics, economics and security*. 3ª ed. Abingdon: Routledge, 2012.

INFORMATION-TECHNOLOGY PROMOTION AGENCY (IPA). *Industrial Cyber Security Center of Excellence (ICSCoE).* S.d. Disponível em: <https://www.ipa.go.jp/icscoe/english/index.html>. Acesso em: 29 jan. 2023

JAPAN COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTER (JPCERT/CC). *About JPCERT/CC*. 2022. Disponível em: <https://www.jpcert.or.jp/english/about/>. Acesso em: 23 jan. 2023

JAPAN INSTITUTE FOR LABOUR POLICY AND TRAINING (JILPT). 「第 7 回勤労生活に関する調査」結果 *("Dai 7-kai kinrō seikatsu ni kansuru chōsa" kekka).* 2019. Disponível em: <https://www.jil.go.jp/press/documents/20160923.pdf>. Acesso em: 08 abr. 2023.

JAPAN INTERNATIONAL COOPERATION AGENCY (JICA). 2021. *Installation of Equipment for DDoS Attack Mitigation System*. Disponível em: <https://www.jica.go.jp/project/english/vietnam/052/news/general/210313.html>. Acesso em 17 mai. 2022.

JERVIS, Robert. *Perception and Misperception in International Politics*. Princeton: Princeton University Press, 1976.

JESUS JUNIOR, Helvécio de. *Rumo ao "estado normal": a Política de Defesa do*

Japão desde o Fim da Guerra Fria. Dissertação de Mestrado em Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro, 2008.

KALLENDER, Paul. Japan, the Ministry of Defense and Cyber-Security. *The RUSI Journal*, vol. 159, n. 1, pp. 94–103, 2014.

KALLENDER, Paul; HUGHES, Christopher W. Japan's Emerging Trajectory as a "Cyber Power": From Securitization to Militarization of Cyberspace. *Journal of Strategic Studies*, 2016.

KATAGIRI, Nori. From cyber denial to cyber punishment: What keeps Japanese warriors from active defense operations? *Asian Security*, vol. 17, n. 3, 2021.

KEOHANE, Robert; NYE, Joseph. Power and Interdependence. In BETTS, Richard. *Conflict after the Cold War*. Pearson, 2008.

KLIMBURG, Alexander; HEALEY, Jason. Strategic Goals & Stakeholders. In: KLIMBURG, Alexander (ed.). *National Cyber Security Framework Manual*. NATO Cooperative Cyber Defence Centre of Excellence, 2012.

KOSHINO, Yuka; GADY, Franz-Stefan. Japan and cyber capabilities: how much is enough? *Military Balance Blog*, International Institute for Strategic Studies, 2020. Disponível em: <https://www.iiss.org/online-analysis//military-balance/2020/08/japan-cyber-capabilities>. Acesso em: 12 abr. 2023.

KOSUKE, Takahashi. *Japan Needs a Cyber Ministry: Former JGSDF Major General*. The Diplomat, 2022. Disponível em: <https://thediplomat.com/2022/09/japan-needs-a-cyber-ministry-former-jgsdf-major-general/>. Acesso em: 04 abr. 2023.

KRAVTSEVICH, Andrey I. Soviet-Japanese Relations during World War II: the Origins of Territorial Dispute. In: STRELTSOV, Dmitry; NOBUO, Shimotomai (eds.). *A History of Russo-Japanese Relations:* Over Two Centuries of Cooperation and Competition. Leiden; Boston: Brill, 2019.

KSHETRI, Nir. Japan's Changing Cybersecurity Landscape. *Computer*, vol. 47, n. 1, pp. 83–86, 2014.

KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, Franklin D.; STARR, Stuart; WENTZ, Larry K (eds.). *Cyberpower and National Security*. Washington D.C.: National Defense UP, 2009

KUHARA, Sonoko. Can the US-Japan Alliance Handle Cyberattacks? *The Diplomat*, 25 fev. 2020. Disponível em: <https://thediplomat.com/2020/02/can-the-us- japan-alliance-handle-cyberattacks/>. Acesso em 13 mai. 2022.

KUSHNER, Barak. *Men to Devils, Devils to Men*: Japanese War Crimes and Chinese

Justice. Cambridge: Harvard University Press, 2015.

KYŌDŌ TSŪSHINSHA. サイバー部隊、5000人へ拡充　防衛省、27年度5倍超に (*Saibā butai, 5000 hito e kakujū bōeishō, 27-nendo 5-bai-chō ni*). 2022. Dísponível em: <https://www.47news.jp/8505741.html>. Acesso em: 19 fev. 2023.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Fundamentos de Metodologia Científica*. São Paulo: Atlas, 2003.

LEITE, Alexandre César Cunha; OLIVEIRA, Ahmina Raiara Solsona. "Conflitos Cibernéticos: um overview sobre a participação asiática recente". Boletim Meridiano 47, vol. 15, n. 144, pp. 3–9, 2014.

LEWIS, James Andrew. *U.S.-Japan Cooperation in Cyberspace*. Center for Strategic & International Studies, 2015.

LUIIJF, Eric; BESSELING, Kim. Nineteen national cyber security strategies. *Int. J. Critical Infrastructures*, vol. 9, n. 1–2, pp. 3–31, 2013.

LUKOYANOV, Igor V. Russia and Japan in the Late 19th to 20th Centuries: the Road to War and Peace. In: STRELTSOV, Dmitry; NOBUO, Shimotomai (eds.). *A History of Russo-Japanese Relations:* Over Two Centuries of Cooperation and Competition. Leiden; Boston: Brill, 2019.

MATSUBARA, Mihoko. A Glimpse into Private-Sector Cybersecurity in Japan. *Lawfare*, 2018a. Disponível em: <https://www.lawfareblog.com/glimpse-private-sector-cybersecurity-japan>. Acesso em: 08 abr. 2023.

MATSUBARA, Mihoko. How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace. *Council on Foreign Relations*, 2018b. Disponível em: <https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace>. Acesso em: 03 abr. 2023.

MATSUBARA, Mihoko. Tokyo 2020 and Japan's ongoing cybersecurity efforts. In: MATSUBARA, Mihoko; MOCHINAGA, Dai. *Japan's Cybersecurity Strategy:* From the Olympics to the Indo-Pacific. Asie.Visions, n. 119, 2021.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. *The Fundamental Conceptual Trinity of Cyberspace*. Contexto Internacional, vol. 42, n. 1, 2020.

MIN, Kyoung-Sik; CHAI, Seung-Woan; HAN, Mijeong. "International Comparative Study on Cyber Security Strategy". International Journal of Security and Its Applications, vol. 9, n. 2, pp. 13–20, 2015.

MINISTÉRIO DA DEFESA. Doutrina Militar de Defesa Cibernética. MD31-M- 07,

2014. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf>. Acesso em: 14 jul. 2022.

MINISTRY OF DEFENSE (MOD). *Toward Stable and Effective Use of Cyberspace*. 2012. Disponível em: <https://warp.da.ndl.go.jp/info:ndljp/pid/11591426/www.mod.go.jp/e/d_act/others/pdf/stable_and_effective_use_cyberspace.pdf>. Acesso em: 29 mar. 2023.

MINISTRY OF DEFENSE (MOD). *Defense of Japan*. 2021. Disponível em: <https://www.mod.go.jp/en/publ/w_paper/wp2021/DOJ2021_EN_Full.pdf>. Acesso em: 17 jul. 2022.

MINISTRY OF DEFENSE (MOD). *Defense of Japan*. 2022. Disponível em: <https://www.mod.go.jp/en/publ/w_paper/wp2022/DOJ2022_EN_Full_02.pdf>. Acesso em: 27 jul. 2022.

MINISTRY OF FOREIGN AFFAIRS OF JAPAN (MOFA). *Adoption of the new "National Security Strategy (NSS)". (Statement by Foreign Minister HAYASHI Yoshimasa)*. 2022a. Disponível em: <https://www.mofa.go.jp/press/release/press4e_003192.html>. Acesso em: 22 jan. 2023.

MINISTRY OF FOREIGN AFFAIRS OF JAPAN (MOFA). *Japan-U.S. Security Treaty*. 1960. Disponível em: <https://www.mofa.go.jp/region/n-america/us/q&a/ref/1.html>. Acesso em 13 mai. 2022.

MINISTRY OF FOREIGN AFFAIRS OF JAPAN (MOFA). *Japan-U.S. Security Consultative Committee (Japan-U.S. "2+2")*. 2019. Disponível em: <https://www.mofa.go.jp/na/fa/page3e_001008.html>. Acesso em 13 mai. 2022.

MINISTRY OF FOREIGN AFFAIRS OF JAPAN (MOFA). *National Security Strategy*. 2013. Disponível em: <https://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf>. Acesso em: 05 fev. 2023.

MINISTRY OF FOREIGN AFFAIRS OF JAPAN (MOFA). *Northern Territories Issue*. S.d. Disponível em: <https://www.mofa.go.jp/region/europe/russia/territory/overview.html>. Acesso em: 04 mar. 2023.

MINISTRY OF FOREIGN AFFAIRS OF JAPAN (MOFA). *National Security Strategy of Japan*. 2022b. Disponível em: <https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf>. Acesso em: 22 jan. 2023.

MINISTRY OF FOREIGN AFFAIRS OF JAPAN (MOFA). *Official Development Assistance (ODA)*. 2022c. Disponível em:

<https://www.mofa.go.jp/policy/oda/page22_001434.html>. Acesso em 29 dez. 2022.

MINISTRY OF FOREIGN AFFAIRS OF JAPAN (MOFA). *White Paper on Development Cooperation 2017*. 2017. Disponível em: <https://www.mofa.go.jp/files/000406636.pdf>. Acesso em 29 dez. 2022.

MINISTRY OF JUSTICE (MOJ). *The Basic Act on Cybersecurity*. Japanese Law Translation, 2014. Disponível em: <https://www.japaneselawtranslation.go.jp/en/laws/view/3677>. Acesso em: 14 jul. 2022.

NAÇÕES UNIDAS. *Estudo da ONU revela que mundo tem abismo digital de gênero*. ONU News, 2019. Disponível em: <https://news.un.org/pt/story/2019/11/1693711>. Acesso em 16 jul. 2021.

NATIONAL CENTER OF INCIDENT READINESS AND STRATEGY FOR CYBERSECURITY (NISC). *About NISC*. S.d. Disponível em: <https://www.nisc.go.jp/eng/index.html#sec1>. Acesso em 12 abr. 2022.

NATIONAL CENTER POR INCIDENT READINESS AND STRATEGY FOR CYBERSECURITY (NISC). *Cybersecurity Strategy*. Cabinet Office, 2015. Disponível em: <https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf>. Acesso em 23 jun. 2022.

NATIONAL CENTER POR INCIDENT READINESS AND STRATEGY FOR CYBERSECURITY (NISC). *Cybersecurity Strategy*. Cabinet Office, 2018. Disponível em: <https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf>. Acesso em 23 jun. 2022.

NATIONAL CENTER POR INCIDENT READINESS AND STRATEGY FOR CYBERSECURITY (NISC). *Cybersecurity Strategy*. Cabinet Office, 2021. Disponível em: <https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf>. Acesso em 23 jun. 2022.

NATIONAL POLICE AGENCY (NPA). *Arrests and Consultations of Cybercrime in 2003*. S.d. Disponível em: <https://bit.ly/3IWPepk>. Acesso em 22 jul. 2022.

NATIONAL POLICE AGENCY (NPA). サイバー犯罪の現状 *(Saibā hanzai no genjō)*. 2022. Disponível em: <https://www.npa.go.jp/hakusyo/h23/honbun/html/1-toku2_1_1.html#:~:text=サイバー犯罪の検挙件数,過去最高となった。>. Acesso em 19 fev. 2023.

NITTA, Yoko. *Japan's Approach Towards International Strategy on Cyber Security Cooperation*. Japan Science and Technology Agency, Research Institute of Science and Technology for Society, 2013.

NITTA, Yoko. Review of the Japan Cybersecurity Strategy. *ISPSW Strategy Series:*

Focus on Defense and International Security, vol. 290, 2014.

NOBUO, Shimotomai. The Rise to Power of Mikhail Gornachev and the Policy of "Expanding Equilibrium". In: STRELTSOV, Dmitry; NOBUO, Shimotomai (eds.). *A History of Russo-Japanese Relations:* Over Two Centuries of Cooperation and Competition. Leiden; Boston: Brill, 2019.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Development Co-operation Profiles: Japan*. S.d.a. Disponível em: <https://www.oecd-ilibrary.org/sites/b8cf3944-en/index.html?itemId=/content/component/b8cf3944-en>. Acesso em 29 dez. 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Official development assistance (ODA)*. S.d.b. Disponível em: <https://www.oecd.org/dac/financing-sustainable-development/development-finance-standards/official-development-assistance.htm>. Acesso em 29 dez. 2022.

OWENS, Neil J. Japan's Strategic Renaissance: Implications for US Policy in the Asia-Pacific. In: LAI, David; TROXELL, John F.; GELLERT, Frederick J. (ed.). *Avoiding the Trap*: US Strategy and Policy for Competing in the Asia-Pacific Beyond the Rebalance. Carlisle: United States Army War College Press, 2018.

NYE, Joseph S. *Cyber Power*. Belfer Center for Science and International Affairs, 2010.

OLIVEIRA, Alana Camoça Gonçalves de; FERNANDES, Felipe Gusmão Carioni. O raiar do sol no Sudeste Asiático: a projeção japonesa no Mar do Sul da China e seus interesses estratégicos. *Revista da Escola de Guerra Naval*, vol. 5, n. 2, 2019, p. 449–491.

OLIVEIRA, Eliézer Rizzo de. O Brasil diante da guerra contra o Iraque. *Jornal da Unicamp*, 2003. Disponível em: https://www.unicamp.br/unicamp/unicamp_hoje/jornalPDF/208-pag05.pdf>. Acesso em 23 mai. 2022.

PAGANINI, Pierluigi. *Japan is investigating security breach of Defence Information Infrastructure*. Security Affairs, 2016. Disponível em: <https://securityaffairs.co/53856/cyber-warfare-2/defence-information-infrastructure-breach.html>. Acesso em: 25 jan. 2023.

PAGLIARI, Graciela de Conti; AYRES PINTO, Danielle Jacon; VIGGIANO, Juliana. Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratégica: Um estudo prospectivo. In: OLIVEIRA, Marcos Aurélio Guedes de (org.). *Defesa cibernética e mobilização nacional*. Recife: Editora UFPE, 2020.

PESTUSHKO, Yuril S.; SHULATOV, Yaroslav A. Russo-Japanese Relations from 1905 to 1916: from Enemies to Allies. In: STRELTSOV, Dmitry; NOBUO, Shimotomai (eds.).

A History of Russo-Japanese Relations: Over Two Centuries of Cooperation and Competition. Leiden; Boston: Brill, 2019.

PINKSTON, Daniel A. North Korea's Objectives and Activities in Cyberspace. *Asia Policy*, vol. 15, n. 2, pp. 76– 83, 2020.

POPPER, Karl. *A lógica da pesquisa científica*. São Paulo: Cultrix, 1975.

RID, Thomas. Cyber War Will Not Take Place. *Journal of Strategic Studies*, vol. 35, n. 1, pp. 5–32, 2012.

RYŪHEI, Hatsuse. Pan-Asianism in international relations: prewar, postwar, and present. In: SAALER, Sven; KOSCHMANN, Victor J. (eds.). *Pan-Asianism in Modern Japanese History*: Colonialism, regionalism and borders. Abingdon: Routledge, 2007.

SAALER, Sven. Pan-Asianism in modern Japanese history: overcoming the nation, creating a region, forging an empire. In: SAALER, Sven; KOSCHMANN, Victor J. (eds.). *Pan-Asianism in Modern Japanese History*: Colonialism, regionalism and borders. Abingdon: Routledge, 2007.

SAHASHI, Ryo. *Japan's Vision for the East Asian security order*. East Asia Forum, 2016. Disponível em: <https://www.eastasiaforum.org/2016/02/23/japans-vision-for-the-east-asian-security-order/>. Acesso em: 19 mar. 2023.

SAMUEL, Cherian; SHARMA, Munish (eds.). "Securing Cyberspace: International and Asian Perspectives". Pentagon Press, 2016.

SAINT-PIERRE, Héctor Luis. *Política de defesa e relações internacionais no Brasil:* o destinos das paralelas. In: XXVI International Congress of Latin American Studies, 2006.

SCHMIDT, Brian C. On the History and Historiography of International Relations. In: CARLSNAES, Walter; RISSE, Thomas; SIMMONS, Beth A. *Handbook of International Relations*. Londres: SAGE, 2013, 2a. ed.

SCHUETZE, Julia. Japan's cybersecurity policy: an introduction. *Research in Focus*, EU Cyber Direct, 2020.

SCHUMACHER, Daniel. Asia's 'Boom' of Difficult Memories: Remembering World War Two Across East and Southeast Asia. *History Compass*, vol. 13, n. 11, pp. 560–577, 2015.

SEGAL, Adam. China's Pursuit of Cyberpower. *Asia Policy*, vol. 15, n. 2, pp. 60– 66, 2020.

SHIN, Hyonhee. *North Korea says U.S. is setting up Asian NATO; vows stronger defence*. Reuters, 2022. Disponível em: <https://www.reuters.com/world/asia-pacific/north-korea-says-us-is-setting-up-asian-nato-vows-stronger-defence-2022-06-27/>. Acesso em: 28 dez. 2022.

SIRIPALA, Thisanka. Japanese Companies Fall Victim To Unprecedented Wave of Cyber Attacks. *The Diplomat*, 23 dez. 2020. Disponível em: <https://thediplomat.com/2020/12/japanese-companies-fall-victim-to-unprecedented-wave-of-cyber-attacks/>. Acesso em 13 fev. 2023.

SOESANTO, Stefan. *Comparing the Cyber Defense Postures of Japan, the Netherlands and the United States in Peace Time*. Konrad Adenauer Stiftung, n. 449, 2021.

SOESANTO, Stefan. *Japan's National Cybersecurity and Defense Posture*: Policy and Organizations. Center for Security Studies, ETH Zurich, 2020.

TAKEDA, Keiji. Cyber Defense of Japan - Proposal of Conceptual Framework. In: GAYCKEN, Sandro (ed.). *Cyber Defense - Policies, Operations and Capacity Building*. Amsterdam: IOS Press BV, 2019.

THE NEW YORK TIMES (NYT). *Hirohito quit Yasukuni Shrine visits over concerns about war criminals*. 2007. Disponível em: <https://www.nytimes.com/2007/04/26/world/asia/26iht-japan.1.5447598.html>. Acesso em 27 dez. 2022.

THOMAS, Nicholas. Cyber Security in East Asia: Governing Anarchy. *Asian Security*, vol. 5, n. 1, pp. 3–23, 2009.

TICKNER, Judith Ann. You Just Don't Understand: Troubled Engagements between Feminists and IR Theorists. *International Studies Quarterly*, vol. 41, n. 4, pp. 611– 632, 1997.

TOGO, Kazuhiko. O Japão e as novas estruturas de segurança do multilateralismo asiático. In: CALDER, Kent E.; FUKUYAMA, Francis. (ed.). *Multilateralismo na Ásia Oriental*: Perspectivas para a estabilidade regional. Rio de Janeiro: Rocco, 2008.

WAKABAYASHI, Bob Tadashi. *The Nanking atrocity, 1937–38: complicating the picture*. Oxford: Berghahn Books, 2007.

WALTZ, Kenneth. *Theory of International Politics*. Reading: Addison-Wesley Publishing Company, 1978.

WELCH, David. Embracing Normalcy: Toward a Japanese 'National Strategy'. In: SOEYA, Yoshihide; TADOKORO, Masayuki; WELCH, David (eds.). *Japan as a Normal Country?* A Nation in Search of Its Place in the World. Toronto: University of Toronto Press, 2011.

WENDT, Alexander. Anarchy is What States Make of It: The Social Construction of Power Politics. *International Organization*, vol. 46, n. 2, pp. 391–425, 1992.

WORK, Robert; GRANT, Greg. Beating the Americans at their Own Game: An Offset Strategy with Chinese Characteristics. Washington D.C.: Center for a New Security, 2019.

YOKOHAMA, Shin'ichi. *Business Management and Cybersecurity*: Digital Resiliency for Executives. NTT Corporation, 2018. Disponível em: <https://group.ntt/en/topics/CfBE2018/pdf/201803_Business_Management_and_Cybersecurity.pdf>. Acesso em: 08 abr. 2023.