10.21544/2359-3075.v28n2.c

AUKUS, NPT AND PROSUB

Alvaro Augusto Dias Monteiro [1]
José Augusto Abreu de Moura[2]

ABSTRACT

The AUKUS partnership foresees an effort by the United States of America and the United Kingdom to provide Australia, a non-nuclear-armed country such as Brazil, with conventional nuclear-powered submarines, which requires complex negotiations with the International Atomic Energy Agency (IAEA), having raised proposals to avoid the weakening of the nuclear non-proliferation regime. Such a situation could affect the political conditions of Brazil's recently begun negotiations with the IAEA. In order to evaluate such possibilities, the conditions for the creation of AUKUS are analyzed in strategic and non-proliferation terms through documentary research, as well as two of the aforementioned proposals, one that provides for the debate of the issue by the Member States of the Agency and another that provides for requirements to be met by states claiming such naval means. As a result, the former may raise questions about the Brazilian program, and the latter proves to be inappropriate as a general standard, as it implies dependence on nuclear-armed states. The conclusion is that the Brazilian bodies involved, having now started negotiations with the Agency, should follow the developments of the AUKUS partnership and be prepared to defend the program in the relevant forums.

Keywords: AUKUS; Australia; United Kingdom; United States United States of America; INFCIRC / 965.

[1] Postgraduate Program in Maritime Studies (PPGEM) of the Naval War College (EGN), Rio de Janeiro — RJ, Brazil. Email: alvaroadmonteiro@yahoo.com.br - ORCID http://orcid.org/0000-0002-8922-5008.

[2] Center for political and Strategic Studies of the Brazilian Navy (CEPE-MB), Rio de Janeiro; Strategic Studies Institute, Federal Fluminense University (INEST-UFF), Niterói— RJ, Brazil. Email: jaamourad38@gmail.com - ORCID http://orcid.org/0000-0001-6474-5632.

INTRODUCTION[3]

On September 15, 2021, through a joint statement, the president of the United States of America (USA), Joe Biden, and the Prime Ministers of the United Kingdom (UK), Boris Johnson, and Australia, Scott Morrison, announced the creation of a "strengthened trilateral security partnership" called AUKUS, an acronym for the names of the three states, whose purpose, according to the declaration itself, would be to "deepen diplomatic, security and defense cooperation in the Indo-Pacific region", [...] "to meet the challenges of the Twenty-First Century".

The remarkable aspect of this partnership, already highlighted in this first declaration, consists of the effort of the two powers to provide the Australian Navy with nuclear-powered submarines (The White House, 2021). This represents a paradigm shift and a historical political shift of the US, which, with the exception of the UK, has never supported the acquisition of such naval means by other states, even allies.

With the British, on the contrary, they have cooperated widely since 1958, when they signed the Agreement between the UK and the USA for Cooperation in The Uses of Atomic Energy for Mutual Defense Purposes, by which they have already provided the propulsion plant for their first nuclear-powered submarine and the enriched uranium necessary for the production of fuel to operate it for the first ten years (United Kingdom, 2014; BAE, 2022).

AUKUS caused the cancellation of the large contract, signed in 2019, by Australia with the French state *Naval Group* (Gady, 2019), for the construction of 12 diesel-electric propulsion submarines, which was felt by France as a betrayal, provoking strong expressions of displeasure from authorities of its government (Wood, 2021).

Such a partnership, along with other US initiatives, has the clear purpose of increasing the US ability to deter China, whose naval power is expanding, as part of the construction of the "world-class armed forces" announced by its leader Xi Jinping, with a view to full Chinese projection in the Indo-Pacific region (Shoebridge, 2021).

It is important to note that Australia is a "Non-Nuclear Weapons State" (NNWS), according to the classification of the Treaty on the Non-

[3] This article was produced under the project PROCAD-DEF20191325566P of the Coordination for the improvement of Higher Education Personnel (CAPES). The perspectives, opinions and conclusions presented in it are the sole responsibility of the authors, and should not be interpreted as having the support or endorsement of any organ or policy of the Brazilian government.

Proliferation of nuclear weapons (NPT) (United Nations Office for Disarmament Affairs, 2022, art. III and IX). Although the operation of nuclear-powered submarines by such states is not prohibited by this treaty, the arrangements and understandings with the International Atomic Energy Agency (IAEA) are extremely complex (Rockwood, 2017), for the reason explained in the next topic, a circumstance that directly affects Brazil.

This is because, until the launch of the partnership, Brazil was the closest state to facing such a problem, as it was the only NNWS that conducted a program for the development of a conventionally armed nuclear-powered submarine (CNPS[4]), the submarine program (PROSUB). Thus, AUKUS, in addition to taking away the uniqueness of the Brazilian initiative, may also end its pioneering, if Australia obtains its submarine in the shortest term, although, with regard to nuclear propulsion, there is a significant difference between these two initiatives, since the Brazilian is totally indigenous — Brazil's agreement with France in PROSUB does not involve nuclear propulsion. In addition — what is more important and was the problem that motivated this study — to what extent can this partnership cause changes in the political conditions that will shape the country's understandings with the IAEA, now in its early stages?

Thus, this work has the main purpose of analyzing some aspects, considered more relevant by the authors, that involve the launch of AUKUS, its developments and its effective achievement through the delivery of the first CNPS to Australia, both in the political scope of the NPT, treaty that constitutes the theoretical basis of this article, and in the strategic, from the convergence, previously not so well characterized, of Australia's national security interests with those of the United States, in its hegemonic competition with China, to its influence on the Nuclear Non-Proliferation Regime (NNPR), in that this affects the current PROSUB momentum.

In this sense, initially, the aspects related to the scope of the partnership are analyzed, with regard to the interaction with the dictates of the NPT, as well as with its implementation in the plan of relations between the partners, on the basis of the agreements with the IAEA providing about the commitments of the States Parties to the Treaty. It is worth considering that the prospect of Australia obtaining CNPS, with the support of the US and UK, provoked reactions in defense of the NNPR,

[4] Term by which the Brazilian Navy began to classify nuclear attack submarines, known in the English literature as SSN. This new designation is intended to mark its difference from the nuclear-armed ballistic missile-launching submarines, the SSBN, employed by the powers that possess such weapons.

two of which, issued by influential actors, are analyzed in this article.

Next, we analyze how Australia's submarine force, whose planned renewal was conditioned by the limits of its National Defense, became the main object of the creation of the partnership in question, tending to become, in the future, a major player in the Indo-Pacific region. This analysis considered the data contained in the Australians defense white papers[5] (WP) from 2009 to 2020 and the AUKUS agreements.

Finally, the Brazilian conditions for meeting the aforementioned requirements are analyzed, comparing them with those of Australia, which shows a radical difference between these two countries. The implications for Brazil of the two reactions mentioned are also analyzed, which presupposes a probable emergence of questions about the Brazilian CNPS program.

The conclusion seeks to situate AUKUS in the context of global hegemonic competition, highlighting: the ascendancy of the strategic needs arising from it on the non-proliferation of nuclear weapons; the impropriety of the requirements proposed as a general standard; and the convenience for Brazil, having already started in the understandings with the IAEA, to monitor the development of the partnership and prepare its representatives for the defense of PROSUB against probable questions.

AUKUS AND THE NPT

The NPT, issued in 1968 and in force since 1970, divided States Parties into two groups: those that had detonated a nuclear device by 01/01/1967 (the "Nuclear Weapons States" - NWS); and the others, the NNWS, already mentioned (United Nations Office for Disarmament Affairs, 2022, art. III and IX). The latter, by acceding to the Treaty, undertake not to receive, transfer or produce nuclear weapons or explosives, as well as to sign a "Comprehensive Safeguards Agreement" (CSA) with the IAEA, by which this agency applies safeguards to all nuclear material in the territory, under the jurisdiction or under the control of the state, with the objective of verifying that the commitment assumed is being effectively fulfilled; that is, that part of this material is not diverted for the manufacture of nuclear weapons or nuclear explosive devices. Safeguards are defined as

[5] Defense White Papers are the public documents in which states, which prepare them, seek to confer transparency on the activities of their defense sectors.

> "a set of technical measures applied by the IAEA on nuclear material and activities through which the agency seeks to independently verify that nuclear facilities are not misused and nuclear material is not diverted from peaceful uses. States accept these measures through the conclusion of safeguards agreements" (International Atomic Energy Agency, 2022)

The terms of the CSA are those contained in the INFCIRC /153 (corrected) document[6] of 1972 (International Atomic Energy Agency, 1972) for all NNWS except Argentina and Brazil, for which the requirements of document INFCIRC/435 of 1994 are met.

These two states constitute special cases of NNWS with regard to CSA, because their accession processes to the NPT were atypical. In 1991, when they were not yet States Parties to this treaty, they signed the Bilateral Agreement for the Exclusively Peaceful Uses of Nuclear Energy, creating the Common System of Accounting and Control of Nuclear Materials (SCCC). To manage it and implement the necessary verification actions in both countries, they created the Brazilian - Argentine Agency for Accounting and Control of Nuclear Materials (ABACC) (International Atomic Energy Agency, 1991).

That same year, the two states, ABACC and IAEA signed the Quadripartite agreement, which became INFCIRC/435 in 1994 (International Atomic Energy Agency, 1994). Its text was based on INFCIRC / 153 (corrected) and approved the bilateral agreement. Subsequently, after the accession of Argentina and Brazil to the NPT (respectively in 1995 and 1998), the IAEA recognized INFCIRC / 435 as the Comprehensive Safeguards Agreement (CSA), to be accomplished by both States (International Atomic Energy Agency, 1997; International Atomic Energy Agency, 2000), instead of INFCIRC/153 (corrected), applied to the other NNWS.

In turn, the five NWS — USA, UK, France, Russia and China, permanent members of the United Nations Security Council (UNSC) - do not sign CSA, but "voluntary offer agreements"(VOA), by which they offer only those facilities in whose material they admit the application of safeguards (those intended for peaceful uses), among which the IAEA selects those in which they will be effectively applied, with the

[6] INFCIRC is the term used by the IAEA for the documents by which that agency discloses its instructions and standards. It's short for "*Information Circular*".

aim of verifying whether the material in them remains used in peaceful activities (International Atomic Energy Agency, 2022a).

Despite being a "non — proscribed military activity", the operation of nuclear — powered submarines by the NNWS is considered harmful to the NNPR since it implies periods of interruption in the normal form of application of safeguards to which their fuel-produced with enriched uranium-is subjected. Such periods would begin on the occasion of a recharge (or the first charge) of the reactor, when the fuel was removed from the structure in which it is manufactured (which is subject to safeguards) and would end when, after its use in the submarine reactor (which is not subject to safeguards), it was placed in the tailings repository, where it would be safeguarded again.

It is worth considering, however, that there is a slight difference between the existing CSA regarding the periods of interruption of the application of safeguards. Under INFCIRC/153 (corrected) (paragraph 14), this is the "period of non-application of safeguards to nuclear material"; while under INFCIRC/435 (Article 13), adopted only by Argentina and Brazil, such periods are those in which "special procedures" agreed with the IAEA are employed and applied while the nuclear material is used for propulsion or in the operation of any vehicle, including submarines and prototypes (International Atomic Energy Agency, 1994; International Atomic Energy Agency, 1972; Rockwood, 2017).

It is therefore clear that only with regard to Argentina and Brazil there would, in fact, be no interruption at any time in the application of safeguards.

Several scholars, whose focus essentially considers what is contained in INFCIRC / 153 (corrected), consider the existence of these moments a "loophole" in the safeguards system (Kaplow, 2017; Acton, 2021), for preventing its application during the entire time, which would theoretically make it possible for the undetected diversion of part of it, leading to the manufacture of nuclear explosives.

However, paragraph 14 of INFCIRC/153 (corrected), and even Article 13 of INFCIRC/435 (International Atomic Energy Agency, 1994; International Atomic Energy Agency, 1972), stipulate only general conditions, which explains the complexity of negotiations with the IAEA to develop the necessary arrangements, in these periods, to minimize the risk of diversion of fissile material and, therefore, the fact that submarines built with nuclear propulsion belong only to states that do not have to comply with "comprehensive safeguards" — the NWS and India, which is

not a signatory to the NPT (Rockwood, 2017; Acton, 2021).

Specifically, in regard to this aspect, the AUKUS partnership statement predicts Australia will commit to:

> "adhering to the highest standards of safeguards, transparency, verification and accounting measures, to ensure the non-proliferation, safety and security of nuclear material and technology. Australia remains committed to fulfilling all of its obligations as a non-nuclear armed state, including with the International Atomic Energy Agency. Our three nations are deeply committed to sustaining our leadership in global nonproliferation." (The White House, 2021).

The first period of the citation states that, even though it has nuclear-powered submarines, Australia, in addition to meeting high standards of safeguards, intends to ensure non-proliferation; thus alluding to a solution to the "loophole", which would be the first NNWS to adopt. The second indicates that Australia will remain an NNWS – the submarines it obtains will not carry nuclear weapons, and are therefore CNPS, intended for naval warfare rather than nuclear deterrence. The latter, on the other hand, nods to the leadership of the three countries "in global nonproliferation", which implies that the above-mentioned solution to the "gap" will be obtained with the support of the power and reputation of the partners involved, thus making it possible to meet strategic needs that transcend the Australian context, as set out below.

THE STRATEGIC CONTOURS OF THE PARTNERSHIP

Australia's 2009 Defence White Paper (WP) provided for the "Force 2030", process by which the Australian government intended to structure its defence forces for the contingencies expected over the next two decades, as noted in the following paragraphs.

Among the strategic interests pointed out, the stability of Southeast Asia stood out, to reduce threats to its security and prevent it from serving as a means ("*conduit*") for the projection of military power over its territory by another country. In addition, Australia should also contribute to regional and global security by participating in coalitions, especially with the USA.

Thus, naval forces should prepare, primarily, for the establishment of control of sea areas, while, specifically, submarines should contribute to the defense of approaches to the country, even at considerable distances, as well as protect and support other forces. To this end, Australia's submarine force of six would be doubled.

The existing submarines, still in activity (July 2022), are conventional diesel-electric propulsion, Collins class, of Swedish design, although built in Australia between 1996 and 2003, whose size, 3.400 tons, gives them reasonable autonomy, in addition to being well equipped and armed, with US made MK-48 torpedoes and Sub-Harpoon anti-ship missiles (Willet, 2020), but which are at the end of their useful lives.

The new submarines to be obtained should have greater mobility, range and endurance than the Collins, with high operational readiness, able for short-notice contingencies, long transits and patrols. In addition to normal capabilities (attack on ships, anti-submarine warfare, mine-laying, data collection, etc.), should also be able to detect mines, support special operations (with infiltration and exfiltration of personnel), carry out strategic cruise missile attacks on land targets, operate unmanned underwater vehicles and perform secure communications in real time. Despite these high requirements, the Australian authorities aimed at their attendance within the possibilities of diesel-electric submarines, as they ruled out nuclear propulsion (Australian, 2009, p. 34, 35, 47, 60, 64, 70 and 81).

EXAMINANDO A PERSPECTIVA DAS POLÍTICAS PÚBLICAS NA ÁREA DE DEFESA CIBERNÉTICA: O CASO BRASILEIRO

RESUMO

Este artigo analisa a importância de políticas públicas voltadas para a ciberdefesa no Brasil no período de 2000 a 2023. A pergunta que norteia o texto é: como os governos do Brasil nesse período apresentaram seus objetivos de ciberdefesa em seus respectivos "Livros Brancos de Defesa Nacional", a Estratégia Nacional de Defesa de 2008 e 2020 e outros documentos de alto nível da defesa nacional, transformando-os em ações efetivas?

A metodologia adotada é a pesquisa exploratória, com abordagem qualitativa. A hipótese desta pesquisa é que embora tenha havido a criação de normas e o desenvolvimento de iniciativas que demonstrem a maior importância da defesa cibernética para o Brasil no século XXI, podemos verificar a falta de iniciativas marcadas pela concepção de políticas públicas de longo prazo. Este artigo está estruturado em três tópicos. O primeiro traz um debate sucinto sobre as políticas públicas na área de defesa. O segundo tópico analisa o desenvolvimento de normas e políticas públicas no Brasil voltadas para a defesa cibernética. O terceiro tópico apresenta algumas políticas adotadas e exemplos da capacidade cibernética obtida por este país.
Palavras-chave: Brasil; Defesa Cibernética; Políticas Públicas; Capacidade Cibernética.

REFERENCES

ALMEIDA, Carlos W. Política de defesa no Brasil: considerações do ponto de vista das políticas públicas. **Opinião Pública,** Campinas, v. 16, n. 1, p. 220-250, jun. 2010.

ARTICLE 19. **Desenvolvimento de políticas de cibersegurança e ciberdefesa na América do Sul** - Estudo de caso sobre a atuação governamental brasileira. São Paulo, Artigo 19, Brasil, 2017.

BASTOS, Eduardo H. S. **O Brasil e o diálogo de defesa Sul-americano no foro para o progresso e integração da América do Sul (PROSUL).** Dissertação em Ciências Militares, Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2021.

BRASIL. **Estratégia nacional de defesa.** Brasília, DF, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 17 ago. 2021.

BRASIL. **Política nacional de defesa e estratégia nacional de defesa.**

Brasília, DF, 2012a. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf. Acesso em: 17 ago. 2021.

BRASIL. **Livro branco de defesa nacional.** Brasília, DF, 2012b. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/lbdn.pdf. Acesso em: 25 jan. 2022.

BRASIL. **Doutrina militar de defesa cibernética.** Ministério da Defesa, Brasília, DF, 2014. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: 19 set. 2022.

BRASIL. **Planejamento estratégico setorial 2020-2031.** Brasília, DF, 2019. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/lai/institucional/diagra_planejamentoa_estrategicoa_17a_04a_2020.pdf. Acesso em: 17 ago. 2021.

BRASIL. Ministério da Defesa. **Decreto nº 9637, de 16 de novembro de 2020.** Diário Oficial da União: seção 1, Brasília, DF, 17 nov. 2020. Disponível em: https://www.in.gov.br/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860. Acesso em: 22 jan. 2022.

BRUSTOLIN, Vitelio. Comparative analysis of regulations for cybersecurity and cyber defence in the United States and Brazil. **Revista Brasileira de Estudos de Defesa.** v. 6, n. 2, p. 93-123, jul./dez. 2019.

CIGE. **Estágio internacional de defesa cibernética.** Comando de Comunicações e Guerra Eletrônica do Exército. Brasília, 2023. Disponível em: http://www.cige.eb.mil.br/index.php/en/estagio-internacional-de-defesa-cibernetica. Acesso em: 20 mar. 2023.

CISO ADVISOR (2022). **Começa o exercício guardião cibernético 4.0.** Disponível em: https://www.cisoadvisor.com.br/comeca-o-exercicio-guardiao-cibernetico-4-0/. Acesso em: 22 de maio de 2023.

CEPIK, Marco. Inteligência e Políticas Públicas: dinâmicas operacionais e condições de legitimação. **Security and defense studies review**, v. 2, p.

246-267, Winter, 2002.

EXAME. Brasil e Argentina avançam na cooperação em ciberdefesa. **Revista Exame**, São Paulo, 22 nov. 2013. Disponível em: https://exame.com/tecnologia/brasil-e-argentina-avancam-na-cooperacao-em-ciberdefesa/. Acesso em: 11 jul. 2022.

FEBRABAN. Brasil é segundo país mais atingido por ciberataques na América Latina, diz relatório. **Febraban Tech**, 21 mar. 2023. Disponível em https://febrabantech.febraban.org.br/temas/seguranca/brasil-e-segundo-pais-mais-atingido-por-ciberataques-na-america-latina-diz-relatorio. Acesso em: 22 maio 2023.

FREITAS, Riva S. ; PINTO, Danielle J.A. **Segurança e defesa cibernética: uma perspectiva das iniciativas legislativas na América do Sul**. *In*: XXVIII Encontro Nacional do CONPEDI, 2019, Goiânia.

FOLSOM, Thomas. Defining cyberspace - Finding real virtue in the place of virtual reality. **Tulane journal of technology & intellectual property**, vol. 9, p. 75-121, 2007.

GÓMEZ, Mariano O. **Políticas públicas de defesa cibernética em perspectiva comparada – República Argentina**. *In*: Ciclo de Estudos Estratégicos. Rio de Janeiro, 2019. Disponível em: http://www.eceme.eb.mil.br/images/docs/PalestrasCEE/POLITICAS_PUBLICAS_DE_DEFESA_CIBERNETICA.pdf. Acesso em: 25 jan. 2022.

ITU, International Communication Union. Digital trends in the Americas region 2021: information and communication technology trends and developments in the Americas region, 2017-2020. **ITU Publications**, Americas, 2021.

KESSEM, Limor. The Brazilian malware landscape: a dime a dozen and going strong. **Security intelligence**, 21 jul. 2016. Disponível em: https://securityintelligence.com/the-brazilian-malware-landscape-a-dime-a-dozen-and-going-strong/. Acesso em: 20 maio 2023.

KSHETRI, Nir; DEFRANCO, Joanna F. The economics of cyberattacks on

Brazil. computer, **IEEE Computer**, p. 85-90, 2020.

KUEHL, Daniel T. From cyberspace to cyberpower: defining the problem. **Cyberpower and national security**, Lincoln: University of Nebraska Press, v. 53, n. 9, p. 24-42, 2011.

LIBICKI, Martin. **Cyberdeterrence and cyberwar**. Pittsburgh: RAND Corporation, 2009.

LOBATO, Luísa C.; KENKEL, Kai M. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, v. 58, n. 2, p. 23-43, 2015.

LOTTA, Gabriela (org.). **Teorias e análises sobre implementação de políticas públicas no Brasil**. Brasília: Enap, 2019.

NASCIMENTO, Luiz. Agência Brasil. **Brazil ratifies Budapest Convention on cybercrime:** service providers may be required to disclose user data, 2023. Disponível em: https://agenciabrasil.ebc.com.br/en/geral/noticia/2023-04/brazil-enacts-convention-cybercrime. Acesso em: 22 maio 2023.

NOBERTO, Cristiane. Brasil salta para 18ª posição em ranking mundial de cibersegurança. **Correio Braziliense**, 20 jun. 2022. Disponível em: https://www.correiobraziliense.com.br/politica/2022/06/5016461-brasil-avanca-em-ranking.html. Acesso em: 10 ago. 2022.

NYE JR., Joseph. **Cyber power**. Harvard Kennedy School, Belfer Center for Science and International Affairs, maio 2020.

OLIVEIRA, Marcos G. *et al*. **Guia de defesa cibernética na América do Sul.** UFPE, 2017.

OPPERMANN, Daniel. A discourse analysis of cyber defense in Brazil. **Anais do 7° Encontro da Associação Brasileira de Relações Internacionais**, Belo Horizonte, MG, 2019.

ORTIZ, Brenda. Por suspeita de ataque hacker, TRF-1 retira do ar portal

da Justiça Federal do DF e de 13 estados. **G1**, 27 nov. 2020. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2020/11/27/por-suspeita-de-ataque-hacker-trf-1-retira-do-ar-portal-da-justica-federal-do-df-e-de-13-estados.ghtml. Acesso em: 21 maio 2023.

PASQUALETTI, Fabio; DÖRFLER, Florian; BULLO, Francesco. Control-theoretic methods for cyberphysical security: geometric principles for optimal cross-layer resilient control systems. **IEEE Control Systems Magazine**, p. 110-127, 2015.

PINHEIRO, Luíza M. **O Centro de gestão e estudos estratégicos e as políticas públicas de estado**. Monografia (Bacharelado em Ciências Sociais). Universidade de Brasília. Brasília, DF, 2014.

PINTO, Danielle J.A.; MEDEIROS, Sabrina E. Inteligência artificial e seu uso no contexto militar: desafios e dilemas éticos. **Cadernos Adenauer XXIII**, n. 2, p. 97-113, 2022.

RODRIGUES, Marta M. A. Políticas públicas, coleção. **Folha Explica**, São Paulo: Publifolha, 2010.

RUA, Maria das Graças. **Análise de políticas públicas:** conceitos básicos. *In:* RUA, Maria das Graças; VALADAO, Maria Izabel. O Estudo da Política: temas selecionados. Brasília: Paralelo 15, 1998.

RUA, Maria das Graças. **Políticas públicas**. Florianópolis: Departamento de Ciências da Administração, UFSC; [Brasília]: CAPES: UAB, 2009.

SANTOS, Bruno Ígaro L. **O emprego da capacidade cibernética nas operações militares em grandes eventos no Brasil:** emprego do centro de defesa cibernética nos jogos olímpicos de 2016. Dissertação em Ciências Militares, Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2019.

SENADO FEDERAL. **Relatório de Avaliação de Política Pública**: a política nacional sobre a defesa cibernética. Senado Federal, Brasília, DF, 2019. Disponível em: http://legis.senado.leg.br/sdleg-getter/documento?dm=8054598&ts=1576151 065975&disposition=inline. Acesso em: 20 jan. 2023.

SOUZA, Celina. Políticas públicas: uma revisão da literatura. **Sociologias**, Porto Alegre, v. 8, n. 16, p. 20-45, jul/dez 2006.

TUBIN, George. Boleto malware targeting brazilian banks. **Security intelligence**, 10 jul. 2014. Disponível em: https://securityintelligence.com/boleto-malware-two-new-variants-discovered/. Acesso em: 21 maio 2023.

VIANNA, Eduardo W.; CAMELO, José R. S. Defesa cibernética no Brasil: primícias de uma história de sucesso. **Revista da Escola Superior de Guerra**, v. 35, n. 75, p. 127-154, set./dez. 2020.

VILLA, Rafael D.; BRAGA, Camila de M. Segurança internacional. *In*: SAINT-PIERRE, Héctor L.; VITELLI, Marina G.. (org.). **Dicionário de segurança e defesa.** São Paulo: Editora Unesp Digital, p. 1047-1056, 2018.

*** Recebido em 01 de janeiro de 2023, e aprovado para publicação em 18 de julho de 2023.**