HEMISFERIO

Revista del Colegio Interamericano de Defensa

Vol. 10, 2024

Journal of the Inter-American Defense College

FORT LESLEY J. McNAIR

WASHINGTON, DC.

ISSN 2412-0715

Índice

Nota Editorial..... 4

Guerra Cibernética e Terrorismo Cibernético: uma Análise da invasão Russa na Ucrânia.

Eduardo de Souza CUNHA..... 7

La población como objetivo estratégico de las acciones cibernéticas: Desafíos para la defensa y seguridad multidimensional presentes (o no) en las Políticas y Estrategias Nacionales de Seguridad Cibernética.

Coronel Aviador (FAB) Claudio D. FARIA 26

A ameaça da guerra cognitiva na América: desafios e oportunidades para a cooperação interamericana.

Mario Brasil do Nascimento..... 44

Application of Future Studies by Intelligence Service to Optimize Public Policies.

Fabio Nogueira de Miranda Filho 68

A anualidade orcamentaria e os projectos de defesa: a caso basileiro.

Franselmo Araújo Costa 91

.

Nota Editorial

> HAL 9000: "I'm sorry Dave, I'm afraid I can't do that. (...) I know that you and Frank were planning to disconnect me and I'm afraid that's something I cannot allow to happen". [1]

En las últimas dos décadas la inteligencia artificial (IA) ha venido transformando el ámbito de defensa y seguridad con impactos tanto a nivel estratégico como operativo. Se han implementado sistemas de ciberseguridad automatizados con herramientas avanzadas para el análisis y procesamiento de datos. Esto ha permitido identificar patrones ocultos y predecir escenarios futuros con mayor precisión, al mismo tiempo que se redefinen políticas de prevención y respuesta ante amenazas complejas y diversas. En este contexto dinámico es que los artículos presentados en el décimo volumen de Hemisferio adquieren especial relevancia.

Los trabajos aquí publicados analizan algunos de los problemas y estrategias necesarias para lograr una mejor defensa y resiliencia. Las naciones que tendrán ventajas competitivas en un plazo de 10 años serán aquellas que hoy están logrando adaptarse con relativa rapidez a los nuevos y disruptivos usos de la IA, ya sea en la defensa y seguridad como en la economía en general. Tal como en el film de Stanley Kubrick, las nuevas tecnologías serán un elemento clave en la toma de decisiones, no obstante, los desafíos éticos y de seguridad inherentes.

La creciente sofisticación de la IA y su uso en ataques cibernéticos dibuja un escenario único en la actualidad. El artículo de Eduardo Cunha nos brinda un análisis de la ciberguerra y el terrorismo cibernético, a través de la invasión rusa en Ucrania como caso de estudio. Comprender bien estos fenómenos permitiría diseñar estrategias de mitigación más efectivas para preservar las infraestructuras críticas y la población civil.

Claudio Duarte Faria también se adentra en el mismo campo analítico, pero haciendo énfasis en el rol de la educación en ciberseguridad y la creación de políticas públicas centradas en las personas. El objetivo es proteger a la población contra

[1] Un fragmento del film de 1968: "2001: A Space Odyssey" dirigido por Stanley Kubrick. https://www.youtube.com/watch?v=ARJ8cAGm6JE

eventuales influencias psicológicas y evitar que ésta sea usada como arma al servicio de atacantes en el ciberespacio. En este sentido propone una revisión de las estrategias nacionales de ciberseguridad en la región para que se incluya a la población como "infraestructura crítica". Una mejor protección y resiliencia ante las ciberamenazas requiere un marco político y normativo acorde con los nuevos tiempos.

La evolución tecnológica, donde se incluye la IA, las redes sociales y la hiperconectividad han dado cuerpo al concepto de guerra cognitiva, tal como nos plantea Mario Brasil do Nascimento. El autor plantea el desafío de cómo proteger las democracias sin tender hacia el autoritarismo y restringir la libertad de expresión. Este tercer artículo resalta que al comprender mejor esta amenaza y sus condicionantes es posible que se transforme la defensa cognitiva en una oportunidad que derive en una cooperación interamericana más fortalecida.

En el ámbito de la toma de decisiones la IA juega un rol fundamental. Fabio Nogueira de Miranda analiza cómo los estudios de futuro permiten un proceso de optimización en las políticas públicas frente a un escenario incierto y voluble. Su abordaje sobre las seis fases del ciclo proporciona un marco lo suficientemente flexible como para implementar los estudios de futuro a la planificación y ejecución de las políticas de gobierno. Este enfoque prospectivo aporta a la gestión de amenazas y oportunidades en defensa y seguridad, principalmente a partir de la irrupción de la IA.

Finalmente, Francelmo Araujo Costa estudia las fallas y efectos del concepto de anualidad presupuestaria en los proyectos de inversión en defensa, que por su naturaleza son de largo plazo. Con Brasil como ejemplo, el autor hace recomendaciones para minimizar la falta de previsibilidad y mejorar el uso de los recursos públicos. Este análisis contribuye a garantizar la continuidad y eficiencia de los proyectos estratégicos en defensa de forma tal que logren cumplir con los objetivos de la Política Nacional de Defensa. Este es otro de los campos en los que la IA está siendo empleada, y pudiera complementar los esfuerzos normativos por el uso más eficiente de los recursos.

En conjunto, estos trabajos ofrecen una visión comprehensiva de los desafíos y oportunidades en la interconexión de la ciberseguridad, la guerra cognitiva, y la gestión de políticas públicas y proyectos de inversión de defensa. Con ellos queda la invitación hecha a la reflexión sobre la relevancia de contar con una estrategia integrada y colaborativa ante las actuales amenazas.

.

Para los países de la región, garantizar la resiliencia y seguridad nacional es un imperativo, especialmente en un contexto marcado por la vertiginosa evolución tecnológica y la irrupción de la inteligencia artificial.

Mirlis Reyes Salarichs, Ph.D.
Editora Ejecutiva

Guerra Cibernética e Terrorismo Cibernético: uma Análise da invasão Russa na Ucrânia.

Eduardo de Souza CUNHA[1]

Recibido: 13 de mayo de 2024; Aceptado: 02 de julio de 2024.
Eduardo de Souza CUNHA. "Guerra Cibernética e Terrorismo Cibernético: uma Análise da invasão Russa na Ucrânia." *Hemisferio Revista del Colegio Interamericano de Defensa* 10 (2024): 7-25. https://doi.org/10.59848/24.1207.HV10n1

Resumo:

Este artigo examina a complexa interseção entre guerra cibernética e terrorismo cibernético, utilizando como estudo de caso a invasão da Ucrânia pela Rússia e os ataques cibernéticos subsequentes. Buscar-se-á explorar brevemente o contexto histórico, assim como as motivações por trás dos ataques e os efeitos sobre a população civil e as infraestruturas críticas. Serão abordados os efeitos cibernéticos cinéticos e não cinéticos sofridos pela Ucrânia, destacando a necessidade de uma compreensão mais profunda desses fenômenos e de estratégias mais eficazes para mitigação dos seus impactos. Ao final, buscar-se-á entender a correlação e peculiaridades da Guerra Cibernética e do Terrorismo Cibernético.

Palavras Chave: Guerra Cibernética - Terrorismo Cibernético - Invasão da Ucrânia - População Civil - Infraestruturas Críticas

Abstract:

This article examines the complex intersection between cyber warfare and cyber terrorism, using the Russian invasion of Ukraine and the subsequent cyber attacks as a case study. It will briefly explore the historical context, the motivations behind the attacks, and the effects on the civilian population and critical infrastructure. The article will address both kinetic and non-kinetic cyber effects experienced by Ukraine, highlighting the need for a deeper understanding of these phenomena and more effective strategies for mitigating their impacts. In conclusion, it will seek to understand the correlation and peculiarities of Cyber Warfare and Cyber Terrorism.

[1] O autor é Oficial do Exército Brasileiro com mais de 33 anos de serviço, tendo atuado como Subchefe do Estado-Maior do Comando de Defesa Cibernética do Brasil. Com Mestrado em Ciências Militares, atualmente é professor de Segurança Cibernética no Colégio Interamericano de Defesa. Ao longo de sua carreira, tem se dedicado à proteção das infraestruturas críticas nacionais e à formação de novos profissionais na área de segurança cibernética. Contato: eduardo.cunha@iadc.edu. https://orcid.org/0009-0008-7060-7840

***Keywords**: Cyber Warfare - Cyber Terrorism - Ukraine Invasion - Civilian Population - Critical Infrastructure*

Introdução:

Há algum tempo tem-se tornado cada vez mais complexa a profundidade das ameaças cibernéticas como os crimes, a espionagem e o hacktivismo. Porém, duas delas, até fruto da minha natureza militar, me chamam mais a atenção: a Guerra e o Terrorismo cibernéticos. A linha que separa esses dois ramos da cibernética é muito tênue. Entre elas está a população civil que se serve dos serviços oferecidos pelas infraestruturas críticas e mais sofrem quando essas são impactadas.

A era digital trouxe consigo para sociedade uma série de benefícios, mas por outro lado, junto a elas novos desafios e ameaças, as quais se incluem a guerra cibernética e o terrorismo cibernético. A invasão da Ucrânia pela Rússia, em conjunto com os ataques cibernéticos direcionados, oferece um bom exemplo vívido das interações complexas entre esses fenômenos e seus efeitos sobre a segurança internacional.

Durante a invasão, especificamente no período compreendido entre os anos de 2022 e 2024, e mesmo antes desse, uma série de ataques cibernéticos foi perpetrada contra infraestruturas críticas e sistemas de comunicação ucranianos. Esses ataques tinham por objetivo a desorganização da comunicação e coordenação militar, desestabilização do governo ucraniano e minar a confiança da população nas instituições governamentais, além de espionagem, inteligência, propaganda e guerra psicológica.

Os ataques cibernéticos perpetrados pela Rússia durante a invasão da Ucrânia foram diversificados e altamente coordenados, o que sinaliza um planejamento prévio e reforça o emprego da arma cibernética como novo e importante elemento no combate. Eles incluíram não só ataques de Negação de Serviço (Distributed Denial of Service, DDoS) contra infraestruturas de comunicação e sites governamentais, bem como ataques direcionados a redes elétricas e sistemas de controle industrial. Esses ataques tinham por objetivos minar a capacidade da Ucrânia de se comunicar, coordenar uma resposta militar eficaz e manter a estabilidade interna.

Esses ataques cibernéticos tiveram consequências significativas para a população civil e as infraestruturas críticas ucranianas. As interrupções nos serviços de comunicação dificultaram a coordenação das operações militares e a disseminação de informações

precisas para o público. Além disso, os ataques contra redes elétricas e sistemas de controle industrial causaram cortes de energia em áreas críticas, afetando negativamente hospitais, instalações de água e outros serviços essenciais.

Como conclusão parcial, fica latente que os objetivos dos ataques cibernéticos russos durante a invasão da Ucrânia eram multifacetados, buscando alcançar vantagens militares, políticas e psicológicas para facilitar os esforços de guerra da Rússia e minar a resistência ucraniana. A proposta desse Artigo é tentar compreender o uso da arma cibernética em alvos militares e seus impactos na população civil se pode ser considerado como um ato terrorista ou não, concluindo sobre a importância na atribuição e classificação de ataques cibernéticos e como podemos agir para mitigar ou dissuadir essas ações.

Breve Histórico:

As relações entre Rússia e Ucrânia têm sido historicamente complexas, marcadas por tensões políticas, étnicas e territoriais. Fato relevante e recente para isso foi a anexação da Crimeia pela Rússia em 2014, que exacerbou essas tensões, levando a um conflito armado no leste da Ucrânia entre forças pró-russas e ucranianas.

A escalada da guerra cibernética entre Rússia e Ucrânia teve início em 2014, como desdobramento do conflito mais amplo entre esses dois países. A crise política na Ucrânia teve início após o então presidente Viktor Yanukovych recusar-se a assinar um acordo comercial com a União Europeia em novembro de 2013, resultando em uma deterioração da situação política no país. Em fevereiro de 2014, tropas russas ocuparam a Crimeia, enquanto uma série de ciberataques coordenados interromperam os serviços de telecomunicações e sites governamentais ucranianos.

Os ataques cibernéticos prosseguiram com diferentes graus de intensidade, envolvendo invasões de sistemas, interrupções de serviços online e vazamentos de informações confidenciais. Grupos de hackers pró-Ucrânia e pró-Rússia, como "Cyber Hundred", "Null Sector" e "CyberBerkut", estiveram ativos em diferentes momentos, conduzindo ataques DDoS e comprometendo sistemas de informação.[2]

[2] Ronaldo Oliveira de Souza et al., “Guerra híbrida e ciberconflitos: uma análise das ferramentas cibernéticas nos casos da síria e conflito rússia-ucrânia” (Revista eletrônica Estácio Recife, 2019), 6-17.

Antes mesmo da escalada para a guerra entre Rússia e Ucrânia, as atividades cibernéticas desempenharam um papel fundamental na competição e nos conflitos entre esses dois países. A Rússia empregou operações cibernéticas ofensivas (OCO) como parte de sua estratégia de guerra irregular, buscando desestabilizar a Ucrânia e influenciar a opinião pública a seu favor. Isso incluiu ataques distribuídos de DDoS e a alteração de sites para controlar a narrativa pró-Rússia e prejudicar a capacidade do governo ucraniano de operar eficazmente.

Por sua vez, a Ucrânia também se engajou em operações de informação, utilizando plataformas de mídia social, televisão e redes sociais para promover uma narrativa alternativa e resistir às ações russas. Essas atividades cibernéticas faziam parte de um ambiente informacional mais amplo, onde a rivalidade entre os dois países se transformou em conflito armado em 2022. A interseção entre o domínio cibernético e o físico tornou-se evidente, com a ciberguerra sendo uma extensão das operações no campo de batalha convencional.[3]

Dessa forma, podemos dizer então que as complexas relações entre Rússia e Ucrânia, exacerbadas pela anexação da Crimeia em 2014, desencadearam um conflito armado no leste da Ucrânia e uma escalada da guerra cibernética entre os dois países. Desde então, os ataques cibernéticos têm sido uma parte crucial das estratégias de ambos os lados, refletindo não apenas uma rivalidade política, mas também se tornando uma extensão das hostilidades no campo de batalha convencional.

Formas de ataques:

Os ataques cibernéticos levados a efeito pela Rússia podem ser entendidos dentro do contexto mais amplo das estratégias militares e políticas do Kremlin. Além de objetivos militares convencionais, como minar a capacidade de defesa da Ucrânia, os ataques cibernéticos também visavam desestabilizar a sociedade ucraniana e minar a confiança nas instituições governamentais.

[3] Defibaugh, "Past and Present Russian Information Operations in Ukraine: Competition into Conflict", Anais da 19ª Conferência Internacional sobre Guerra Cibernética e Segurança, ICCWS 2024, 64-65.

Atualmente, a "zona cinzenta" e ou "guerra híbrida", que são ações ou estratégias que ficam entre a paz e a guerra aberta. Essas atividades são deliberadamente ambíguas e difíceis de atribuir, projetadas para obter vantagens sem desencadear uma resposta militar convencional. Elas representam uma evolução nas formas de conflito contemporâneas, caracterizadas pela ambiguidade, complexidade e integração de uma variedade de métodos e técnicas de guerra. Esses conceitos desafiam as noções tradicionais de segurança e exigem respostas adaptativas e multidimensionais por parte das instituições estatais e internacionais.

Na zona cinzenta dos conflitos pós-Guerra Fria, uma variedade de ferramentas e táticas tem sido empregadas para conduzir atividades que se encontram entre a paz e uma guerra declarada. Essas ferramentas e táticas são empregadas de forma gradual por atores estatais e não estatais, combinando elementos militares e não militares. O objetivo tem sido em geral de minar, desestabilizar, enfraquecer ou atacar um adversário, muitas vezes explorando as vulnerabilidades do estado-alvo.[4]

Nesse mister, os ataques cibernéticos conduzidos pela Rússia em apoio às operações militares, mesmo antes da invasão, mas sobretudo com grande intensidade no dia “D”, foram conduzidos de forma organizada e planejada, a fim de atingir principalmente objetivos estratégicos. Dentre elas, podemos destacar as principais formas de ataque cibernético perpetrados pela Rússia e seus objetivos militares:

- Ataques de DDoS: visavam sobrecarregar e inutilizar sistemas de comunicação e infraestrutura de defesa ucraniana, dificultando a coordenação e a resposta militar.

- Infiltração e Espionagem Cibernética: tinham por objetivo principal obter informações confidenciais e estratégicas sobre as capacidades militares e planos de defesa da Ucrânia.

- Ataques de Ransomware: visavam paralisar instituições e setores estratégicos da Ucrânia, como governamentais e de infraestrutura crítica, de formas a desestabilizar o país e minar sua capacidade de resposta militar.

[4] Henrique et al., “OSINT e relações internacionais: o caso dos militares russos em Donbas entre 2014 e 2021” Revista Brasileira de Estudos Estratégicos REST V15 Nº29 (Jan-Jun 2023), 70-92.

- Desinformação e Manipulação de Mídia: um dos mais empregados, visavam influenciar a opinião pública nacional e internacional, distorcendo a narrativa do conflito e minando o apoio à Ucrânia, enquanto promoviam a agenda russa.

- Ataques a Infraestrutura Crítica: interrupção de serviços essenciais, como eletricidade, água e transporte, visando desestabilizar a população e prejudicar as capacidades de defesa e resposta da Ucrânia.

- Ataques de Engenharia Social: enganar e manipular funcionários e oficiais ucranianos para obter acesso não autorizado a sistemas e informações sensíveis, comprometendo a segurança nacional.

- Ataques de wiper: os ataques "wiper" podem ter sido usados para interromper a infraestrutura crítica da Ucrânia, como sistemas de energia, transporte e comunicação. Ao destruir dados e comprometer sistemas, esses ataques podem ter causado danos significativos com consequências não só para o governo ucraniano, mas sobretudo para população civil.

Nesse sentido, um exemplo interessante ocorrido em 2022 foi que um ataque cibernético mirado contra uma estação elétrica na Ucrânia desencadeou um apagão não planejado. Este evento acarretou consequências significativas não apenas para a infraestrutura elétrica ucraniana, mas também para a segurança nacional e a percepção global sobre a vulnerabilidade das infraestruturas críticas.[5]

O ataque destacou a habilidade de grupos de hackers, possivelmente respaldados por estados ou atores não estatais com agendas geopolíticas, de infligir danos consideráveis através de ataques cibernéticos direcionados. Essa situação ressaltou a importância de salvaguardar as infraestruturas críticas contra ameaças cibernéticas e a necessidade de adotar medidas de segurança mais sólidas e vigilantes.

A resposta a esse incidente não se limitou apenas à restauração da energia afetada, mas também incluiu uma investigação meticulosa para identificar os responsáveis e avaliar a extensão dos danos causados. Adicionalmente, estimulou um debate

[5] Mueller et al., “Cyber Operations during the Russo-Ukrainian War From Strange Patterns to Alternative” Center for Strategic and International Studies (CSIS), julho 2023, 15-26.

internacional sobre a segurança cibernética das infraestruturas críticas em escala global, resultando em uma maior conscientização e implementação de medidas preventivas.

Em última análise, esse episódio serviu como um alerta para a comunidade internacional sobre os riscos crescentes associados à guerra cibernética e a necessidade premente de uma cooperação mais estreita entre os países para enfrentar esses desafios em matéria de segurança cibernética.

Podemos concluir parcialmente que os ataques cibernéticos durante a invasão da Ucrânia pela Rússia são parte de estratégias militares e políticas mais amplas, visando desestabilizar a sociedade ucraniana e minar a confiança nas instituições governamentais. Esses ataques demonstram a complexidade da "zona cinzenta" e da "guerra híbrida", desafiando conceitos tradicionais de segurança. Os objetivos dos ataques incluem negação de serviço, manipulação de mídia e interrupção de infraestrutura crítica.

Efeitos sobre a População Civil nos ataques às Infraestruturas Críticas:

Os impactos dos ataques cibernéticos às infraestruturas críticas ucranianas trouxeram consequências graves para população civil, pois causaram perturbações em serviços primordiais, tais como energia e comunicações. Essas ações também acarretaram prejuízos econômicos e emocionais, uma vez que a falta de informações, seja pela mídia tradicional ou mesmo pelas novas redes sociais, comprometeram a estabilidade nacional e agravaram a situação humanitária. Tente se colocar na situação em que seu país é atacado por uma Força militar estrangeira e as poucas informações que chegam são muitas vezes incorretas. Poderia isso ser considerado um ato terrorista?

Vimos anteriormente que os ataques cibernéticos às infraestruturas críticas ucranianas tinham objetivos militares e estratégicos. Uma pergunta que se deve fazer então é no sentido de procurar entender se houve por parte da Rússia uma judiciosa análise de riscos. A análise de riscos em operações cibernéticas é fundamental para compreender as potenciais consequências e impactos das ações realizadas. No contexto das operações contra infraestruturas críticas, essa avaliação envolve considerar a possibilidade de retaliação, escalada do conflito, repercussões diplomáticas e o impacto na população civil, entre outros fatores relevantes.

No caso específico dos momentos em que se sucederam as invasões por tropas russas os ataques perpetrados às infraestruturas críticas da Ucrânia causaram um impacto devastador na população civil, manifestando-se em diversas áreas, tais como:

- Perda de serviços essenciais: hospitais, escolas, residências e empresas foram privadas de eletricidade, água, aquecimento e comunicação. Esse cenário acarretou considerável sofrimento e privação das necessidades básicas das pessoas.

- Interrupções na economia: os ataques tiveram um efeito severo na economia ucraniana, interrompendo cadeias de suprimentos, operações comerciais e transporte. Isso resultou em um aumento do desemprego, da pobreza e da insegurança econômica.

- Crise humanitária: milhões de indivíduos foram obrigados a deixar suas residências devido aos conflitos e à destruição da infraestrutura. Como resultado, uma grande crise humanitária emergiu, com muitos ucranianos lutando para acessar alimentos, abrigo e assistência médica.

- Impacto ambiental: os ataques também provocaram danos ambientais significativos, incluindo vazamentos de substâncias químicas perigosas e incêndios em refinarias de petróleo. Tais incidentes terão implicações de longo prazo para a saúde pública e o meio ambiente da Ucrânia.

O Relatório de 2022 da Microsoft traz as primeiras lições da guerra cibernética no estudo de caso da Ucrânia. Durante a guerra, houve relatos de ataques cibernéticos coordenados com ataques de mísseis contra ferrovias e sistemas de transporte que transportavam armas e suprimentos militares. Esses ataques visavam interromper as operações logísticas e prejudicar a capacidade de movimentação de recursos essenciais, afetando indiretamente a população civil que dependia desses sistemas para transporte e abastecimento.

Outro relato do referido relatório diz que os militares russos direcionaram ataques cibernéticos destrutivos do tipo wipers às redes informáticas locais do governo ucraniano. Esses ataques visavam comprometer a infraestrutura digital do governo, potencialmente causando interrupções nos serviços públicos e nas operações governamentais, o que impactou a população civil que dependia desses serviços.

Porém, os ataques com maiores efeitos negativos para população foram no setor de energia e finanças. A Ucrânia foi alvo de ataques cibernéticos que resultaram em cortes de energia em várias regiões do país. Esses ataques comprometeram a infraestrutura da

rede elétrica, causando interrupções no fornecimento de eletricidade para residências, empresas e serviços essenciais. A falta de eletricidade teve impactos graves na vida cotidiana da população, afetando a iluminação, o aquecimento, a refrigeração de alimentos e a operação de equipamentos essenciais.

Durante a guerra, também houve relatos de ataques cibernéticos direcionados a ativos financeiros na Ucrânia. Esses ataques podem ter visado instituições financeiras, sistemas de pagamento e outras infraestruturas relacionadas ao setor financeiro. A interrupção ou comprometimento desses ativos financeiros causaram instabilidade econômica, perda de fundos e impactaram negativamente a população civil que dependia desses serviços para transações financeiras e acesso a recursos financeiros.[6]

Apesar de não ser um ataque específico a infraestrutura crítica, existe um campo em que a Rússia já trabalha a muito tempo em todo mundo que é o da desinformação. No caso específico foram identificadas campanhas de desinformação russa durante a guerra cibernética na Ucrânia. Essas campanhas visavam disseminar narrativas falsas e enganosas para manipular a opinião pública e influenciar a percepção dos eventos em curso. As campanhas de desinformação russa envolveram a amplificação de narrativas falsas por meio de sites patrocinados pela Rússia, que publicavam histórias promovendo uma determinada narrativa.

Conclui-se então que os ataques cibernéticos às infraestruturas críticas na Ucrânia causaram danos graves à população civil, incluindo interrupções nos serviços essenciais, prejuízos econômicos e uma crise humanitária emergente. A coordenação entre ataques cibernéticos e cinéticos levanta questões sobre a análise de riscos por parte da Rússia. Danos ambientais, cortes de energia e ataques financeiros ilustram o impacto generalizado sobre a vida cotidiana. As campanhas de desinformação russa agravaram a situação. Esses eventos destacam a necessidade urgente de proteger infraestruturas críticas e a população civil contra ameaças cibernéticas e suas consequências humanitárias.

[6] Brad Smith, “Defending Ukraine: Early Lessons from the Cyber War”, Microsoft, (Junho 2022), 10-27.

Guerra Cibernética e Terrorismo Cibernético:

A distinção entre guerra cibernética e terrorismo cibernético nesse contexto é complexa. Enquanto alguns ataques tinham como objetivo principalmente alvos militares e infraestrutura crítica, os efeitos sobre a população civil e a motivação para instilar o medo e o caos também refletem em elementos de terrorismo cibernético. Faz-se necessário então definir o que é Terrorismo, Guerra Cibernética e Terrorismo Cibernético.

O terrorismo é uma forma de violência política que busca gerar medo, intimidação e coerção através do uso deliberado de violência contra civis ou não combatentes. Geralmente, os atos terroristas são realizados por grupos ou indivíduos com motivações políticas, ideológicas, religiosas ou sociais, com o objetivo de promover uma agenda específica, desestabilizar governos ou sociedades, ou causar impacto emocional e psicológico.[7]

O ciberterrorismo é uma forma específica de terrorismo que envolve o uso de ataques cibernéticos, como hacking, malware, DDoS e outras técnicas de ciberataque, com o objetivo de causar danos, instilar medo e atingir objetivos políticos, sociais ou ideológicos. O ciberterrorismo combina elementos do terrorismo tradicional com o uso de tecnologia da informação e comunicação para realizar ataques.

O ciberterrorismo é ainda definido como a utilização de ativos computacionais e outras tecnologias de informação e comunicação para conduzir ataques terroristas ou promover causas terroristas. Esses ataques podem incluir a disseminação de propaganda, roubo ou manipulação de dados e a perturbação de infraestruturas críticas. Em outra análise o ciberterrorismo envolve ameaçar ou causar danos corporais para obter poder político ou ideológico através de ameaça ou intimidação. Perceba-se que nessa definição não há o componente militar.

O impacto do ciberterrorismo na sociedade pode ser devastador. Pode resultar em perdas financeiras, perdas de vidas, danos à reputação e perda de estabilidade. Além disso, o ciberterrorismo pode afetar a economia de uma nação, causar instabilidade política e gerar medo e ansiedade na população. A interrupção de infraestruturas vitais, como redes

[7] Usman et al., "Cyber-warfare Versus Cyber-terrorism: An Emerging 21st Century Trend", Journal of Politics and International Studies, (10 de dezembro de 2023), 149-155.

de transporte, redes elétricas e redes bancárias, é um dos maiores efeitos desse tipo de ataques cibernéticos.[8]

A guerra cibernética é uma forma de conflito que ocorre no ciberespaço, envolvendo ataques e operações realizadas por meio de sistemas de computadores e redes digitais. Nesse contexto, a guerra cibernética se concentra em explorar e comprometer sistemas de informação e comunicação para obter vantagens estratégicas, causar danos, interromper operações inimigas e promover objetivos militares, políticos ou econômicos.

Do que foi pesquisado até aqui, a grande pergunta se as ações de Guerra Cibernética promovidas pela Rússia durante a invasão da Ucrânia podem ser consideradas também como Terrorismo Cibernético não possui um consenso, pois está sujeita às diversas interpretações. Vejamos.

Não é incomum que governos e entidades estatais sejam acusados de envolvimento em atividades cibernéticas que possam ser consideradas como ciberterrorismo. No caso da Rússia e sua relação com a Ucrânia, houve alegações e evidências de ataques cibernéticos e operações de desinformação que visavam desestabilizar o país vizinho.

Durante a invasão da Crimeia pela Rússia em 2014 e o conflito contínuo no leste da Ucrânia, houve relatos de ciberataques contra infraestruturas críticas, sistemas de comunicação e redes governamentais ucranianas. Além disso, a disseminação de desinformação e propaganda online também foi uma estratégia utilizada para influenciar a opinião pública e minar a estabilidade do país.

Embora não haja um consenso universal sobre a definição de terrorismo cibernético e suas ramificações legais, as ações cibernéticas da Rússia durante o conflito com a Ucrânia podem ser interpretadas como parte de uma estratégia mais ampla de guerra híbrida, que inclui elementos cibernéticos, de informação e militares.

É importante ressaltar que a atribuição de responsabilidade por ataques cibernéticos, que é uma etapa fundamental, é um processo complexo que envolve investigações detalhadas, análise forense digital e cooperação internacional. As relações

[8] Iftikhar, “Cyberterrorism as a global threat: a review on repercussions and countermeasures”, Faculty of Computer Studies, Arab Open University, Riyadh, Saudi Arabia (15 de janeiro de 2024), 3-32.

entre Rússia e Ucrânia no contexto cibernético são sensíveis e sujeitas a interpretações diversas, dependendo do ponto de vista principalmente político.

Alguns argumentos a favor da caracterização como ciberterrorismo argumentam que esses ataques cibernéticos constituem ciberterrorismo porque visaram civis e tiveram o objetivo de causar medo e dano.

Eles apontam para a Convenção do Conselho da Europa sobre o Cibercrime, que define ciberterrorismo como o uso de tecnologia da informação para causar medo ou dano com o objetivo de coagir um governo ou população civil. Também argumentam que a Rússia tem um histórico de uso de ataques cibernéticos como arma de guerra e que a invasão da Ucrânia faz parte de um amplo esforço para minar a Ucrânia e sua democracia.

Outros argumentos contra a caracterização como ciberterrorismo dizem que esses ataques cibernéticos não constituem ciberterrorismo porque não visaram diretamente civis e não tiveram como objetivo causar morte ou ferimentos graves. Os ataques foram direcionados principalmente a infraestrutura militar e governamental e que eram táticas militares legítimas no contexto de um conflito armado.

A definição de ciberterrorismo é vaga e subjetiva e não há consenso internacional. Não há, dentro dessa visão, até mesmo consenso se a Rússia cometeu ciberterrorismo durante a invasão da Ucrânia. A caracterização dependerá da definição específica de ciberterrorismo que está sendo usada e das circunstâncias específicas de cada ataque individual. Trata-se então, muito mais uma definição por parte da expressão do poder Político.

Abaixo podemos verificar uma coordenação de ataques cibernéticos com ataques cinéticos:

Fonte: Microsoft Defending Ukraine Early Lessons from the Cyber War, 2022.

É fato que a guerra cibernética entre Rússia e Ucrânia afetou diretamente as vidas das pessoas comuns, gerando medo, incerteza e insegurança. Os ataques cibernéticos não apenas visavam infraestruturas críticas e instituições governamentais, mas também tiveram impacto sobre a população civil, que enfrentou interrupções nos serviços essenciais, como eletricidade, água e comunicações.

Imagine-se em uma situação em que você não consegue acessar a internet para se comunicar com seus entes queridos ou o sistema de transporte público para chegar ao trabalho está fora de operação. Esses são apenas alguns exemplos das dificuldades enfrentadas pelas pessoas durante esses ataques, como vimos anteriormente.

Além disso, os ataques cibernéticos tiveram efeitos devastadores sobre a economia, levando ao desemprego, à perda de renda e à dificuldade em garantir o sustento básico. As empresas sofreram com interrupções em suas operações, o que afetaram não apenas os proprietários, mas também os funcionários e suas famílias.

É importante lembrar que por trás de cada ataque cibernético há pessoas reais, cujas vidas são afetadas de maneiras profundas e muitas vezes duradouras. Portanto, é crucial abordar essas questões não apenas como questões técnicas ou geopolíticas, mas também como problemas que impactam diretamente o bem-estar e a segurança das pessoas comuns.

Porém, conforme demonstrado no estudo da Microsoft, onde houve uma coordenação entre ataques cibernéticos e ataques cinéticos, todos levando a danos físicos

com efeitos trágicos para população civil, poderíamos considerar então que esses foram realizados dentro de um planejamento com objetivos militares de guerra. Então, num sentido mais amplo, dentro de um contexto de "guerra", onde sobressaem os ataques cinéticos, o conceito de terrorismo também deve ser bem avaliado. Fato é que durante esta pesquisa, não foi encontrado consenso até mesmo entre a relação guerra e terrorismo. Portanto, ressalta-se, mais uma vez que essa atribuição se deva muito mais a expressão Política do poder, que varia de país para país.

Do exposto, podemos inferir que a distinção entre guerra cibernética e terrorismo cibernético é um assunto complexo, especialmente quando estamos tratando de um assunto ainda andamento como é o conflito entre Rússia e Ucrânia, onde os ataques cibernéticos afetaram tanto infraestruturas quanto civis. A coordenação entre ataques cibernéticos e cinéticos torna a classificação desses eventos ainda mais desafiadora. Apesar da falta de consenso sobre a definição precisa de terrorismo cibernético, é crucial reconhecer o impacto direto desses ataques na vida das pessoas e adotar medidas para proteger sua segurança e bem-estar.

Estratégias de Mitigação e Resposta:

Para enfrentar esses desafios, é necessário um enfoque abrangente que inclua medidas defensivas e ofensivas, cooperação internacional e aprimoramento da capacidade de resiliência cibernética. Além disso, é crucial um diálogo contínuo sobre normas e princípios no ciberespaço para evitar escaladas descontroladas e garantir a estabilidade internacional.

Se nós extrapolarmos para o campo da guerra híbrida dentro da chamada "zona cinza", onde diariamente ocorre uma guerra muitas vezes "não declarada", podemos citar o Manual de Tallinn 2.0, que fornece informações sobre a aplicação do direito internacional às operações cibernéticas, incluindo o terrorismo cibernético. Embora o manual não se concentre especificamente no ciberterrorismo como uma categoria separada, aborda vários aspectos relacionados com operações cibernéticas que podem ser consideradas como ciberterrorismo.

Por exemplo, o manual discute os princípios da soberania, da responsabilidade do Estado e do direito dos conflitos armados no contexto das operações cibernéticas. Abrange também temas como contramedidas, proporcionalidade e proibição de ações que

afetem os direitos humanos fundamentais. Globalmente, o Manual de Tallinn 2.0 oferece um quadro abrangente para a compreensão das implicações jurídicas das atividades cibernéticas, que pode ser aplicado a vários cenários, incluindo aqueles que envolvem o terrorismo cibernético.[9]

A verdade é que falta de uma maior adesão mundial em convenções e leis internacionais não só como o Manual de Tallin, mas também de outras legislações, como a Convenção de Budapeste, que falam sobre o crime cibernético, contribuem significativamente para o aumento dos ataques cibernéticos por vários motivos, entre eles podemos citar a impunidade, a dificuldade na cooperação internacional, a crescente sofisticação dos ataques e o aumento da frequência de ataques.[10]

O Departamento de Defesa dos Estados Unidos (DoD), por meio da Estratégia Cibernética de 2023, apresenta várias estratégias de mitigação de incidentes cibernéticos, visando fortalecer a segurança cibernética e proteger as infraestruturas críticas dos EUA. Algumas das estratégias mencionadas no documento incluem:

Parcerias Público-Privadas: o DoD pretende expandir as parcerias público-privadas para garantir que os recursos, conhecimentos e informações do DoD sejam disponibilizados para apoiar as principais iniciativas do setor privado. Isso inclui aproveitar os conhecimentos técnicos e as capacidades analíticas do setor privado para identificar atividades cibernéticas maliciosas baseadas no exterior e mitigar vulnerabilidades em larga escala.

Operações no Ciberespaço: o DoD utilizará operações no ciberespaço para limitar, frustrar ou interromper as atividades dos adversários abaixo do nível de conflito armado, visando alcançar condições de segurança favoráveis. O Comando Cibernético dos EUA (USCYBERCOM) apoiará campanhas em todo o Departamento para reforçar a dissuasão e obter vantagens.

Exercícios de Treinamento: o Departamento realizará exercícios de treinamento holísticos, baseados em cenários realistas, para preparar e fortalecer suas capacidades de

[9] Jensen, "The Tallinn Manual 2.0: highlights and insights", Brigham Young University Law School, 2017, 15-44.

[10] Dang, "The Prevention of Cyberterrorism and Cyberwar", GA First Committee: Disarmament and International Security (DISEC), 2011, 4-6.

defesa cibernética. Esses exercícios ajudarão a criar uma abordagem integrada de ameaças, operações e processos no ciberespaço.[11]

Um bom exemplo de treinamento é o Exercício Guardião Cibernético, maior exercício de segurança cibernética do hemisfério sul. Trata-se de uma simulação conduzida pelo Ministério da Defesa do Brasil e coordenado pelo seu Comando de Defesa Cibernético (ComDCiber). Em sua 5ª edição, no ano de 2023 a atividade reuniu as três Forças Armadas e cerca de 150 instituições, entres entes governamentais e diversas empresas brasileiras. O objetivo final é fortalecer a segurança cibernética das principais infraestruturas estratégicas do Brasil.

A importância desses exercícios é acima de tudo é a de fortalecer as relações de confiança entre os entes, permitindo um melhor compartilhamento de informações de incidentes, integração, somar esforços e dar pronta respostas. Em resumo, gerenciar a crise de forma integrada e com a rapidez necessária. Duas palavras se sobressaem em qualquer exercício ou treinamento nessa direção: confiança e integração.

Para mitigar os riscos associados aos ataques cibernéticos podemos adicionar, ainda, algumas estratégias a serem adotadas, como é o caso da Cooperação Internacional, essa largamente empregada até os dias de hoje em apoio à Ucrânia. Inclua-se a essa cooperação o compartilhamento de informações, fundamental para uma maior velocidade na resposta a incidentes e principalmente a prevenção. Outras medidas incluem a capacitação de profissionais, o monitoramento contínuo e a participação em iniciativas internacionais.

Na verdade, a resposta aos desafios da guerra cibernética e do ciberterrorismo requerem uma abordagem abrangente, que inclua medidas defensivas e ofensivas, cooperação internacional e o fortalecimento da resiliência cibernética. A adesão global a convenções internacionais, como o Manual de Tallinn e a Convenção de Budapeste, é essencial para enfrentar o aumento dos ataques cibernéticos. Além disso, estratégias como parcerias público-privadas, operações no ciberespaço e exercícios de treinamento são fundamentais para fortalecer a segurança cibernética. A cooperação internacional, o compartilhamento de informações e a capacitação de profissionais são medidas adicionais

[11] U.S. Department of Defense “DOD Cyber Strategy Summary”, 2023, 18-24.

cruciais para mitigar os riscos associados aos ataques cibernéticos e garantir uma resposta eficaz e preventiva.

Conclusão:

A invasão da Ucrânia pela Rússia e os ataques cibernéticos subsequentes destacam a complexidade e os desafios associados à guerra cibernética e ao terrorismo cibernético. É essencial uma compreensão mais profunda desses fenômenos e a implementação de estratégias eficazes para mitigar seus impactos sobre a segurança internacional e a estabilidade global.

A expansão contínua do mundo digital é praticamente ilimitada e nenhum órgão ou governo jamais conseguirá restringir completamente sua capacidade de abranger quase todos os aspectos da vida no futuro. Como resultado dessa vastidão, as ameaças e os ataques cibernéticos assumem formas cada vez mais diversas e evolutivas, mirando uma variedade maior de alvos. Os perpetradores desses ataques empregam tecnologia avançada e inteligência, resultando em um novo cenário com lacunas significativas em relação ao passado.

Essa evolução transforma não apenas os conflitos e guerras no mundo real, mas também os ataques cibernéticos e as guerras virtuais. Paralelamente, o terrorismo também avança constantemente, adotando tecnologia de ponta e ferramentas inteligentes, o que resulta no correspondente ciberterrorismo. Tudo isso gera desafios significativos para a segurança dos sistemas de informação e para a prevenção de ataques contra infraestruturas nacionais, bem como para a segurança e a paz das pessoas.[12]

A análise mais abrangente das ameaças cibernéticas, como guerra e terrorismo cibernético, revelam a interconexão complexa entre esses fenômenos, especialmente no contexto das relações entre Rússia e Ucrânia. A invasão russa na Ucrânia entre 2022 e 2024 exemplifica essa complexidade, destacando a diversidade e coordenação dos ataques cibernéticos e seu impacto adverso sobre a estabilidade interna e as infraestruturas críticas. Esses eventos ressaltam a importância de compreender os efeitos da guerra cibernética sobre a população civil e sublinham a necessidade urgente de proteger tanto as infraestruturas quanto os civis contra tais ameaças. A distinção entre guerra e

[12] Ferrag et al. “Hybrid Threats, Cyberterrorism and Cyberwarfare”, CRC Press, 2024, 9-17.

terrorismo cibernéticos continua sendo um desafio, especialmente em contextos como o conflito Rússia-Ucrânia, onde os ataques afetam ambos.

A guerra cibernética na Ucrânia é um lembrete de que o ciberespaço se tornou um campo de batalha crucial no mundo moderno. A proteção da população civil e das infraestruturas críticas contra ataques cibernéticos exige uma resposta global coordenada e multifacetada. A comunidade internacional deve trabalhar em conjunto para desenvolver mecanismos eficazes de prevenção, detecção e resposta a essas ameaças crescentes.

A verdade é que o tema "terrorismo cibernético" deve ser aprofundado. Essa "guerra" vem sendo travada diariamente em todo mundo dentro da zona cinzenta, mesmo fora do contexto Ucrânia e Rússia, seja perpetrado por criminosos em busca de dinheiro, seja até mesmo por atores Estatais com objetivos não diplomáticos. Nesse mister, a questão da atribuição é fundamental e deve ser tratado pelo nível político por meio da gestão de uma política de segurança cibernética. A elevação desses crimes cibernéticos ao status de "terrorismo", podem dar o arcabouço legal para criação de leis mais rígidas que visem acima de tudo a dissuasão.

Bibliografia:

Defibaugh. "Past and Present Russian Information Operations in Ukraine: Competition into Conflict." In *Proceedings of the 19th International Conference on Cyber Warfare and Security, ICCWS 2024*, 64-65.

Dang. "The Prevention of Cyberterrorism and Cyberwar." GA First Committee: Disarmament and International Security (DISEC), 2011, 4-6. Acessado em 2 de abril de 2024. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5422c0fb4c95e3c8d47bf7263a06d0c51b2e01cd.

Ferrag, M.A., Kantzavelou, I., Maglaras, L., and Janicke, H. "Hybrid Threats, Cyberterrorism and Cyberwarfare." CRC Press, 2024, 9-17.

Henrique, Silva, and Daniel Belmonte. "OSINT e relações internacionais: o caso dos militares russos em Donbas entre 2014 e 2021." *Revista Brasileira de Estudos Estratégicos REST* V15 Nº29 (Jan-Jun 2023), 70-92. Acessado em 8 de abril de 2024. http://rest.uff.br/index.php/rest/article/view/291.

Iftikhar. "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures." Faculty of Computer Studies, Arab Open University, Riyadh, Saudi Arabia (15 de janeiro de 2024), 3-32. Acessado em 20 de abril de 2024. https://peerj.com/articles/cs-1772/.

Jensen. "The Tallinn Manual 2.0: Highlights and Insights." Brigham Young University Law School, 2017, 15-44. Acessado em 17 de abril de 2024. https://heinonline.org/HOL/LandingPage?handle=hein.journals/geojintl48&div=30&id=&page=.

Mueller, Jensen, Valeriano, Maness, and Macias. “Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative.” *Center for Strategic and International Studies (CSIS)*, julho 2023, 15-26.

Oliveira de Souza, Ronaldo. “Guerra híbrida e ciberconflitos: uma análise das ferramentas cibernéticas nos casos da Síria e conflito Rússia-Ucrânia.” *Revista eletrônica Estácio Recife*, 2019, 6-17. Acessado em 15 de abril de 2024. https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/XIII_cadn/guerra_hibrida_e_ciberconflitos_uma_analise_das_ferramentas_ciberneticas_nos_casos_da_siria_e_conflito_russiaucrania.pdf.

Smith, Brad. “Defending Ukraine: Early Lessons from the Cyber War.” *Microsoft*, (Junho 2022), 10-27.

U.S. Department of Defense. “DOD Cyber Strategy Summary”, 2023, 18-24.

Usman, Tabbasum, Ahmad, Shahzad, See fewer. “Cyber-warfare Versus Cyber-terrorism: An Emerging 21st Century Trend.” *Journal of Politics and International Studies*, (10 de dezembro de 2023), 149-155. Acessado em 10 de abril de 2024. https://plantsghar.com/index.php/45/article/view/1321/1310.

La población como objetivo estratégico de las acciones cibernéticas: Desafíos para la defensa y seguridad multidimensional presentes (o no) en las Políticas y Estrategias Nacionales de Seguridad Cibernética.

Coronel Aviador (FAB) Claudio D. FARIA [1]

Recibido: 15 de mayo de 2024; Aceptado: 26 de junio de 2024.
Revisión al español: Coronel Pedagogo (FARD) Adamilca Emelinda Rodríguez Martínez
Claudio D. Faria, "La población como objetivo estratégico de las acciones cibernéticas: Desafíos para la defensa y seguridad multidimensional presentes (o no) en las Políticas y Estrategias Nacionales de Seguridad Cibernética," *Hemisférico Revista del Colegio Interamericano de Defensa 10* (2024): 26-43. https://doi.org/10.59848/24.1207.HV10n2

Resumen

Este artículo explora el contexto contemporáneo del ciberespacio, destacando la creciente importancia de la ciberseguridad. Se enfatiza la necesidad de defensas efectivas para proteger la información y se subraya la ciberhigiene como una posible línea de defensa a través de la concientización del usuario. El texto discute la persistencia de la cultura de la transgresión, en relación con este concepto y examina el papel de la educación en ciberseguridad en la promoción de la resiliencia nacional. Se aborda la importancia de proteger a la población contra influencias psicológicas de ataques cibernéticos, abogando por que la revisión de las Estrategias Nacionales de Ciberseguridad incluya a la población como una "infraestructura crítica". Las políticas públicas centradas en las personas son esenciales para anticipar los efectos adversos de tales amenazas cibernéticas sobre la población, a fin de evitar que se convierta en arma eficaz y eficiente que exija su seguridad y defensa.

Palabras clave: Ciberhigiene - resiliencia nacional – ciberataques - operaciones psicológicas - infraestructura crítica – anarquía - estrategia nacional de ciberseguridad.

Abstract

This article explores the contemporary context of cyberspace, highlighting the increasing importance of cybersecurity. It emphasizes the need for effective defenses to

[1] El Coronel Claudio Faría se desempeña actualmente en el Colegio Interamericano de Defensa como Jefe de la División de Facilitadores y Mentores del Departamento de Estudios y egresado distinguido de la Clase 62 del CID. Es piloto de la Fuerza Aérea de Movilidad, y su última asignación fue en el Comando de Estado Mayor de la Fuerza Aérea Brasileña, donde tuvo la oportunidad de trabajar en la implementación del nuevo Centro de Operaciones de Ciberdefensa de la Fuerza Aérea. El presente artículo refleja sus propios puntos de vista y reflexiones personales sobre temas del ciberespacio, explorando lo que había aprendido durante su tiempo como estudiante del Colegio Interamericano de Defensa. Correo electrónico: *Claudio.faria@iadc.edu*. https://orcid.org/0009-0009-0582-7019

protect information and underscores cyber hygiene as a possible line of defense through user awareness and education and its implications. The text discusses the persistence of the culture of transgression, especially in Latin America, regarding this concept and examines the role of cybersecurity education in promoting national resilience.

The importance of protecting the population against psychological influences resulting from cyber-attacks is also addressed, advocating that the revision of National Cybersecurity Strategies should include the population as a "critical infrastructure". People-centered public policies are essential to anticipate and mitigate the adverse effects of such cyber threats on the population, aiming to prevent it from becoming an effective and efficient weapon that demands its security and defense.

***Keywords**: Cyber hygiene - national resilience - cyber-attacks - psychological operations - critical infrastructure – lawlessness - national cybersecurity strategy*

Introducción

"*Es necesario esconderse en el seno de la tierra, como las venas de agua, cuyas ramificaciones son insondables. Así ocultarás todas tus diligencias*".[2]

Basándome en estas frases atribuidas a Sun Tzu y que son, para mí, fuente de inspiración, empiezo este artículo creyendo que las palabras que se le atribuyen durante siglos encajan perfectamente, pero con una diferencia: "tierra" sería "ciberespacio", tiempo en el que, evidentemente, esto no existía.

Haciendo las comparaciones y reflexiones, el "Arte de la Guerra" encaja muy bien como referencia y base para que las personas activas en este nuevo dominio creen su propio "Arte Operacional" y que esto sea para el beneficio general de la humanidad y en defensa de los más débiles y oprimidos. Por lo tanto, tal frase del general chino encaja en el tema cibernético, que ahora se está desarrollando.

El lector podrá reflexionar mejor y en consecuencia correlacionar los conocimientos derivados de la seguridad multidimensional, la defensa y la economía de la seguridad, la aplicación de teóricos y pensadores estratégicos, las relaciones

[2] Sueli Cassal, "Sobre el arte de maniobrar las tropas", en Arte da guerra (Porto Alegre: L&PM, 2006), 24.

internacionales, entre otros. Todo ello reafirma el papel transversal que tiene como principal característica la actividad cibernética.

La creciente dependencia de la tecnología e Internet ha hecho que la ciberseguridad sea una preocupación cada vez más importante para los gobiernos, las empresas y las personas. Los medios de defensa son indispensables. Negar ventajas operativas en el ciberespacio por acciones maliciosas es un factor crucial para mantener la confidencialidad, integridad y disponibilidad de este nuevo dominio, recordando que estas tres palabras representan las principales propiedades de la ciberseguridad contenidas en la Recomendación UIT-T X.1205, 2008 de la Unión Internacional de Telecomunicaciones (UIT), organismo de las Naciones Unidas.

Así, en este artículo, describiré cómo entiendo que el ser humano se ha convertido en una pieza fundamental y centro de gravedad para ser considerado como un importante contribuyente a la ciberseguridad y, al mismo tiempo, un objetivo compensador frente a las acciones subversivas surgidas del ciberespacio de hoy y también del mañana.

Primera línea de defensa: higiene cibernética

¿Qué es la higiene cibernética?

En primer lugar, podemos entender el concepto de ciberhigiene, consultando a una de las empresas líderes en el sector: Kaspersky, que la define como los pasos que deben dar los usuarios de ordenadores y dispositivos conectados a internet para aumentar la seguridad de su información, a través de una postura mental y hábitos diarios, con el fin de mitigar las posibles aperturas y posibilidades ante un intruso.[3]

Algunos ejemplos de procedimientos de saneamiento cibernético incluyen el uso de firewalls para evitar el acceso no autorizado; uso de contraseñas seguras; cambios frecuentes de contraseñas; no usar contraseñas 1234...; usar contraseñas diferentes para dispositivos IoT; emplear autenticación multifactor (evitar acciones de robots e IA); realizar copias de seguridad de sus datos personales y de interés en dispositivos de disco duro externos; evite publicar datos personales en las redes sociales (observe el fondo de sus fotos antes de publicarlas); no responder a encuestas que soliciten sus datos

[3] Kaspersky, "Los mejores consejos para la higiene cibernética para mantenerse seguro en línea. Cyber Hygiene Definition," acessado em 11 de fevereiro de 2023, https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

personales; evitar acceder a redes Wi-Fi gratuitas en lugares públicos (contratar un servicio de proveedor privado de internet con contrato y políticas de privacidad); mantener actualizadas las aplicaciones y el software (programar el móvil para que lo haga de madrugada); eliminar las aplicaciones que ya no sean útiles; no utilizar su *nombre personal como nombre de las* redes WiFi domésticas*; utilizar servicios contratados de encriptación de datos en la nube; entre otros.*

¿Por qué no es totalmente eficiente y eficaz? ¿Qué hacer?

Aun considerando que existen varias iniciativas para alertar a los usuarios; sin embargo, lamentablemente, la cultura de la transgresión sigue presente en la vida cotidiana de las personas, especialmente en América Latina, como nos traen Sorj y Martuccelli.[4]

Muchos, a pesar de tener acceso a materiales de orientación en ciberhigiene, no los consultan y no los implementan en casi nada, porque entienden que las reglas y normas son solo para otros y no tienen nada que ver con ellos mismos, corrompiéndose con este pensamiento egoísta que afecta a la colectividad, especialmente cuando se trata de ciberseguridad, a nivel mundial. Muchas personas se conectan cada año.

Sin embargo, esta situación no debe desanimar un proceso de instrucción y fortalecimiento de la doctrina de la ciberhigiene. Para reforzar esta tesis, traigo a Newmeyer.[5] Él, a través de sus recomendaciones, afirma que el sector educativo debe ser tomado en cuenta en la elaboración y ejecución de las Estrategias Nacionales de Ciberseguridad (ENSC).

Su comparación con el sector de la salud pública es perfecta, a mi juicio, para entender más fácilmente el poder de las acciones preventivas (higiene) aplicadas al ámbito cibernético (ciberhigiene) como forma de mitigar las diligencias indeseables ocultas en el ciberespacio. De hecho, en lo que respecta a la ENSC, al consultar a mi país, noté que en dos de sus Objetivos Estratégicos hay un punto a la necesidad de aumentar la

[4] Bernardo Sorj y Danilo Martuccelli, "Problemas y promesas: economía informal, crimen y corrupción, normas y derechos," en *El desafío latinoamericano: cohesión social y democracia* (São Paulo/Río de Janeiro: Instituto Fernando Henrique Cardoso, 2008).

[5] Kevin Newmeyer, "Elements of National Security Strategy for Developing Nations," en *National Cybsersecurity Institute Journal* Vol.1, No.3 (Nueva York: Excelsior College, 2015), 17, consultado el 11 de febrero de 2023, http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf, 13-15.

resiliencia brasileña frente a las amenazas cibernéticas y fortalecer el desempeño de la ciberseguridad en el escenario internacional.

Newmeyer continúa afirmando que, a medida que más y más sistemas están interconectados, se hace imprescindible contar con campañas educativas dirigidas a difundir materiales doctrinales e informativos que contengan buenas prácticas que permitan a los ciudadanos protegerse y contribuir a que todos los componentes de la infraestructura general de las tecnologías de la información y la comunicación (TIC) funcionen de manera satisfactoria y, sobre todo, resiliente.

Si las personas evitan cambiar su conducta de seguridad frente al uso de las TIC, considerando el ciberespacio, es poco probable que las acciones maliciosas de los ciberdelincuentes o ciberatacantes no logren el éxito esperado, porque si las personas confían solo en el desempeño del aparato estatal, aún no está dimensionado para soportar tal demanda de defensa y ciberseguridad.

Digo esto en términos del número de especialistas, así como en términos de sus cualificaciones profesionales apropiadas y sus necesidades de cursos constantemente actualizados.

Pero ¿por qué este énfasis en la individualidad como refuerzo de una colectividad?

Educación en ciberseguridad y resiliencia nacional

Pues bien, para tratar de presentar una posible respuesta a esta pregunta, traigo a la mente los elementos componentes de la actividad cibernética, tal y como se enseña en el CID, y también con lo que entiende Microsoft, que son: Perpetrador, Objetivo, Acción e Impacto, destacando que el usuario común puede, sí, ser un perpetrador de una ciberamenaza, sirviendo como un *útil Insider*[6] comprometiendo los sistemas con su mala praxis y conducta, como aprendí de Mariano Bartolomé en sus clases en este mismo Colegio.[7] [8]

[6] Por definición general, sería la persona que tiene alguna relación con la institución (personal o profesional) objeto de acciones cibernéticas maliciosas que, intencionadamente o no, sirven como agentes facilitadores de las consecuencias perjudiciales de estos actos.

[7] Mariano Bartolomé, "*Características de las cibercomodidades,"* (Washington-DC: Colegio Interamericano de Defensa, Curso de Ciberseguridad y Seguridad Pública de la Maestría en Defensa y Seguridad, 2023), diapositiva 29.

[8] Microsoft, "Evaluating Behavior in Cyberspace," em *International Security Norms: Reducing conflict in an Internet-dependent world*, acessado em 11 de fevereiro de 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA, 6.

Se puede ver que muchas personas siguen siendo víctimas de técnicas de *phishing* y terminan contribuyendo a un proceso de *ransomware* en su vida personal y profesional. Esta situación se ha agravado durante la pandemia, como también nos traen Bartolomé y Lima en un artículo haciendo hincapié en el trinomio Crimen, Terrorismo y Ciberespionaje. Los autores nos muestran que, solo en el primer semestre de esta enfermedad en 2020, los ciberataques crecieron un 34% en comparación con el mismo periodo anterior.[9]

De esta manera, considero importante fortalecer la educación de la persona común a través de la enseñanza y difusión de las mejores prácticas en materia de ciberhigiene como una forma de contribuir a lograr un mayor nivel de seguridad ciudadana en general.

Vale la pena subrayar aquí en este punto que los derechos de una persona están limitados por los derechos de los demás, por la seguridad de todos y por las justas exigencias del bienestar común y general, como nos ha traído el artículo XXVIII de la Declaración Americana de los Derechos y Deberes del Hombre desde 1948.

Creo que, al hacerlo, estaríamos contribuyendo a un mayor grado de resiliencia nacional frente a las acciones malvadas que se esconden en el entorno del ciberespacio. Esto puede ayudar mucho a los países del hemisferio, ya sea con más o menos recursos, a ofrecer un mayor grado de dificultad a los ciberdelincuentes, que tendrían más dificultades para actuar.

Sin embargo, como ciudadano interamericano, me sigue preocupando ver indicadores como los presentes en el Informe de Ciberseguridad de la OEA.[10] Los países de América Latina aún tienen un desempeño inferior al satisfactorio, especialmente en base a los resultados de las dimensiones nº 2 y nº 3, en sus ítems D2.1, D2.3 y D3.1.

Estos tres anteriores se refieren al tema de la Madurez Cibernética analizado en los estándares de esta organización internacional y se relacionan con la mentalidad de ciberseguridad, la comprensión del usuario de la protección de la información personal en internet y la concienciación, respectivamente, que traigo aquí para reforzar que el

[9] Mariano Bartolomé e André Lima, "La pandemia como uma amenaza a la vida y a la seguridad del Estado. El ciberespacio, durante y después de la pandemia COVID-19," em *Revista Academica de Guerra del Ejército Ecuatoriano*, Vol.14, No. 1 (Quito: CEHE, 2021), 72

[10] Organización de los Estados Americanos, "Perfiles de países," en *Informe de Ciberseguridad 2020: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe* (Washington-DC: BID, 2020), consultado el 21 de febrero de 2023, https://www.cybersecurityobservatory.org/#/final-report, 45-179.

usuario común sigue siendo un objetivo útil capaz de ser explotado por ciberdelincuentes y similares, afectando así a la ciberseguridad nacional en el ámbito de una seguridad multidimensional en esta parte del mundo.[11]

Al consultar con la UIT, apunta en cierta medida en la dirección de lograr cierto grado de ciberseguridad nacional, sugiriendo que los gobiernos y el sector privado deberían prevenir, detectar y responder a la ciberdelincuencia y al uso indebido de las TIC a través de una legislación que permita la investigación y el enjuiciamiento con el fin de ofrecer asistencia mutua; fortalecer el apoyo institucional a nivel internacional y fomentar la educación con el consiguiente aumento de la conciencia situacional del problema.

Me llama la atención aquí sobre la ratificación de la UIT en el punto en cuestión sobre la importancia de la cibereducación ciudadana como forma de sumar esfuerzos para reducir el poder de penetración maliciosa desde el ciberespacio. Este conocimiento se proporciona a través de su Resolución nro. 174.

En general, creo que esas contribuciones internacionales son válidas e incluso pueden alentar a los Estados a adoptar medidas preventivas, incluida la cuestión del uso del ciberespacio. Las Organizaciones no Gubernamentales (ONG) también están entrando en escena para unir fuerzas en esta misma dirección. Veamos un ejemplo de mi país. Louise Huriel, del Instituto Igarapé, propone algunas recomendaciones para la redacción/actualización de la Estrategia Nacional de Ciberseguridad de Brasil.[12]

En ellos, hay algunos en cuanto a elevar el nivel de madurez de la sociedad en ciberseguridad. Este ítem tiene 14 preguntas para mejorar este documento nacional. Destaco aquí algunos de ellos como ejemplos: crear eventos formativos para la ciudadanía, llevar a cabo acciones de sensibilización de la sociedad en general; y crear políticas públicas que promuevan la concientización permanente, entre otras que han sido propuestas por esta ONG dedicada.

[11] Siempre en relación con la ciberseguridad nacional, es importante aportar sus cinco perspectivas expuestas en el Manual de "Seguridad Cibernética Nacional" elaborado por el CCDCOE de la OTAN, a saber: Ciberseguridad Militar; la lucha contra la ciberdelincuencia; Inteligencia y Contrainteligencia de la Fuente Cibernética; Protección de Infraestructuras Críticas Nacionales y Gestión de Crisis; y la Ciberdiplomacia, para entender que todo está interconectado y debe ser visto como un único ecosistema global.

[12] Louise Huriel, "Ciberseguridad en Brasil: un análisis de la estrategia nacional," en *Artículo Estratégico 54*, (Río de Janeiro: Instituto Igarapé, 2021), visitado el 21 de febrero de 2023, https://ciberseguranca.igarape.org.br/estrategia/, 39

Además, creo que, si tengo la oportunidad, ofrecería la sugerencia de insertar otra recomendación para las ENSC de los países que aún no las han implementado, esto es: adoptar el término Ciberhigiene, ya que esta palabra, a mi juicio, tiene la fuerza suficiente para una fácil comprensión y absorción por parte del ciudadano común, así como aprovechar la comparación con la actividad sanitaria es un factor muy apropiado y oportuno para facilitar la comprensión y lograr para tener más éxito en el esfuerzo educativo.

Además, otros documentos internacionales ya lo han adoptado, como el Manual Nacional de Ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN) y el Manual de Derecho Internacional Humanitario aplicable a la Guerra Cibernética, también de la OTAN/CCDCOE y adoptado por países de este hemisferio como fuente y referencia.[13]

En mi paso por el Estado Mayor de la Fuerza Aérea de Brasil, participé especialmente en los equipos de trabajo para la creación e implementación del Sistema de Ciberdefensa de la Fuerza Aérea. En ese momento, el equipo tuvo cuidado de incluir un sector específico para la ciber educación en las propuestas para la estructura organizativa de la unidad responsable de actuar como órgano central de este sistema. Así, una de sus tareas era, precisamente, promover la concienciación del público interno con el fin de obtener un mayor grado de resiliencia, es decir, del público objetivo interno en su vertiente de conducta individual y grupal.

Quisiera recordarles que hemos utilizado muchos productos fabricados por la Junta Interamericana de Defensa y el CSIRT brasileño (CTIR.GOV), con el fin de obtener un mayor grado de solidez frente a una iniciativa de este tipo.[14] [15]

Ahora veo que hemos contribuido, indirectamente, también al público externo, es decir, a la gente común, porque los militares y servidores civiles de la Fuerza Aérea tienen familias y estas son potenciales difusores de técnicas de ciberhigiene en sus hogares, propagándolas de manera beneficiosa y, de esta manera, contribuyendo a la concientización general, lo que resulta en un excelente aporte al esfuerzo nacional.

[13] El Centro de Excelencia Cooperativo de Defensa Cibernética (CCDCOE) es una estructura de la OTAN dedicada a ayudar a los países en cuestiones de ejercicio e investigación con un enfoque en el fortalecimiento de las capacidades de defensa y ciberseguridad, considerando las áreas de entrenamiento, operaciones, tecnología, estrategia y legal.

[14] Junta Interamericana de Defensa, "Cyberdefense: News Bulletins," consultado el 24 de febrero de 2023, https://www.jid.org/ciberdefensa-2/.

[15] Centro Gubernamental de Prevención, Tratamiento y Respuesta a Incidentes Cibernéticos, "Recomendaciones," consultado el 23 de febrero de 2023, https://www.gov.br/ctir/pt-br.

Por lo tanto, la percepción sería que mantener altos estándares de higiene cibernética constantemente como una doctrina individual y colectiva por parte de los ciudadanos comunes, fortalecería el poder de resiliencia cibernética de un país. En consecuencia, también se puede inferir que cada país, al hacerlo, un grupo de países podría alcanzar un mayor grado de resiliencia en términos regionales. Esta sería una iniciativa para crear una cadena regional de defensa y ciberseguridad si todos lo hacen de manera coordinada. ¡Qué bonito sería eso! Sin embargo...

El eslabón más débil de la cadena

Después de haber estudiado el caso de Estonia en 2007, en el que el país sufrió una serie de acciones maliciosas orquestadas en el ciberespacio, noté un factor interesante que podría recibir atención. Allí, en palabras del general ruso Sergey Chekinov, citado por Beskow y Carley, señaló en 2013 que la nueva generación de guerra se caracterizará por operaciones de información y psicológicas que debilitarán a las Fuerzas Armadas y a la población del rival.

Así, el general continúa afirmando que estas acciones serán fundamentales para preparar el terreno para la victoria en lo que él llama la Revolución de las Tecnologías en el campo de batalla. Un año después, el brigadier Philip Breedlove afirma, en la OTAN, que Rusia está librando la más increíble *guerra relámpago* informativa, haciendo menciones a tácticas que implican el concepto de utilizar varias maniobras coordinadas con varios medios avanzando constantemente sobre un conjunto de objetivos y de manera rápida para no dar al enemigo oportunidades de reaccionar o reorganizarse para un nuevo ciclo de reacciones defensivas.

Llegados a este punto, la comparación sería muy oportuna, analizando el ciberespacio.

Vemos que, en el mismo año de 2014, los rusos intervienen en la guerra civil siria, en apoyo de Bashar al-Assad, y comienzan a apoyar a los separatistas prorrusos en la provincia de Donbass, en el este de Ucrania.

En tal escenario, los rusos también utilizan el ciberespacio para su campaña de desinformación, ya que Matos Barboza nos plantea el uso de la técnica del troll[16] para impulsar la opinión pública y ejercer presión sobre la población objetivo.[17] A los trolls se les encomendó la tarea de publicar comentarios en artículos de noticias 50 veces al día. Los que escribían *blogs* tenían que mantener seis cuentas de Facebook y publicar al menos tres *posts diarios*. En Twitter (ahora X), necesitaban tener al menos 10 cuentas, en las que publicaban 50 veces para mantener los efectos de este proceso.

En mi opinión, siguiendo a Visacro, digo que ya estamos en una guerra informativa contemporánea a través del ciberespacio.[18] El Jefe del Estado Mayor General de la Federación Rusa, General Valery Gerasimov, es citado por el autor en su disertación sobre los aspectos de una Guerra Híbrida, donde los medios no militares de carácter político, económico, social, humanitario e informativo aumentan la eficacia, con el fin de lograr objetivos políticos y estratégicos, y este punto también es visible en la doctrina rusa. Además de lo mismo que se nota en la doctrina china.

Traigo aquí al debate a Tarien y Priisalu que son unánimes en destacar en sus relevantes ponencias que hay, sí, presente en el mundo actual y comportándose como un hecho que lleva[19] el futuro en el que el objetivo de provocar el caos en un determinado grupo de ciudadanos, a través del sentimiento de pérdida de confianza y el sentimiento de impotencia y aislamiento por parte de sus gobiernos hacia ellos como resultado de los ciberataques.[20] [21]

¡Este es el punto clave de este artículo!

Cabe destacar que más que proteger las Infraestructuras Críticas, per se, lo importante sería conseguir que la población no entre en esta fase de influencia psicológica

[16] Según el contenido del libro, los trolls son personas contratadas y entrenadas para denigrar a los opositores de Putin, con más de 600 personas empleadas en toda Rusia y un presupuesto anual de 10 millones de dólares.

[17] Carlos Eduardo de Matos Barboza, "La estrategia rusa en el conflicto de Ucrania: contribuciones a la doctrina militar brasileña," (Río de Janeiro: Escuela de Estado Mayor del Ejército, 2018), visitado el 24 de febrero de 2023, https://bdex.eb.mil.br/jspui/bitstream/123456789/3868/1/MO%205965%20-%20MATOS%20BARBOZA.pdf, 54-55.

[18] Alessando Visacro, "Doing the Right Things: Security and Defense of the Modern State," en *Cadernos de Estudos Estratégica* nº 1 (Río de Janeiro: ESG, 2019), visitado el 21 de febrero de 2023, http://www.ebrevistas.eb.mil.br/CEE/article/view/6725/5821, 70.

[19] Definición disponible en el manual de Planificación Estratégica de la Escuela Superior de Guerra de Brasil.

[20] Jaak Tarien, "Ciberseguridad en Estonia 2020: Lo que ha cambiado", mesa redonda, 15 de junio de 2020, vídeo, 23:32.

[21] Jaan Priisalu et al, "Six Colours: War in cyberspace", OTAN-OTAN, 27 de abril de 2007, video, 8:25.

(pánico) y actúe como motor descontrolado para desequilibrar el equilibrio y las capacidades de las fuerzas de defensa nacional y de seguridad pública.

Recordando a Contreras, creo que el poder asimétrico sobre la seguridad multidimensional que las ciberamenazas imponen al mundo se puede correlacionar con el modelo número 2 de Beaufré, teniendo en cuenta objetivos, medios y libertad de acción.[22] Este sería el modelo de Presión Indirecta, mediante el cual se busca alcanzar objetivos políticos a través de la presión psicológica, sin utilizar la fuerza física directa.

En este caso, los medios utilizados son la propaganda, la diplomacia, el espionaje y el sabotaje, con el objetivo de debilitar la resistencia del oponente y facilitar la consecución de los objetivos políticos previstos. La libertad de acción es alta, ya que el uso de medios indirectos y no violentos le da al agente un gran margen de maniobra y flexibilidad, lo que permite la adaptación de las tácticas según lo requiera la situación.

En este contexto, me llamó la atención el caso de Estonia, especialmente cuando reflexioné sobre Andžāns y Bērziņa-Čerenkova, cuando fue posible darse cuenta de que, como resultado de las lecciones aprendidas en 2007, hubo un reordenamiento de la clasificación de sus Infraestructuras Críticas a Funciones Críticas y... *¡Sorpresa!* La sociedad estonia se considera la principal, y debe ser informada al Consejo Europeo sobre sus aspectos críticos y vulnerables.[23] Cabe destacar que en la ENSC de Estonia existe la disposición del Objetivo Estratégico número 1 que demuestra la atención prestada por los estonios en términos de que su sociedad esté digitalizada, cohesionada y, especialmente, ciberresiliente.[24]

Me parece, al leer su ENSC, que los estonios tienen un orgullo nacional de ser una sociedad verde/*sin papel*, así como confían en su sistema nacional de identificación personal protegido por encriptación. Esto aparece en muchas partes del texto del documento. De hecho, hasta este momento, ha sido el único país que hace referencia al concepto de reputación para que otros puedan considerarlo confiable y deseen hacer negocios con él a todos los niveles. Esto sería similar a cuando compramos a un vendedor,

[22] Arturo Contreras, "Estrutura y Lógica de la Estrategia Contemporánea" en *Estrategia: Las Viejas y las Nuevas Amenazas*, (Santiago: Mago Editores, 2007): 4.

[23] Consejo de la Unión Europea, *Directiva 2008/114/CE del Consejo*, en Diario Oficial de la Unión Europea, (Bruselas: UE, 2008), acessado em 26 de fevereiro de 2023, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF#:~:text=This%20Directive%20establishes%20a%20procedure,to%20the%20protection%20of%20people, 78-79. Nota del autor: Esta é referente ao Artigo IV da Diretriz 2008/114/EC.

[24] República de Estonia, "Cybersecurity Strategy - Strateegilised Eesmärgid," (Tallin: Ministerio de Asuntos Económicos y Comunicaciones, 2019), acessado em 26 de febrero de 2023, *https://www.mkm.ee* › medios › descargar.

pero primero comprobamos su aceptación en cuanto a cuántas *estrellas* tiene, o incluso consultamos webs especializadas en internet para saber de antemano si el distribuidor es fiable y si debemos o no seguir adelante con la compra o contratación del servicio.

Recordando una vez más a Newmeyer, nos ofrece los siguientes paradigmas en su obra: seguridad nacional, economía y salud.[25] Al estudiar los posibles casos recientes en los que las actividades cibernéticas pueden haber sido parte de los ataques a una entidad extranjera, llego a pensar que también sería oportuno añadir, a los conceptos que el autor presenta, uno más por mi cuenta. Sería el paradigma psicosocial como una cuarta parte de esta lista. Llego a esta conclusión después de analizar el poder de las personas y su fuerza en la seguridad multidimensional.

De hecho, otro factor importante que Newmeyer también había destacado en su investigación sobre la ENSC sería que una de las grandes dificultades es la falta de consenso sobre qué agencia se encargaría de liderar el proceso de resolución de crisis en casos cibernéticos. Reflexionando ahora: quienquiera que sea una agencia de este tipo, ¿tendría el personal capacitado para prever la posibilidad de ocurrencias de disturbios sociales cuya ignición habría sido originada, motivada, iniciada debido a una influencia cibernética engañosa?

Sé que esta fue una pregunta retórica solo para mostrar, elocuentemente, la importancia que veo en el aspecto del ciudadano, de la persona humana, de las personas mismas, como un actor racional, pero ampliamente influenciado hasta el punto de que es objeto de operaciones psicológicas por parte de ciberatacantes, algo que ninguna ENSC a la que he tenido acceso trata directamente y con la debida claridad ante la importancia de proteger a las personas del miedo, desesperación, agonía y tantos otros malos sentimientos, que pueden llevar a una manifestación masiva en oleadas de violencia. Que los ciudadanos comunes practiquen actos oscuros porque perciben cualquier posibilidad de perder la satisfacción de sus necesidades básicas, como se aprende consultando la pirámide de Maslow.

Veo que la regla 29 del Manual de Tallin[26] contribuye en este sentido y puede considerarse desde mi punto de vista que la persona humana en la sociedad se convierte

[25] Newmeyer, 9-19.

[26] La regla 29 del Manual de Tallin se refiere a la protección de que los civiles puedan ser considerados combatientes si se demuestra que participan en actos de beligerancia u hostilidades entre las partes. Tiene como referencia el Primer Protocolo Adicional (1977) de los Convenios de Ginebra (1949) en su esencia

en un objetivo primario no combatiente hoy y cada vez más en el mañana, como nos trae Schmitt.[27]

Desde Oriente, los autores Xiangsui y Liang traen la confirmación de que esta misma sociedad está en la lista de posibles objetivos a explotar, según la doctrina china.[28] Esto se llevaría a cabo a través de una mezcla de tácticas convencionales agregadas con tácticas informativas que, a través de un combate cruzado y coordinado, tiene como objetivo generar sinergia en la acción y, así, obtener un mayor grado de impacto en el adversario de adentro hacia afuera. Además de traer una parte clara de la doctrina china que explora una acción híbrida en el combate contemporáneo, los autores del libro Guerra sin restricciones también se refieren a la importancia de contar con un Comando Conjunto como estándar de liderazgo y que esté compuesto por varios especialistas multidisciplinarios.

En mi experiencia profesional, tuve la oportunidad de pertenecer a algunos Comandos Conjuntos de la estructura de defensa militar brasileña. No recuerdo que existiera una célula, un sector, una sección, un departamento, una división diseñada para predecir y proporcionar acciones psicológicas sobre una población objetivo o parte de ella. Sí, ya sé que existe una estructura de relación Cívico-Militar, pero con otras atribuciones diferentes al enfoque de este artículo, es decir: la población como Infraestructura Crítica a proteger... y voy a ir más allá: un Sistema Crítico para tener en cuenta.

En la época en que tuve la oportunidad de participar en el proceso de revisión de la ENSC en mi país, antes de ser estudiante del CID (Clase 62),[29] recuerdo que el equipo hizo sugerencias en la época, sin embargo, no teníamos la percepción, idea o reflexión de que la población brasileña, independientemente del avance de las tecnologías disruptivas, podría convertirse en uno de los centros de gravedad y talón de Aquiles para infligir mayores demandas de apoyo y atención por parte de la población brasileña, parte de los medios de seguridad y defensa nacional hasta una gran escala. Por lo tanto, lamentablemente no sugerimos nada al respecto, pero siempre habrá nuevas oportunidades al reanudar el debate público sobre la revisión de la ENSC en Brasil.

[27] Michael Schimitt, "Conferencia PILAC sobre Operaciones Cibernéticas y DIH: Líneas de Falla y Vectores," *Programa HLS sobre Derecho Internacional y Conflictos Armados*, 3 de abril de 2015, 56:23.

[28] Xiangsui, Wang y Liang, Qiao. "Diez mil métodos combinados en uno: combinaciones que trascienden las fronteras" en *Unrestricted War* (Pekín: Casa del EPL, 1999).

[29] *¡La Mejor!* (Esta es una referencia a una tradición muy particular del Colegio Inter-Americano de Defensa cuando se nombra la clase actual, con la que se dice en voz alta: *¡La Mejor!*)

¿Y qué?

Ahora... ¡sencillo!

No es posible *prever* si no somos capaces de *prever*.

Para predecir, es necesario explorar el debate de manera amplia con la debida diversidad de pensamiento y experiencia. Ideas innovadoras. Ampliar las percepciones.

Objetivo: Predecir, predecir y predecir qué puntos pueden ser explotados por el ciberatacante.

¿Cuál de estos tiene el potencial de generar efectos psicológicos negativos y, en consecuencia, revueltas masivas en la población, o en parte de ella, es editar una lista priorizada de tales puntos en los planes nacionales de resiliencia, capaz de orientar la idealización, elaboración, implementación y revisión de las políticas públicas con el fin de fortalecer la respuesta gubernamental que sea realmente perceptible para la población y que esta sea oportunamente rápida? De esta manera, creo que también tendríamos un cierto efecto disuasorio sobre los aspirantes a aventureros del ciberespacio.

Dato: Estamos jugando con el equipo en desventaja y defensivamente.

El adversario tiene un comportamiento operativo difícil de predecir, detectar y que se adapta rápidamente utilizando el avance *supersónico* de las tecnologías disruptivas.

De hecho, no conozco soluciones fáciles que se apliquen a muchos casos al mismo tiempo; soluciones definitivas y decisivas. Sin embargo, creo que tenemos que ser más ágiles en términos de planificación estratégica a largo plazo. Por cierto, me pregunto ahora: ¿Qué sería a largo plazo, teniendo en cuenta la cibernética? Pues bien, las ENSC suelen recibir sus revisiones y posibles actualizaciones en ciclos de unos pocos años, dependiendo del país que las haya editado.

¿Sería esto coherente con la realidad de los cambios en el escenario percibido por el ciudadano común a través de los medios de comunicación globalizados en estos días?

Así, nos acercamos al final de este artículo considerando lo mencionado en párrafos anteriores sobre el tema de la importancia de definir un organismo centralizador para la planificación de acciones que logren el grado de resiliencia en niveles satisfactorios. Teniendo en cuenta la velocidad y los impactos que las actividades maliciosas tienen en las infraestructuras críticas; considerando que, en ocasiones, los medios de defensa y seguridad nacional no están a la altura de lo que realmente necesita

un país, e incluso por su extensión geográfica, que tiene dificultades para satisfacer más de una demanda al mismo tiempo en su territorio; que el adversario es consciente de tales debilidades y está seguro de que puede explotarlas; y, finalmente, considerando que, una vez que se percibe la ineficiencia del Estado para proveer a la seguridad de su pueblo y la satisfacción de sus necesidades básicas, el adversario los utiliza como fuerza anárquica e impulsora para agotar todos los medios y, así, interferir en el mantenimiento de la deseable y necesaria paz social, surge una reflexión: no es tan simple como se dijo en la apertura de esta parte.

Sin embargo, me gustaría reiterar que debemos revisar nuestras ENSC. Entender que la población debe ser concebida como la "*infraestructura*" crítica más importante de una nación. Por lo tanto, una vez que este concepto sea constante y ampliamente debatido, ya que estaría contemplado en un documento al más alto nivel estatal, derivará de él políticas públicas más coherentes con la realidad del escenario operativo.

Aquí está nuestro "¿y qué?"

El centro de atención se centra más en *las personas* y menos en *las cosas*.

De este modo, nos damos la oportunidad de predecir mejor el comportamiento anárquico causado por estas variables abordadas. Prever en tiempos de paz. Documentar para no olvidar y debatir con más frecuencia y agilidad gubernamental. Mejorar nuestro proceso de planificación estratégica basado en capacidades para aquellos que lo han implementado.

En consecuencia, es mejor predecir para proporcionar mejor.

Reflexiones finales

Al final, el lector se da cuenta de que mi enfoque estaba en las personas. Creo que, en el funcionamiento de cualquier tecnología, el ser humano siempre será el eslabón más débil de la cadena. Por lo tanto, está claro que la higiene cibernética es un tema crucial y contribuye al poder de resiliencia cibernética de un país y a mitigar las posibilidades de interferencia ilícita que surgen y se ocultan en las "ramificaciones insondables de las venas de agua" del ciberespacio, recordando el pasaje de Sun Tzu dicho en la introducción de este artículo.

No se puede dejar de lado los sentimientos de las personas. Lo que les hace sentir miedo, angustia y desesperación. Perder su dinero, perder la seguridad de su casa... de su familia, debido a los ataques cibernéticos que fueron exitosos por el adversario. Este es

más un reino para operaciones psicológicas y para obtener ventajas sobre los objetivos con el fin de obtener su estado final deseado sobre otros que no estaban preparados y no eran conscientes.

Un asesor estratégico de alto nivel, que también ha sido capacitado por el CID, no debe olvidar esto y la redacción de los diversos y variados resultados de aprendizaje descritos en cada *Syllabus*, de los cuales traigo aquí algunos relacionados con el tema de la ciberseguridad, haciendo hincapié en el trabajo de la asesoría de más alto nivel, que son: abordar los riesgos que las amenazas cibernéticas representan para la seguridad pública, defensa y seguridad nacional; diagnosticar los principales desafíos críticos de ciberseguridad en el hemisferio e interpretarlos desde una perspectiva de seguridad multidimensional; ofrecer diferentes medidas y recomendaciones para abordar los desafíos de la ciberseguridad; integrar diferentes conocimientos y saberes sobre el tema; formular recomendaciones y colaborar en el proceso de toma de decisiones a nivel estratégico, para abordar los desafíos de ciberseguridad, incluyendo respuestas multilaterales, entre otros.

Al fin y al cabo, todos somos conscientes de que somos servidores públicos en la esencia de la palabra y, como tales, tenemos en la persona humana la razón de nuestro trabajo. Así que, finalmente, el mensaje sería que podemos ser más atentos, creativos, inteligentes y perspicaces. Igualmente, estar en hermandad con las naciones vecinas, ya que el entorno cibernético no tiene en cuenta ningún límite físico para lanzar su interferencia.

El bienestar de nuestros pueblos debe ser la tónica frente a este nuevo espacio dimensional, que aún no es la última frontera,[30] que requiere un enfoque multidisciplinario y multidimensional, explorando la diversidad del pensamiento crítico y libre de ataduras. También nos desafía a saber hasta dónde puede llegar la humanidad para bien o para mal; individual o colectiva; en el hoy y en el mañana, yendo audazmente a donde antes no imaginábamos.

Bibliografía.

[30] Menciona el inicio de la serie de televisión iniciada en los años 60 y creada por Gene Roddenberry. Siguió durante décadas más tarde como la franquicia de Star Trek y presenta los viajes de la nave espacial Enterprise al espacio, la última frontera, en su misión de cinco años para explorar nuevos mundos, nuevas civilizaciones, yendo audazmente a donde ningún humano ha ido antes. Aquí, es apropiado hacer un paralelismo con el ciberespacio.

Barboza, Carlos Eduardo de Matos. "La estrategia rusa en el conflicto de Ucrania: aportes a la doctrina militar brasileña." (Río de Janeiro: Escuela de Estado Mayor del Ejército, 2018). Consultado el 24 de febrero de 2023, ttps://bdex.eb.mil.br/jspui/bitstream/123456789/3868/1/MO%205965%20-%20MATOS%20BARBOZA.pdf, 54-55.

Bartolomé, Mariano. "*Características de los ciberservicios."* (Washington-DC: Colegio Interamericano de Defensa, Curso de Ciberseguridad y Seguridad Pública de la Maestría en Defensa y Seguridad, 2023). Diapositiva 29.

Bartolomé, Mariano e Lima, André. "La pandemia como uma amenaza a la vida y a la seguridad del Estado. El ciberespacio, durante y después de la pandemia COVID-19." Em *Revista Academica de Guerra del Ejército Ecuatoriano.* Vol.14. No. 1 (Quito: CEHE, 2021), 72.

Brasil. Centro Gubernamental de Prevención, Tratamiento y Respuesta a Incidentes Cibernéticos. "Recommendations." consultado el 23 de febrero de 2023. https://www.gov.br/ctir/pt-br.

Cassal, Sueli. "Sobre el arte de maniobrar las tropas." en *Arte da guerra* (Porto Alegre: L&PM, 2006). 24.

Contreras, Arturo. "Estrutura y Lógica de la Estrategia Contemporánea" en *Estrategia: Las Viejas y las Nuevas Amenazas.* (Santiago: Mago Editores, 2007): 4.

Estados Unidos de América. Junta Interamericana de Defensa. "Ciberdefensa: Boletines de Noticias." consultado el 24 de febrero de 2023. https://www.jid.org/ciberdefensa-2/.

Unión Europea. El Consejo de la Unión Europea. *Directiva 2008/114/CE del Consejo.* En Diario Oficial de la Unión Europea, (Bruselas: UE, 2008). Acessado em 26 de fevereiro de 2023. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF#:~:text=This%20Directive%20establishes%20a%20procedure,to%20the%20protection%20of%20people, 78-79.

Huriel, Louise. "Ciberseguridad en Brasil: un análisis de la estrategia nacional. en *Artículo Estratégico 54*, (Río de Janeiro: Instituto Igarapé, 2021). Visitado el 21 de febrero de 2023, https://ciberseguranca.igarape.org.br/estrategia/. 39

Kaspersky. "Los mejores consejos de higiene cibernética para mantenerse seguro en línea. Cyber Hygiene Definition." acessado em 11 de fevereiro de 2023. https://www.kaspersky.com/resourse-center/preemptive-safety/cyber-hygiene-habits.

Kevin Newmeyer. "Elements of National Security Strategy for Developing Nations." en *National Cybsersecurity Institute Journal* Vol.1. No.3 (Nueva York: Excelsior College, 2015). 17, consultado el 11 de febrero de 2023, http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf, 13-15.

Microsoft. "Evaluating Behavior in Cyberspace." em *International Security Norms: Reducing conflict in an Internet-dependent world*, acessado em 11 de febrero de 2023. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA, 6.

Organización de los Estados Americanos. "Perfiles de país", en *Informe de Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe* (Washington-DC: BID, 2020). Consultado el 21 de febrero de 2023, https://www.cybersecurityobservatory.org/#/final-report, 45-179.

Priisalu, Jaan et al. "Six Colours: War in cyberspace." OTAN-OTAN, 27 de abril de 2007, video. 8:25.

República de Estonia. "Cybersecurity Strategy - Strateegilised Eesmärgid." (Tallin: Ministerio de Asuntos Económicos y Comunicaciones, 2019). acessado em 26 de fevereiro de 2023. *https://www.mkm.ee* › medios › descargar.

Schimitt, Michael. "Conferencia de PILAC sobre Operaciones Cibernéticas y DIH: Líneas de Falla y Vectores." *Programa de HLS sobre Derecho Internacional y Conflictos Armados*. 3 de abril de 2015, 56:23.

Sorj, Bernardo y Martuccelli, Danilo. "Problemas y promesas: economía informal, crimen y corrupción, normas y derechos." en *El desafío latinoamericano: cohesión social y democracia* (São Paulo/Río de Janeiro: Instituto Fernando Henrique Cardoso. 2008).

Tarien, Jaak. "Ciberseguridad en Estonia 2020: Lo que ha cambiado." mesa redonda. 15 de junio de 2020, vídeo, 23:32.

Visacro, Alessandro. "Hacer lo correcto: seguridad y defensa del Estado moderno." en *Cadernos de Estudos Estratégica* nº 1 (Río de Janeiro: ESG, 2019) Visitado el 21 de febrero de 2023. http://www.ebrevistas.eb.mil.br/CEE/article/view/6725/5821, 70.

Xiangsui, Wang y Liang, Qiao. "Diez mil métodos combinados en uno: combinaciones que trascienden las fronteras." en Unrestricted War (Pekín: Casa del EPL, 1999).

A ameaça da guerra cognitiva na América: desafios e oportunidades para a cooperação interamericana.

Mario Brasil do Nascimento[1]

Recibido: 23 de abril de 2024; Aceptado: 26 de junio de 2024.
Mario Brasil do Nascimento, "A ameaça da guerra cognitiva na América: desafios e oportunidades para a cooperação interamericana". *Hemisferio Revista del Colegio Interamericano de Defensa 10 (2024): 44-67.* https://doi.org/10.59848/24.1207.HV10n3

Resumo

Este artigo trata da ameaça da guerra cognitiva no Continente Americano no âmbito das ameaças híbridas. Mediante pesquisa bibliográfica e estudo de casos de guerra cognitiva contra estados nacionais, foi possível delinear as características desse fenômeno, seus objetivos, estratégias e táticas. A acelerada evolução tecnológica, o surgimento das mídias sociais e a hiperconectividade das pessoas têm dado forma àquela modalidade de guerra e ao pensamento de Sun Tzu de vencer os oponentes sem necessariamente enfrentá-los de forma cinética. É plausível considerar que a América já está em guerra. O grande desafio é definir como preservar as democracias sem tender ao autoritarismo, ao cerceamento da liberdade de expressão e sem sucumbir diante da mudança da mente das pessoas. Por outro lado, a ameaça, se bem compreendida, pode se transformar em uma oportunidade para a integração de esforços e o estabelecimento de uma defesa cognitiva dos países e do hemisfério.

Palavras-chave: Guerra Cognitiva; Defesa Cognitiva; Cognição; Ameaça Híbrida; Continente Americano

Abstract

This article deals with the threat of cognitive warfare on the American Continent within the scope of hybrid threats. Through bibliographical research and case studies of cognitive warfare against national states, it was possible to outline the characteristics of this phenomenon, its objectives, strategies, and tactics. The accelerated technological evolution, the emergence of social media and the hyperconnectivity of people have shaped that type of war and Sun Tzu's thought of defeating opponents without necessarily facing

[1] Mario Brasil do Nascimento – Coronel veterano do Exército Brasileiro. Doutor em Relações Internacionais pela Atlantic International University, Mestre em Relações Internacionais e Resolução de Conflitos pela American Military University e Mestre em Segurança e Defesa Hemisférica pela ANEPE, Foi Aluno do CID – Classe 52 "La Mejor" em 2012 e Chefe dos Facilitadores em 2013. Atualmente, trabalha na Escola Superior de Defesa. mariobrasil86@gmail.com. https://orcid.org/0000-0003-1973-594X

them in a kinetic way. It is plausible to consider that America is already at war. The great challenge is to define how to preserve democracies without tending towards authoritarianism and restricting freedom of expression; and without succumbing to the change in people's minds. On the other hand, the threat, if well understood, can be transformed into an opportunity to integrate efforts, and establish a cognitive defense of countries and the hemisphere.

Keywords: *Cognitive Warfare; Cognitive Defense; Cognition; Hybrid Threat; American Continent*

Introdução

O Continente Americano possui aproximadamente 42 milhões de quilômetros quadrados,[2] constituindo-se o segundo maior continente do mundo depois da Ásia. Essa imensidão territorial abriga recursos importantes como água doce e biodiversidade, que já são alvos da cobiça internacional. 45,5% dos fluxos fluviais do mundo, por exemplo, estão na América.[3] 29% das florestas do planeta, fundamentais para regulação climática, se concentram no Continente Americano, sendo que esse abriga a Floresta Amazônica, maior floresta tropical e maior fonte de biodiversidade da Terra.[4] Além desses recursos, muitas outras riquezas se encontram presentes na América, como minerais, metais, petróleo, gás e solos agricultáveis. Nesse imenso território habitam cerca de 1 bilhão de pessoas,[5] onde predominam países democráticos (algumas democracias plenas e outras imperfeitas) e poucos regimes considerados híbridos (mistura de democracia e autocracias).[6]

A América tem conseguido se manter afastada das guerras que têm ocorrido ao longo dos tempos, particularmente na Europa, Oriente Médio e na Ásia. O último conflito

[2] Dado obtido a partir da soma das áreas de 35 países e algumas ilhas pertencentes ao Continente. Central Intelligence Agency. CIA World. Factbook.

[3] Vincent Dubreuil e François-Michel LeTourneau. "A água nas Américas. 2020". (março 2020), https://doi.org/10.4000/ideas.8459 Acessado em 05 de abril de 2020. https://journals.openedition.org/ideas/8459#quotation.

[4] Food and Agriculture Organization (FAO). "The State of the World's Forests: Forests, Biodiversity and People. 2020" (2020): 42. Acessado em 05 de abril de 2024. https://www.fao.org/3/ca8642en/online/ca8642en.html

[5] Worldometer (2024). Acessado em 05 de abril de 2020. https://www.worldometers.info/population/latin-america-and-the-caribbean/ e https://www.worldometers.info/world-population/northern-america-population/

[6] Álvaro Merino. "El mapa del índice de democracia en el mundo". (2024). Acessado em 05 de abril de 2024. https://elordenmundial.com/mapas-y-graficos/el-mapa-del-indice-de-democracia/.

entre países da região ocorreu em 1995 entre Equador e Peru.[7] Os últimos episódios de conflito envolvendo nações de outros continentes na América, que trouxeram algum risco para o Continente, foram: 1) a crise dos mísseis de Cuba em 1962;[8] e 2) a Guerra das Malvinas em 1982.[9] De acordo com dados do Institute for Economics & Peace, agregando os dados da América do Norte, América Central e Caribe e América Latina, tem-se que o Continente Americano ocupa a segunda melhor posição quanto ao índice global da paz (que abrange dados sobre conflitos internos e externos; segurança social; e militarização).[10] Quando se trata apenas da ocorrências de guerras interestatais, o Continente Americano, segundo os dados do Uppsala Conflict Data[11] se encontra em uma situação melhor que a dos demais continentes.

No entanto, as riquezas e a relativa paz que o Continente dispõe estão ameaçadas pelas guerras híbridas, sobretudo por aquelas que incidem sobre o pensamento e os valores das pessoas. A ameaça recai, em especial, sobre aqueles que formam a cultura estratégica relativa à segurança hemisférica.[12] Nesse contexto tem-se o fenômeno da guerra cognitiva, modalidade de guerra decorrente da combinação da evolução tecnológica das comunicações, do advento das mídias sociais, da hiperconectividade das pessoas; e dos avanços de conhecimentos da Neurociência, da Ciência de Dados e da Inteligência Artificial para identificar e atuar sobre as vulnerabilidades da mente humana. Na verdade, essa ameaça começou a ser delineada há muito tempo, quando Sun Tzu propôs que a mais alta excelência estava em obter a vitória de um inimigo sem lutar.[13]

---

[7] Oswal Sigüeñas Alvarado. "O Conflito do Cenepa em seus 25 Anos: Lições aprendidas Uma Análise do Uso dos Princípios do Poder Aeroespacial Peruano". *Revista Profissional da Força Aérea dos EUA*. no.3 (2021): 155. Acessado em 05 de abril de 2024. https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%203%20Issue%203/06-Siguenas_port.pdf

[8] William M. Morgan. "The Cuban Missile Crisis at 60 Where do we stand?" *Marine Corps History*. v.9. no.1. (Summer 2023):32. Acessado em 05 de abril de 2024. https://www.usmcu.edu/Portals/218/Marine%20Corps%20History_9_1_Summer%202023_Morgan_web.pdf

[9] Rodrigo Milindre Gonzalez Zimmermann. "A guerra das Malvinas/Falklands Desclassificada: A Arquitetura do Conflito a partir da Revisão dos Arquivos Oficiais da Argentina, Estados Unidos e Reino Unido" (2023):12. Acessado em 05 de abril de 2024. https://lume.ufrgs.br/bitstream/handle/10183/271073/001193928.pdf?sequence=1

[10] Institute for Economics & Peace. "Global Peace Index 2023." (2023):8-9. Acessado em 05 de abril de 2024. https://www.economicsandpeace.org/wp-content/uploads/2023/09/GPI-2023-Web.pdf

[11] Acessado em 05 de abril de 2024. https://ucdp.uu.se/downloads/index.html#armedconflict

[12] Yuriy Danyk e Chad M Briggs. "Modern Cognitive Operations and Hybrid Warfare." Journal of Strategic Security v.16, no.1. (2023): 39. https://doi.org/10.5038/1944-0472.16.1.2032.

[13] Sun Tzu. "A Arte da Guerra: Por uma Estratégia Perfeita." Tradução Heloísa Sarzana Pugliesi, Márcio Pugliesi. — São Paulo: Madras. (2005): 63.

Para a guerra cognitiva, o campo de batalha é a mente das pessoas[14] e os sistemas cognitivos não-humanos;[15] e seu objetivo vai além de modificar o pensamento dos homens.[16] Dessa maneira, o problema norteador deste artigo é o seguinte: quais são os desafios e as oportunidades para o Continente Americano em face da ameaça de guerra cognitiva, que já pode estar em curso, e muitos países americanos ainda não se aperceberam sobre tal fenômeno?

O tema é relevante pois a guerra cognitiva está inserida no âmbito da guerra híbrida,[17] que pode, efetivamente, ser empreendida contra países do Continente Americano, visando a fragmentação, a promoção do caos social e o atingimento de objetivos estratégicos contrários aos da América.

Diante desse cenário, o objetivo de artigo é analisar os desafios impostos pela guerra cognitiva ao Continente Americano e as oportunidades que o estudo do tema pode gerar, particularmente para cooperação interamericana. O artigo compreenderá: 1) uma seção relativa ao entendimento do fenômeno; 2) dois casos históricos do emprego de guerra cognitiva contra atores estatais; 3) uma seção referente aos desafios impostos por essa ameaça híbrida para a América; 4) uma seção acerca das oportunidades, sobretudo a cooperação hemisférica para o desenvolvimento da defesa cognitiva; e 5) conclusão.

Desenvolvimento

Guerra Cognitiva – entendendo o fenômeno

O primeiro registro de uso do conceito de "guerra cognitiva" não é preciso. Usando os motores de busca da Internet, verifica-se que a citação mais antiga a respeito de guerra cognitiva é de 1990,[18] referindo-se ao conflito decorrente da pressão sobre o

[14] James Giordano. Citado por François Du Cluzel. "Cognitive Warfare, a Battle for the Brain." STO-MP-AVT-211. NATO (2022):.KN3-4. Acessado em 09 de abril de 2024 https://doi.org/10.14339/STO-MP-HFM-334-KN3-PDF

[15] Frank Flemisch. "Human-machine teaming towards a holistic understanding of Cognitive Warfare." In Y. R. Masakowski, J. M. Blatny (eds.) Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-ET-356. (2023): 9-1 – 9:10. Acessado em 09 de abril de 2024. https://doi.org/10.14339/STO-TR-HFM-ET-356.

[16] Organização do Tratado do Atlântico Norte. "Cognitive Warfare: Strengthening and Defending the Mind." (2023). Acessado em 26 de março de 2024. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

[17] Tzu-Chieh Hung e Tzu-Wei Hung. "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars." *Journal of Global Security Studies*. (2020):2-3. https://doi.org/10.1093/jogss/ogac016.

[18] B. Pritchard. Cognitive Wars A-I Theory: An Appraisal *In Theory Vědy*. Tchéquia: Ústav, v.1/2. (1990):7:23.Acessado em27 de março de 2024. http://dk.kramerius.org/cdk/view/uuid:17fd3622-2e83-11e2-1418-001143e3f55c?page=uuid:17fd362b-2e83-11e2-1418-001143e3f55c&fulltext=cognitive%20war&source=knav

comportamento. Posteriormente, há duas referências ao assunto em 1996. A primeira é feita por Elam,[19] referindo-se à exploração potencial do uso da ofensiva informacional. Na tese, citou-se a expressão "guerra cognitiva", sem defini-la, e associou-a ao conceito de guerra da informação. A segunda referência foi feita por Dahl,[20] abordando a "guerra cognitiva" como uma estratégia para reduzir a velocidade e a acurácia do processo decisório inimigo. Dahl destacou o emprego da guerra cognitiva sobre o ciclo: observação, orientação, decisão e ação, também conhecido como ciclo OODA.[21]

O conceito de guerra cognitiva é emergente na literatura acadêmica[22] e não há, até o momento, uma definição universal para o assunto. Não obstante, os conceitos difundidos nos âmbitos acadêmico, institucional ou privado permitem o delineamento da ameaça. Claverie e Du Cluzel asseveram que guerra cognitiva é uma forma não convencional de guerra,[23] Backes e Swab a definem como uma estratégia;[24] e a Organização do Tratado do Atlântico Norte (OTAN) considera-a como um conjunto de atividades conduzidas em sincronização com outros instrumentos de poder.[25] Em relação aos objetivos da guerra cognitiva, os pesquisadores também divergem, por exemplo: 1) segundo Rosner e Siman-Tov, a guerra cognitiva pretende minar a unidade social e prejudicar a confiança do público no sistema político; [26] 2) Backes e Swab indicam que o objetivo é alterar o pensamento e o modo de agir de uma determinada população-alvo;[27]

[19] Donald Emmet Elam. "Attacking the Infrastructure: Exploring Potential Uses of Offensive Information Warfare." (1996):14. Acessado em 05 de abril de 2024. https://apps.dtic.mil/sti/tr/pdf/ADA311391.pdf.

[20] Arden B. Dahl. "Command Dysfunction: Minding the Cognitive War." (1996): 37. Acessado em 05 de abril de 2024. http://uploads.worldlibrary.net/uploads/pdf/20121023231948command_dysfunction_pdf.pdf

[21] Idem. p.38.

[22] Marie Morelle, Damien Marion, Julien Cegarra e Jean-Marc André. "Towards a Definition of Cognitive Warfare." Conference on Artificial Intelligence for Defense, DGA Maîtrise de I'Information, Rennes. France. (novembro 2023):1. Acessado em 05 de abril de 2024. https://hal.science/hal-04328461/document

[23] Bernard Claverie e François Du Cluzel. "Chapter 2 – "Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare. In Cognitive Warfare: First NATO Scientific Meeting on Cognitive Warfare. (2021):2-1. Acesso em 08 de abril de 2024. https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf

[24] Oliver Backes e Andrew Swab. "Cognitive Warfare. The Russian Threat to Election Integrity in the Baltic States." Policy Analysis Exercise. Harvard Kennedy School. Belfer Center for Science and International Affairs. (2019): v. Acessado em 07 de abril de 2024 https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf

[25] Organização do Tratado do Atlântico Norte. Acessado em 08 de abril de 2024. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/

[26] Yotam Rosner e David Siman-Tov. "Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion." *INSS Insight* no.1031 (março 2018):1. Acessado em 08 de abril de 2024. https://www.inss.org.il/publication/russian-intervention-in-the-us-presidential-elections-the-new-threat-of-cognitive-subversion/.

[27] Oliver Backes e Andrew Swab. (2019):1.

3) Ottewell considera que o foco é estabelecer um percepção predeterminada para um público-alvo a fim de que os interessados nessa mudança obtenham vantagem;[28] 4) a OTAN considera que o objetivo é afetar atitudes e comportamentos pela influência, proteção e/ou disrupção cognitiva individual ou coletiva[29]; e 5) Divyanshu entende que os objetivos são: minar a confiança em instituições oficiais do estado, redirecionar ou afastar a população de fontes confiáveis de informação, causar uma sobrecarga informacional; e controlar a narrativa.[30]

A guerra cognitiva tem relação, principalmente, com dois fenômenos relativamente recentes: 1) a aceleração da evolução tecnológica dos meios de comunicação e a democratização de acessos a esses meios; e 2) o surgimento das redes sociais digitais.[31]Basta ver que o número de dispositivos móveis de comunicação (celulares e tablets) no mundo gira ao redor de 17,72 bilhões,[32] e há mais de 100 redes sociais em uso para diversos fins.[33]

A operacionalização da guerra cognitiva se dá por diversos meios de forma combinada. As operações psicológicas, por exemplo, constituem um dos instrumentos utilizados para: 1) alterar crenças e valores das pessoas; 2) distorcer percepções da realidade; 3) criar ilusões culturais; 4) fomentar a ansiedade, medo, raiva e a fragmentação social; e 5) explorar as fraquezas ou fortalezas de personalidade.[34] Noutra vertente têm-se as operações que usam as capacidades relacionadas à informação para influenciar, interromper ou degradar a tomada de decisão adversa.[35] Aquelas capacidades podem

[28] Paul Ottewell. "Defining the Cognitive Domain'. (2020):4. Acessado em 08 de abril de 2024. https://overthehorizonmdos.wpcomstaging.com/2020/12/07/defining-the-cognitive-domain/?ref=stratagem.no.

[29] Organização do Tratado do Atlântico Norte

[30] Divyanshu Jindal. "The War on Conscience: India in the Age of Cognitive Warfare." India Foundation Monography 1. (2023):7. Acessado em 10 de abril de 2024. https://indiafoundation.in/wp-content/uploads/2023/09/Divyanshu-Jindal-combined-Final-48-pages.pdf

[31] Paul Ottewell. (2020):2.

[32] Federica Laricchia In Statista. "Forecast number of mobile devices worldwide from 2020 to 2025 (in billions) *" Acessado em 16 de abril de 2024. https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/#:~:text=In%202021%2C%20the%20number%20of,devices%20compared%20to%202020%20levels.

[33] Jacinda Santora. "116 social media sites you need to know in 2024". Acessado em 16 de abril de2024. https://influencermarketinghub.com/social-media-sites/

[34] Claverie e Du Cluzel (2021): 2-3.

[35] Joint Chiefs of Staff. "Joint Publication 3-13. Information Operations." (2012):II-1. Acessado em 09 de abril de 2024. https://irp.fas.org/doddir/dod/jp3_13.pdf.

compreender, por exemplo, a desinformação, as narrativas, as atividades de engenharia social e exploração de vieses cognitivos.[36]

Tabela 1 - Diferenças entre guerra psicológica, guerra de informação e guerra cognitiva

Guerra psicológica	Guerra de informações	Guerra cognitiva
Atua sobre as crenças	Atua sobre capacidades relacionadas à informação (CRI)	Atua sobre a cognição
Distorce percepções	Influencia o processo de tomada de decisão (PTD), utilizando as CRI	Provoca sobrecarga sensorial e perceptiva
Cria ilusões culturais	Interrompe o PTD com as CRI	Satura o sistema atencional
Provoca ansiedade e medo	Corrompe o PTD com as CRI	Canaliza a atenção
Explora fraquezas ou fortalezas da personalidade	Usurpa o PTD com as CRI	Provoca erros de julgamento
-	-	Fomenta a criação de vieses cognitivos

Fontes: Próprio autor com base em Claverie de Du Cluzel, 2021 e Manual Operações de Informação do Exército Brasileiro

Sob a perspectiva tecnológica, as operações cibernéticas podem ser utilizadas para afetar tanto o sistema cognitivo humano quanto a aprendizagem de máquinas, no processo de inteligência artificial. Essa situação é ainda mais grave, pois, como Claverie, argumenta, a cognição já não é mais uma questão puramente cerebral, mas uma relação de compartilhamento de informações com a tecnologia digital.[37] Du Cluzel indica que o cérebro humano é incapaz de distinguir se uma informação particular é certa ou errada sem o aprofundamento de pesquisa.[38] Danyk e Briggs consideram que quando não há informação com significado suficiente, o cérebro tende a sofrer uma distorção, aceitando o que é mais rápido e mais prático.[39] Du Cluzel, Danyk e Briggs concordam que, em caso de sobrecarga informacional,[40] o cérebro é levado a buscar atalhos para determinação da confiabilidade, assim como é levado a acreditar em informações

[36] Federico Borgonovo. "Strategies, disinformation techniques and cognitive warfare of jihadist organisations." *Journal of Stability Policing – Advanced Studies*. v.I. no.1.(2022):41. Acessado em 09 de abril de 2024. https://www.coespu.org/articles/strategies-disinformation-techniques-and-cognitive-warfare-jihadist-organisations.

[37] Bernard Claverie. "What Is Cognition? And How to Make it One of the Ways of the War?" In *Cognitive Warfare: The Future of Cognitive Dominance*, NATO Collaboration Support Office, (2022):4-3 Acessado em 10 de abril de 2024. https://hal.science/hal-03635907v1/document.

[38] François Du Cluzel. "The vulnerabilities of the human brain." In. The Centrality of Human Brain. Cognitive Warfare. Innovation Hub. (2020):.13. Acessado em 12 de abril de 2024. https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf

[39] Yuriy Danyk e Chad M Briggs. "Modern Cognitive Operations and Hybrid Warfare." Journal of Strategic Security 16, n.1. (2023): 35-50. Acessado 10 de abril de 2024. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=2032&context=jss.

[40] Grande volume de informação, normalmente associado com o pouco tempo para processamento.

conhecidas anteriormente como verdade, ainda que possam ser falsas – viés da confirmação.[41] O fluxo intenso de informações durante a pandemia de COVID-19 exemplificou a sobrecarga informacional, misturando informações corretas, informações incorreta e desinformação. Ademais, o cérebro aceita informações como verdadeiras se suportadas por supostas evidências, sem considerar a questão da autenticidade desses dados.[42] Dany e Briggs ainda alertam: 1) a exiguidade de tempo para respostas promove o uso da intuição ou daquilo que é costumeiro; e 2) há uma relação entre o lembrado e o esquecido. Essa última situação é ilustrada pela Curva de Esquecimento de Hermann Ebbinghaus, que mostra a velocidade com que uma informação é esquecida pela mente humana ao longo tempo, logo a guerra cognitiva faz uso da "repetição espaçada" da informação para que o assunto seja retido na memória[43] e os comportamentos sejam alterados.

Um dos grandes objetivos da guerra cognitiva é a mudança do pensamento ou do processo de pensamento das pessoas conforme a conveniência e os interesses do atacante. Elder e Paul mostram que, em todo pensamento, estão presentes oitos estruturas básicas: 1) identificação do propósito ou objetivo; 2) a definição do problema; 3) o levantamento de dados, fatos, observações e experiências anteriores; 4) intepretação, inferências, conclusões ou soluções; 5) a associação da situação com conceitos, teorias, axiomas, princípios e modelos; 6) o levantamento de hipóteses ou suposições; 7) implicações e consequências; e 8) pontos de vista, perspectivas e orientações.[44] A mudança do pensamento pela guerra cognitiva se dá pela manipulação de informações e dos sentimentos, usando ações como: *reframing, priming, emotioneering* e/ou a inoculação. O *reframing* do pensamento do público-alvo constitui o reenquadramento da percepção da audiência,[45] para influir sobre as estruturas básicas do pensamento. No reenquadramento, situações boas são convertidas em ruins e vice-versa. A Rússia, por exemplo, noticiou que lançou uma "operação especial" para defender a segurança do próprio país e libertar os ucranianos de um regime nazista. Por outro lado, a Ucrânia tornou público que a invasão visava subjugar os ucranianos e apagar sua identidade

[41] François Du Cluzel. (2021): 14, Yuriy Danik e Chad M Briggs. (2023):39.
[42] François Du Cluzel (2021): 14.
[43] Divyanshu Jindal. (2023): 8.
[44] Elinda Elder e Richard Paul. "Analytic Thinking: How to take thinking apart and what to look for when you do. The elements of thinking and the standards they must meet." (2007): 5. Acessado em 13 de abril de 2024. https://www.criticalthinking.org/files/Concepts_Tools.pdf.
[45] James P. Robson e Meredith Troutman-Jordan. "A Concept Analysis of Cognitive Reframing." *Journal of Theory Construction&Testing; Liste*. V.18. no 2 (Fall/Winter 2014):55-59. Acessado em 10 de abril de 2024. https://www.proquest.com/docview/1629019978?sourcetype=Scholarly%20Journals

nacional, assim os ucranianos defendiam a liberdade e a integridade territorial.[46] Cada ator tenta modular a percepção das pessoas conforme seus interesses e afetar os fatos, os objetivos, as consequências e os pontos de vista. O *priming* se refere a processos de aprendizagem implícitos[47] que usam de associações mentais para influenciar o comportamento e o julgamento. O uso de bandeiras e de heróis nacionais, por exemplo, pode ter o efeito associativo de nacionalismo e poder, visando o fortalecimento da coesão nacional. O *Emotioneering* diz respeito ao uso de informações para causar emoções específicas que podem influenciar a receptividade da comunicação, sendo largamente empregado nos games utilizados pelos jovens.[48] A inoculação trata da exposição do público-alvo a informações contrárias a um ponto de vista específico para torná-la resistente à mudança.[49]

Dessa forma, diferentemente das guerras com características cinéticas, a guerra cognitiva independe de meios militares e pode ser desencadeada de forma silenciosa, sem que o atacado nem saiba que está debaixo de uma ofensiva cognitiva. Para demonstrar tal situação, na próxima seção serão verificados alguns casos concretos do emprego da guerra cognitiva.

Casos históricos do emprego da guerra cognitiva

Guerra cognitiva russa contra os Países Bálticos

Backes e Swab pesquisaram e apresentaram o emprego da guerra cognitiva pela Rússia contra Estônia, Letônia e Lituânia, ex-integrantes da União da República Socialista Soviética (URSS), também conhecidos como Países Bálticos. Durante o tempo da URSS, os Países Bálticos sofreram um processo de "russificação,"[50] resultando em profunda ambivalência com a Rússia. Por um lado, havia profunda antipatia; e por outro

[46] Dr. András Rácz. "Socially Inclusive and Exclusive Warfighting: Comparing Ukraine and Russia's Ways of War." *In Russia1s Imperial Endeavor and Its Geopolitical Consequences.* Central European University Press (novembro 2023): 27. Acessado em 10 de abril de 2024. https://dgap.org/en/research/publications/socially-inclusive-and-exclusive-warfighting-comparing-ukraine-and-russias

[47] Alvaro Pastor. "Cognitive Warfare." Barcelona. Spain. 2023. Publicado em PsyArXiv Preprints. (versão de 27 de junho de 2003): 6. https://doi.org/10.31234/osf.io/zgsej Acessado em 10 de abril de 2024.

[48] D Freeman." Creating Emotion in Games: The Crat and Art of Emotioneering." *In Computers in entertainment.* v.2. no.3. (2004). https://doi.org/10.1145/1027154.1027179.

[49] Benjamin J Knox. "Chapter 5- Cognitive and Behavioral Science (Psychological Interventions) In Mitigating and Responding to Cognitive Warfare". STO-TR-HFM-ET-356 (2022): 5-3. https://doi.org/10.14339/STO-TR-HFM-ET-356.

[50] Transformação visando se parecer com a Rússia, seja pelo idioma, etnias e adoção de hábitos e costumes russos.

o estabelecimento laços culturais, históricos, políticos e econômicos com aquele país. Desde 1991, ocasião da independência daqueles países, a Rússia tem promovido campanhas para desestabilizá-los, mas, principalmente depois de 2004 quando Estônia, Letônia e Lituânia ingressaram na OTAN. A posição geográfica dos três países é fundamental para o acesso pleno da Rússia ao Mar Báltico, bem como a manutenção territorial em face de eventuais ofensivas do Ocidente. No entanto, foi nos períodos eleitorais que as vulnerabilidades dos Países Bálticos foram acentuadas. A Rússia aproveitou o período das campanhas eleitoras, pois havia cobertura ininterrupta da mídia, o debate público era intenso e de elevada tensão; e os eleitores podiam expressar sua vontade para determinar o futuro de suas nações. Backes e Swab identificaram que a Rússia tinha os seguintes objetivos: 1) minar o processo político interno dos Países Bálticos; 2) interferir nas eleições para atingir interesses geopolíticos russos; 3) interferir politicamente nos Países Bálticos; 4) inflamar a divisão dentro da sociedade; e 5) mudar a forma como os eleitores pensavam e como eles iriam votar. A macro visão russa era de restaurar o poder e manter a influência em países anteriormente ocupados pela URSS; promover a ordem mundial multipolar; e usar os Países Bálticos para desacreditar as instituições ocidentais como a União Europeia e a OTAN. Como estratégia para promover a guerra cognitiva, a Rússia priorizou o emprego do vetor informacional sobre o vetor cibernético, que foi utilizado secundariamente. As táticas russas englobaram: 1) o emprego da desinformação, da propaganda e do vazamento de documentos; 2) a disseminação de informações manipuladas nas mídias sociais; 3) a instrumentalização da memória história da população daqueles países;4) o apelo pelos russos étnicos e minorias localizados na Estônia, Letônia e Lituânia; 5) a promoção das narrativas para dividir a sociedade dos Países Bálticos, inclusive relacionando à imagem do apartheid da África do Sul; 6) o uso do idioma russo para influenciar a população, seja de origem russa ou falantes do russo; 7) suborno a partidos políticos; 8) financiamentos ilegais e a ligação russa com ONG manipuladas. O caso dos pôsteres na cidade de Tallinn, na Estônia, ilustra a tentativa russa de fomentar a cizânia entre russos e não russos do país e, eventualmente, permitir uma ação da Rússia para proteger as minorias. Os pôsteres foram colocados em paradas de transporte público e três deles, com círculos azuis sobre fundo branco, diziam "somente estonianos aqui". Do outro lado, separados por uma faixa vermelha, outros três pôsteres com círculos vermelhos sobre fundo branco com a inscrição "somente russos aqui". Essa tentativa de influir na percepção da sociedade estoniana, buscou explorar a

questão de uma divisão étnica entre estonianos e russos (moradores da Estônia), sendo explorada pela mídia russa para ecoar entre os eleitores.[51]

Figura – "Somente estonianos aqui" – "Somente russos aqui"

Fonte: Agaate Antson e Sander Punamäe[52]
Crédito da imagem: Sander Ilvest

As narrativas foram largamente empregadas pelos russos na guerra cognitiva contra os Países Bálticos, como por exemplo:

Tabela 2 - Narrativas russas

Narrativas utilizadas	Aspectos de cognição atacados
Os governos da Estônia, Letônia e Lituânia são fascistas ou pró-fascistas. Buscou-se atingir principalmente a população idosa, em datas mais significativas.	Percepção, associação, memória e linguagem
Os Estados Bálticos são estados falidos porque são incapazes de proporcionar boa condição de vida para os cidadãos. As elites são corruptas e há conivência com valores ocidentais que destroem as sociedades. Explorou a falta de oportunidade econômica.	Percepção, juízo, pensamento e linguagem
Os governos dos Estados Bálticos discriminam os russos, falantes de russo e residentes não natos. Explorou-se o "*apartheid*" e os desrespeitos aos direitos humanos.	Percepção, juízo, pensamento e linguagem

[51] Backes e Swab (2019): v.
[52] Agaate Antson e Sander Punamäe. "Estonia 200 provocative posters". 2019. Acessado em 12 de abril de 2024. https://news.postimees.ee/6494099/estonia-200-provocative-posters

Fonte: próprio autor com base nos dados de Backes e Swab

As lições apreendidas nesse caso mostram que a resposta à guerra cognitiva envolve muito mais do que questões técnicas. Requer-se a preparação da sociedade quanto ao desenvolvimento do pensamento crítico e a adequada difusão de informações para combate às desinformações. Para a detecção, faz-se necessário ampliar a capacidade de inteligência e de monitoramento de fontes e narrativas de notícias falsas. Para a defesa, verificou-se a necessidade de ampliar a capacidade de cibersegurança para os processos eleitorais, assim como melhorar as capacidades dos grupos de trabalho ligados à segurança da informação e combate à desinformação. É necessário que haja planos de contingência para as eleições face à guerra cognitiva e esses sejam treinados. No tocante às vulnerabilidades, é preciso promover a coesão nacional e promover políticas para grupos minoritários. Finalmente, deve-se buscar as boas práticas dos aliados.[53]

Guerra cognitiva chinesa contra Taiwan

A China empreende guerra cognitiva contra Taiwan e os Estados Unidos da América em função da disputa geopolítica para unificação de Taiwan, pela busca do domínio de todo o Mar do Sul China; e a projeção de seu poder naval, visando se contrapor à contenção norte-americana, inspirada por Spykman,[54] estabelecida pela Teoria do *Rimland.*[55] De acordo com Hung e Hung a guerra cognitiva chinesa procura aumentar o conflito interno em Taiwan, fomentar as opiniões contrárias à independência; e, principalmente, promover a unificação de Taiwan à China continental. A guerra cognitiva chinesa se vale de quatro ações:1) intimidação militar à Taiwan; 2) promoção da desinformação sobre a população taiwanesa; 3) influência à mudança de pensamento sobre independência; e 4) interferência na cognição da população taiwanesa usando a religião.[56] A China busca intimidar a população de Taiwan mediante sortidas de aeronaves de combate, lançamentos de mísseis e a realização de exercícios simulados com seu poder naval. Essas ações militares causam medo e ansiedade, contribuindo para a afetação do sistema cognitivo e, por conseguinte, a resposta da sociedade à

[53] Backes e Swab (2019): vi.

[54] Braz Baracuhy. "Os Fundamentos da Geopolítica Clássica: Mahan, Mackinder, Spykman". Fundação Alexandre de Gusmão. (2021):33.

[55] Teoria do controle dos mares, oceanos e rotas comerciais em oposição à Teoria do Heartland (controle do coração do mundo) desenvolvida por Nicholas Spykman.

[56] Tzu-Chieh Hung e Tzu-Wei Hung. "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars." Journal of Global Security Studies, v.7. no.4. (2000):1–18. https://doi.org/10.1093/jogoss/ogac016.

independência ou à unificação.[57] Quanto ao uso da desinformação, Shimbun argumenta que a China tem utilizado das mídias sociais para demonizar o governo de Taiwan e provocar a divisão da sociedade taiwanesa.[58] Para isso coleta dados das pessoas por intermédio da oferta de jogos e de testes psicológicos pelo Facebook, utilizando empresas como a WuWei Technology,[59] para identificar o perfil dos habitantes e elaborar as notícias falsas. Segundo Shen, outras empresas como WeChat e GTCOM também têm sido utilizadas para coletar dados que alimentam a elaboração da desinformação.[60] Um caso concreto de desinformação chinesa se relaciona ao incidente no Aeroporto Internacional de Osaka/Japão (com problemas de estabilidade do solo), quando diversas notícias em redes sociais informaram que a China estaria realizando o resgate de seus nacionais, mas só resgataria os taiwaneses que lá estivessem se se declarassem chineses. Essa situação foi explorada em redes sociais para mostrar a fragilidade de Taiwan em apoiar sua população, ao contrário da China.[61]

No tocante à desinformação ligada aos Estados Unidos, de acordo com Burton e Stweart, em 2019 a China promoveu campanha de guerra cognitiva para desacreditar os taiwaneses sobre o eventual apoio norte-americano à Taiwan, visando criar a desconfiança entre os EUA e seus aliados, bem como e promover a cisão entre a população de Taiwan.[62]

Além disso, para influenciar os habitantes de Taiwan a modificarem suas convicções, a China tem ofertado benefícios econômicos e socioculturais como o acesso à educação.[63] Noutra vertente de influência, a China utiliza da religião Mazuísta, crença popular relacionada à cultura marítima. Ao redor de 70% dos taiwaneses pertencem a esse

[57] James A. Siebens. "China's Use of Armed Coercion: To win without fighting.2024". London: Routledge, Taylor & Francis Group.

[58] Youmiuri Shimbun. "China's cognitive warfare aims to influence views in Taiwan." The Japan News.(outubro 2022). Acessado em 13 de abril de 2024. https://asianews.network/chinas-cognitive-warfare-aims-to-influence-views-in-taiwan/.

[59] Puma Shen. "How China Initiates Information Operations Against Taiwan". *Taiwan Strategists No.12.* (2021): 20. Acessado em 14 de abril de 2024. https://www.airitilibrary.com/Article/Detail?DocID=P20220613001-202112-202206130009-202206130009-19-34.

[60] Puma Shen. (2021):20

[61] Taipei Times. 2018. Acessado em 15 de abril de 2024. https://www.taipeitimes.com/News/taiwan/archives/2018/09/09/2003700087

[62] Rachael Burton e Devin Stweart. "China's Cognitive Warfare," with Rachael Burton. New York: Newstex. 2019. Acessado em 14 de abril de 2024. https://www.carnegiecouncil.org/media/series/asia/20190211-china-cognitive-warfare-rachael-burton.

[63] Gunter Schubert. "China's 31 Preference Policies for Taiwan: An Opportunity, no Threat". (2018). Acessado em 15 de abril de 2024. https://taiwaninsight.org/2018/03/21/chinas-new-31-preference-policies-for-taiwan-an-opportunity-no-threat/

credo religioso, que tem raízes na China. O Mazuísmo tem sido usado modelar a percepção dos taiwaneses de que ambos os países compartilham laços religiosos comuns; e devem perseguir a política de "uma só China" com base na unificação pacífica.[64]

Em virtude das ações de guerra cognitiva chinesa, Taiwan estabeleceu um Centro de Pesquisa de Guerra Cognitiva, destinado a estudar a desinformação online que ameaça a democracia e a segurança do país. Esse Centro é estruturado em três divisões: 1) compilação e pesquisa de dados; 2) análise da guerra cognitiva; e 3) unidade de resposta rápida às notícias falsas.[65]

No caso envolvendo China e Taiwan, as lições aprendidas mostram a necessidade de estruturação de organismo próprio para lidar com as ameaças de guerra cognitiva de forma que a resposta seja unificada e a mais rápida possível. Essa lição fica caracterizada pela ação concreta de Taiwan ao criar um Centro de Pesquisa de Guerra Cognitiva dedicado exclusivamente para enfrentar esse tipo de ameaça.

Na sequência, serão abordados alguns desafios que a guerra cognitiva impõe à América.

Os desafios impostos à América pela guerra cognitiva

O Sistema Internacional atual ainda pode ser considerado como uni-multipolar,[66] onde os Estados Unidos se mantêm como potência militar hegemônica. No entanto, China e Rússia têm buscado a superação norte-americana e a transformação do mundo para um sistema multipolar. No âmbito econômico, a China já tem reduzido a diferença de seu produto interno bruto em relação ao PIB dos EUA. Em 2022, a diferença era ao redor de 6,7 trilhões a favor dos EUA e, em 2023, essa diferença caiu para 5,6 trilhões.[67] Ellis argumenta que a expansão chinesa no Continente Americano nas áreas de comércio, negócios, militar e política está transformando o ambiente político-econômico do Hemisfério.[68] Em 2003, o comércio chinês com a Região era em torno de 29 bilhões de dólares, mas em 2013 houve um salto para 270 bilhões.[69] Ademais, áreas estratégicas

[64] Tzu-Chieh Hung e Tzu-Wei Hung. (2000):1–18.

[65] Chien Li-chung e Jason Pan. "Research center set up to combat cognitive warfare." 2024. Acessado em 15 de abril de 2024. https://www.taipeitimes.com/News/front/archives/2024/01/19/2003812310.

[66] Samuel Huntington. "The Lonely Superpower.' *Foreign Affairs*. v.78. no.1. (março 1999): 36.

[67] Dados do Banco Mundial. Acessado em 15 de abril de 2024. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD

[68] Robert Evan Ellis. "The Rise of China in the Americas." Security and Defense Studies Review. v. 16. (2014): 90.

[69] Idem

como exploração mineral e petrolífera, telecomunicações e infraestrutura têm sido alvo dos aportes de investimentos chineses na América. Concomitantemente à inserção econômica, a China tem se imiscuído em aspectos políticos na América, que podem ampliar o ambiente conflituoso com os EUA, em virtude de: 1) promover orientação para lideranças políticas da América Latina; 2) influenciar algumas Forças Armadas da Região em países como Venezuela, Cuba, Equador e Bolívia;[70] 3) influenciar países em assuntos de direitos humanos e democracia; e 4) patrocinar a viabilidade econômica do bloco político opositor aos EUA.[71] O relacionamento competitivo EUA-China atrai o emprego da guerra cognitiva para o Hemisfério, com o objetivo geopolítico de promover o declínio norte-americano e implantar a multipolaridade em sua plenitude.

Noutra vertente, a guerra Rússia – Ucrânia acirra o conflito Rússia – EUA em virtude do apoio norte-americano à Ucrânia e à OTAN. Essa situação aproxima a guerra cognitiva russa sobre o Continente Americano, seja para fragmentar o apoio dos países da América Latina e do Caribe aos EUA, à OTAN e à própria Ucrânia

Para mostrar que a guerra cognitiva já é uma ameaça real para os países do Continente, observe-se o caso do Canadá. Segundo um relatório de 2019 da Clairvoyance Cyber Corp for Public Safety, serviços de inteligência de atores hostis continuariam a interferir e influenciar os interesses canadenses; e a as companhias de tecnologia chineses tentariam controlar os canadenses por intermédio da desinformação, interferência, manipulação da mídia, guerra psicológica e do *lawfare*.[72] Segundo McMahon, tanto Rússia quanto China usam desinformação para prejudicar a economia canadense e a estrutura sócio-político democrática do país. McMahon argumenta que um relatório de 2021, da Global News, apontou uma rede de websites ligada à Rússia ao espalhamento de informações falsas sobre COVID-19, contribuindo para a ocorrência de cerca de 2.800 óbitos no Canadá a um custo de aproximadamente 300 milhões de dólares.[73]

As democracias imperfeitas ou híbridas do Continente Americano são alvos vulneráveis à guerra cognitiva promovida por países de outros continentes, particularmente por contarem com diversas fragilidades como: 1) disparidade econômica;

[70] Robert Evan Ellis. “Chinese Security Engagement in Latin America.” Center For Strategic & International Studies. (2020): 4-5.

[71] Idem

[72] Dave McMahon. “Maligned Influence and Interference in Canada”. Canadian Global Affairs Institute. (2023): 2. Acessado em 15 de abril de 2024. https://assets.nationbuilder.com/cdfai/pages/5323/attachments/original/1688675087/Maligned_Influence_and_Cognitive_Warfare.pdf?1688675087

[73] Idem

2) desigualdade e conflitos raciais; 3) migrações populacionais; 4) desrespeito aos direitos humanos; 5) luta de classes; 6) conflitos envolvendo grupos minoritários; 7) debilidade nos fundamentos e valores que sustentam as nações; 8) conflitos originados da diversidade religiosa; 9) significativos índices de criminalidade; e 10) pouco envolvimento da sociedade em assuntos de segurança e defesa. Essas fragilidades são temas para narrativas e desinformação, visando provocar a segmentação, discórdia e a ruptura do tecido social de muitos países da América.

O ambiente informacional da América é muito proveitoso para a guerra cognitiva. Estima-se, por exemplo, que haja cerca de 987 milhões de celulares no Continente Americano,[74] ou seja quase 1 celular/habitante da América. No tocante às redes sociais, a distribuição estimada de usuários no Continente é a seguinte: 1) 447,82 milhões na América do Norte; 2) 316,78 milhões na América do Sul; e 3) 28,99 milhões na América Central, perfazendo 793,59 milhões de pessoas.[75] Segundo a DATAREPORTAL, o tempo médio diário que um usuário dispende nas redes sociais é de aproximadamente 2 horas e 23 minutos.[76] Lindström *et al*, argumentam que o longo tempo de conexão nas redes sociais estimula a produção de dopamina[77] e cria a necessidade psicológica de recompensas sociais, como as "curtidas ou likes", favorecendo a manipulação cognitiva contida nas informações ou desinformações presentes nas mídias.[78]

Considerando a predominância de estados democráticos na América, tem-se outro problema extremamente sensível: como equilibrar a liberdade de expressão e de imprensa, característica basilar das democracias, ao mesmo tempo que se estabelecem controles para as mídias tradicionais e mídias sociais para o evitamento da profusão de notícias falsas e manipulações. Ademais, tem-se o desafio que alguns países americanos

[74] Obtido a partir da conjugação de dados do Statista. Acessado em 08 de abril de 2024. https://www.statista.com/statistics/1258906/worldwide-smartphone-adoption-rate-telecommunication-by-region/

[75] Rohit Shewale. "Social Media Users 2024 (Global Data & Statistics)". Acesso em 08 de abril de 2024. https://www.demandsage.com/social-media-users/

[76] DATAREPORTAL. Kepios. "Global Social Media Statistics". 2024. Acessado em 08 de abril de 2024. https://datareportal.com/social-media-users.

[77] Neurotransmissor ligado à recompensa, prazer e aprendizado.

[78] Bjorn Lindstrom, Martin Bellander, David Schltner, Allen T. Chang, Phillippe Tobler e David M. A. Amodio. "A computational reward learning account of social media engagement". Nature Communications. 2021.

considerem a ameaça da guerra cognitiva como "teoria da conspiração,"[79]facilitando a fragmentação de propósitos para o estabelecimento de uma defesa cognitiva hemisférica. Outro desafio que muitos países do Continente enfrentam é o processo de deslegitimação das forças armadas, particularmente pelo emprego das tropas em problemas domésticos. Essa situação é explorada cognitivamente para gerar a descrença nas forças armadas e o afastamento da sociedade dos assuntos de segurança e defesa. Esse problema pode, ainda, afetar a "vontade de lutar" dos cidadãos de um Estado, quando necessário. Segundo a RAND Corporation a motivação pode ser afetada por ideologias, vinganças e falta de coesão. Dessa forma, mediante a guerra cognitiva para deslegitimar as forças armadas, pode-se reduzir a motivação das pessoas para defenderem seus países,[80] bem como reduzirem os orçamentos de defesa.

O Continente conta com o Tratado Interamericano de Assistência Recíproca (TIAR), elaborado sob a perspectiva de guerra com ações cinéticas. No entanto, a guerra cognitiva se vale de ações não cinéticas de difícil caracterização de origem em virtude da multiplicidade de meios que usa. Dessa forma, constitui-se um desafio invocar o Órgão de Consulta da Organização dos Estados Americanos a fim de estabelecer medidas de defesa cognitiva com base no TIAR.[81]

Enfim, o Continente Americano está diante de um conjunto de desafios, pois, sob uma aparente paz, o Hemisfério já está inserido no contexto de uma guerra, cujas manobras adversárias parecem ser invisíveis pois incidem sobre a mente das pessoas.
A seguir serão vistas algumas oportunidades que a guerra cognitiva apresenta para o Continente Americano.

As oportunidades para a cooperação hemisférica contra as guerras cognitivas

[79] Kimberly Orinx1 Pr. Tanguy Struye de Swielande. Chapter 8 – China and Cognitive Warfare: why is the west losing? In Cognitive Warfare: First NATO Scientific Meeting on Cognitive Warfare. Bordeaux. France. (2021): 8-3. Acessado em 12 de abril de 2024. https://innovationhub-act.org/mwg-internal/de5fs23hu73ds/progress?id=tE7YMt51TuGRY0SG6ARUMa--KkN7jWT61Ua5NpPkvL8.

[80] RAND Corporation. "Will to Fight: Returning to the Human Fundamentals of War." (2018): 12. Acessado em 16 de abril de 2024. https://www.rand.org/mwg-internal/de5fs23hu73ds/progress?id=Cuxof9VGEJnmyoY92tjWYKhsyLIPeQa0C1ZfJD9_Rk0,

[81] Organization of American States. Inter-American Treaty of Reciprocal Assistance. Acessado em 17 de abril de 2024. https://www.oas.org/juridico/english/treaties/b-29.html

A primeira oportunidade visualizada diz respeito à promoção do debate do tema entre os países para a conscientização da ameaça que paira sobre o Continente.[82] Sem a consciência do risco que a guerra cognitiva constitui, os países se tornam presas fáceis da manipulação e da perda de soberania.

O incremento das ações educacionais para o desenvolvimento do pensamento crítico das pessoas que habitam na América constitui-se em uma grande oportunidade para o Continente. De acordo com o Luberisse, o fortalecimento da resiliência dos indivíduos frente à guerra cognitiva se dá por intermédio da educação desde jovem. É fundamental que as pessoas adquiram a capacidade de analisar as informações quanto às fontes, a identificação de vieses e a tentativa de manipulação das percepções.[83] Masakowski e Sivertsen reforçam a mesma ideia, afirmando que as crianças devem, desde cedo, ser ensinadas a reconhecerem notícias falsas (fake News) em mídias sociais; e pensarem criticamente contra as manipulações de percepção.[84] Nesse sentido, instituições como a Organização dos Estados Americanos, Junta Interamericana de Defesa e Colégio Interamericano de Defesa são essenciais para ampliarem a propagação da educação do pensamento crítico para todo o Continente.

O desenvolvimento de capacidades de compartilhamento de inteligência na América contra guerra cognitiva é outra oportunidade significativa e, ao mesmo tempo, difícil de se operacionalizada. Tradicionalmente, há reservas entre Estados para o compartilhamento de informações, contudo é crucial que ocorra a troca de dados para a detecção da ameaça e/ou a identificação do modus operandi das ações cognitivas ofensivas.[85] Nesse contexto de compartilhamento de inteligência, Michael e Kuperwasser, citando Robert Koslosky, sugerem o estabelecimento da inteligência pública (PUBINT) , na qual certos dados devem ser compartilhados com a população para que seja possível detectar e identificar as ameaças.[86]

---

[82] Lea Kristina Petronella Bjørgul. "Chapter 12 – Legal and Ethical Implications Related to Defence Against Cognitive Warfare." In Mitigating and Responding to Cognitive Warfare. (2023):12-3. Acessado em 17 de abril de 2024. https://doi.org/10.14339/STO-TR-HFM-ET-356.

[83] Josh Luberisse. Cognitive Warfare in the Age of Unpeace: Strategies, Defenses, and New Battlefield of the Mind. eBook Kindle. Chapter 11: Defensive Strategies: Countermeasures and Resilience. (2023): 89 - 94.

[84] Yvonne R. Masakowski e Eskil Grendahl Sivertsen. "Chapter 7 – Defence Against 21st Century Cognitive Warfare: Considerations and Implications of Emerging Advanced Technologies". (2023): 7-7. In Mitigating and Responding to Cognitive Warfare. 2023. Acessado em 17 de abril de 2024. https://doi.org/10.14339/STO-TR-HFM-ET-356.

[85] Josh Luberisse. (2023): 89 – 94.

[86] Kobi Michael e Yossi Kuperwasser. "Cognitive Intelligence: The Theoretical Aspect. In The Cognitive Campaign: Strategic and Intelligence Perspectives". (2019): 85. Acessado em 17 de abril de 2024. https://www.inss.org.il/wp-content/uploads/2019/10/Memo197_e_compressed.pdf.

O desenvolvimento de soluções tecnológicas para detecção e alerta[87] de ações cognitivas ofensivas pode ser uma oportunidade a ser explorada conforme ocorra o amadurecimento das relações dos países do Continente e o aumento da confiança mútua sobre o tema.

À medida que os países do Continente se tornem conscientes da ameaça, é possível o estudo de alternativas para comporem o arcabouço legal de medidas de defesa cognitiva. Em fases posteriores, há de se considerar a possibilidade de estabelecimento de um regime internacional de tratamento da ameaça cognitiva no Hemisfério.[88]

Finalmente, a América pode buscar integração com outros atores que também estejam pesquisando essa área como a Bulgária, que proporcionou o Curso Piloto de Guerra Cognitiva[89] para integrantes da OTAN e o Centro de Pesquisa para Combate à Guerra Cognitiva de Taiwan.[90]

Conclusão

> *Nosso maior desafio é que estamos no meio de uma guerra cognitiva ... e nosso foco permanece quase exclusivamente na (guerra) cinética*[91]*. (Edward L. Haugland)*[92]

O Continente Americano parecia estar longe das guerras, considerando que os principais conflitos ocorreram na Europa, Oriente Médio ou na Ásia e lá se encontram as principais áreas de tensão na atualidade. Desafortunadamente essa situação parece ter mudado e de uma maneira bastante singular, pois o conflito geopolítico existente para transformar o sistema internacional uni-multipolar em multipolar pleno aproximou as ameaças para a América. Assim, a guerra cognitiva ocorre sem movimentações de tropas, disparos de artilharia ou sortidas de aeronaves de caça. A mente de cada habitante do

[87] Idem

[88] Josh Luberisse (2023): 89 – 94.

[89] Cognitive Warfare Course. Acessado 19 de abril de 2023. https://cmdrcoe.org/menu.php?m_id=40&c_id=108

[90] Chien Li-chung e Jason Pan. Research center set up to combat cognitive warfare. (2024). https://www.taipeitimes.com/News/front/archives/2024/01/19/2003812310.

[91] Tradução livre e adaptada. Acrescentou-se o termo "guerra", para proporcionar maior clareza à citação.

[92] Edward L.Haugland. "Future Military Intelligence CONOPS and S&T Investment Road Map 2035 – 2050: The Cognitive War". (2019): 42. Acessado em 17 de abril de 2024. https://nsiteam.com/mwg-internal/de5fs23hu73ds/progress?id=PapgANAfqJnsqHF-_9NX9_V0jEDIW4DOqT1UumFhJro,

Continente Americano se transformou em um campo de batalha. Parece que já estamos em guerra.

A acelerada evolução tecnológica dos meios de comunicação, o surgimento de fenômenos como as redes sociais e hiperconectividade das pessoas vieram a dar corpo à proposta de Sun Tzu de obter vitórias sem lutar. Assim a guerra cognitiva poder ser comparada a uma guerra de "balas invisíveis voando em todas as direções".[93]

Verificou-se que são diversos os desafios enfrentados pelo Hemisfério, mas destaca-se a ameaça à democracia uma vez que os Estados enfrentam o dilema de: 1) ou constrangerem os princípios da liberdade de expressão e de imprensa para reduzirem as ameaças; 2) ou manterem aqueles princípios e verem a cognição de seus habitantes serem afetadas, fazendo ruir a soberania. Emerge, portanto uma questão central: qual deve ser a medida de afirmação de autoridade do Estado frente à ameaça da guerra cognitiva em um contexto distinto do período pós Westfaliano? Esse problema tem que ser discutido conjuntamente na América.

Finalmente, a situação deve ser encarada como uma oportunidade de integração do Hemisfério para estabelecer sua defesa cognitiva, sobretudo fomentando o desenvolvimento do pensamento crítico dos habitantes, em particular dos líderes tão sujeitos à interferência da guerra cognitiva nos processos de tomada de decisão político-estratégicos.

Bibliografia

Alvarado, Oswal Sigüeñas. "O Conflito do Cenepa em seus 25 Anos: Lições aprendidas Uma Análise do Uso dos Princípios do Poder Aeroespacial Peruano". *Revista Profissional da Força Aérea dos EUA.* no.3 (2021): 155. Acessado em 05 de abril de 2024. https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%203%20Issue%203/06-Siguenas_port.pdf

Anston, Agaate e Punamäe, Sander. "Estonia 200 provocative posters". 2019. Acessado em 12 de abril de 2024. https://news.postimees.ee/6494099/estonia-200-provocative-posters

Backes, Oliver e Swab, Andrew . "Cognitive Warfare. The Russian Threat to Election Integrity in the Baltic States." Policy Analysis Exercise. Harvard Kennedy School. Belfer Center for Science and International Affairs. (2019): v. Acessado em 07 de abril de 2024 https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf

[93] Kazumi Naganuma. "Warfare in the Cognitive Domain: Narrative, Emotionality, and Temporality". (2021):1. Acessado em 17 de abril de 2024. https://www.nids.mod.go.jp/mwg-internal/de5fs23hu73ds/progress?id=F9V2rhIikzcVSUVO9zEG_u0X28P_LJodSFDjxndAxgs.

Banco Mundial. Dados. Acessado em 15 de abril de 2024. https://data.worldbank.org/indicator/NY. GDP. MKTP. CD

Baracuhy, Braz. "Os Fundamentos da Geopolítica Clássica: Mahan, Mackinder, Spykman". Fundação Alexandre de Gusmão. 2021.

Bjørgul, Lea Kristina Petronella. "Chapter 12 – Legal and Ethical Implications Related to Defence Against Cognitive Warfare." In Mitigating and Responding to Cognitive Warfare. (2023):12-3. Acessado em 17 de abril de 2024. https://doi.org/10.14339/STO-TR-HFM-ET-356.

Borgonovo, Federico. "Strategies, disinformation techniques and cognitive warfare of jihadist organisations." Journal of Stability Policing – Advanced Studies. v.I. no.1. (2022):41. Acessado em 09 de abril de 2024. https://www.coespu.org/articles/strategies-disinformation-techniques-and-cognitive-warfare-jihadist-organisations.

Brasil. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. Manual de Campanha Operações de Informações. 2ª Ed. 2019.

Burton, Rachael e Stweart, Devin. "China's Cognitive Warfare," with Rachael Burton. New York: Newstex. 2019. Acessado em 14 de abril de 2024. https://www.carnegiecouncil.org/media/series/asia/20190211-china-cognitive-warfare-rachael-burton.

Claverie, Bernard e Du Cluzel, François. "Chapter 2 – "Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare. In Cognitive Warfare: First NATO Scientific Meeting on Cognitive Warfare. (2021):2-1. Acesso em 08 de abril de 2024. https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf.

Claverie, Bernard. "What Is Cognition? And How to Make it One of the Ways of the War?" In Cognitive Warfare: The Future of Cognitive Dominance, NATO Collaboration Support Office, (2022):4-3 Acessado em 10 de abril de 2024. https://hal.science/hal-03635907v1/document.

Dahl, Arden B. "Command Dysfunction: Minding the Cognitive War."(1996): 37. Acessado em 05 de abril de 2024. http://uploads.worldlibrary.net/uploads/pdf/20121023231948command_dysfunction_pdf.pdf.

Danyk, Yuriy e Briggs, Chad M "Modern Cognitive Operations and Hybrid Warfare." Journal of Strategic Security 16, n.1. (2023): 35-50. Acessado 10 de abril de 2024. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=2032&context=jss.

DATAREPORTAL. Kepios. "Global Social Media Statistics". 2024. Acessado em 08 de abril de 2024. https://datareportal.com/social-media-users.

Du Cluzel, François. "Cognitive Warfare, a Battle for the Brain." STO-MP-AVT-211. NATO. p.KN3-4.

"The vulnerabilities of the human brain." In The Centrality of Human Brain. Cognitive Warfare. 2020.

Dubreuil, Vincent e LeTourneau, François-Michel. . "A água nas Américas. 2020". (março 2020), https://doi.org/10.4000/ideas.8459 Acessado em 05 de abril de 2020. https://journals.openedition.org/ideas/8459#quotation.

Elam, Donald Emmet. "Attacking the Infrastructure: Exploring Potential Uses of Offensive Information Warfare." (1996):14. Acessado em 05 de abril de 2024. https://apps.dtic.mil/sti/tr/pdf/ADA311391.pdf.

Elder, Elinda e Paul, Richard. "Analytic Thinking: How to take thinking apart and what to look for when you do. The elements of thinking and the standards they must meet." (2007): 5. Acessado em 13 de abril de 2024. https://www.criticalthinking.org/files/Concepts_Tools.pdf.

Ellis, Robert Evan. “The Rise of China in the Americas.” Security and Defense Studies Review. v. 16. (2014): 90.

Ellis, Robert Evan. “Chinese Security Engagement in Latin America.” Center For Strategic & International Studies. (2020): 4-5.

Flemisch, Frank. “Human-machine teaming towards a holistic understanding of Cognitive Warfare.” In Y. R. Masakowski, J. M. Blatny (eds.) Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-ET-356. (2023): 9-1 – 9:10. Acessado em 09 de abril de 2024. https://doi.org/10.14339/STO-TR-HFM-ET-356.

Food and Agriculture Organization (FAO). “The State of the World’s Forests: Forests, Biodiversity and People. 2020” (2020): 42. Acessado em 05 de abril de 2024. https://www.fao.org/3/ca8642en/online/ca8642en.html.

Freeman, D. “Creating Emotion in Games: The Crat and Art of Emotioneering.” *In Computers in entertainment.* v.2. no.3. (2004). https://doi.org/10.1145/1027154.1027179.

Haugland, Edward L. “Future Military Intelligence CONOPS and S&T Investment Road Map 2035 – 2050: The Cognitive War”. (2019): 42. Acessado em 17 de abril de 2024. https://nsiteam.com/mwg-internal/de5fs23hu73ds/progress?id=PapgANAfqJnsqHF-_9NX9_V0jEDIW4DOqT1UumFhJro,

Hung, Tzu-Chieh e Hung, Tzu-Wei Hung. “How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars.” 2020.

Institute for Economics & Peace. “Global Peace Index 2023.” (2023):8-9. Acessado em 05 de abril de 2024. https://www.economicsandpeace.org/wp-content/uploads/2023/09/GPI-2023-Web.pdf.

Jindal, Divyanshu. “The War on Conscience: India in the Age of Cognitive Warfare.” India Foundation Monography 1. (2023):7. Acessado em 10 de abril de 2024. https://indiafoundation.in/wp-content/uploads/2023/09/Divyanshu-Jindal-combined-Final-48-pages.pdf.

Joint Chiefs of Staff. “Joint Publication 3-13. Information Operations.” (2012): II-1. Acessado em 09 de abril de 2024. https://irp.fas.org/doddir/dod/jp3_13.pdf.

Kimberly Orinx1 Pr. Tanguy Struye de Swielande. Chapter 8 – CHINA AND COGNITIVE WARFARE: WHY IS THE WEST LOSING? In Cognitive Warfare: First NATO Scientific Meeting on Cognitive Warfare. Bordeaux. France. (2021): 8-3. Acessado em 12 de abril de 2024. https://innovationhub-act.org/mwg-internal/de5fs23hu73ds/progress?id=tE7YMt51TuGRY0SG6ARUMa--KkN7jWT61Ua5NpPkvL8

Knox, Benjamin. “Chapter 5- Cognitive and Behavioral Science (Psychological Interventions) In Mitigating and Responding to Cognitive Warfare”. STO-TR-HFM-ET-356 (2022): 5-3. https://doi.org/10.14339/STO-TR-HFM-ET-356.

Laricchia, Federica *In* Statista. “Forecast number of mobile devices worldwide from 2020 to 2025 (in billions)*” Acessado em 16 de abril de 2024. https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/#:~:text=In%202021%2C%20the%20number%20of,devices%20compared%20to%202020%20levels.

Li-chung, Chien e Pan, Jason. Research center set up to combat cognitive warfare. (2024). https://www.taipeitimes.com/News/front/archives/2024/01/19/2003812310.

Lindstrom, Bjorn; Bellander, Martin; Schltner, David; Chang, Allen T., Tobler, Phillippe e Amodio, David M. A. “A computational reward learning account of social media engagement.” Nature Communications. 2021

Luberisse, Josh. Cognitive Warfare in the Age of Unpeace: Strategies, Defenses, and New Battlefield of the Mind. Ebook Kindle. Chapter 11: Defensive Strategies: Countermeasures and Resilience. (2023): 89 - 94.

Masakowski, Yvonne R e Sivertsen, Eskil Grendahl. “Chapter 7 – Defence Against 21st Century Cognitive Warfare: Considerations and Implications of Emerging Advanced Technologies”. p 7-7. In Mitigating and Responding to Cognitive Warfare. 2023.

McMahon, Dave. “Maligned Influence and Interference in Canada”. Canadian Global Affairs Institute. (2023): 2. Acessado em 15 de abril de 2024. https://assets.nationbuilder.com/cdfai/pages/5323/attachments/original/1688675087/Maligned_Influence_and_Cognitive_Warfare.pdf?1688675087.

Merino, Álvaro. “El mapa del índice de democracia en el mundo”. (2024). Acessado em 05 de abril de 2024. https://elordenmundial.com/mapas-y-graficos/el-mapa-del-indice-de-democracia/.

Michael, Kobi e Kuperwasser, Yossi. “Cognitive Intelligence: The Theoretical Aspect. In The Cognitive Campaign: Strategic and Intelligence Perspectives”. (2019): 85. Acessado em 17 de abril de 2024. https://www.inss.org.il/wp-content/uploads/2019/10/Memo197_e_compressed.pdf.

Morelle, Marie, Marion, Damien, Cegarra, Julien e André, Jean-Marc. “Towards a Definition of Cognitive Warfare.” Conference on Artificial Intelligence for Defense, DGA Maîtrise de I’Information, Rennes. France. (novembro 2023):1. Acessado em 05 de abril de 2024. https://hal.science/hal-04328461/document.

Naganuma, Kazumi. “Warfare in the Cognitive Domain: Narrative, Emotionality, and Temporality”. (2021):1. Acessado em 17 de abril de 2024. https://www.nids.mod.go.jp/mwg-internal/de5fs23hu73ds/progress?id=F9V2rhIikzcVSUVO9zEG_u0X28P_LJodSFDjxndAxgs

Organização do Tratado do Atlântico Norte. Organização do Tratado do Atlântico Norte. Acessado em 08 de abril de 2024. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/

Organização do Tratado do Atlântico Norte. “Cognitive Warfare: Strengthening and Defending the Mind.” (2023). Acessado em 26 de março de 2024. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

Organization of American States. Inter-American Treaty of Reciprocal Assistance. Acessado em 17 de abril de 2024. https://www.oas.org/juridico/english/treaties/b-29.html

Ottewell, Paul. “Defining the Cognitive Domain’. (2020):4. Acessado em 08 de abril de 2024. https://overthehorizonmdos.wpcomstaging.com/2020/12/07/defining-the-cognitive-domain/?ref=stratagem.no.

Pastor, Álvaro. “Cognitive Warfare.” Barcelona. Spain. 2023. Publicado em PsyArXiv Preprints. (versão de 27 de junho de 2003): 6. https://doi.org/10.31234/osf.io/zgsej Acessado em 10 de abril de 2024.

Pritchard, B. “Cognitive Wars A-I Theory: An Appraisal” In *In Theory Vědy.* Tchéquia: Ústav, v.1/2. (1990): 7:23. Acessado em27 de março de 2024. http://dk.kramerius.org/cdk/view/uuid:17fd3622-2e83-11e2-1418-001143e3f55c?page=uuid:17fd362b-2e83-11e2-1418-001143e3f55c&fulltext=cognitive%20war&source=knav

Puma Shen. “How China Initiates Information Operations Against Taiwan”. *Taiwan Strategists No.12.* (2021): 20. Acessado em 14 de abril de 2024. https://www.airitilibrary.com/Article/Detail?DocID=P20220613001-202112-202206130009-202206130009-19-34.

Rácz, Dr. András. “Socially Inclusive and Exclusive Warfighting: Comparing Ukraine and Russia’s Ways of War.” *In Russia1s Imperial Endeavor and Its Geopolitical Consequences.* Central European University Press (novembro 2023): 27. Acessado em 10 de abril de 2024. https://dgap.org/en/research/publications/socially-inclusive-and-exclusive-warfighting-comparing-ukraine-and-russias

RAND Corporation. “Will to Fight: Returning to the Human Fundamentals of War.” (2018): 12. Acessado em 16 de abril de 2024. https://www.rand.org/mwg-internal/de5fs23hu73ds/progress?id=Cuxof9VGEJnmyoY92tjWYKhsyLIPeQa0C1ZfJD9_Rk0.

Rosner, Yotam e Siman-Tov, David. . “Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion.” *INSS Insight* no.1031 (março 2018):1.

Acessado em 08 de abril de 2024. https://www.inss.org.il/publication/russian-intervention-in-the-us-presidential-elections-the-new-threat-of-cognitive-subversion/.

Santora, Jacinda. "116 social media sites you need to know in 2024". Acessado em 16 de abril de2024. https://influencermarketinghub.com/social-media-sites/

Schubert, Gunter. "China's 31 Preference Policies for Taiwan: An Opportunity, no Threat". (2018). Acessado em 15 de abril de 2024. https://taiwaninsight.org/2018/03/21/chinas-new-31-preference-policies-for-taiwan-an-opportunity-no-threat/.

Shewale, Rohit. "Social Media Users 2024 (Global Data & Statistics)". Acesso em 08 de abril de 2024. https://www.demandsage.com/social-media-users/.

Shimbun, Youmiuri. "China's cognitive warfare aims to influence views in Taiwan." The Japan News. (outubro 2022). Acessado em 13 de abril de 2024. https://asianews.network/chinas-cognitive-warfare-aims-to-influence-views-in-taiwan/.

Siebens, James A. "China's Use of Armed Coercion: To win without fighting.2024". London: Routledge, Taylor & Francis Group.

Taipei Times. 2018. Acessado em 15 de abril de 2024. https://www.taipeitimes.com/News/taiwan/archives/2018/09/09/2003700087

Tzu, Sun. "A Arte da Guerra: Por uma Estratégia Perfeita". Tradução Heloísa Sarzana Pugliesi, Márcio Pugliesi. — São Paulo: Madras. (2005): 63

Worldometer. Acessado em 05 de abril de 2020. https://www.worldometers.info/population/latin-america-and-the-caribbean/ e https://www.worldometers.info/world-population/northern-america-population/

Zimmermann, Rodrigo Milindre Gonzalez "A guerra das Malvinas/Falklands Desclassificada: A Arquitetura do Conflito a partir da Revisão dos Arquivos Oficiais da Argentina, Estados Unidos e Reino Unido" (2023):12. Acessado em 05 de abril de 2024. https://lume.ufrgs.br/bitstream/handle/10183/271073/001193928.pdf?sequence=1

Application of Future Studies by Intelligence Service to Optimize Public Policies.

Fabio Nogueira de Miranda Filho[1]

Recibido: 31 de enero de 2024; Aceptado: 26 de junio de 2024.
Fabio Nogueira de Miranda Filho, "Application of Future Studies by Intelligence Service to Optimize Public Policies." *Hemisferio Revista del Colegio Interamericano de Defensa* 10 (2024): 68-90.
https://doi.org/10.59848/24.1207.HV10n4

Resumen.

Ante un futuro lleno de incertidumbre y un entorno turbulento, los países tratan de aprovechar las oportunidades y resolver los problemas de forma cada vez más oportuna. Para ello, los gobiernos recurren a las políticas públicas como instrumento de gestión. Para asesorar a los decisores gubernamentales, los Servicios de Inteligencia proporcionan productos, entre ellos el Estudio de Futuro, la cual explica la probable evolución futura de las políticas públicas. Por lo tanto, este artículo pretende analizar en qué condiciones el Estudio de Futuro contribuye a la planificación, ejecución y evaluación de políticas públicas por parte de los gobiernos. Más detalladamente, buscamos entender cómo se puede aplicar el Estudio de Futuro, considerando las razones y criterios para su adopción o no adopción. A través de investigaciones cualitativas y exploratorias, los estudios apuntaron el siguiente modelo flexible de utilización del Estudio de Futuro, de acuerdo con las seis fases del ciclo de las políticas públicas: Recepción de Demandas (no recomendada), Establecimiento de la Agenda (recomendada), Formulación de Alternativas (no recomendada), Selección de Opciones (recomendada), Implementación (recomendada a través de indicadores) y Evaluación (no recomendada).

Palabras clave: Inteligencia - Políticas Públicas - Estudio de Futuro - Defensa - Proceso Nacional de Toma de Decisiones

Abstract:

Faced with a future full of uncertainty and a turbulent environment, countries are seeking to seize opportunities and solve problems in an increasingly timely manner. To this end, governments rely on public policies as a management instrument. To advise government decision-makers, the Intelligence Services provide products, including the Future Study, which explains likely future developments in public policies. Therefore, this article aims to analyze under what conditions the Future Study contributes to the

[1] Fabio Nogueira de Miranda Filho é servidor público da Agência Brasileira de Inteligência, Brasil, e possui Mestrado em Defesa e Segurança Hemisférica pelo CID e Mestrado em Administração pela PUC Minas, Brasil. https://orcid.org/0000-0002-4838-8943

planning, execution and evaluation of public policies by governments. In more detail, we seek to understand how the Future Study can be applied, considering reasons and criteria for its adoption or non-adoption. Through qualitative and exploratory research, the studies pointed to the following flexible model for using the Future Study, according to the six phases of the public policy cycle: Reception of Demands (not recommended), Agenda Setting (recommended), Formulation of Alternatives (not recommended), Selection of Options (recommended), Implementation (recommended through indicators) and Evaluation (not recommended).

Keywords: *Intelligence – Public Policy – Future Study – Defense – National Decision-Making Process*

Introduction

Countries constantly seek to develop economically and socially to provide a better standard of living for their citizens. Each nation, without neglecting security and stability, creates its own objectives and structures itself to achieve them. Sometimes, there are setbacks in achieving these goals. For example, the actions to achieve these goals are in competition with the actions of other countries, or the country does not have all the resources necessary for this purpose. For these reasons, States plan and execute what they will do.

For example, Brazil's objectives already appear, in a generic way, in the 1988 Federal Constitution in its article 3º, such as building a free society, eradicating poverty and promoting well-being without any type of discrimination.[2] In the search for more efficiency and in a more specific way, State planning is consolidated in Public Policies. In other words, based on demands and after political discussion, the government decides how to allocate resources to a certain area, such as public security or defense, in response to the population's demands.[3] Therefore, it is up to society to pay attention to what is planned and executed by the State, especially which social forces influence the content of policies and what the impacts of public policies are for everyone.

[2] Senado Federal do Brasil, *Constituição da República Federativa do Brasil*, Brasília, 1988, 1-3.
[3] João Martins Tude, Daniel Ferro, Fabio Pablo Santana, *Políticas Públicas*, Curitiba: IESDE Brasil S.A., 2009, 15-20.

However, it is increasingly noted that the world faces uncertainty, that is, "the inability to know in advance the real probability or impact of future events".[4] Revolutions in communications and the more frequent emergence of disruptive technologies contribute to the acceleration of changes in the world. As a result, dealing with various issues, such as large-scale immigration, population aging, polarization and decline in trust, and increased income concentration, become more complex.[5] It remains for governments to prepare for the unexpected and start imagining possible outcomes of current events in order to plan and act to achieve their own objectives.

Faced with these difficulties, public policies then need to be well chosen, developed and monitored for possible corrections. Countries have several government structures that contribute to the implementation of public policies. There are bodies inherent to the central themes of public policies. For example, the Ministerio de Relaciones Exteriores manages Bolivia's foreign public policy.[6] In addition, other structures complement the advice to the decision-maker on the best course of action. Among them, Intelligence, which often acts through a body that coordinates the activities of an Intelligence system. In Colombia, the Dirección Nacional de Inteligencia is responsible for providing information to State authorities at the highest hierarchical level on matters of national interest. [7]The youngest intelligence service on the American continent, Paraguay's Secretaria Nacional de Inteligencia (SNI), established in 2018, acts in line with the Sistema Nacional de Inteligencia (SINAI).[8]

The Intelligence Services generate classified reports with content that deal with matters of strategic value for the country and disseminated to government authorities. These reports are about the past, to clarify facts, or about the future, to anticipate problems or opportunities.

It is worth noting that reports on the future, hereinafter referred to as Future Studies, have the main objective of outlining plausible scenarios and exploring the

[4] Diário Oficial da República Federativa do Brasil, *Instrução Normativa Conjunta MP-CGU n. 01, de 10 de maio de 2016*. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal, Brasília, 2016, 1-2.

[5] Organisation for Economic Co-operation and Development, *Strategic Foresight for Better Policies*, 1, accessed September 02, 2023, https://www.oecd.org/strategic-foresight/ourwork/Strategic%20Foresight%20for%20Better%20Policies.pdf.

[6] Ministerio Relaciones Exteriores, *Marco Legal*, accessed July, 02, 2023, https://cancilleria.gob.bo/webmre/node/1179.

[7] Dirección Nacional de Inteligencia, *La Entidad*, accessed June 04, 2023, https://dni.gov.co/la-entidad/mision-vision-funciones-y-deberes/.

[8] Secretaría Nacional de Inteligencia Paraguay, *Marco Legal*, accessed July 14, 2023, https://www.sni.gov.py/institucion/marco-legal/leyes.

impacts they may have on public policies to then assist government planning of action. Several countries use future studies to guide public policies, for example, the Estados Unidos Mexicanos through the report " Visión 2030: el México que queremos"[9], or the European Union with the report "Global Trends to 2030: challenges and choices for Europe "[10].

Therefore, this article aims to analyze under what conditions the Future Study makes can contribute to the achievement of public policies by States. Here, the term "conditions" indicates the way in which the Future Study can be applied, considering reasons and criteria for its adoption or non-adoption. In more detail, whether or not to recommend the use of the Future Study will be based, on the one hand, on the methodology adopted in the Future Study itself and the results that can be achieved with it; and, on the other hand, in the way public policies are constructed in general in the countries of the American continent.

This analysis explains in which phases of public policy implementation it is recommended or not to apply the aforementioned Future Study. It is based here that the Future Study contributes to the achievement of public policies, when properly applied to their cycle. This statement is supported by the following arguments. First, the State governs through public policies. Second, the creation and implementation of public policies occur in a context of uncertainty. Third, the Intelligence Activity has a vocation for "anticipation" and "reducing uncertainty", especially through future studies. It is also worth highlighting the caveat that the adequacy of the Future Study is not integral, that is, it does not apply to certain phases of the development of public policies.

Taking the teachings of Gil[11], this research was characterized by being basic (i.e. not applied), as it explained the relationship between future studies and Public Policy and proposing an action model; qualitative, by delving deeper into subjective issues of the phenomenon studied; and exploratory, by seeking familiarity with little-known problems. As technical procedures, explanatory, bibliographic and documentary research was carried out in the collections of various Intelligence Services in the countries of the American continent, in addition to research on the development of public policies.

[9] Gobierno del Mexico, *Visión 2030: El México que queremos*, accessed April 18, 2023, https://globaltrends.thedialogue.org/publication/1416/.

[10] European Union, *Global Trends to 2030: challenges and choices for Europe*, European Strategy and Policy Analysis System: Bruxelas, 2019.

[11] Antônio Carlos Gil, *Métodos e Técnicas de Pesquisa Social*, 6. Ed. São Paulo: Atlas, 2008, 26-31.

In addition to this introduction, the article presents the definition and detail of the public policy cycle. Next, the general concept of Future Study is presented, and then the methodology used is detailed. The paper ends with the comparison of the future study and Public Policy, that is, how it is possible to use the first to make the second efficient. By way of conclusion, the main points covered in the research are revisited and the main implications for the fields of study of Intelligence and Political Science are presented.

Public Policy

According to several authors, there is no single and indisputable definition of Public Policy.[12] Laswell coined perhaps the best-known definition, which consists of answering the following questions: who gets what, why and what difference it makes.[13] Dye adds an important aspect to the definition, which consists of also including in Public Policy what the government does not do.[14] Teixeira details the concept of Public Policy as guidelines for action by the Public Power, in addition to rules and procedures that govern relations between actors in society and the State.[15] In addition to the definition, it is important to highlight that the study of Public Policies is inserted in the branch of political science, but not restricted to this branch. This study encompasses several disciplines, theories and analytical models coming from other areas of knowledge.[16] Examples include economics, administration and future studies.

To better understand Public Policies, Lowi divided them into four types.[17] Distributive policies are characterized by privileging a portion of the population, in which the benefits are clear, but the costs are diffused throughout society. Here the government disregards the issue of limited resources. An example is the aid given by the government to those affected by earthquakes in Chile. Redistributive policies are conflict-oriented and are therefore the most difficult for the government to implement. These policies affect large social groups, but to the detriment of others. For example, fiscal policies in which

[12] Celina Souza, Políticas públicas: uma revisão de literatura, *Sociologias*, n.16, Porto Alegre, jul./dez. 2006, 24.
João Martins Tude, Daniel Ferro, Fabio Pablo Santana, 11-13.
Ricardo Agum, Priscila Riscado, Monique Menezes, Políticas Públicas: conceitos e análise em revisão, *Revista Agenda Política*, São Carlos: Vol. 3 n.2, julho/dezembro 2015, 14-16.
[13] Harold D. Laswell, *Politics: who gets what, when, how*, Cleveland: Meridian Books, 1956, 3.
[14] Thomas Dye, Understanding Public Policy, Englewood Cliffs: N.J.: Prentice Hall, 1984, 1-19.
[15] Elenaldo Celso Teixeira, *O papel das políticas públicas no desenvolvimento local e na transformação da realidade*, Salvador: ATTR, 2002, 2.
[16] Celina Souza, 25-26.
[17] Theodore J. Lowi, Four systems of policy, politics, and choice, *Public Administration Review*, 32: 298-310, 1972, 299-300.

the American government, through the tax system, subsidizes the agricultural sector.[18] The third type, Regulatory, is the one with the greatest visibility for society. As the name suggests, standards are established through decrees and norms for the behavior of the actors involved. Conflict may arise during the execution of the policy, not at its establishment. An example would be the regulation of land transport services in the country. Finally, Constitutive policies are responsible for the procedures with which other policies will be structured. In other words, these policies determine the rules of the game. Brazil's Fiscal Responsibility Law is an example of this type of policy.[19]

It should be noted that each Public Policy may not fit perfectly into a type described above.[20] And it may fits into more than one type. However, the typological division presented is justified by the fact that each policy will have different forms of support and rejection, as well as taking different paths in its application and continuity.[21]

Once the nature of public policies is understood, we turn to the study of the construction cycle in which temporal dynamics stand out. Based on the study of several authors, it is summarized, here, the decomposition of the Public Policy cycle into six phases, as follows: Reception of Demands, Agenda Setting, Formulation of Alternatives, Selection of Options, Implementation and Evaluation.[22] These phases, despite being presented sequentially, are not watertight in themselves. There is a back and forth between phases, characteristic of social constructions.

The first phase of the cycle is Reception of Demands. Reality presents itself in countless problems and opportunities. In turn, the budget is scarce. Therefore, political actors cannot meet all demands. At this stage, the government receives from state institutions and civil society problems to be solved and opportunities that need to be seized. This phase also involves clearly defining all these situations, as well as the determining causes. In the case of a complex public issue, there is a need to subdivide the problem or opportunity so that specific solutions can be devised and the causes can be addressed individually.[23]

[18] Adelson Martins Figueiredo, Maurinho Luiz dos Santos, Maria Aparecida Silva Oliveira, Antônio Carvalho Campos, Impactos dos subsídios agrícolas dos Estados Unidos na expansão do agronegócio brasileiro, *Estudos Econômicos*, São Paulo, 40(2), abr.-jun. 2010, 445-467, accessed August 10, 2023, https://www.scielo.br/j/ee/a/nPVdMG4SH7HMPYdwN9vjbqS/

[19] Author's note: Lei Complementar No. 101 of May 4, 2000.

[20] João Martins Tude, Daniel Ferro, Fabio Pablo Santana, 20-21.

[21] Celina Souza, 28.

[22] Author's note: see Appendix A.

[23] João Martins Tude, Daniel Ferro, Fabio Pablo Santana, 21-37.

It is necessary here to provide better clarification on who the actors, state and private, involved in public policies may be. State actors are those directly linked to public administration. Elected politicians from both the Legislative and Executive branches come into play here. Public servants are also included, who ultimately provide information for decision-making and are responsible for implementing Public Policies. Private actors are the other actors that interfere in the Public Policy cycle: non-governmental organizations (NGOs), media, social movements, research centers, unions, business corporations, political groups, international entities, among others.[24] The media distinguishes itself from others by being able to influence the process in a different way, by focusing the population's attention on certain facts.[25] These actors, whether state or private, can form pressure groups, and, some to a lesser extent act throughout the public policy cycle. It is worth noting that the dispute between the actors serves as a stimulus for improving the conditions of society, as long as they are practiced within the limits of the law.[26]

The process of selecting what is or is not on the list of priorities is called Agenda Setting, the second phase of the Public Policy cycle. Once the situation is known, Public Policy needs, at least, to meet two criteria to enter this agenda.[27] The first is to draw the attention of the actors responsible for setting the agenda. This may be due to the emergency need to resolve or take advantage of the issue. The emergency is calculated by the size of the impact of not solving the problem or not taking advantage of the opportunity, *versus* the probability of occurrence. A good measure is the use of parameters that allow you to monitor what is happening at the moment. Another measure is to collect *feedback* on actions already underway. The second criterion for entering the agenda is that the issue analyzed can be resolved by the public sector, such as the situation of school dropout. Cavalcanti also adds that the asymmetry in the distribution of power make some issues enter the political agenda and others do not.[28]

[24] Author's Note: International entities include foreign governments, international bodies, foreign companies, etc.

[25] John Kingdom, *Agendas, Alternatives and Public Policies*, New York: Longman, 2003, 225-240.

[26] SEBRAE/MG. *Public Policies: concepts and practices* , Belo Horizonte: Sebrae/MG, 2008, 6.

[27] Roger W. Cobb, Charles D. Elder, *Participation in American politics: the dynamics of agenda-building*, Baltimore, Johns Hopkins University Press, 1983, 1-17.

[28] Paula Arcoverde Cavalcanti, *Sistematizando e comparando os enfoques de avaliação e de análises de políticas públicas: uma contribuição para a área educacional*, Tese Doutorado – Curso de programa de pós-graduação em educação, Departamento de Educação, Universidade Estadual de Campinas – Unicamp, Campinas, 2007, 181.

Once the decision has been made to include a problem or opportunity on the political agenda, the third phase begins, Formulation of Alternatives. At this stage, alternative actions and instruments used that may be appropriate to resolve the issue are presented.[29] In other words, it is the establishment of what will be addressed in forwarding the solution. There is now, then, a clear outline of possible government programs, action strategies and what conduct will be followed, as well as objectives and goals to be achieved.[30]

To develop these alternatives, it is necessary to listen to the technical staff about the feasibility of the actions studied.[31] This technical body can be made up of public servants and/or private sector employees, depending on the subject of Public Policy. Another important analysis to be carried out concerns the risk management of implementing a given alternative. The description of the alternative must include the mapping and assessment of operational, image, legal and financial risks according to the risk appetite that the government is willing to accept.[32]

The fourth phase is Selection of Options. It is a process, as it involves knowing how the decision to select options is made, which actors are involved and which factors influence it.[33] The decision whether the Public Policy will be implemented and the choice of the best alternative does not occur in an orderly and rational way, it depends on the type of negotiation and power relations existing at the time of the decision.[34] It should be made clear that the option chosen may not satisfy all interested groups.

Lindblon defines the decision process as complex, with no beginning, middle and end and whose results are uncertain.[35] The author adds that no matter how technical the decision may be, it will always be confronted with political complexity. Therefore, Lindblon adopts the theoretical model of incrementalism to analyze the decision-making process.[36]

For incrementalism, government resources for Public Policy do not start from scratch, but rather from marginal and incremental decisions. Formulations, decisions and adjustments made in the past constrain future decisions, limiting the decision-maker's

[29] Paula Arcoverde Cavalcanti, 177-192.
[30] Ricardo Agum, Priscila Riscado, Monique Menezes, 26-27.
[31] Sebrae-MG, 12-13.
[32] Diário Oficial da República Federativa do Brasil, 1-2.
[33] Paula Arcoverde Cavalcanti, 181-192.
[34] João Martins Tude, Daniel Ferro, Fabio Pablo Santana, 38-49.
[35] Charles E. Lindblon, *Politics and Markets*, The World's Political-Economic System, New York: Basic, 1977, 154-155.
[36] Charles E. Lindblon, 314-318.

capacity. The chosen solution is only the one that is politically viable at that moment. Ultimately, the political side overlaps the rational side. The criticism of this model is that it does not explain the deep structuring reforms that also take place in the public sector.[37]

Another theoretical model to explain decision-making in public policies is Game Theory. According to Almeida, this theory has the function of trying to predict the movement of other players (decision makers for this article).[38] Decision makers can behave as competitors or allies, and thus position themselves to obtain the best result. One's choice depends on the choices made by other decision makers.[39] In contrast to incrementalism, it presupposes that actors act rationally when making choices.

It should be noted that in this fourth phase, decision-makers define resources and the time frame of the Public Policy. They also define how future decisions will be made during the implementation of the Public Policy. For the public good, the choice of alternative should ideally fall on the most efficient and effective alternative.

Implementation is the fifth phase of the Public Policy cycle. Here the transformation of political action into something concrete takes place. For Sabatier, there are two ways to implement Public Policy: top- down, in which decision-makers are separated from those who will implement it; and bottom-up, in which the implementers and beneficiaries of the action participate, together with the decision-makers, in choosing the winning alternative.[40]

The first mode, centralizing, is preferred by politicians, as it provides an excuse in the event of failure to implement Public Policy. In this case, failure belongs only to the implementers.[41] In the second, more participatory mode, the bureaucrats who will implement the policy and decision-makers act to overcome problems and learn from the implementation process.

Another theoretical interpretation for the public policy implementation process is the so-called "View of Implementation as a Game". For this interpretation, there are several situations that unfold in the Implementation phase that are different from what

[37] Celina Souza, 29.

[38] Alecsandra Neri de Almeida, *Teoria dos Jogos: as origens e os fundamentos da teoria dos jogos*, São Paulo: UNIMESP, 2006, 3-5.

[39] Author's note: The classic example of this theory is the case of two suspects being arrested and both being able to walk free, or both being arrested, or just one of them being arrested. It all depends on how they will behave during the interrogation, whether denouncing or denying their colleague's participation.

[40] Paul A. Sabatier, Top-down and bottom-up approaches to implementation research: a critical analysis and suggested synthesis, *Journal of Public Policy*, Cambridge, vol. 6, no. 1, 1986, 22-36.

[41] Ricardo Agum, Priscila Riscado, Monique Menezes, 28-30.

was planned.[42] This entails a constant re-editing of the elaboration of alternatives, decisions and implementations. Especially when it comes to complex policies that involve different levels of power: federal, state and local.[43] This view also highlights that during the previous phases, it is essential for decision-makers and bureaucrats to anticipate future setbacks to facilitate implementation.

In addition to the factors already mentioned, practice shows that other elements contribute to making the Implementation phase the most difficult to execute. Examples are distrust between government agencies that should rather cooperate; technical incapacity of managers; hostile political environment, when there is a change of government; boycotts by groups negatively affected by the policy; corruption of public agents; changes in costs due to macroeconomic factors (such as changes in the dollar exchange rate); communication between the actors involved, among others.[44]

The sixth and final phase, Evaluation, is characterized by analyzing the cost x benefit relationship of implementing the Public Policy. The results of government intervention in society are measured and assessed. The measurement is based on the comparison of the results obtained with the objectives and parameters previously established in the Formulation of Alternatives phase.[45]

Evaluation is divided into two types: internal and external. The implementers themselves conduct the internal evaluation. This is about comparing the resources spent with the established parameters. These parameters normally include aspects of time (timely), cost (lower), quality (higher) and sustainability (preservation of scarce resources).

On the other hand, experts who did not participate in the program typically conduct external evaluation. They compare the results obtained with the objectives of Public Policies. The important thing is to determine the relevance, impacts and functions fulfilled by the policy. The experts assess the redistribution of resources and affected segments. Furthermore, attention must be paid to the fact that the impacts generated can provoke new demands, which can generate other public policies. Another point that

[42] João Martins Tude, Daniel Ferro, Fabio Pablo Santana, 41-43.
[43] Sebrae-MG, 15-18.
[44] Maria das Graças Rua, Alessandra T. Aguiar, A política industrial no Brasil 1985-1992: políticos, burocratas e interesses organizados no processo de policy making, In: *Planejamento e Políticas Públicas*, n.12, jul/dez, 1995, 236-253.
Sebrae-MG, 15-18.
João Martins Tude, Daniel Ferro, Fabio Pablo Santana, 48.
[45] João Martins Tude, Daniel Ferro, Fabio Pablo Santana, 38-49.

deserves attention is to check whether the policy produced an unforeseen impact, a type of side effect, a situation that may deserve special treatment.

The eminently technical external and internal evaluations can give rise to questions about the actions of politicians, especially if the actions adopted are not appropriate for the issue faced. Politicians, in turn, claim that the evaluation needs to be technical as well as political, and that there will always be a tangle of causes and that public policy, to be well assessed, would need an infinity of parameters.[46] Another defense alleged by politicians is that public policies need approximately 10 years after the end of implementation to mature, which makes evaluation difficult immediately after the end of the actions.[47]

It is noteworthy that the Evaluation phase does not necessarily happen after implementation. On many occasions, it is opportune to carry out the Evaluation during Implementation, precisely to propose corrections when necessary.[48] Furthermore, the Evaluation contributes to increasing cooperation between actors, justifying the actions adopted and generating useful information for other public policies.

Figure 1 below illustrates the dynamics of these six phases of the Public Policy cycle.

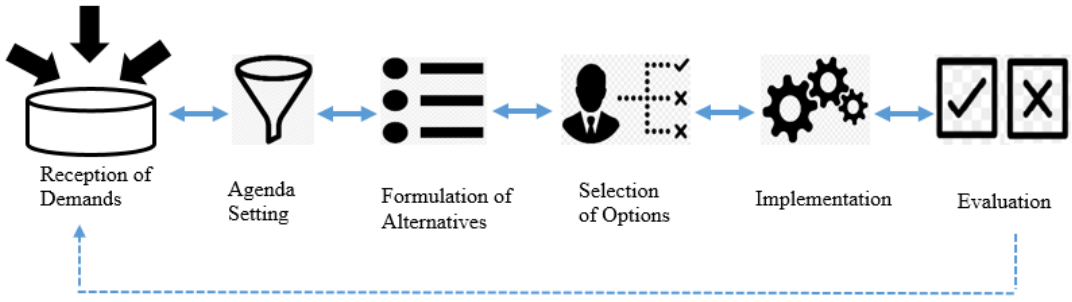


Figure 1: Diagram of the phases of the Public Policy cycle
Source: elaborated by the author

Future Study

Although the study of the future dates back to the time of ancient Egypt when people sought to predict the outcome of harvests[49], it was in the 1950s that the prospective attitude coined by Berger appeared.[50] Now the aim is to assist the decision-making process of companies and governments. The idea is to look broadly at distant futures

[46] Ricardo Agum, Priscila Riscado, Monique Menezes, 30-31.
[47] Paul A. Sabatier, 33-36.
[48] Sebrae -MG, 18-23.
[49] Peter Schwartz, *The art of the long view*, New York: Doubleday, 1991, 105-106.
[50] Gaston Berger, *L'attitude prospective*, Revue Prospective n1 1-10, Paris: 1958.

through the perspective of experts. In other words, draw panoramas of possible futures, weighing the past and comparing the projects of the actors working on the issue studied.[51] According to the Organisation for Economic Co-operation and Development (OECD), foresight, another name given to the Future Study, is looking beyond current expectations and taking into account a range of plausible future developments in order to identify implications for today's policies.[52]

To better clarify the definition of Future Study, it is also worth highlighting what it is not: neither prediction nor projection.[53] Prediction is asserting that the future will be a certain way. It would be choosing one of the scenarios outlined and stating that the future would be exactly that way.[54] Similarly, the projection also considers a single future, drawn from econometric models. The past behavior of the variables would be modeled and projected into the future; in short, the future would have to be a simple projection of the past.[55]

The characteristics of the future regulate the development of the Future Study. According to Godet,[56] the future is multiple and uncertain. From the beginning of its study, there are multitude of possible futures and none are pre-determined to happen. Furthermore, it is uncertain, there is no way to predict what will happen. This uncertainty is due to the forces that influence the future, namely, the variables or trends and the actions of the actors. Thus, the construction of these possible futures is the fruit of our imagination.[57]

One way to operationalize the study of the future, observing all the characteristics described above, is through scenario building. Scenarios are the set formed by the description, in a coherent way, of a future situation and the course of events that allow moving from the original situation to the future situation.[58] The focus of the scenarios is the events and issues of interest to decision makers. The study of scenarios is effective when it changes the decision maker's behavior.[59] This change in behavior occurs through

[51] Michel Godet, *Manual de prospectiva estratégica: da antecipação a ação*, Lisboa: Publicações Dom Quixote, 1993, 105-126.

[52] Organisation for Economic Co-operation and Development, 2.

[53] Elaine Coutinho Marcial, *Academic Citation* (presenttion, Construção de Cenários Prospectivos, Brasília, September 17, 2021 – October 13, 2021).

[54] Organisation for Economic Co-operation and Development, 3.

[55] Michel Godet, 29-36.

[56] Michel Godet, 1-5.

[57] Elaine Coutinho Marcial.

[58] Michel Godet, *Scenarios and Strategic Management*, London: Butterworths Scientific, Ltd., 1987, 70.

[59] Peter Schwartz, 214.

the study of the scenarios themselves and by monitoring the environment as the future unfolds.

The purpose of constructing scenarios is to identify opportunities and threats to the organization and thus allow thinking about alternatives to pursue in the future.[60] Faced with these strategic options, the organization can take an active stance in building its own future, or at least influencing this future; or a defensive posture when trying to reduce the risks of a hostile future. Other authors also emphasize that scenarios generate organizational learning by encouraging both the change of mental models, especially at the top, and increased communication within the organization regarding the possibilities of the future.[61]

It may seem counterintuitive, but scenarios are built in the knowledge that the future will not turn out the way they were written. Based on the study of the constructed scenarios, the organization makes decisions that affect other actors, who, in turn, will react, unfolding in different situations. Therefore, future studies consider all constructed scenarios, not just one. The intention is to reduce risks while maximizing opportunities by influencing the future by making decisions today.

There are several examples of the use of futures studies by various governments. Brazil has the Estratégia Federal de Desenvolvimento (EFD), prepared for the period from 2020 to 2031. Three scenarios are outlined that must be considered in the planning of all bodies and entities of the federal public administration. The government's objective is for this strategy to be part of a structuring platform for Public Policies.[62] In Peru, the Centro Nacional de Planeamento Estratégico (CEPLAN) has the mission of helping government bodies achieve a future with harmonious and sustainable development. To this end, CEPLAN carries out several future studies, such as in 2017 with “Escenarios de futuro

[60] Michael E. Porter, *Competitive advantage*, New York: Free Press, 1985, 470-481.
Michel Godet, 57-82.
Organisation for Economic Co-operation and Development, 3.

[61] Arie de Geus, *Living Company: habits for survival in a turbulent business environment*, Boston: Harvard Business School Press, 2002, 101-135.
Thomas J. Chermack , Susan A. Lynham, Definitions and outcome variables of scenario planning, *Human Resource Development Review* , v.1, n.3, p. 366-383, 2002, 373-377.

[62] Diário Oficial da República Federativa do Brasil, *Decreto n°10.531, de 26 de outubro de 2020*, Institui a Estratégia Federal de Desenvolvimento para o Brasil no período de 2020 a 2031, Brasília, 2020, 1.

para el Perú", projecting the future until 2030. [63]In Chile, in 2023, debates were held projecting the country in 2050 through the "Chile crea futuro" project of the Consejo Nacional de Ciência, Tecnología, Conocimiento e Innovación para el Desarrollo.[64] Furthermore, at a global level, more examples can be cited, such as the report "Global Economic Prospects" made by the World Bank in January 2021 and "Government Foresight Community Annual Meeting Report 2020: strategic foresight for future- ready public policy" created by the OECD in October 2020.

Future Studies and Intelligence

The Intelligence Services, as the public policy of the Intelligence Activity itself advocates, are responsible, among others, for executing and coordinating Intelligence activities in their respective country. Taking Brazil as an example, the law that established the Agência Brasileira de Inteligência (Abin) defines Intelligence as activity that aims to get, analyze and disseminate knowledge within and outside the national territory about facts and circumstances of immediate or potential influence on the decision-making process and government action and on the protection and security (and safety) of society and the State.[65]

Figure 2 illustrates the concept of Intelligence defined in this law.

[63] Centro Nacional de Planeamiento Estratégico, *Escenarios de futuro para el Perú* - Julio 2017, accessed September 3, 2023, https://cdn.www.gob.pe/uploads/document/file/3518877/Escenarios%20de%20Futuro%20para%20el%20Per%C3%BA%20-%20Expositor%3A%20Jordy%20Vichez%20Astucuri%2C%20director%20nacional%20de%20Prospectiva%20y%20Estudios%20Estrat%C3%A9gicos%20de%20CEPLAN.pdf.

[64] Ministerio de Economía, Fomento e Turismo del Chile. Chile crea future: Mirada diversa com proyección de país al 2050, accessed July 05,2023, https://www.economia.gob.cl/2023/06/29/chile-crea-futuro-mirada-diversa-con-proyeccion-de-pais-al-2050.htm.

[65] Diário Oficial da República Federativa do Brasil, *Lei Nº 9.883, de 7 de dezembro de 1999*, Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências, Brasília, 1999, 1.

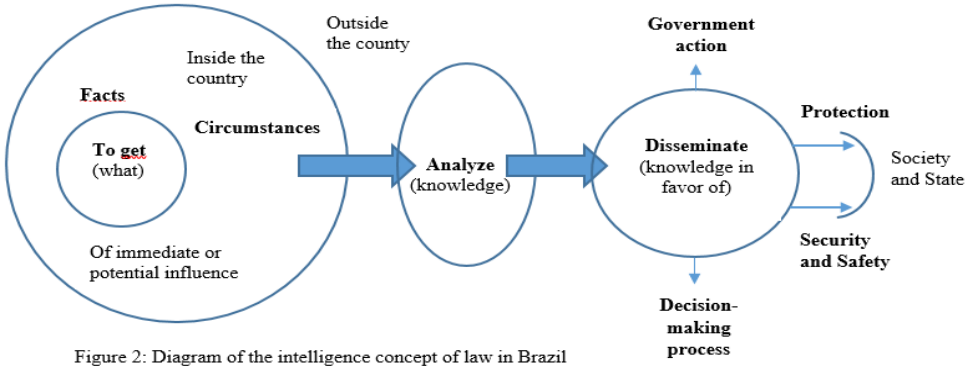


Figure 2: Diagram of the intelligence concept of law in Brazil
Source: elaborated by the author

To analyze the knowledge that is obtained, the Intelligence Service uses specialized techniques, especially in the case of the Future Study. The method for this study follows the Intelligence cycle that comprises planning, data collection, data analysis, dissemination of the generated product and monitoring of the situation studied.[66] Monitoring can take place through indicators that are facts, events, conditions, indices that reveal which scenario is materializing. Examples of indicators include the basic interest rate, number of riots, number of new patents, troop movements, among others. Over time, intelligence monitors these indicators to find out how reality unfolds and which scenario is closest to this reality. At this stage, Intelligence reports are necessary to alert the decision-maker about aspects that may motivate some action on the part of the State. If there is any fact that causes profound transformation, it may be necessary to carry out a new Future Study.

The method used to carry out future studies by the Intelligence Services are subject to secrecy, as the techniques and methodologies used in general are part of the secret of the activity. However, future studies are based mainly on the works of Michel Godet, who, in turn, was based on the La Prospective school developed by Gaston Berger in the 1950s. In order to adapt Godet 's method to the specificities of Intelligence activity, ideas and tools from other academics can be incorporated, such as the cross-impact matrices outlined by Gordon.[67] Furthermore, it is very common to use the Delphi method.[68] Regardless of the method, the formation of a multidisciplinary group of intelligence analysts and constant consultation with experts on the subject are part of the good

[66] Marco Cepik, Inteligência e Políticas Públicas: dinâmicas operacionais e condições de legitimação, *Security and Defense Studies Review*, Volume 2, n.2, Winter 2002, 249-251.

[67] Author's note: the concept and all theory related to the Cross-Impact method can be found in the following work: Theodore Gordon, *Cross- impact method* (MID), United Nations: 1994.

[68] Author's note: a possible source of consultation on the Delphi Method can be found in: James T. C. Wright and Renata A. Giovinazzo, Delphi - uma ferramenta de apoio ao planejamento prospectivo, Caderno de Pesquisas em Administração, São Paulo, v. 1, n. 12, 2000.

practices in preparing the Future Study. Finally, variables and actors that interfere in the studied environment and their implications for each other are evaluated, and how these factors would behave in the future.

The Future Study, as a variation of foresight in the field of Intelligence, aims to advise the government to make the best decisions for society today regarding future issues. The immediacy of the challenges leads governments to worry only about the here and now. If the government does not get involved with the future, it will be ill-prepared to deal with unexpected and unconventional issues.[69] The Future Study helps governments get out of this situation of inefficiency, especially in turbulent and uncertain environments.

In particular, the Intelligence Services product differs from other information flows due to the possibility of including data denied by the opponent or difficult to obtain by conventional means. This confidential information can help construct scenarios that would otherwise go unnoticed. Another point that deserves to be highlighted is the fact that the Intelligence Service has the vocation of monitoring the environment to anticipate the future, that is, problems and opportunities. In this way, it is already inherent to the analyst's work to monitor the indicators of the outlined scenarios.

The use of the Future Study is suitable for both national issues (macro or strategic) and sectoral issues (micro or tactical). Examples of national decisions include choose alternative actions to deal with the consequences of forced immigration or face the expansion of organized crime or even how to manage alliances in international trade agreements. At another level, on a smaller scale, there are examples in the definition of defense industry development policy or how to combat cross-border drug and arms trafficking. You can also specialize even more in specific issues such as the potential of applying artificial intelligence in Defense[70] or the use of a space rocket launch base or even if it is worth building a nuclear submarine. Futures studies efforts at both broad and specific levels can interconnect and reinforce each other as part of a continuous system of integrating futures thinking applied to public policy formulation.[71]

The Future Study is criticized mainly in two aspects: cost, both due to the time it takes to prepare the report, around two months, and the number of analysts dedicated to

[69] Organisation for Economic Co-operation and Development, 2-3.

[70] Author's note: an example of this potential is the use of Artificial Intelligence (AI) against hypersonic missiles, since missiles travel at speeds greater than 5 times that of sound. In addition to high-speed processing of missile trajectory data, AI is also a key element in countering this threat.

[71] Organisation for Economic Co-operation and Development, 4.

the work, at least five; and report size, no less than ten pages. Defenders of the Future Study argue that not every subject deserves to be covered by it. It is only suitable for the most complex ones, with significant impact and requiring a distant future study, for four years or more. Therefore, to prepare such studies, the preparation time and the team dedicated to the task present a favorable cost/benefit given the return obtained. Regarding the size of the report, it is assumed that Presidents and Ministers of State would hardly read extensive documents, however their advisors or senior and middle government management could focus on texts that really matter. Furthermore, the construction of the Future Study already provides a better understanding of the topic, which facilitates oral reports for senior authorities and monitoring of developments. Monitoring is most notable when experts from the Intelligence Service together with those from the country's Intelligence System construct the Future Study.

Perhaps the most famous Futures Study produced by the Intelligence Services of the Americas is the report entitled “Global Trends” published by the National Intelligence Council and produced by the American Intelligence System, led by the Central Intelligence Agency (CIA). Several publishers around the world publish the ostensible version.[72] CIA distributes the confidential version only to sectors of the American government that need to know about a specific topic.

Public Policy and Future Studies

The function of the Intelligence Service is to advise the national decision-making process whenever necessary or requested, regardless of the moment in the Public Policy cycle in question. Various types of Intelligence’s reports materialize this advice. It is up to the Intelligence Service to identify the best way to respond to the decision-maker's call. The Future Study is used to improve long-term decisions. As the complexity of reality does not allow defining a single way of acting, the aim, by optimizing the use of the Future Study based on the Public Policy cycle, is to propose a flexible model of action. The use of the Future Study will be more effective if the indication follows technical criteria that provide more legitimacy and usefulness to this tool.

Keeping this premise of technical criteria in mind, we turn to the first phase of the cycle, Reception of Demands. Receiving problems and opportunities from society describes this phase. At this stage, decision-makers would not use the Future Study, as

[72] Author's note: for example - Relatório da CIA: a nova era. Original title “Global Trends 2035”. Published by *Geração no Brasil* in March 2019.

precisely the free movement of ideas and projects characterizes the phase. There is no point in limiting the clash of actors at this moment.

On the other hand, in the Agenda Setting phase, decision-makers are provided with assistance in carrying out the activity of selecting, albeit in a preliminary way, the policies that will make up the agenda. At this point, the decision-maker does not know the consequences of implementing or not implementing a Public Policy. The product of the Future Study, possible scenarios, sheds light on this issue by helping the decision-maker understand the situation and choose policies that provide better well-being for the population, whether to avoid undesirable scenarios or to strengthen favorable scenarios. It is noteworthy that here, there is a clash between state and private actors to influence the formation of the agenda. However, it is up to the decision-maker to understand the situation, based on the Future Study, and make the best choice.

In the third phase, Formulation of Alternatives, the technical team develops possible ways of acting to implement a given Public Policy. The Future Study is not essential in developing alternative courses of action, since at this stage technicians need to use objectivity and data that clarify the current situation to create a way of government action that allows progress for society. However, nothing prevents the Future Study carried out in the previous phase from being used to guide the construction of alternatives if technicians feel the need to understand how the future would unfold based on the premises established in the preliminary choice of Public Policy. The Future Study would be another element of assessment by technicians to develop alternative actions, but it is not fundamental.

In the Selection of Options phase, it is defined whether the Public Policy will be implemented, as well as which implementation alternative will be chosen. At this moment, the decision-making process needs to be based on evidence, observing ethical and legal guidelines.[73] However, the situation to be faced appears diffuse and for this type of decision, the weight of facts is low, while the weight of judgments is high.[74] Thus, the decision-maker, through subjective assessments, seeks to identify and define current and potential developments. To do this, it is common to turn to specialists, who can offer the Future Study, which reduces the probability of an inappropriate decision. In this way, the

[73] Diário Oficial da República Federativa do Brasil (2020), 26.

[74] Morgan D. Jones, *The Thinker's toolkit: 14 powerful techniques for problem solving,* New York: Editora Crown Business, 1998, 7-9.

Future Study becomes a useful element for the decision-maker, as already identified in the Agenda Setting phase.

Note that the Future Study used in this fourth phase may or may not be the same as the one already used in the Agenda Setting phase. What will define whether the Future Study will be another, different from the first, is the fact that there is a cyclical change in the time lapse between these two phases. If situations have occurred that have transformed the environment in which Public Policy will take place, it may be necessary to carry out a new Future Study.

Execution characterizes the Implementation of Public Policy, the fifth phase of the cycle. As already mentioned, this phase is the most difficult due to several factors such as communication between actors and boycotts from adverse groups, among others. As Public Policy unfolds, the public agents responsible for its execution become aware of difficulties and try to overcome them. Whenever possible, they seek to anticipate these problems to maximize the resources available for implementing Public Policy.

The Future Study necessarily has a phase in which indicators are developed. Measuring these indicators is useful for monitoring the environment in question. Through the collection of indices and situational studies, it is possible to outline which scenario reality is approaching. If a scenario proves to be inappropriate, corrective actions are necessary. If the scenario is favorable, reinforcement actions are still necessary. Therefore, at this stage the use of the Future Study is much more valid for the indicators generated and the respective monitoring than for the Future Study itself. Still, the use of the Future Study is useful. After all, the public agents involved in implementation are constantly learning.

In the Evaluation phase, the binomial controlling and judging Public Policy prevails. Although this phase formally constitutes the last of the cycle, it is also spread throughout the previous Implementation phase. To remember, government oversight bodies to check the occurrence of corruption and other wrongdoings exercise control of Public Policy. Bureaucrats carry out the evaluation through the comparison of parameters collected before and after the implementation of the Public Policy, in addition to other ways of measuring the impacts of this policy. It appears that in these tasks, both control and judgment, the Future Study does not seem to be the most appropriate to assist decision-makers and public agents. The scenarios generated in the Future Study are speculations of possible scenarios and when the Evaluation phase takes place, the future has already arrived and has become the present, with no room for assumptions.

It is clear that the Future Study takes place in the national decision-making process considering the Public Policy cycle in three of its phases. Especially in the decision-making phases, whether preliminary or definitive selection of what will be put into practice. Furthermore, during Implementation, the Future Study is also useful by delivering indicators that monitor the environment and allow for better calibration of Public Policy.

Figure 3 below illustrates the proposed model for recommending the application of the Future Study in each phase of the Public Policy cycle.

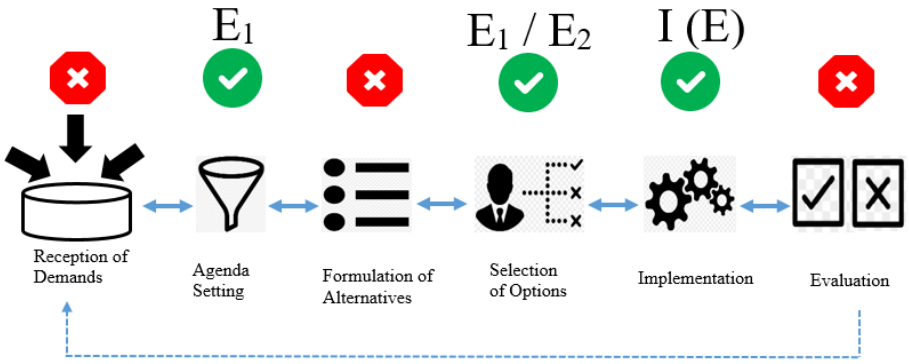


Figure 3: Application of the Future Study according to the phases of the Public Policy cycle
Source: elaborated by the author

Final considerations

According to Gaddis, strategy is the alignment of potentially unlimited aspirations with necessarily limited capabilities.[75] Society and the governments that represent it have an intense desire for full social and economic development; however, the State's production power is insufficient to meet all these objectives. Thus, public policies emerge to be the alignment between aspirations and capabilities. Moreover, the Future Study contributes to choosing the best alignment through adjustments and regulations.

Similarly, the OECD recommends that governments establish anticipatory governance.[76] In other words, governments systematically incorporate and apply strategic predictions throughout the governance architecture, that is, throughout the Public Policy cycle. By strategic forecasts, the international organization understands it to be the structured and explicit exploration of multiple futures, in order to assist decision-making. For the Intelligence Services, Future Studies are the way to operationalize these strategic predictions.

[75] John Lewis Gaddis, *As grandes estratégias*, São Paulo: Editora Planeta do Brasil, 2019, 33.
[76] Organisation for Economic Co-operation and Development, 3.

On the part of an Intelligence Service, exploiting the potential of the Future Study increases its rapport with other areas of the State. In this way, your Intelligence analysts develop skills that they did not have before carrying out the Future Study. On the part of the decision-maker, by understanding how future studies work, he or she is encouraged to have new thoughts to develop innovative and appropriate public policies to take advantage of opportunities and overcome challenges.

Reflectively, the Intelligence Activity itself is a Public Policy, and as such, those responsible for it, i.e. the bodies that make up the country's Intelligence System, must see it. Therefore, the Future Study on Intelligence itself and its developments is a good practice to help decision-makers implement this policy.

At the end of this exposition, one can understand how the argument was supported. In the case of the first argument, which the State governs through public policies, it was highlighted that public policies are produced within a cycle with six phases. Second, the achievement of public policy occurs in a world of great and rapid transformations, which generates uncertainty about the future. Third, Intelligence's main function is to anticipate facts and events to advise the national decision-making process, in particular, using the Future Study. It is worth noting, however, that the adequacy of the Future Study is partial, that is, it does not apply to all phases of the development of public policies. Based on this, the conclusion is, in fact, the Future Study contributes to the achievement of public policies, when applied appropriately to the public policy cycle.

The model proposed in this study can serve as a basis for future empirical investigations into the use of Future Studies to aid the national decision-making process according to the phases of the Public Policy cycle. To complement the current research, it also suggests checking how other Intelligence products can be useful in achieving public policies. These studies would be necessary to expand the results obtained here.

Mahatma Gandhi said that the future will depend on what we do in the present. Paraphrasing the Indian political leader in consideration of the context of this research, the future will depend on the Future Study we carry out and the decisions we make in the present.

Bibliography

Agum Ricardo, Riscado Priscila and Menezes Monique. “Políticas Públicas: conceitos e análise em revisão”. Revista Agenda Política, São Carlos: Vol. 3 n.2, julho/dezembro 2015.

Almeida Alecsandra Neri. “Teoria dos Jogos: as origens e os fundamentos da teoria dos jogos”. São Paulo: UNIMESP, 2006.

Berger Gaston. “L’attitude prospective”. Revue Prospective n1 1-10. Paris: 1958.
Brasil. “Constituição da República Federativa do Brasil”. Brasília: Senado, 1988.
Brasil. “Lei Nº 9.883, de 7 de dezembro de 1999”. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Diário Oficial da República Federativa do Brasil. Brasília, 1999.
Brasil. “Instrução Normativa Conjunta MP-CGU n. 01, de 10 de maio de 2016”. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Diário Oficial da República Federativa do Brasil. Brasília,2016a.
Brasil. “Decreto n°10.531, de 26 de outubro de 2020”. Institui a Estratégia Federal de Desenvolvimento para o Brasil no período de 2020 a 2031. Diário Oficial da República Federativa do Brasil: Brasília, 2020.
Cavalcanti Paula Arcoverde. “Sistematizando e comparando os enfoques de avaliação e de análises de políticas públicas: uma contribuição para a área educacional”. Tese Doutorado – Curso de programa de pós-graduação em educação, Departamento de Educação, Universidade Estadual de Campinas – Unicamp, Campinas, 2007.
Cepik Marco. “Inteligência e Políticas Públicas: dinâmicas operacionais e condições de legitimação”. Security and Defense Studies Review. Volume 2, n.2, Winter 2002.
Chermack Thomas J. and Lynham Susan A. “Definitions and outcome variables of scenario planning”. Human Resource Development Review, v.1, n.3, p. 366-383, 2002.
Cobb Roger W. and Elder Charles D. “Participation in American politics: the dynamics of agenda-building”. Baltimore. Johns Hopkins University Press, 1983.
Dye Thomas. “Understanding Public Policy”. Englewood Cliffs: N.J.: Prentice Hall, 1984.
European Union. “Global Trends to 2030: challenges and choices for Europe”. European Strategy and Policy Analysis System: Bruxelas, 2019.
Frey Klaus. “Políticas Públicas: um debate conceitual e reflexões referentes à prática da análise de políticas públicas no Brasil”. Planejamento e Políticas Públicas. Brasília: IPEA, 2000.
Gaddis John Lewis. “As grandes estratégias”. São Paulo: Editora Planeta do Brasil, 2019.
Geus Arie de. “Living Company: habits for survival in a turbulent business environment”. Boston: Harvard Business School Press, 2002.
Gil Antônio Carlos. “Métodos e Técnicas de Pesquisa Social”. 6. Ed. São Paulo: Atlas, 2008.
Godet Michel. “Scenarios and Stragic Management”. London: Butterworths Scientific, Ltd., 1987.
Godet Michel. “Manual de prospectiva estratégica: da antecipação a ação”. Lisboa: Publicações Dom Quixote, 1993.
Gordon Theodore. Cross-impact method (MID). United Nations: 1994.
Jones Morgan D. “The Thinker’s toolkit: 14 powerful techniques for problem solving”. New York: Editora Crown Business, 1998.
Kingdom John. “Agendas, Alternatives and Public Policies”. New York: Longman, 2003.
Laswell Harold D. “Politics: who gets what, when, how”. Cleveland: Meridian Books, 1956.
Lindblon Charles E. “Politics and Markets”. The World’s Political-Economic System, New York: Basic, 1977.
Lowi Theodore J. “Four systems of policy, politics, and choice”. Public Administration Review, 32: 298-310. 1972.
Marcial Elaine Coutinho. “Análise Estratégica: Estudos de futuro no contexto da inteligência competitiva”. V. 1. Brasília: Thesaurus Editora, 2011.
Organisation for Economic Co-operation and Development (OECD). “Strategic Foresight for Better Policies”. https://www.oecd.org/strategic-foresight/ourwork/Strategic%20Foresight%20for%20Better%20Policies.pdf.
Porter Michael E. “Competitive advantage”. New York: Free Press, 1985.
Rua Maria das Graças and Aguiar Alessandra T. “A política industrial no Brasil 1985-1992: políticos, burocratas e interesses organizados no processo de policy making”. In: Planejamento e Políticas Públicas, n.12, jul/dez, 1995.
Sabatier Paul A. “Top-down and bottom-up approaches to implmentation research: a critical analysis and suggested synthesis”. Journal of Public Policy, Cambridge, v. 6, n. 1, 1986.

Schwartz Peter. “The art of the long view”. New York: Doubleday, 1991.
Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (Sebrae/MG). “Políticas Públicas: conceitos e práticas”. Belo Horizonte: Sebrae/MG, 2008.
Souza Celina. “Políticas públicas: uma revisão de literature”. Sociologias, n.16, Porto Alegre, jul./dez. 2006.
Teixeira Elenaldo Celso. “O papel das políticas públicas no desenvolvimento local e na transformação da realidade”. Salvador: ATTR, 2002.
Tude João Martins, Ferro Daniel and Santana Fabio Pablo. “Políticas Públicas”. Curitiba: IESDE Brasil S.A., 2009.
USA. “Global Trends 2040: a more contested world”. National Intelligence Council: Washington, 2021.
Wright James T. C. and Giovinazzo Renata A., Delphi - uma ferramenta de apoio ao planejamento prospectivo, Caderno de Pesquisas em Administração, São Paulo, v. 1, n. 12, 2000.

Appendix A

Phases of the Public Policy Cycle

Authors / Phases	Frey, 2000	Souza, 2003	Kingdom, 2003	Cavalcanti, 2007; Tude, Ferro, Santana, 2009	Sebrae/MG, 2008	Agum, Riscado e Menezes, 2015	**Adopted in the article**
1	Perception and definition of problems	X	X	X	X	Problem Identification	**Reception of Demands**
2	Agenda Setting	Agenda setting	Agenda Establishment	Formulation of public policies	Formation of the Agenda	Formation of the Agenda	**Agenda Setting**
3	Program development and decision-making	Identification of alternatives	Compose Alternatives for possible resolution of the problem		Policy formulation	Formulation of Alternatives	**Formulation of Alternatives**
4		Evaluation of options			Decision-making process	Decision making	**Selection of Options**
		Selecting options	Choice of Alternative				
5	Policy implementation	Implementation	Implementation of the Decision	Implementation of public policies	Implementation	Implementation of public policy	**Implementation**
6	Policy assessment and action correction	Evaluation	X	Evaluation of public policies	Evaluation	Evaluation	**Evaluation**

A anualidade orcamentaria e os projectos de defesa: a caso basileiro.

Franselmo Araújo Costa[1]

Recibido: 30 de abril de 2024; Aceptado: 01 de julio de 2024.
Franselmo Araújo Costa, "A anualidade orcamentaria e os projectos de defesa: a caso basileiro."
Hemisferio Revista del Colegio Interamericano de Defensa 10 (2024): 91-105.
https://doi.org/10.59848/24.1207.HV10n5

Resumo

O presente texto apresenta as falhas, causas e efeitos do princípio da anualidade orçamentária sobre os projetos plurianuais de defesa. De acordo com a CF/88 e a Lei nº 4.320/64, as previsões e autorizações orçamentárias coincidem com o ano civil, com estimativa de receitas e fixação de despesas compreendendo o período de 1º de janeiro a 31 de dezembro de cada exercício financeiro. Porém, não há um instrumento plurianual que respalde ou dê garantias orçamentárias mínimas para a continuidade de contratos de longo prazo firmados no setor de defesa. O Plano Plurianual – PPA de quatro anos se constitui historicamente em uma lei que rapidamente cai em desuso, principalmente em função de não possuir bases fiscais sólidas e não ser de execução obrigatória. Assim, o que se observa é um alongamento constante de prazos para conclusão de investimentos estratégicos de defesa, com aumento de custos e perda de eficiência para a consecução dos objetivos da Política Nacional de Defesa – PND. O texto apresenta, ainda, algumas alternativas que poderiam minimizar a imprevisibilidade de recursos financeiros para projetos estratégicos de defesa e que poderiam contribuir para o melhor uso de recursos públicos, na linha de um orçamento voltado para resultados.

Gostaria de agradecer a todos os Doutores da classe 62 (2022-2023) do Colégio Inter-Americano de Defesa - CID, em especial a Doutora Mirlis Reyes, pelo compartilhamento de bibliografia sobre o tema, fundamental para a produção desse artigo.

Palavras-chave: Anualidade, Plurianualidade, Projetos Estratégicos, Política Nacional de Defesa, Estratégia Nacional de Defesa, Livro Branco de Defesa.

[1] O autor é Analista de Planejamento e Orçamento do governo federal desde 1996, mestre em Defesa e Segurança Hemisféricas pelo Colégio Interamericano de Defesa em 2023, com especialização em Economia do Setor Público pela Fundação Getúlio Vargas de Brasília em 2002 e em Teoria e Operação de Economia Nacional Moderna pela George Washington University em 2011. Email: franselmo.costa@gmail.com. https://orcid.org/0009-0003-9401-2351

Abstract

This article presents the failures, causes and effects of the principle of budgetary annuality on multi-year defense projects. According to CF/88 and Law nº 4,320/64, budget forecasts and authorizations coincide with the calendar year, with estimated revenues and expenses for the period from January 1 to December 31 of each financial year. However, there is no multi-year instrument that supports or provides minimum budgetary guarantees for the continuity of long-term contracts signed in the defense sector. The four-year Multi-Year Plan (PPA) has historically been a law that quickly falls into disuse, mainly due to the fact that it does not have solid fiscal bases and is not mandatory. Thus, what is observed is a constant lengthening of deadlines for the completion of strategic defense investments, with increased costs and a loss of efficiency for the achievement of the objectives of the National Defense Policy (PND). The article presents some alternatives that could minimize the unpredictability of financial resources for strategic defense projects and that could contribute to the best use of public resources, according to result-oriented budgeting.

I would like to express my gratitude to all Ph. D. of class 62 (2022-2023) of the Inter-American Defense College - IACD, especially Dr. Mirlis Reyes, for sharing bibliography related to the topic, that was essential for writing this article.

***Keywords**: Annuality, Multiannuality, Strategic Projects, National Defense Policy, National Defense Strategy, Defense White Paper.*

Introdução

Os recentes conflitos mundiais têm levado os países e as alianças de segurança cooperativa, como a OTAN, a intensificar as ações necessárias à defesa nacional. As decisões relativas aos investimentos no setor, consequentemente, comprometerão recursos orçamentários de médio e longo prazos, o que requer previsibilidade aliada à responsabilidade fiscal.

Apesar do privilégio geográfico de estar longe dos grandes conflitos bélicos e religiosos, o Brasil não se encontra fora desse xadrez geopolítico, principalmente em função de suas riquezas naturais. Assim, não deve se esquivar do debate e definição sobre a sua capacidade futura de defesa, procurando compatibilizar o que é desejável com o que é possível.

Um dos grandes desafios é garantir que a decisão política para investimentos encontre amparo nas peças orçamentárias, sob o risco de deixar obras e projetos inacabados. No Brasil, o princípio constitucional da anualidade orçamentária é responsável, de maneira significativa, pela imprevisibilidade de recursos para investimentos já iniciados.

Esse princípio, previsto no art. 165 da Constituição Federal e no caput do art. 2º da Lei nº 4.320/64, resulta em um horizonte de curtíssimo prazo para as previsões e autorizações orçamentárias, coincidindo com o ano civil, 1º de janeiro a 31 de dezembro. Essa anualidade tem causado efeitos danosos sobre os projetos de defesa, que, por natureza, são de caráter plurianual e possuem um horizonte de vários anos para a realização das suas entregas.

Dados os fatores negativos das flutuações orçamentárias, são necessários debates entre as áreas técnica e política para mitigar os riscos de alongamento de prazos dos projetos, que é resultado,
em grande medida, de cenários fiscais desfavoráveis durante os anos de vigência dos contratos.

Dessa forma, o presente texto tem por objetivo apresentar as consequências desse princípio sobre os projetos estruturantes de defesa, que são de longo prazo e de montantes significativos. Além disso, traz algumas alternativas para discussão, que demandariam um novo marco regulatório para o setor no Brasil.

Projetos Estruturantes de Defesa Nacional

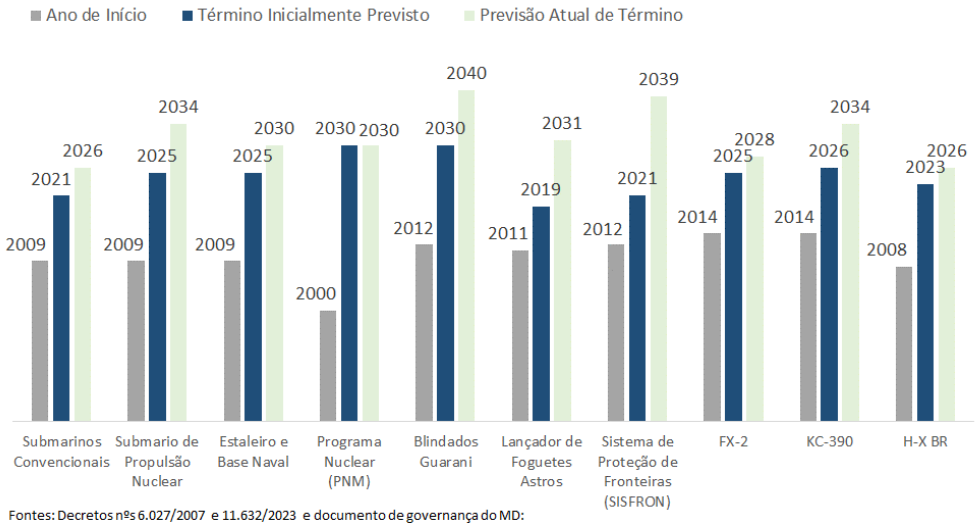
Inicialmente, cabe pontuar que o Brasil vem, desde os anos 2000, conforme previsto na Política Nacional de Defesa e suas revisões,[2] optando por promover a autonomia tecnológica e produtiva na área de defesa, o que resulta em projetos de longo prazo para sua maturação. Esse modelo tem por objetivo, além da independência em relação a outras nações, o desenvolvimento da Base Industrial de Defesa Nacional em substituição à compra de produtos prontos para entrega ofertados por outros países e/ou empresas.

O marco na definição do rol dos projetos estratégicos de defesa foi o Decreto nº 6.025/2007, onde foram concebidos doze investimentos no Programa de Aceleração do

[2] Item III dos Objetivos Nacionais da Política Nacional de Defesa apresentada ao Congresso Nacional em 2020.

Crescimento (PAC). Desse total, dois foram concluídos (satélite geoestacionário e desenvolvimento do KC-X 390) após mais de quinze anos. Porém, o que mais chama a atenção é que a quase totalidade teve seus prazos de conclusão alongados, decorrentes principalmente da insuficiência de recursos (vide gráfico 1 a seguir).

Gráfico 1: Previsão de Ano de Conclusão dos Projetos de Defesa



Fontes: Decretos nºs 6.027/2007 e 11.632/2023 e documento de governança do MD: https://www.gov.br/defesa/pt-br/orgaos-vinculados/conselho-superior-de-governanca-do-ministerio-da-defesa/arquivos/2022/pped_final_aprovado_versao_para_impressao.pdf
Elaboração Própria.

Observa-se que as decisões para os projetos de defesa possuem uma falha de inconsistência intertemporal, conforme apresentado por Marcel, Guzman e Sanguinés,[3] que consiste em "transferir os custos a gerações futuras, problema esse que aumenta pelo fato de o mandato das autoridades eleitas ser limitado no tempo". Isso é agravado no Brasil pelas dificuldades orçamentárias que impedem a conclusão de projetos no prazo inicialmente previsto.

Esse alongamento se dá pelos erros iniciais em projeções fiscais, cuja inclinação é ser otimista em relação ao cenário econômico. Vejamos a tendência histórica do próprio Plano Plurianual – PPA, que define as diretrizes, objetivos e metas de governo para quatro anos, e que rapidamente fica em desuso e cai no esquecimento, pois não possui o caráter vinculante em relação a uma disciplina e compromissos fiscais de médio prazo e não é de execução obrigatória. O último PPA 2020-2023, por exemplo, na avaliação que diz respeito ao setor de defesa, traz no relatório de monitoramento do ano base 2021 a constatação de que "as principais restrições reportadas, além daquelas decorrentes da pandemia, **foram dificuldades de ordem orçamentária-financeira** e, em alguns casos,

[3] Mario Marcel, Marcel Guzmán e Mario Sanginés, *"Presupuesto para el desarrollo en América Latina"*, Washington-DC, BID, 2013.

dificuldades de ordem técnica que afetaram as entregas contratuais (materiais e serviços) acarretando a necessidade de postergações e repactuações de contratos".[4] **(grifo nosso)**

Ressalva-se que em um cenário internacional de conflitos, as estimativas econômicas se tornaram cada vez mais complexas. Para Kay e King "ao negligenciarem a incerteza radical, os decisores políticos incorrem num duplo fracasso intelectual: i) eles entendem mal a racionalidade humana, e ii) ilusoriamente tendem a acreditar que boas políticas públicas devem basear-se exclusivamente em previsões."[5] Assim, as bases fiscais iniciais de sustentação dos projetos tornam-se meros exercícios de adivinhação, em uma economia mundial em constante crise. A única garantia legal de orçamento abrange uma pequena fração incluída na Lei Orçamentária Anual (LOA), o que eleva a necessidade de proteção dos fornecedores quanto a descumprimentos de marcos contratuais, que vem na forma de elevação nos preços dos produtos ofertados às Forças Armadas (FFAA).

Destaca-se que uma vez que os projetos são iniciados, a decisão sobre sua continuidade torna-se praticamente irreversível, pois dificilmente uma autoridade vai assumir os custos afundados, com milhões já aplicados, bem como não vai avocar para si o desgaste político por sua paralisação. Essa situação leva à inércia na rediscussão da real necessidade dos investimentos mais antigos.

De acordo com Franko, "para os formuladores de políticas de defesa, talvez profanas sejam as escolhas difíceis e conflitantes entre modernização e autonomia da defesa com uma fonte de recursos relativamente fixa."[6] Ou seja, com orçamento relativamente fixo para defesa no Brasil, novas necessidades orçamentárias ficam reprimidas pela pressão de alocação de recursos para projetos que já se iniciaram há décadas e cuja validade não é mais debatida.

Temos observado que as previsões iniciais de desembolso por parte do Governo se deparam, inevitavelmente, ano após anos, com a realidade orçamentária restritiva, que impede honrar o cronograma pactuado. Além do mais, há uma concorrência natural com

[4] República Federativa do Brasil, "Relatório Anual de Monitoramento do Plano Plurianual, ano base 2021", página 51, 2022. https://www.gov.br/planejamento/pt-br/assuntos/plano-plurianual/arquivos/monitoramento/relatorio-anual-de-monitoramento.pdf

[5] John Kay and Mervyn King, *"Radical Uncertainty, Decision-Making Beyond the Number"*, New York: W.W. Norton, 2020.

[6] Patrice Franko, *"O Trilema das aquisições de defesa: o caso do Brasil"*, Strategic Forum, National Defense University, 2014.

outros setores de governo pelo mesmo fundo orçamentário, que vem sendo acentuada nos últimos anos com o incremento da participação de emendas parlamentares impositivas ao orçamento federal.[7]

A concorrência por recursos se dá até mesmo entre programações do próprio Ministério da Defesa, uma vez que, excetuados os gastos com inativos e pensionistas, as despesas com pessoal ativo consomem cerca de 57% dos recursos orçamentários destinado ao setor no Brasil, enquanto os investimentos representaram 13% do total em 2023.[8] A título de comparação, tem-se que os três países pertencentes simultaneamente à Organização do Tratado do Atlântico Norte (OTAN) e ao Conselho de Segurança da ONU, quais sejam, Estados Unidos, Reino Unido e França, destinam respectivamente do total de seus orçamentos de defesa 38,8%, 31% e 41,7% para pessoal, e 28,8%, 30,1% e 31,6% para investimentos.[9] Isso demonstra a necessidade de se buscar maior equilíbrio entre despesas de pessoal e investimentos no orçamento brasileiro de defesa.

Almeida aponta que há um forte componente inercial nos orçamentos de defesa no Brasil, onde o futuro tende a repetir o passado.[10] Acrescentaria que há ondas orçamentárias, que dependem da situação fiscal e da força política do setor junto aos poderes executivo e legislativo. Essa situação é ilustrada nos empenhos anuais para investimentos em defesa ao longo da última década (gráfico 2, a seguir), em que se observam picos esporádicos e momentâneos de aplicação de recursos.

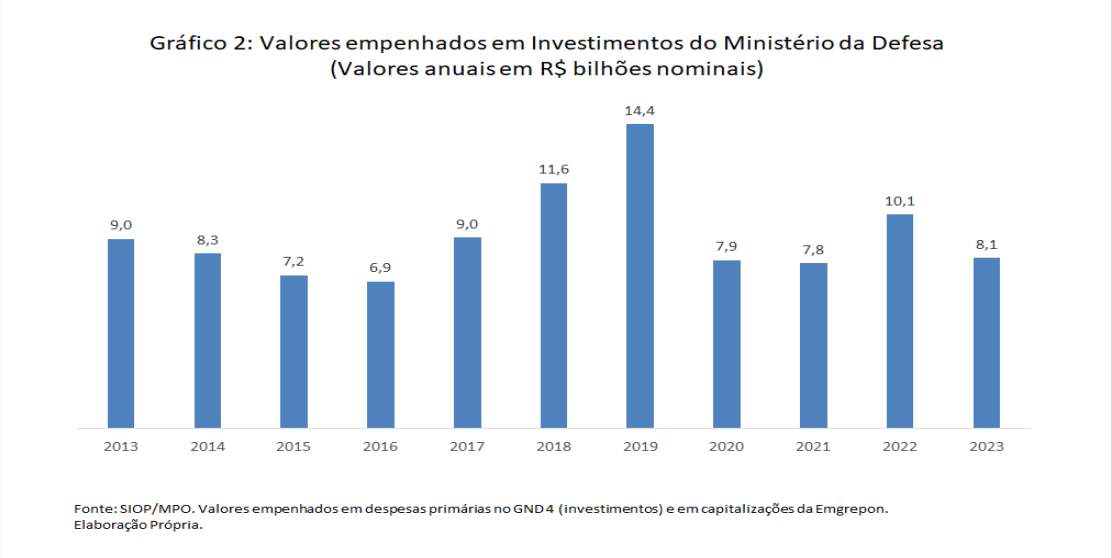
[7] Notas do autor: em 2014, primeiro ano da vigência das emendas individuais impositivas, o percentual de emendas correspondia a aproximadamente 5% das despesas discricionárias da União, excetuado o pagamento de dívida e de despesas obrigatórias. Esse percentual se elevou para 18% nas dotações da LOA de 2023.

[8] SIOP/MPO, valores empenhados.

[9] Relatório Anual da OTAN 2022, págs. 164 e 165. https://www.nato.int/cps/en/natohq/opinions_212795.htm.

https://www.nato.int/cps/en/natohq/opinions_212795.htm

10 Carlos Wellington Leite de Almeida, “Gastos de Defesa no Brasil 1999-2021”, Revista da Escola Superior de Guerra, v38 n. 82 (2023), página 72. https://revista.esg.br/index.php/revistadaesg/article/view/1291/1070.



Atrelada à questão fiscal, outro elemento essencial para otimizar os escassos recursos orçamentários é o de implementação de uma metodologia institucionalizada que contenha premissas e exigências para a apresentação de projetos, levando em consideração, entre outros, o ciclo de vida, as capacidades já instaladas, os custos envolvidos e o tempo em que o produto será disponibilizado.[11] Dessa maneira, poderiam ser reduzidas as chances de escolhas de projetos cujo custo-benefício acaba por se revelar, anos depois, prejudiciais à nação, tantos em termos qualitativos como em termos monetários.

Em 2018, foi instituído o Conselho Superior de Governança que tem, entre outras, a atribuição de "promover o alinhamento estratégico e a interação dos programas e projetos das Forças Singulares que integrarão o portfólio estratégico de defesa, de modo a priorizá-los".[12] Mas, no âmbito de suas resoluções, não se constatou o estabelecimento de requisitos mínimos e critérios objetivos para orientar a análise, priorização e deliberação do Conselho.

Relevante frisar que o mundo vive em constante ebulição e em movimentos que mudam rapidamente os atores e os interesses geopolíticos. Segundo Haider, "o mundo está muito mais difuso em um momento no qual a governança global implementada após

[11] Ruy Barcellos Capetti, "Base Industrial de Defesa – um estudo de caso", Universidade Federal Fluminense, 28 de junho de 2014, página 9. https://defesa.uff.br/wp-content/uploads/sites/342/2020/11/BID1.pdf.

[12] República Federativa do Brasil, Decreto nº 9.628, de 26 de dezembro de 2018, "Dispõe sobre o Conselho Superior de Governança no âmbito do Ministério da Defesa".

a 2ª Guerra Mundial simplesmente não está funcionando."[13] Levando em consideração que grande parte dos acordos de transferência de tecnologia de defesa são celebrados com outros países, os atrasos podem prejudicar ou mesmo inviabilizar a continuidade dos projetos, dados novos eventos que possam conduzir a uma revisão de posicionamento dos até então parceiros/aliados.

Importante reforçar também o aspecto de que defesa é uma política de estado, pois, conforme ensinamentos de Bernazza,[14] "não pertencem a um governo ou partido, são perenes no tempo e estão estabelecidos em normas (Política Nacional de Defesa - PND, Estratégia Nacional de Defesa - END e Livro Branco de Defesa - LBD)".[15] Logo, projetos do setor deveriam ser fruto de um consenso político, com as devidas garantias financeiras para seu adequado andamento após tomada a decisão política de sua implementação.

No entanto, são evidentes as carências de debate e de conhecimento em torno do tema no Brasil. Jungmann aponta uma ausência da discussão sobre defesa entre os atores políticos. Em entrevista à Globo News, em 11 de dezembro de 2022, afirma que "o poder político não discute e não exerce seu papel de dar rumo à defesa nacional, passando os militares a assumir uma função tutelar em relação aos destinos da defesa do país." [16] Reflexo dessa realidade é o fato de que a última PND, encaminhada em 2020, não foi apreciada pelo parlamento até o momento.

Tem-se, ainda, que, por ser um bem público puro,[17] [18] defesa nacional não deve ser objeto de terceirização para o setor privado, não obstante o surgimento de organizações paramilitares mercenárias em alguns países, como o caso do grupo Wagner

[13] Notas do autor: Ziad Haider é diretor global de risco geopolítico da McKinsey. McKinsey, "Risco geopolítico: como se orientar em um mundo em transformação", entrevista em 9 de março de 2023. https://www.mckinsey.com/featured-insights/destaques/risco-geopolitico-como-se-orientar-em-um-mundo-em-transformacao/pt.

[14] Cláudia Bernazza, *"Projetos nacionais ou políticas de Estado? Contribuições para a linguagem da política"*, Reseñas y Debates en español, maio 2011.

[15] República Federativa do Brasil, Lei Complementar nº 97, de 9 de junho de 1999, "Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas".

[16] Fonte: Globo News, *"WW edição especial – a estratégia da política de defesa do novo governo Lula – 11, de dezembro de 2022"*. https://m.youtube.com/watch?v=FI78K7V1upQ

[17] Notas do autor: de acordo com Samuelson, as principais características de bens públicos puros são a não rivalidade (o uso por um não impede o uso por outro) e a não excludência (todos são beneficiados pelo serviço, independente de pagamento de taxas).

[18] Paul Anthony Samuelson, "The Pure Theory of Public Expenditure", The Review of Economics and Statistics, vol. 36, págs. 387-189, 1954.

na Rússia. Logo, o Estado deve ser o único provedor do serviço, o que torna fundamental a existência de uma fonte orçamentária estável e previsível para o seu financiamento.

O desinteresse político em defesa pode ser um dos fatores responsáveis pela imprevisibilidade orçamentária plurianual, resultando uma série de disfuncionalidades e má aplicação de recursos públicos. Dentre os principais problemas associados à imprevisibilidade podemos citar: i) falta de prontidão dos serviços necessários para a defesa nacional, ii) atrasos recorrentes nas entregas, iii) aumento de custos aos cofres públicos, inclusive com multas contratuais, iv) perda da utilidade dos equipamentos, dado o surgimento de novas tecnologias, e v) fuga de mão-de-obra qualificada do país.

Para superação da armadilha da anualidade orçamentária, apresentam-se algumas modelagens alternativas. Ressalva-se que são ideias iniciais do autor que carecem de maior análise, discussão, consensos e detalhamentos, tendo em vista que exigirão uma quebra de paradigma e de revisão de dispositivos constitucionais e/ou legais.

Alternativas:

O caso dos Navios Fragatas Classe Tamandaré

Entre os anos de 2017 e 2019, o governo passou a capitalizar a Empresa Gerencial de Projetos Navais - Emgepron para a construção de quatros navios de guerra, que foi seguida por outras capitalizações até atingir o custo total do projeto.[19] Assim, ao assinar o contrato de construção em 2020, a Marinha do Brasil (MB) já contava com recursos financeiros garantidos para todas as etapas de seu desenvolvimento, cujo prazo será de pelo menos 10 anos.

Nesse desenho, após prontos para uso, os navios serão disponibilizados à MB por meio de contrato específico, cabendo àquele Comando Militar ressarcir à Emgepron os valores referentes à sua depreciação. Ou seja, foi criado um modelo de negócios para a Empresa, que contará com uma fonte permanente de recursos para outros empreendimentos.

[19] Notas do autor: As capitalizações foram possíveis com créditos orçamentários por meio das seguintes Leis: a) Lei 13.534/2017, R$ 500 milhões; b) Lei 13.587/2018, R$ 2.500 milhões; c) Lei 13.808/2019, R$ 2.500 milhões; e d) Lei 13.951/2019, R$ 4.000 milhões.

Desse modo, tornou-se o primeiro modelo normatizado, com todas as capitalizações aprovadas pelo legislativo, de um orçamento plurianual para um projeto de defesa. Ou seja, foram mitigados os riscos financeiros à sua conclusão.

Destaca-se que a Emgepron é uma empresa estatal não-dependente,[20] cuja despesa não fica limitada anualmente pelo comportamento da arrecadação federal e nem pelas limitações da Lei Complementar – LC 101/2000 – Lei de Responsabilidade Fiscal (LRF). Logo, possui uma maior previsibilidade e garantia de cumprimento dos planejamentos orçamentários realizados.

Por óbvio, dificilmente haverá, no ato de contratação, recursos orçamentários disponíveis para cobrir o custo total de futuros projetos. Todavia, ao transferir recursos para uma empresa pública não-dependente com competência legal para realização de investimentos em defesa, parte significativa do cronograma de desembolso poderia ficar garantido a partir da definição política de realização da despesa.

Ressalva-se que, os recursos de capitalizações a empresas foram incorporadas, a partir de 2024, aos limites fiscais previstos na LC nº 200/2023 (novo arcabouço fiscal). Além disso, devem ser observados os termos do Acórdão nº 681/2023 – TCU – Plenário, de 5 de abril de 2023 em futuras capitalizações.[21]

Fundos Extra-Orçamentários

Dadas as características peculiares dos projetos em defesa (monopólio estatal, alta complexidade, montante elevado e longo prazo), seria razoável a adoção de um regime diferenciado para a execução orçamentária e financeira. Uma das possibilidades seria a de criação de um fundo extra-orçamentário administrado por um banco público.

Nessa modelagem, por meio de lei, deveriam ser instituídos os requisitos para que as Forças Armadas – FFAA se habilitassem aos recursos, as regras de governança, os atores responsáveis pela apresentação e aprovação dos projetos, os detentores do

[20] Notas do autor: considera-se empresa estatal não-dependente: empresa controlada que não receba do Tesouro Nacional recursos para pagamento de despesas com pessoal ou de custeio em geral ou de capital, excluídas as capitalizações (LC Nº 101/2000, art. 2º).

[21] República Federativa do Brasil, Tribunal de Contas da União: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/ACORDAO-COMPLETO-2559261.KEY/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/%2520.

patrimônio e a prestação de contas. O ponto chave seria a definição de fontes permanentes de financiamento dos projetos.

Como se tratam de ativos de guerra, de monopólio das FFAA, a posição da instituição financeira seria de mera intermediária, que incorreria em despesas para gerenciar os recursos e seria ressarcida pelo referido serviço.

Para ser mais efetiva e menos burocrática, a engenharia orçamentária poderia ser por meio de transferência direta dos recursos vinculados para a instituição financeira administradora do fundo, sem precisar transitar pelo orçamento federal. Assim, somente a definição dos projetos seria, de fato, submetida à aprovação do Congresso Nacional. Seria semelhante ao que ocorre com o bônus de assinatura para Empresa Brasileira de Administração de Petróleo e Gás Natural S.A. - Pré-Sal Petróleo S.A. (PPSA), nos termos do art. 7º da Lei nº 12.304/2010.

Uma das possíveis fontes vinculadas poderia ser a de parcela dos recursos de futuras concessões para exploração da área da plataforma continental, que foi ampliada para 350 milhas náuticas a partir da linha da costa na região Sul com a autorização da Organização das Nações Unidas (ONU) em 2019. Seria plenamente justificável, tendo em vista que a "Estratégia Nacional de Segurança de Infraestruturas Críticas" estabelece, em seu item 2.4, que "as vulnerabilidades encontradas nas imensas extensões territoriais da nossa fronteira implicam na necessidade de reforço dos dispositivos atuais de defesa e segurança."[22]

Autorização para empenhos plurianuais para contratos de defesa

Conforme previsto na Lei nº 4.320 e nas Leis Orçamentárias Anuais, as despesas devem ser fixadas apenas para o mesmo exercício financeiro de sua execução (anualidade). Porém, se observa que, provavelmente, essa determinação não venha sendo seguida em sua plenitude, dado o elevado montante de restos a pagar (valores empenhados, mas não pagos).[23] Logo, por que não considerar a possibilidade de

[22] República Federativa do Brasil, DECRETO Nº 10.569, de 9 de dezembro de 2020**,** "Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas".

[23] Notas do autor: para 2023, o montante de restos a pagar atingiu R$ 255,2 bilhões, conforme "Relatório de Avaliação dos Restos a Pagar" da Secretaria do Tesouro Nacional. Isso corresponde a mais de 2,5 vezes o valor de gastos discricionários anuais de custeio e investimentos do governo federal, que exclui despesas de pessoal, outras despesas obrigatórias e pagamento de dívida pública. "https://www.tesourotransparente.gov.br/publicacoes/relatorio-de-avaliacao-dos-restos-a-pagar/2023/114"

comprometimento (empenho) plurianual para despesas já contratadas, especialmente para aqueles gastos que são projetos de estado como os de Defesa?

Mencione-se que o que deve ser evitado são os restos a fazer decorrentes de mero aproveitamento de recursos ao final do exercício sem qualquer planejamento prévio, que se constituem em verdadeiro descaso com a coisa pública. Porém, essas não são as características dos projetos estratégicos de defesa.

A possibilidade de empenho no final de exercício de sobras de recursos para projetos estruturantes já contratados na área de defesa atenuaria a necessidade de novos debates orçamentários em anos subsequentes, bem como significaria a melhoria da qualidade dos restos a pagar.

Todavia, para ser ainda mais efetivo, o Tesouro Nacional poderia admitir a possibilidade de criação de uma Conta Vinculada de Defesa, para a qual também seriam feitas as transferências de numerário correspondente aos valores empenhados, com a contabilização do impacto fiscal no Caixa Único da União no mesmo exercício do empenho realizado. Assim, esses recursos já não mais concorreriam com os limites de pagamentos e não teriam impacto fiscal em anos posteriores, e seriam destinados aos fornecedores mediante requisições dos responsáveis pelos contratos nas FFAA após a comprovação da prestação dos serviços.

Vinculação de percentual do PIB ao Gasto com Defesa

A Estratégia Nacional de Defesa - END encaminhada ao Congresso em 2020 apresenta como sua décima quarta ação estratégica “buscar a destinação de recursos orçamentários e financeiros capazes de atender as necessidades de articulação e equipamento para as Forças Armadas, por meio da Lei Orçamentária Anual, no patamar de 2% do Produto Interno Bruto - PIB.” Esse percentual, que se situou em torno de 1,5% do PIB entre 2010 e 2020, ficou em 1,13% do PIB no exercício de 2023.[24]

Apesar de essa vinculação significar um incremento orçamentário e proporcionar uma maior previsibilidade de gastos para o Ministério da Defesa no médio prazo, é preciso fazer algumas ressalvas, pois a mera vinculação de um percentual do PIB à defesa

[24] Fonte: SIOP/MPO, valores empenhados.

apresenta fatores que podem torná-la ineficiente. Entre essas ressalvas, estão a questão da composição de gastos em defesa e a relação PIB e arrecadação federal.

Em relação a composição de gastos de defesa como proporção do PIB, o percentual previsto na END inclui despesas de pessoal (ativos, inativos e pensionistas), que representam montante significativo do total das despesas (tabela 1). Ou seja, o aumento de recursos com a vinculação ao PIB, conforme pensado, não está obrigatoriamente associado à sua destinação para projetos estratégicos, tornando-se necessária a discussão e inclusão na END de percentuais desejáveis para cada item de gasto, em especial para investimentos, a fim de que não se torne ineficaz.

Tabela 1 – Despesas empenhadas em 2023 do Ministério da Defesa

Tipo de Despesa	R$ bilhões	% do PIB	Participação % no total
Subtotal, sem Inativos e Pensionistas	**60,3**	**0,56%**	**100%**
- Pessoal ativo	34,5	0,32%	57%
- Investimentos	8,1	0,08%	13%
- Outras Despesas Primárias (custeio, despesas obrigatórias e emendas)	15,8	0,15%	26%
- Despesas de Financiamentos	1,9	0,02%	3%
Inativos e Pensionistas	**60,9**	**0,57%**	
TOTAL	**121,2**	**1,13%**	

Fontes: SIOP/MPO e PIB estimado para 2023 pelo FMI (World Economic Outlook de Nov-2023).

Assim, uma alternativa poderia ser uma vinculação específica a investimentos, nos moldes da deliberação plenária OTAN de 2014, que estabeleceu um patamar de, no mínimo, 20% para aquisição de equipamentos, incluídas pesquisa e desenvolvimento, no total dos orçamentos de defesa. [25]

Por fim, apesar de influenciar na arrecadação de receitas orçamentárias, o crescimento do PIB isoladamente não garante que haja recursos para o financiamento do

[25] Fonte: OTAN, Wales Summit Declaration, item 14, 2014. "https://www.nato.int/cps/en/natohq/official_texts_112964.htm"

setor. Pois, há outros fatores que afetam o comportamento de receitas públicas, tais como isenções fiscais, taxas de câmbio e índices inflacionários.

Considerações Finais

Pelo exposto, fica notório que o horizonte temporal anual para as autorizações orçamentárias é incompatível com a garantia mínima de cumprimento dos marcos contratuais assumidos para projetos estratégicos de defesa. Logo, alternativas precisam ser debatidas publicamente para defesa nacional, por se tratar de uma política de estado e de um bem público puro, não podendo ser negligenciada.

Deve ser buscado um consenso entre os atores e poderes, a fim de evitar judicializações e contestações sobre eventuais soluções propostas. Para isso, é fundamental a participação do Congresso Nacional, a quem compete privativamente, de acordo com a LC nº 97/1999, apreciar a Política Nacional de Defesa (PND), a Estratégia Nacional de Defesa (END) e o Livro Branco de Defesa (LBD).

Essas definições, por sua vez, devem encontrar lastro em uma disciplina fiscal de médio prazo, visando minimizar os efeitos cíclicos da política e da economia sobre os contratos plurianuais de defesa. Além disso, a priorização de recursos deve ser para projetos em autonomia tecnológica, como definido na PND em vigor, a fim de se buscar um maior equilíbrio entre despesas de pessoal e investimentos.

O estabelecimento de uma metodologia, no nível estratégico, quanto aos critérios de aceitabilidade e de seleção dos projetos de defesa é outro aspecto importante para a otimização de recursos. Para isso, sugere-se que seja debatida e concebida no âmbito do já existente Conselho Superior de Governança do Ministério da Defesa.

De fato, não há soluções fáceis ou mágicas. Mas, a ausência de plurianualidade orçamentária para projetos de defesa mostra-se danosa ao erário e deve ser urgentemente repensada, mesmo que resulte em emendas à Constituição Federal de 1988. Não restam dúvidas que, assim como “defesa não deve ser improvisada”, devemos ter presente que “projetos plurianuais de defesa também não devem ser anualizados”. Afinal de contas, os princípios orçamentários devem se adequar às realidades da sociedade, e não o contrário.

Bibliografia:

Almeida, Carlos Wellington Leite. “Gastos de Defesa no Brasil 1999-2021”, Revista da Escola Superior de Guerra, v38 n. 82 (2023), página 72. https://revista.esg.br/index.php/revistadaesg/article/view/1291/1070

Bernazza, Cláudia. “Projetos nacionais ou políticas de Estado? Contribuições para a linguagem da política”, Reseñas y Debates en español, maio 2011.

Brasil, “Relatório Anual de Monitoramento do Plano Plurianual, ano base 2021”, página 51, 2022. https://www.gov.br/planejamento/pt-br/assuntos/plano plurianual/arquivos/monitoramento/relatorio-anual-de-monitoramento.pdf

Brasil, Constituição Federal da República Federativa do Brasil, 1988.

Brasil, Decreto nº 9.628, de 26 de dezembro de 2018, “Dispõe sobre o Conselho Superior de Governança no âmbito do Ministério da Defesa”.

Brasil, Decreto. Nº 10.569, de 9 de dezembro de 2020, “Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas”.

Brasil, Lei Complementar nº 101, de 4 de maio de 2000 – Lei de Responsabilidade Fiscal.

Brasil, Lei Complementar nº 97, de 9 de junho de 1999, “Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas”.

Brasil, Lei nº 14.535, de 17 de janeiro de 2023 – Lei Orçamentária Anual.

Brasil, Lei nº 4.320, de 17 de março de 1964.

Brasil, Tribunal de Contas da União: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/ACORDAO-COMPLETO-2559261.KEY/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/%2520.

Capetti, Ruy Barcellos. “Base Industrial de Defesa – um estudo de caso”, Universidade Federal Fluminense, 28 de junho de 2014, página 9. https://defesa.uff.br/wp-content/uploads/sites/342/2020/11/BID1.pdf.

Franko, Patrice. “O Trilema das aquisições de defesa: o caso do Brasil”, Strategic Forum, National Defense University, 2014.

Kay, John; King, Mervyn. “Radical Uncertainty, Decision-Making Beyond the Number”, New York: W.W. Norton, 2020.

Marcel, Mario; Guzmán, Marcel; Sanginés, e Mario. “Presupuesto para el desarrollo en América Latina”, Washington-DC, BID, 2013.

OTAN, Declaração de País de Gales 2014. https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

Samuelson, Paul Anthony. “The Pure Theory of Public Expenditure”, The Review of Economics and Statistics, vol. 36, págs. 387-189, 1954.

Silva Filho, Edison Benedito; Moraes, Rodrigo Fracalossi. “Dos "dividendos da paz" à guerra contra o terror: gastos militares mundiais nas duas décadas após o fim da guerra fria – 1991-2009”, IPEA, Rio de Janeiro, Julho de 2012. https://repositorio.ipea.gov.br/handle/11058/1156

Para más información, por favor, visite nuestra web www.colegio-id.org o póngase en contacto con nosotros a través del correo electrónico: hemisferio@iadc.edu
Publicada en Washington, D.C. (EE.UU.). ISSN 2412-0707 (versión impresa); ISSN 2412-0715 (versión digital).

For further information, please visit our website www.colegio-id.org or contact us at email hemisferio@iadc.edu Published in Washington D.C., USA. ISSN 2412-0707 (Print). ISSN 2412-0715 (Online).