GUERRA CIBERNÉTICA RUSSO-UCRANIANA

Lições para o Brasil e o mundo

Paulo Sergio Pagliusi*

Apesar dos inegáveis benefícios da evolução da Tecnologia da Informação, esta torna as pessoas, organizações e nações vulneráveis a um novo tipo de ameaça: a cibernética; que explora o ciberespaço, desconhece fronteiras e pode causar grande prejuízo, paralisar estruturas vitais das nações e até, indiretamente, ceifar vidas. Em termos militares, o ambiente cibernético surge como o 5º domínio da guerra – após o terrestre, marítimo, aéreo e geoespacial, explorado para combate por meio de um novo tipo de guerra: a guerra cibernética.

Este artigo analisa a guerra cibernética russo-ucraniana, componente dissimulado do confronto entre Rússia e Ucrânia, que veio à tona após a recente invasão da Ucrânia por tropas russas. Também descreve a exploração de melhores táticas de combate a cada domínio conquistado, conceitua ciberespaço e analisa as lições da guerra cibernética russo-ucraniana, no que já é tido como o maior conflito europeu desde a 2ª Guerra Mundial.

TÁTICAS DE COMBATE DISTINTAS A CADA NOVO DOMÍNIO

Desde a pré-história, os primeiros conflitos humanos se deram no domínio ***terrestre***, sendo a guerra naval criada quando o homem resolveu lutar entre si a partir de embarcações aquáticas. A organização, tática e os meios empregados na guerra naval, distintos do combate em solo, se aperfeiçoaram com o tempo, acompanhando a evolução militar e náutica, sendo durante a 1ª Guerra Mundial que o poder marítimo atingiu sua máxima importância. Acredita-se que o poderio britânico no domínio ***marítimo*** tenha decidido esta 1ª grande guerra.

Já com a invenção da aeronave, no início do século 20, surge o desafio de se criar Forças Aéreas para melhor explorar o novo domínio aéreo, em uma época em que militares eram especialistas em táticas dos domínios terrestre e marítimo. Em várias localidades, Exércitos e Marinhas competiam e desejavam trazer para si o combate no ambiente recém-conquistado, por meio de seus ramos aéreos. O problema era que os Exércitos e as Marinhas de então aspiravam fazer prevalecer as táticas de seus domínios nativos no novo domínio. Contudo, a organização, meios, tempos de reação e táticas exploradas no ar são distintos dos outros domínios.

Por exemplo, na 1ª Guerra Mundial, os Exércitos – direcionados ao uso de táticas terrestres – transformaram a aeronave numa mera extensão da tática de emprego das metralhadoras em solo, ou seja, uma "metralhadora voadora", subutilizando o potencial aéreo. As táticas de combate no ar foram mais bem exploradas na 2ª Guerra Mundial, via Forças Aéreas independentes, com organização, meios e táticas para o domínio ***aéreo.***

No Brasil, o Ministério da Aeronáutica, fundado em 1941, teve seu ramo militar denominado "Forças Aéreas Nacionais", alterado depois para "Força Aérea Brasileira" (FAB). Os ramos aéreos do Exército (Aviação Militar) e da Marinha (Aviação Naval) foram extintos e todo o pessoal, aeronaves, instalações e equipamentos relacionados, transferidos para a recém-criada FAB. Esta teve batismo de fogo na 2ª Guerra Mundial, lutando na guerra antissubmarino do Atlântico Sul e, na Europa, como parte da Força Expedicionária Brasileira.

Disputa similar houve na conquista do domínio ***geoespacial***. Nos EUA, as Forças Armadas tiveram embates antes de se decidir quem o herdaria. A disputa começou em 1955, com a Marinha à frente, via o *Naval Research Laboratory's Project Vanguard*, criado antes da NASA iniciar suas operações em 1958, unindo este laboratório, o *National Advisory Committee for Aeronautics*, da Força Aérea, o *Jet Propulsion Laboratory* (do *California Institute of Technology for the Army*) e o *Army Ballistic Missile Agency*, do Exército, entre outros, para atender necessidades duais – civis e militares. A corrida espacial foi um dos capítulos da Guerra Fria, em que os EUA e a União Soviética disputaram, entre 1957 e 1975, a hegemonia no domínio geoespacial. A corrida pela conquista do geoespaço foi um episódio marcante da 2ª metade do século 20, resultado direto da Guerra Fria.

Desafiadoras pela quebra de paradigma, ações de adaptação a novos domínios são benéficas à exploração de melhores táticas. Vide a criação de marinhas para combate naval; de forças aéreas para combate no ar; e de entidades de uso dual para disputas no geoespaço. Hoje, o mundo testemunha corrida similar na conquista do domínio ***cibernético***, onde a guerra cibernética, distinta da guerra cinética, requer uma revisão de táticas.

CIBERESPAÇO: O EMERGENTE QUINTO DOMÍNIO DA GUERRA

O terreno cibernético constitui promissor cenário para conflito bélico entre nações, caracterizado pela assimetria, dificuldade de atribuição de responsabilidades e paradoxo da maior vulnerabilidade do mais forte. Quanto mais desenvolvido tecnologicamente um país, maior a superfície digital exposta a ataques. Habituados a ver guerras como operações cinéticas, localizadas geograficamente, com objetivos e alvos identificáveis, é difícil dar importância real ao que ocorre no mundo sem fronteiras do espaço cibernético. Porém, cada vez mais, os combates são virtuais, o que não os faz menos letais, pois são preparação para ações no plano físico.

No domínio de ação da defesa cibernética relativo ao funcionamento de sistemas de Tecnologia de Informação e Comunicação (TIC), ou ***ciberespaço***, é difícil definir fronteiras físicas, mas pode-se observar efeitos nas dimensões física e virtual. A digitalização das atividades, a automação de sistemas de uso dual e a transversalidade do tema tornam o ciberespaço uma dimensão fundamental; dual por excelência, e de crescente importância para cada país. É notório que o ciberespaço já se transformou, há tempos, no quinto domínio da guerra, após o terrestre, marítimo, aéreo e geoespacial, e vem sendo cada vez mais explorado por meio de um novo tipo de guerra: a guerra cibernética.

As ações na guerra cibernética são divididas em três tipos: ***Ofensivas***, ***Defensivas*** e de ***Exploração***. As ações ofensivas buscam destruir, impedir ou dificultar o uso de informação pelo inimigo e de suas capacidades cibernéticas, tanto via ataques físicos como por ataques cibernéticos, pela rede, utilizando armas cibernéticas. As ações defensivas buscam evitar ou minimizar ataques cibernéticos lançados pelo inimigo, protegendo a informação, e restaurar rapidamente danos e limitações advindos desses ataques, impingidas às capacidades cibernéticas, garantindo o uso do ciberespaço. As ações de exploração buscam monitorar o inimigo na busca de informações sigilosas, detectar suas atividades cibernéticas e conhecer suas vulnerabilidades sistêmicas dentro da rede, buscando informações que tragam vantagem tanto no ambiente cibernético quanto cinético.

A fim de diferenciar o combate cibernético do conflito bélico tradicional, Parks e Duggan listam oito princípios da guerra cibernética: (i) Princípio do Efeito Cinético (a guerra cibernética deve produzir efeitos no mundo cinético); (ii) Princípio da Mutabilidade (não existem leis de comportamento imutáveis no ciberespaço, excetuando-se as que necessitam de ação no mundo real); (iii) Princípio do Disfarce (uma entidade no ciberespaço possui autoridade, acesso ou habilidade para pôr em prática qualquer ação que um atacante deseje realizar; o objetivo do atacante é assumir a identidade dessa entidade); (iv) Princípio da Dualidade do Armamento (as ferramentas – ou armamentos – da guerra cibernética são de natureza dual); (v) Princípio da Compartimentação (tanto o atacante como o defensor de um sistema controlam pequena parcela do ciberespaço que utilizam); (vi) Princípio da Usurpação (quem controlar a parte do ciberespaço que o oponente usa, pode controlar o oponente); (vii) Princípio da Incerteza (o ciberespaço não é consistente nem confiável); e (viii) Princípio da Proximidade (limitações físicas de distância e espaço não se aplicam ao ciberespaço).

O combate cibernético envolve desde ações dissimuladas de coleta de inteligência por meio digital, interrupção de serviços on-line via blo-

queio de sites de sistemas financeiros, logísticos, de geolocalização e de atendimento público, até disrupção de infraestruturas críticas do oponente, civis ou militares. Com a expansão de tecnologias digitais disruptivas, como a Internet das Coisas, computação em nuvem, robotização e inteligência artificial, tal ameaça aumenta, exponencialmente, a superfície potencial de ataque, migrando do ambiente da TIC para o da Tecnologia Operacional (TO). A TO abrange qualquer hardware e software que detecta ou provoca alteração, via monitoramento direto e/ou controle de equipamentos, em ativos, processos e eventos, para conectar, monitorar, gerenciar e proteger operações industriais, seja de uma entidade ou país.

Hoje, predominam países dotados de Forças Armadas com ramos cibernéticos. Por doutrina, tais Forças tendem a usar, no combate cibernético, táticas de seus domínios nativos, limitando a exploração do potencial cibernético. Por exemplo, os combatentes cibernéticos espalhados nas Forças americanas compõem diversos comandos, tais como: 688th IOW (Information Operations Wing), centro de excelência cibernética da Força Aérea; NETWARCOM (*Naval Network Warfare Command*) da Marinha; e A-GNOSC (*Army Global Network Operations and Security Center*), sob o comando e inteligência do Exército. É possível antever o próximo passo. Os EUA devem desligar tais ramos de suas Forças atuais, e agrupá-los sob uma única Força Cibernética Militar.

GUERRA CIBERNÉTICA RUSSO-UCRANIANA

A guerra fria cibernética russo-ucraniana é um componente do confronto dissimulado entre Rússia e Ucrânia, existente desde o colapso da União Soviética em 1991. Enquanto os primeiros ataques a sistemas de informação de empresas privadas e instituições estatais ucranianas foram registrados nos protestos em massa em 2013, a arma cibernética russa "Uroburos" existe desde 2005. Em 2013, surge a Operação "Armageddon", campanha russa de ciberespionagem sistemática nos sistemas de agências de governo, policiais e de defesa, a fim de apoiar a Rússia no campo de batalha. Entre 2013 e 2014, os sistemas de TI de agências governamentais ucranianas foram afetados pelo vírus computacional "Snake"/"Uroburos"/"Turla". Em 2014, quando russos entraram na Crimeia, centros de comunicação locais foram invadidos e cabos de fibra ótica adulterados, cortando conexão entre a península e a Ucrânia continental. Sites de notícias e mídias sociais do governo foram derrubados ou sofreram negação de serviço, celulares de parlamentares ucranianos invadidos ou bloqueados.

Empresas de cibersegurança começaram a registrar aumento nos ataques cibernéticos russos em sistemas de TI, tendo como vítimas agências governamentais, da União Europeia, dos EUA, agências de defesa, organizações internacionais e regionais de defesa e políticas, *think tanks*, organiza-

ções de mídia e de dissidentes ucranianos. Em 2015, pesquisadores identificaram dois grupos de hackers russos ativos na guerra cibernética contra a Ucrânia: o APT29 (conhecido como *Cozy Bear* ou *Cozy Duke*) e o APT28 (conhecido como *Sofacy Group*, *Team Czar*, *Pawn Storm* ou *Fancy Bear*). Neste cenário, é alarmante que a doutrina militar russa considere que um ataque cibernético que ameace setores estratégicos do país, em sentido existencial como no caso de usinas nucleares, pode ser respondido com uso de armas atômicas.

A trajetória dos ataques cibernéticos desferidos entre Rússia e Ucrânia demonstram que esta guerra cibernética se intensifica há uma década, sendo componente precursor da posterior guerra física de 2022. A relação na página a seguir mostra os ciberataques originados de ambos os lados. Nota-se, pelas conquistas das operações e pelos ataques em massa, o predomínio de vitórias da Rússia, em face ao melhor preparo tático de suas tropas.

LIÇÕES GLOBAIS DE SEGURANÇA E DEFESA CIBERNÉTICA DA GUERRA RUSSO-UCRANIANA

Avaliando os alvos da guerra cibernética russo-ucraniana, vê-se a necessidade de proteger projetos e serviços de interesse nacional, com ênfase nos de infraestrutura crítica, como instalações, serviços, bens e sistemas que, se interrompidos ou destruídos, provocam sério impacto social, econômico, político e internacional ou à segurança do país. A Política Nacional de Segurança de Infraestruturas Críticas nos orienta a proteger os serviços mais essenciais: energia, transporte, água, telecomunicações, finanças, biossegurança e bioproteção.

A exploração deste novo tipo de combate não se concentra no Leste Europeu ou Oriente Médio, mas pelo ciberespaço não ter fronteiras, pode ocorrer no mundo todo. Veja, por exemplo, os ataques cibernéticos no acirrado conflito entre as Coreias. E o caso clássico do ataque contra sites governamentais e privados da Estônia que, em 2007, praticamente tirou o pequeno país do ar. Houve acusações contra a Rússia, mas nada foi provado, sendo que tais ameaças fizeram da Estônia um país especialista em cibersegurança. Entre 2012 e 2017, três agentes de inteligência russos atacaram o setor de energia, invadindo centenas de empresas e organizações em todo o mundo; *hackers* russos também entraram na rede de computadores de uma empresa de energia nuclear no Kansas, segundo o Departamento de Justiça dos EUA. A inexistência de marcos legais que disciplinem a disputa pelo ciberespaço o transforma no "velho oeste" dos dias atuais, com potencial para suscitar conflitos de proporções e consequências mais danosas à humanidade do que a própria arma nuclear.

A exemplo da criação das Forças Aéreas para melhorar táticas de combate no ar a partir da 2ª Guerra Mundial, percebe-se que as táticas de combates cibernéticos poderão ser mais bem exploradas. É importante não correr o risco do uso de táticas inapropriadas no ciberespaço, advindas de outros domínios – por exemplo, com erro de previsão de tempos de resposta a um cibercombate, em que batalhas são vencidas em horas ao invés de dias ou semanas, como é usual nos combates terrestres, marítimos ou aéreos. Tendo como base a guerra cibernética russo-ucraniana, nota-se que os países ao redor do mundo precisam considerar a criação de nova Força Singular, especializada em táticas para o ciberespaço – a partir de pessoal, redes, ambientes, instalações e equipamentos transferidos dos atuais ramos cibernéticos de suas Forças. Assim como antes havia ramos aéreos e geoespaciais militares inicialmente separados, mas que depois se aglutinaram, tais ramos cibernéticos devem se consolidar em uma nova Força Armada Cibernética, conforme houve em cada conquista de domínio.

Tal movimento deve acontecer em todo o planeta, para que se possa desenvolver melhores táticas de combate no ciberespaço. Com tropas profissionais especializadas, inteligência, doutrina e operação focadas neste domínio, será evitada a criação, às pressas, de um "Exército de TIC" – como fez o Ministro Fedorov, após a invasão russa na Ucrânia, solicitando a um ciberespecialista para 'improvisar' ataques a sites russos.

LIÇÕES AO BRASIL DE SEGURANÇA E DEFESA CIBERNÉTICA DA GUERRA RUSSO-UCRANIANA

O Brasil não pode ficar à margem do processo de transformação digital do mundo, acelerado pela imposição do trabalho remoto face à pandemia. Diante de combates cada vez mais acirrados no ciberespaço, constitui objetivo estratégico nacional participar de discussões sobre controle deste domínio como protagonista.

Por sua relevância, o Brasil precisa se precaver, sendo a publicação da Estratégia Nacional

CIBERATAQUES RUSSOS CONTRA A UCRÂNIA

► **AO LONGO DE 2013:** Operação "Armageddon"
► **FEVEREIRO DE 2014:** Operação "Snake"
► **JUNHO DE 2014:** Ataques ao sistema automatizado de Eleições.
► **DEZEMBRO DE 2015:** Ataque à rede elétrica da Ucrânia. Ataques com Trojan BlackEnergy em empresas que fornecem energia às regiões de Kiev, Ivano-Frankivsk e Chernivtsi. 1º ataque cibernético bem-sucedido a uma rede elétrica de que se tem notícia.
► **DEZEMBRO DE 2016:** Segundo hacking na rede elétrica da Ucrânia.
► **DEZEMBRO DE 2016:** Paralisia do Tesouro do Estado da Ucrânia.
► **JUNHO DE 2017:** Ataques cibernéticos na Ucrânia, incluindo ataque de hackers em massa na cadeia de suprimentos pelo vírus Petya. Este foi o maior ataque de hackers conhecido até então.
► **JANEIRO DE 2022:** Ataque cibernético na Ucrânia, em sites do governo ucraniano, um dia após o fracasso das negociações entre EUA-Rússia sobre o futuro da Ucrânia na OTAN.
► **A PARTIR DE FEVEREIRO DE 2022:** Ataques em massa, após tropas russas invadirem regiões orientais da Ucrânia, derrubando sites governamentais e bancários ucranianos. A inteligência dos EUA os atribui a ciberatacantes russos, embora o governo russo tenha negado tal envolvimento.

CIBERATAQUES UCRANIANOS CONTRA A RÚSSIA

► **MAIO DE 2016:** Operação "Prikormka (Groundbait)".
► **MAIO DE 2016:** Operação "9 de maio de 2016" (nove hackings em sites do grupo separatista República Popular de Donetsk, em sites russos de propaganda anti-ucraniana e em empresas militares privadas russas).
► **JUNHO DE 2016:** Intervalo do "Channel One", em que houve hacking do servidor corporativo do canal russo "Channel One", pela Aliança Cibernética Ucraniana (dos hackers FalconsFlame, Trinity e Rukh8).
► **OUTUBRO DE 2016:** The Surkov Leaks, havendo um vazamento de 2.337 e-mails com centenas de anexos sigilosos, que revelam planos para se tomar a Crimeia da Ucrânia e fomentar distúrbios separatistas em Donbas (documentos datados entre setembro de 2013 e dezembro de 2014).
► **A PARTIR DE FEVEREIRO DE 2022:** "Exército de TIC" da Ucrânia, criado por Mykhailo Fedorov , Vice-Primeiro-Ministro e Ministro da Transformação Digital. Esforço iniciado durante invasão russa da Ucrânia em 2022, para travar guerra cibernética contra a Rússia. Fedorov solicitou assistência de especialista cibernético e twittou um Telegram, listando 31 sites-alvo de empresas e organizações estatais russas.

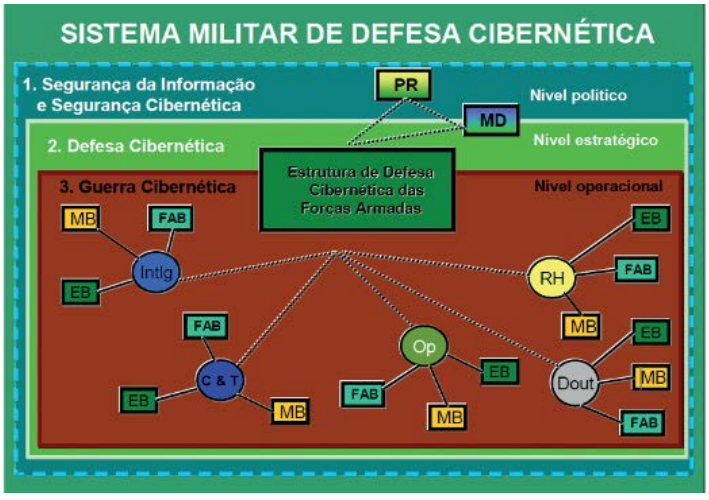
de Segurança Cibernética em fevereiro de 2020, uma importante conquista. Além disto, a Estratégia Nacional de Defesa (END) define, desde 2008, três setores de importância estratégica à defesa nacional: o nuclear, o espacial e o cibernético, cabendo à Marinha do Brasil a gerência do programa nuclear; à FAB, o programa geoespacial; e, ao Exército Brasileiro, a liderança da defesa cibernética em território nacional. Verifica-se que o Setor Cibernético, na visão da END, não se limita a atividades de Segurança e Defesa Cibernética, pois inclui, também, a TIC e os componentes básicos do Setor Cibernético à atuação em rede: (i) estrutura de comando, controle, comunicações, computação e inteligência (C4I), para atuação operacional e funcionamento administrativo das Forças Armadas; (ii) recursos de TIC; e (iii) arquitetura matricial, que viabiliza trânsito de informações em apoio ao processo decisório, em tempo quase real.

Diante das lições da guerra russo-ucraniana, a segurança e a defesa cibernéticas surgem como imperativos de proteção das infraestruturas críticas da informação. Assim, o Brasil deu grande passo ao criar, em 2020, o Sistema Militar de Defesa Cibernética (SMDC), que tem como órgão central o Comando de Defesa Cibernética (ComDCiber), comando operacional permanentemente ativado e integrado por oficiais e praças das três Forças Armadas, mostrado na figura ao lado.

O SMDC conduz ações de proteção, exploração e ataques cibernéticos em prol da defesa nacional, 24/7, com diversos benefícios à sociedade, em apoio à segurança cibernética em atividades interagências, incluindo a proteção de infraestruturas críticas do país.

Embora o Exército Brasileiro realize excepcional trabalho ao liderar a estruturação de segurança e defesa cibernéticas brasileiras, é evidente que as táticas que esta Força domina são baseadas no domínio terrestre, e não no ciberespaço. No passado, tal distorção ficou clara no uso do poder aéreo como "metralhadora voadora" por Exércitos da 1ª Guerra Mundial. Este tipo de erro – o de se usar táticas de um domínio no outro – não deve ser repetido. Chegou a hora de se criar a Força Cibernética Brasileira (FCB).

Mas não se constrói uma nova Força Armada da noite para o dia. Pode-se primeiro identificar e reunir, na futura FCB, militares que atuam nos ramos cibernéticos da Marinha, Exército e Aeronáutica, como os que servem sob o SMDC, além dos ambientes computacionais de redes,



Sistema Militar de Defesa Cibernética do Estado Brasileiro
Fonte: Defesa em Foco, 2020

nuvens, pesquisa, instalações e equipamentos voltados ao combate no ciberespaço. Algo similar ao que houve na criação da Força Aérea, quando os ramos aéreos das outras forças foram transferidos à FAB. Também será preciso contar com órgãos específicos para formação e especialização, logística, abastecimento, inteligência, pesquisa, operações e gestão de pessoal, e desenvolver doutrinas e táticas adequadas ao domínio cibernético.

CONCLUSÃO

A fim de se evitar o risco do emprego de táticas de um domínio em outro, é natural que surja nova categoria de Força para combate no ciberespaço. O aprendizado da guerra russo-ucraniana aponta nesta direção.

Tendo como foco os ataques cibernéticos da guerra russo-ucraniana, é vital se preparar para a crescente ameaça de uma guerra fria cibernética global. É preciso considerar que, com a queda da Ucrânia, o conflito russo-ucraniano pode até protagonizar a 3ª Guerra Mundial, com o ciberespaço tendo relevante papel.

Apesar da existência dos ramos cibernéticos nas forças singulares (no Brasil, pela END, predomina o ramo cibernético do Exército), é bem possível que surja uma nova Força Armada, composta por cibercombatentes especializados, advindos da junção dos ramos cibernéticos das Forças Singulares hoje existentes.

Afinal, a organização, os tempos, meios, princípios e táticas de combate explorados no quinto domínio da guerra são distintos dos demais. Basta observar o que ocorre na guerra russo-ucraniana, em que uma batalha cibernética dura poucas horas, enquanto batalhas terrestres, marítimas e aéreas duram dias ou semanas. Exércitos não se improvisam. Não há lugar para amadores no ciberespaço. Não se pode confiar batalhas no ciberespaço a soldados, marinheiros, aviadores ou astronautas, mas a cibercombatentes profissionais. ■

REFERÊNCIAS

Jen Weedon, FireEye (2015). "Além da Guerra Cibernética: Uso da Rússia de Espionagem Cibernética Estratégica e Operações de Informação na Ucrânia". Em Kenneth Geers (ed.). Guerra Cibernética em Perspectiva: Agressão Russa contra a Ucrânia . Tallinn: OTAN CCD COE Publicações. ISBN 978-9949-9544-5-2. Arquivado a partir do original em 2016-08-16 . Recuperado em 2016-05-10.

Kramer, Andrew E. (2022-01-14). "Hackers derrubam sites governamentais na Ucrânia". O New York Times. ISSN 0362-4331 . Arquivado a partir do original em 15/01/2022. Recuperado 2022-01-17.

Pearson, James (2022-02-27). "Ucrânia lança 'exército de TI' e mira no ciberespaço russo". Reuters. Recuperado 2022-02-27.

PARKS, R.C. e DUGGAN, D.P. Principles of Cyberwarfare. 2001.

Nuvem como Arma Secreta? Agentes Silenciosos da Guerra. Pagliusi Cibersegurança, 2013.

Paulo Sergio Melo de Carvalho. A Defesa Cibernética e as Infraestruturas Críticas Nacionais. Defesa em Foco, original de 2020-10-09. Recuperado em 2022-03-04.

Launching NASA, A Brief History of NASA. National Aeronautics and Space Administration (NASA). Recuperado em 2022-03-04.

Guerra cibernética russo-ucraniana, Wikipedia. Recuperado em 2022-03-03.

Como as ameaças russas fizeram da Estônia um país especialista em Cibersegurança. CNN Brasil. Original de 2021-06-19. Recuperado em 2022-03-04.

Russian hacking group compromised U.S. power companies. CBS News. Original de 2022-04-17. Recuperado em 2022-04-18.

Queda da Ucrânia poderia resultar em guerra mundial, avalia cônsul da Moldova. CNN Brasil. Original de 2022-03-04. Recuperado em 2022-03-07.

Política Nacional de Segurança de Infraestruturas Críticas - PNSIC, Presidência da República, DECRETO nº 9.573, 2018-11-22.

Estratégia Nacional de Segurança Cibernética - E-Ciber, Presidência da República, DECRETO nº 10.222, 2020-02-05.

Força Aérea Brasileira, Wikipedia. Recuperado em 2022-03-11.

Sistema Militar de Defesa Cibernética entra em vigor nesta terça-feira. Ministério da Defesa. Publicado em 2020-11-30. Recuperado em 2022-03-11.

* Capitão de Mar e Guerra (RM1-IM), Ph.D. *in Information Security*, Membro do Grupo CTEMI do Clube Naval