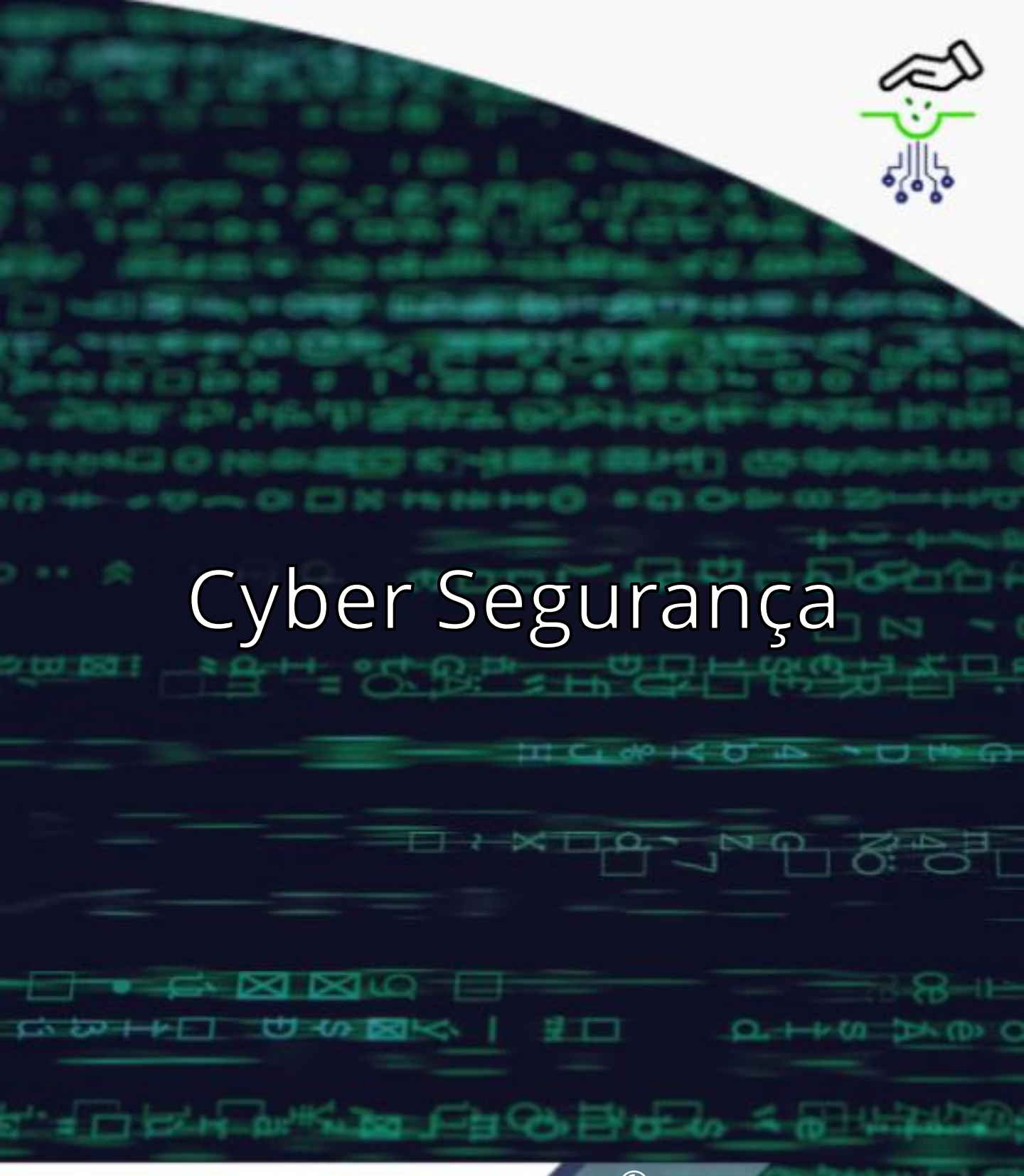


Cyber Segurança

Projeto Sementes de Futuro em Defesa

Vol. 2 Nº 5

EXPEDIENTE

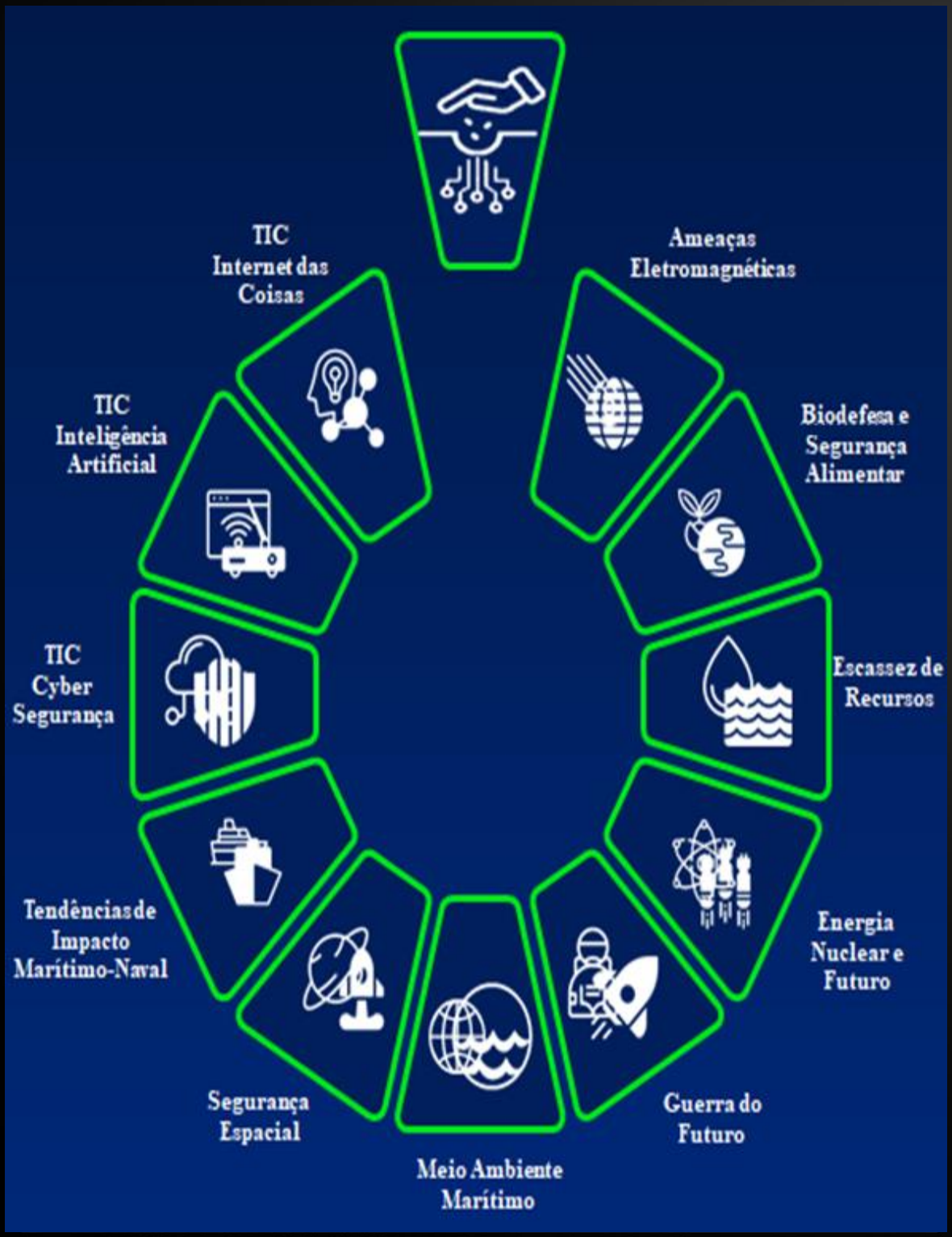
O Projeto Sementes de Futuro em Defesa faz parte do Programa de Cooperação Acadêmica em Defesa Nacional (PROCAD-DEFESA) “Prospectiva para Segurança e Defesa”, projeto da CAPES e do Ministério da Defesa (MD) liderado pela Escola de Guerra Naval (EGN) com 10 outras IES, Instituições e Empresas, para formar uma rede colaborativa de pesquisa e monitoramento de sementes do ambiente futuro, apoiada em plataforma computacional, análise multicritério, com abrangência nacional, participação social pública e privada, civil e militar para acompanhamento dos cenários prospectivos do Ministério da Defesa e uso dual.

O Sementes de Futuro em Defesa é um produto digital e semanal desenvolvido pelos pesquisadores das Linhas de Pesquisa Cenários Prospectivos de Segurança e Defesa do Laboratório de Simulações e Cenários (LSC) da EGN, cuja divulgação visa estimular e disseminar sementes de futuro para temas estratégicos sobre defesa e segurança, subsidiando análises prospectivas altamente qualificadas para auxiliar as Forças Armadas brasileiras no desenvolvimento de estratégias de longo prazo. As matérias deste informativo não representam o posicionamento institucional de qualquer setor das Forças Armadas.

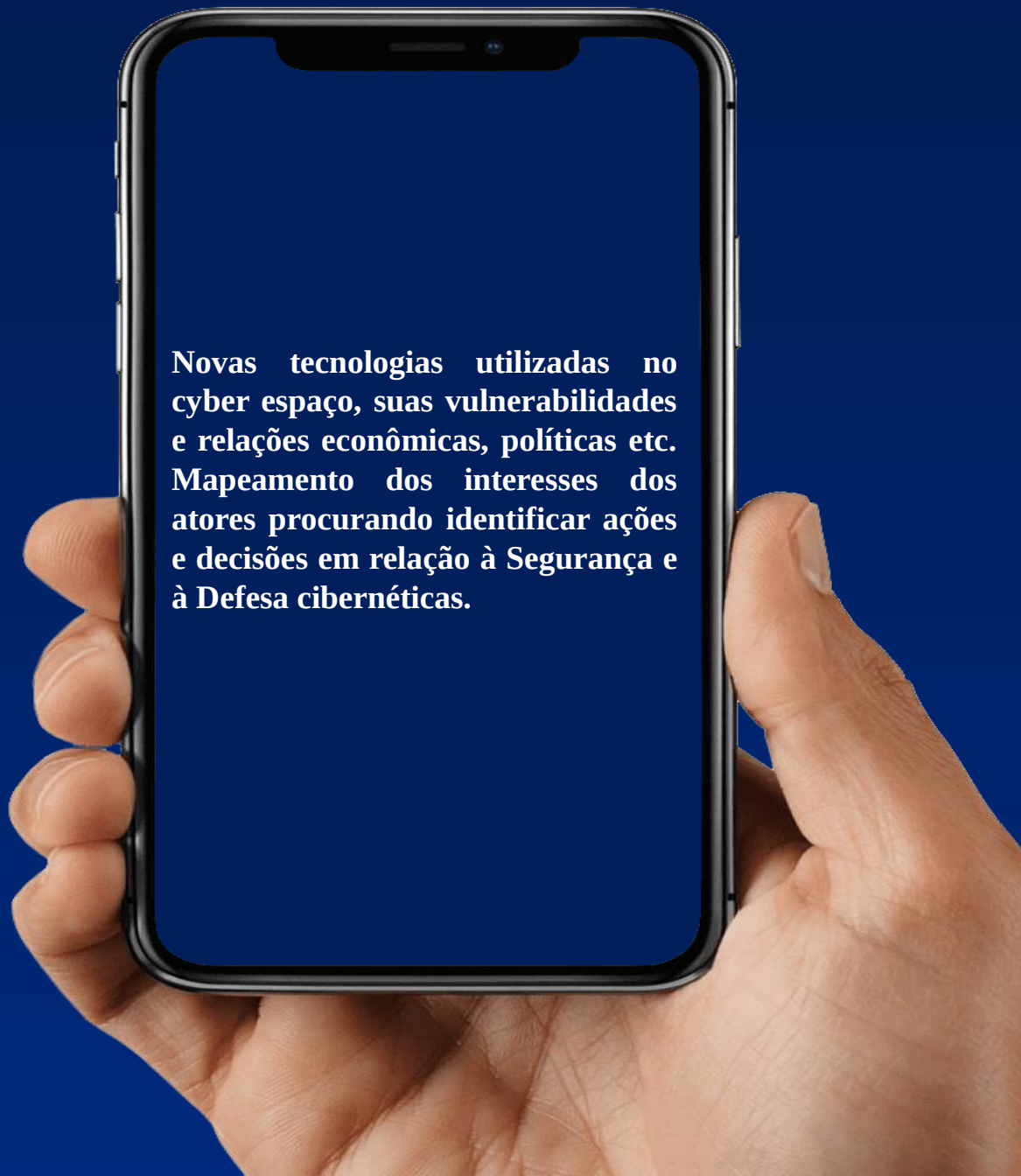
Acompanhe-nos nas Redes Sociais

Laboratório de Simulações e Cenários
Linha de Pesquisa Cenários Prospectivos para Segurança e Defesa
Avenida Pasteur, 480 – Urca, Rio de Janeiro – RJ – Brasil – CEP: 22290-240

OBJETOS DE ESTUDO



TIC Cyber Segurança



SEMENTES DE FUTURO EM DEFESA

TENDÊNCIA DE PESO

São eventos cuja direção e sentido são suficientemente consolidados para que se possa admitir sua continuidade no futuro; retratam processos cujo rompimento requer um esforço hercúleo e improvável de apresentar resultados. (LIMA; CURADO, 2017, pp. 16-17)

FATO PRÉ-DETERMINADO

São eventos já conhecidos, cuja ocorrência é praticamente certa. No geral, as indicações resultantes não se efetivaram ainda, mas se sabe que o evento irá ocorrer no futuro. (LIMA; CURADO, 2017, p. 17)

FATO PORTADOR DE FUTURO

São sinais existentes no ambiente, ínfimos por sua dimensão presente, mas imensos por suas consequências e potencialidades futuras. (MARCIAL, GRUMBACH, 2014, p. 240)

INCERTEZA CRÍTICA

São eventos mais incertos e de maior importância à cenarização; tratam-se das variáveis que determinarão a lógica e a ideia-força dos cenários, portanto, suas mudanças críticas possibilitam múltiplos futuros possíveis. (LIMA; CURADO, 2017, p. 17)

SURPRESA INEVITÁVEL

São forças previsíveis, pois têm suas raízes em forças que já estão em operação neste momento; entretanto, não se sabe quando irão se configurar, quais suas consequências previsíveis e como afetarão. (MARCIAL, GRUMBACH, 2014, p. 244)

CORINGAS (WILD CARDS)

Referem-se a grandes surpresas possuidoras de baixa probabilidade de ocorrência e extremamente difíceis de serem antecipadas; se consolidadas, possuem grande impacto e se materializam rapidamente. (LIMA; CURADO, 2017, p. 18)

PRINCIPAIS ATORES E SUAS ESTRATÉGIAS

Indivíduos, grupos ou organizações que influenciam ou recebem influência significativa do sistema; o ator desempenha importante papel, influenciando o comportamento das variáveis com objetivo de viabilizar seus projetos. (MARCIAL, GRUMBACH, 2014, p. 238)

CAPACIDADE CIBERNÉTICA BRASILEIRA É TEMA DE DEBATE

26/10/2020 – Núcleo de Estudos Estratégicos em Defesa e Segurança da UFSCar

Juraci Ferreira Galdino

Em artigo de opinião, o Coronel Juraci Ferreira Galdino pontua como o Brasil se posiciona em termos de capacidade tecnológica no setor cibernético. Para o autor, a interconectividade está cada vez mais presente no dia a dia da sociedade e faz a Cibernética alcançar o patamar de assunto estratégico, repercutindo simultaneamente nas expressões científica e tecnológica, política, econômica, militar e psicossocial das nações. Desta forma, desenvolver tecnologias cibernéticas de amplo espectro de aplicações tornou-se de extrema importância para incorporar os extraordinários avanços advindos da 4ª Revolução Industrial, sem renunciar à segurança de infraestruturas críticas, ou expor a soberania nacional a riscos sem precedentes. Adicionalmente, os jornais e mídias difundem problemas econômicos, políticos, militares e geopolíticos desencadeados por ações cibernéticas, mostrando que elas são capazes de não apenas provocar a desordem urbana, mas também de negar capacidades operativas militares explorando vulnerabilidades de sistemas, plataformas e produtos de defesa integrados a rede.

É fundamental visualizar em que estágio de evolução se encontra a ameaça cibernética, assim como de que maneira o Brasil se posiciona em termos de capacidade tecnológica nesse setor. Essas questões podem subsidiar a adoção de políticas públicas e estratégicas de Estado visando preparar adequadamente o País para enfrentar os desafios do futuro. Neste sentido, a Agência de Gestão e Inovação Tecnológica do Exército (AGITEC) conduziu um estudo de prospecção tecnológica sobre as principais ameaças cibernéticas, buscando explorar as questões levantadas.

Surpresa Inevitável

Cibersegurança; infraestruturas críticas; soberania nacional; vulnerabilidades.

http://www.needs.df.ufscar.br/artigos_de_opiniao3/97/juraci_ferreira_galdino:_cibernetica-_importancia_e_indicios_da_capacidade_nacional#linha

Marcelo Andrade de Barros – Pós-graduado em Administração de Banco de Dados (UNESA)

INCIDENTES CIBERNÉTICOS EM INFRAESTRUTURAS CRÍTICAS SOFREM AUMENTO

07/02/2022 – Ctir.gov

Redação

Os ataques cibernéticos nas infraestruturas críticas vem se elevando no mundo e recebendo destaque em órgãos de imprensa internacionais. Paralelamente, o Brasil vem sofrendo um aumento contínuo nos números de ataques cibernéticos, conforme identificado pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). Com a finalidade de modificar este quadro, é importante incrementar procedimentos e ativos de segurança cibernética. Assim, busca-se reforçar as infraestruturas críticas para reduzir a superfície de ataque, focando em amenizar a possibilidade de exploração dos vetores, das táticas e das técnicas de ataque.

No caso brasileiro, as infraestruturas críticas são distribuídas em diversos setores. Cada setor possui suas características próprias, suas interdependências com outros setores e seus riscos em sofrer incidentes cibernéticos de acordo com cada área de atuação. Os impactos futuros dos incidentes cibernéticos são a possibilidade da indisponibilidade de infraestruturas que, com a paralisação dos serviços, impactam diretamente no funcionamento do país como um todo.

Fato Pré-Determinado

Infraestruturas críticas; ataques cibernéticos; tecnologia da informação; tecnologia operacional; disponibilidade de ativos.

https://www.gov.br/ctir/pt-br/assuntos/noticias/2022/aumento-de-ataques-as-infraestruturas-criticas

Ines Cardinot – Mestranda de Ciências Aeroespaciais (UNIFA)

BRASIL ESTARIA SERVINDO DE ROTA PARA ATAQUE CIBERNÉTICO À UCRÂNIA

26/02/2022 – Capitaldigital.com.br

Luiz Queiroz

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br) solicitou que as empresas brasileiras de telecomunicações avaliem se suas redes estariam servindo para ataques cibernéticos contra a Ucrânia. Tal fato poderia ocorrer através de redirecionamento da rota de terceiros para esconder a localização de origem dos ataques. É fato que alguns dos ataques estejam ocorrendo através de *botnets* (rede de computadores infectados por *softwares* maliciosos e que podem ser controlados remotamente, enviando *spam*, espalhando vírus ou executando ataques sem o conhecimento dos seus donos) de países terceiros. O comunicado almeja com que as rede no Brasil sejam identificadas, evitando tais ataques cibernéticos.

O redirecionamento de endereço IP é uma prática usada para camuflar a localização original do atacante. Desta forma, ao sofrer qualquer tipo de ataque cibernético, é solicitado identificar a localização do atacante pelo seu endereço de IP e para que providências sejam tomadas. Compreende-se que o impacto futuro é a possibilidade do Brasil estar servindo como intermediário dos reais agressores para ataques às infraestruturas ucranianas, podendo gerar desentendimentos entre as duas nações.

Fato Portador de Futuro

Ataque de negação de serviço; telecomunicações; ataques cibernéticos; *botnets*; Cert.br.

https://capitaldigital.com.br/cert-br-pede-que-teles-avaliem-se-ataque-cibernetico-a-ucrania-esta-partindo-do-brasil/

Ines Cardinot – Mestranda de Ciências Aeroespaciais (UNIFA)

RÚSSIA UTILIZA GUERRA NA UCRÂNIA COMO LABORATÓRIO PARA ARMAS CIBERNÉTICAS

07/03/2022 – *Harvard Business Review*

Stuart Madnick

A Guerra da Ucrânia está servindo como um laboratório para testar a próxima geração de armas cibernéticas da Rússia. Ataques cibernéticos anteriores no país já haviam ocorrido em 2015, após supostos *hackers* cortarem energia elétrica de 230.000 clientes no oeste da Ucrânia, além de agências governamentais e sistemas bancários. Horas antes da invasão russa ao território ucraniano, um *malware* foi lançado visando limpar dados de ministérios do governo e instituições financeiras do país. Durante a invasão, vários sites de bancos e departamentos governamentais ucranianos ficaram inacessíveis. O governo ucraniano relata os ataques atuais como em níveis completamente diferente dos anteriores.

Existe a possibilidade de que os ataques cibernéticos atuais à Ucrânia tenham efeito de transbordamento, incluindo outros Estados e atores internacionais. Segundo a reportagem, é factível também que outros países estejam testando sua própria capacidade cibernética na Ucrânia, como Irã, Coréia do Norte ou China. A comunidade internacional, governos e corporações necessitam prestar atenção a esse cenário, já que uma guerra cibernética a nível internacional, dada tamanha interdependência dos setores críticos de infraestrutura (eletricidade e comunicações), teria efeito devastador e duradouro.

Surpresa Inevitável

Cibersegurança; infraestruturas críticas; ataques cibernéticos; armas cibernéticas; guerra cibernética.

https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare

Fernanda Borges de Carvalho – Assistente de Pesquisa (LSC-EGN)

MALWARE DESTRUTIVO É AMEAÇA AOS DISPOSITIVOS DE ORGANIZAÇÕES NA UCRÂNIA

26/02/2022 – Dciber.org

Redação

Em janeiro e fevereiro de 2022, foram identificados em organizações da Ucrânia *malwares* destrutivos, denominados de *Whispergate* e *HermeticWiper*. Tal fato pode representar uma ameaça direta às operações diárias, impactando a disponibilidade de ativos e dados críticos. Existe a possibilidade de que ocorram outros ataques cibernéticos disruptivos contra organizações na Ucrânia, podendo inadvertidamente se espalhar para outros países. Desta forma, é fundamental que as organizações aumentem a vigilância e avaliem suas capacidades, abrangendo planejamento, preparação, detecção e resposta para tais eventos.

As empresas de telecomunicações fazem parte das infraestruturas críticas dos países. Um *malware* pode causar interrupção desses serviços em cadeia, cortando a comunicação dos países de forma parcial ou total. Assim, é altamente relevante que o Estado brasileiro invista na proteção da arquitetura de rede, da linha de base de segurança, do monitoramento contínuo e das práticas de resposta a incidentes.

Surpresa Inevitável

Malware; dados críticos; ataques cibernéticos; vigilância; disponibilidade de ativos.

https://dciber.org/cisa-alerta-aa22-057a-organizacoes-de-segmentacao-de-malware-destrutivo-na-ucrania/

Ines Cardinot – Mestranda de Ciências Aeroespaciais (UNIFA)

SEMENTES DE FUTURO EM DEFESA

Sinalizar o futuro para defender o presente