ARTIGO DOI 10. 52781/cmm.a157

O papel do Sistema de Engenharia do Exército Brasileiro na segurança da Infraestrutura Crítica de Transporte

The role of the Brazilian Army Engineering System in the Critical Transportation Infrastructure Security

Resumo: Infraestruturas críticas são ativos sujeitos a riscos associados a ameaças humanas ou desastres naturais, nos quais a sociedade confia para manter a economia, a saúde e a segurança pública. Vários países elaboraram planos específicos para garantir a segurança de infraestruturas críticas por meio de cooperação entre autoridades, agências e o setor privado. Ciente das capacidades do Exército Brasileiro de atuar na construção de infraestruturas de transporte, o autor buscou neste artigo relacionar as atividades desempenhadas pelo Sistema de Engenharia do Exército Brasileiro com a capacidade de garantir a segurança da Infraestrutura Crítica de Transporte. Notou-se, por fim, que o Sistema de Engenharia tem colaborado com a segurança ao atuar no gerenciamento e mitigação dos riscos por meio da execução de obras e serviços de engenharia, proporcionando maior resiliência às infraestruturas físicas terrestres.

Palavras-chave: Infraestruturas críticas. Engenharia do Exército Brasileiro. Gerenciamento de riscos. Transportes. Inundações.

Abstract: Critical infrastructure are assets subject to risks associated with human threats or natural disasters, on which society relies to maintain economy, health and public safety. Several countries have developed specific plans to ensure the security of critical infrastructure through cooperation between authorities, agencies and the private sector. Aware of the capabilities of the Brazilian Army to act in the construction of transport infrastructure, the author sought in this article to relate the activities performed by the Brazilian Army Engineering System with the ability to guarantee the security of the Critical Transport Infrastructure. Finally, it was noted that the Engineering System has collaborated with security by acting in risk management and mitigation by civil construction and engineering services, providing greater resilience to transportation infrastructure.

Keywords: Critical infrastructure. Brazilian Army Engineering. Risk management. Transportation. Floods.

Halan Bastos Oliveira
Universidade Federal do Rio de Janeiro.
Programa de Engenharia Urbana.
Exército Brasileiro. Comissão Regional de Obras 7.
Recife, PE, Brasil.
halan_bastos@hotmail.com

Recebido: 27 jun 2023
Aprovado: 17 fev 2025

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 INTRODUÇÃO

Segundo a definição da *Cybersecurity and Infrastructure Security Agency* (Cisa), Infraestruturas Críticas (ICs) podem ser entendidas como quaisquer ativos, sistemas, instalações, redes ou outros elementos dos quais a sociedade confia para manter a economia, a saúde e a segurança públicas. Eventos climatológicos e meteorológicos extremos, ataques a rodovias e ferrovias, além de pandemias ou ataques terroristas são alguns dos riscos aos quais as ICs de uma nação estão sujeitas (EUA, 2019).

O Centre for the *Protection of National Infrastructure* (CPNI) (Reino Unido, 2023) define as ICs como instalações, sistemas, locais, informações, pessoas, redes e processos necessários para o funcionamento de um país e dos quais depende a vida diária. Inclui também algumas funções, locais e organizações que não são críticas para a manutenção de serviços essenciais, mas que precisam de proteção devido ao perigo potencial para o público, como instalações nucleares e químicas civis, por exemplo. Os danos ou destruição de ICs por catástrofes naturais, terrorismo e atividades criminosas podem ter consequências negativas para a segurança do país e o bem-estar dos seus cidadãos.

Apesar da falta de uma definição formal de "Infraestrutura Crítica", vários órgãos governamentais criam legislações próprias para determinar quais partes de suas infraestruturas são cruciais. Entretanto, essas definições costumam ser genéricas, uma vez que fornecem uma perspectiva estratégica que posteriormente deve ser analisada setor por setor.

Alguns países já possuem um plano de defesa de ICs, inclusive com órgãos vocacionados a essa função, a exemplo da Cisa no Estados Unidos, que tem a missão de defender os ativos cibernéticos e a infraestrutura do país e colaborar com a construção de estruturas mais seguras e resilientes (Estados Unidos da América, 2023). No Reino Unido, além de serem frequentemente reclassificados pelo CPNI, os setores de infraestrutura são subdivididos em "subsetores", como os de polícia, ambulância, bombeiros e guarda costeira, pertencentes aos serviços de emergência. Cada um deles tem um ou mais departamentos governamentais responsáveis por garantir a segurança de seus ativos (Reino Unido, 2023).

A Infraestrutura Crítica de Transporte (ICT), além da própria estrutura física de rodovias, ferrovias e aeroportos, engloba também o transporte de cargas e de passageiros. Desastres naturais, atos de terrorismo, de sabotagem ou guerra, além do desenvolvimento humano desordenado em áreas urbanas, formam os principais riscos aos quais essas estruturas estão sujeitas.

No Brasil, as atualizações da Política Nacional de Defesa (PND) e da Estratégia Nacional de Defesa (END) foram aprovadas pela Câmara dos Deputados em dezembro de 2024 e seguiram para promulgação (Câmara..., 2024). Ainda que pese um dos objetivos dos documentos ser conscientizar toda a sociedade da importância da defesa do País (Brasil, 2023, p. 71), Rocha (2019) menciona a desídia das autoridades com prevenção e segurança contra ameaças ou ataques devido à cultura pacífica e à ausência de conflitos recentes com outras nações. O assunto sobre defesa de ICs, por exemplo, só foi introduzido em um documento oficial em 2008 e de forma bem discreta, sem que definisse o termo ou a classificasse os ativos críticos de infraestrutura do país (Brasil, 2008).

Apenas em setembro de 2022 foi aprovado o Plano Nacional de Segurança de Infraestruturas Críticas (Plansic) (Brasil, 2022) com vistas a criar a estrutura operacional que irá subsidiar o

acompanhamento e monitoramento permanente da segurança das ICs do país. Sem elencar nominalmente as estruturas a serem observadas, o Plano define de forma genérica e com prazos dilatados os responsáveis por desenvolver ações específicas para cada setor de IC.

O Exército Brasileiro, no entanto, em sua atribuição subsidiária de cooperar com o desenvolvimento nacional e a defesa civil (Brasil, 1999, art. 16), atua na construção, manutenção e proteção: da infraestrutura de fortificações desde o período do Brasil Colônia; da malha ferroviária e de linhas telegráficas desde o Brasil Império; e, já no período da República, de rodovias que conectam as diversas regiões do país (Figueiredo *et al.*, 2014), inclusive valendo-se de parcerias com empresas privadas na execução de obras e serviços de engenharia (Brasil, 1999, art. 17A).

Nesse sentido, este estudo aborda o papel do Sistema de Engenharia do Exército Brasileiro (SEEx) na execução das ações de segurança da Infraestrutura Crítica de Transporte do Brasil pelo prisma das missões constitucionais e atribuições subsidiárias da instituição, tendo uma abordagem qualitativa por meio de análise dos dispositivos legais e de pesquisa bibliográfica relacionada ao tema. Ademais, pelo fato de a pesquisa bibliográfica ter apontado um maior nível de maturidade sobre o assunto na literatura estrangeira, este artigo busca também colaborar com a literatura nacional sobre o tema da segurança de ICs.

2 METODOLOGIA

2.1 A ICT no cenário internacional

Desde meados dos anos 2000, governos têm projetado e implementado políticas públicas para apoiar a proteção da IC. A maioria dos países da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) (2019) definiu setores de IC, levantou o inventário de ativos e implementou regulamentações, programas nacionais e mecanismos de incentivo para fortalecer a resiliência dessas estruturas diante de perigos ou ameaças.

Nos Estados Unidos, em razão do desenvolvimento econômico e do histórico de guerras e ameaças terroristas, comumente enfrentadas por aquele país, a conscientização sobre o tema de IC iniciou-se bem antes que no Brasil. O governo norte-americano, logo após os atentados terroristas de 11 de setembro de 2001, publicou uma série de diretrizes de segurança interna objetivando a elaboração de um plano nacional abrangente para garantir a segurança de ICs mediante cooperação das autoridades e das agências federais, regionais e locais, além do setor privado e de outras entidades (Brasil, 2020, art. 4º).

O Conselho da União Europeia, definindo de forma ampla as ICs como os ativos e sistemas essenciais para manter as funções vitais da sociedade, concentrou-se mais especificamente nos setores de energia e transporte, cuja perturbação ou destruição afetaria um, ou mais Estados-membros, devendo os impactos serem avaliados com base em critérios abrangentes, incluindo os efeitos resultantes de dependências intersetoriais em relação a outros tipos de infraestruturas.

Outrossim, em 2007 o mesmo Conselho aprovou uma série de conclusões sobre o Programa Europeu de Proteção de Infraestruturas Críticas (Pepic), reafirmando que, em última instância, é responsabilidade de cada Estado-membro garantir a proteção das ICs em seus respectivos territórios nacionais. Essa dinâmica levou à publicação em 2008 da Diretiva do Conselho

Europeu que trata da identificação e designação das ICs Europeias, estabelecendo um procedimento para sua identificação e designação, bem como uma abordagem comum para avaliar a necessidade de aprimorar sua proteção (Natário; Nunes, 2014).

No estudo de Natário e Nunes (2014), realizado a partir da compilação das informações do *International CIIP Handbook 2008/2009* (*apud* Brunner; Suter, 2008), constatou-se que, entre os 25 países pesquisados (Tabela 1), os Estados Unidos (EUA), seguidos da Noruega, eram os países que mais possuíam infraestruturas classificadas como críticas à época dos dados obtidos, entre 2008 e 2009. Apenas a Rússia não classificava o setor de Transportes/Logística como crítico.

Tabela 1. Setores considerados críticos em diversos países, com siglas de acordo com a ISO 3166 (ISO, 2020)

PAÍSES SETORES	AUS	AUT	BRA	CAN	EST	FRA	FIN	DEU	HUN	IND	ITA	JPN	KOR	MAL	NLD	NOR	NZL	POL	RUS	SWE	SGP	ESP	CHE	GBR	USA	Total de países
Bancos e Finanças	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	25
Governo Central		•		•	•	•		•	•		•	•	•	•	•	•	•	•	•		•	•	•	•	20
Indústrias Química e Nuclear				•						•				•	•			•				•	•		•	8
Serviços de Emergência	•		•	•	•	•			•	•	•		•	•		•	•	•	•				•	•	•	17
Eletricidade/Energia	•	•		•	•	•	•	•	•	•	•	•	•		•	•	•	•			•	•	•	•	•	21
Agricultura/Alimentação	•			•	•	•	•	•	•		•	•			•	•					•	•	•	•	•	16
Serviços de Saúde	•		•	•	•	•	•		•		•			•	•	•					•	•	•	•	•	16
Comunicação/Mídia	•	•				•	•		•		•		•		•	•			•	•	•		•		•	14
Defesa						•			•	•			•	•		•			•					•	•	9
Monumentos Nacionais	•																								•	2
Esgoto/Resíduos	•										•			•	•	•		•					•	•	•	9
Telecomunicações	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•		•	•	23
Transportes/Logística	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	24
Distribuição de Água	•		•		•	•	•	•	•		•	•		•	•	•				•	•	•	•	•	•	18
Total de setores	11	6	6	9	9	11	8	7	11	7	11	7	8	9	11	12	6	8	6	6	8	9	11	11	14	

Fonte: Adaptado de Natário e Nunes (2014).

Dada a evidente interdependência desses ativos de infraestrutura, em 2019 a OCDE elaborou outro estudo com seus países-membros, considerando 16 setores (e mais 1 genérico) potencialmente críticos. O relatório apontou que, com exceção da Estônia, todos os demais 31 países da OCDE classificam a infraestrutura de transportes como crítica, ficando esse setor atrás apenas do elétrico em termos de criticidade (Tabela 2).

Liu e Song (2020) citam que rodovias, ferrovias e aeroportos são infraestruturas essenciais para o funcionamento da cadeia logística de quase todos os serviços essenciais à sociedade, e falhas ou ataques causados a alguns desses pode desencadear uma série de consequências de baixo impacto, como no caso de congestionamentos, ou catastróficas, como em ataques terroristas. Em ambientes urbanos, onde normalmente há maior densidade demográfica, até mesmo

falhas simples nessas estruturas, como obstrução das estruturas coletoras de águas pluviais ou baixa aderência do pavimento, causam perdas humanas. Fenômenos naturais como chuvas intensas, terremotos ou furacões, além de não poderem ser controlados pelo homem, representam uma das principais ameaças à ICT de uma cidade.

Tabela 2. Setores considerados críticos nos países da OCDE, com siglas de acordo com a ISO 3166 (ISO, 2020)

PAÍSES SETORES	AUS	AUT	BEL	CAN	CHE	CHL	CZE	DEU	ESP	EST	FIN	FRA	GBR	GRC	IRL	ISL	ISR	ITA	KOR	LAT	LUX	MEX	NLD	NOR	NZL	POL	PRT	SVK	SVN	SWE	TUR	USA	Total de países
Energia	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	32
Indústria Nuclear				•			•		•			•	•				•		•				•	•							•	10
TI e Comunicação	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	31
Transportes/ Logística	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	31
Distribuição de água	•	•	•	•	•		•	•	•	•	•	•	•				•		•	•	•		•	•	•	•		•				•	22
Barragens e inundações	•					•	•					•			•	•		•	•	•		•	•	•				•		•	•	•	15
Fornecimento e distrib de alimentos	•	•		•	•		•	•	•		•	•	•				•				•			•		•				•	•	•	17
Serviços de saúde	•	•	•	•	•	•	•	•	•	•	•	•	•				•		•	•	•			•		•		•		•	•	•	23
Bancos e Finanças	•	•	•	•	•		•	•	•	•	•	•	•				•		•	•	•		•	•		•		•		•	•	•	23
Governo		•		•	•		•	•	•			•	•				•		•	•	•			•		•				•		•	16
Segurança Pública	•	•		•	•		•	•	•				•				•			•	•		•	•						•		•	15
Aplicação da lei		•				•		•				•	•				•			•	•		•	•									10
Indústria Química	•	•			•				•		•	•	•				•			•	•		•	•		•		•				•	15
Setor espacial			•						•			•	•																				4
Indústria de Defesa	•										•	•	•				•			•												•	7
Indústria de fabricação				•							•	•					•							•							•	•	7
Outros		•	•					•	•	•	•	•	•				•		•	•	•		•	•	•	•				•	•	•	19
Total de setores	11	12	8	11	10	6	11	11	13	6	11	16	15	3	4	4	15	4	10	13	12	4	11	15	5	10	2	7	4	9	9	15	

Fonte: OCDE (2019).

2.2 Histórico da Segurança de Infraestruturas Críticas no Brasil

No Brasil, somente em 2006, após ataques da facção criminosa Primeiro Comando da Capital (PCC) no estado de São Paulo, o Gabinete de Segurança Institucional da Presidência da República deu início ao trabalho de identificação e análise de riscos das ICs do País (Rocha, 2019), tendo iniciado com as áreas de comunicações, energia, transportes e águas, em parceria com órgãos públicos e entes privados. Dessa forma, o termo "Infraestruturas Críticas" foi mencionado pela primeira vez em um documento oficial em 2008, na então primeira versão da END,

como componente prioritário da ação estratégica "Segurança Nacional", que visava a colaboração de todo o Estado para a prevenção aos riscos e o incremento da segurança no país (Brasil, 2008).

Em 22 de novembro de 2018, por intermédio do Decreto Presidencial nº 9.573, foi aprovada a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) com o intuito de definir as orientações referentes ao esforço conjunto que órgãos públicos e entidades privadas devem desenvolver a respeito da segurança de ICs, competindo à Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo analisar, discutir e propor a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC) e o Plansic.

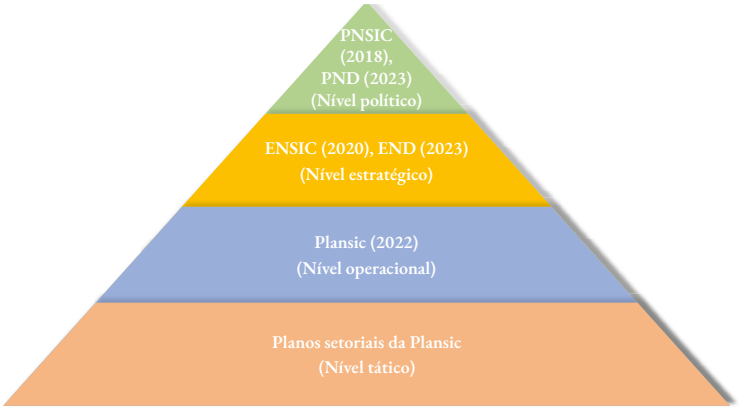
Além disso, a PNSIC enquadrou a segurança dessas infraestruturas como uma atividade de Estado prioritária, elevada a nível institucional. Para alcançar os objetivos, seriam necessários três instrumentos: a Estratégia Nacional de Segurança de Infraestruturas Críticas; o Plano Nacional de Segurança de Infraestruturas Críticas; e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas (Brasil, 2018a).

Dois anos após a aprovação da PNSIC, já em 9 de dezembro de 2020, a Presidência da República, por meio do Decreto nº 10.569, aprovou a ENSIC, no sentido de identificar os riscos às quais as ICs do Brasil estão sujeitas e de definir as principais ações a serem adotadas no sentido de assegurar a integridade da prestação dos serviços indispensáveis ao Estado e à sociedade brasileira (Brasil, 2020, art. 5º).

Em 15 de setembro de 2022, por meio do Decreto nº 11.200, foi aprovado o Plano Nacional de Segurança de Infraestruturas Críticas (Plansic) com objetivo de identificar as ICs do país; analisar os riscos e a interdependência das ICs; avaliar as vulnerabilidades e propor opções para eliminar ou reduzir as fraquezas das ICs e torná-las mais resistentes às ameaças, entre outros objetivos. Além disso, o Plansic prevê a criação de Planos Setoriais complementares para tratar das ações de segurança em cada setor, dependendo essencialmente da atuação integrada das três esferas de governo para sua implementação (Brasil, 2022).

Na primeira fase do Plano, definiram-se ações estratégicas objetivando a construção de uma estrutura de governança, iniciativas de capacitação e conscientização dos atores envolvidos e estabelecimento de ferramentas de armazenamento, gestão e integração dos dados e informações (Brasil, 2022).

Figura 1. Diferentes níveis de legislações acerca da Segurança de Infraestruturas Críticas



Fonte: elaborado pelo autor.

Traçando um paralelo entre as legislações apresentadas e os diferentes níveis de planejamento e condução das operações militares da Sistemática de Planejamento de Emprego Conjunto das Forças Armadas (SisPECFA) (Brasil, 2017b, p. 2-10), pode-se afirmar que o Plansic é o primeiro a abordar a segurança das ICs em um nível operacional, atribuindo responsabilidades específicas, estabelecendo prazos, ainda que dilatados, e definindo metas, ainda que genéricas, a partir de cada ação estratégica (Figura 1). Dessa forma, o Plano deve desempenhar papel crucial na ligação entre os objetivos estratégicos e a implementação tática após a criação dos respectivos Planos Setoriais.

O Plansic, como planejamento em nível operacional, ainda deve ser ajustado de acordo com as condições impostas pelos atores políticos, como o tempo e recurso disponíveis, e ainda pelo propósito exigido pelas ações táticas, mas, ao mesmo tempo, devendo garantir o suporte logístico necessário e fornecer os recursos necessários para o cumprimento dos objetivos estratégicos.

Os Planos Setoriais serão documentos complementares ao Plano que fornecerão orientações sobre os níveis desejáveis de proteção, as atividades de segurança a serem realizadas e a priorização na alocação de recursos, levando em consideração as particularidades e abordando de forma específica as ações de segurança de cada setor. Tanto a implementação do Plansic quanto a dos Planos Setoriais receberão o apoio do Ministério da Defesa, conforme estabelecido pela END (Brasil, 2022, p. 5).

2.3 Identificação da ICT Nacional

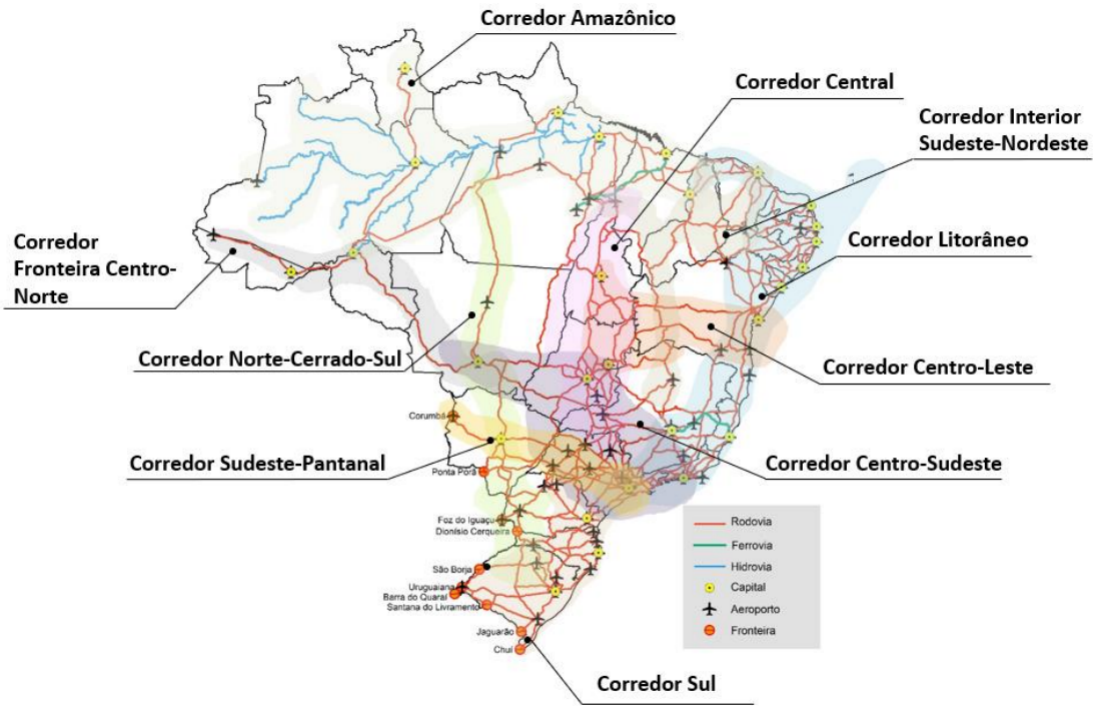
A Lei Federal nº 12.379 (Brasil, 2011) definiu que o Sistema Nacional de Viação (SNV) constitui o conjunto da infraestrutura de transporte, pública e privada, responsável pela circulação de pessoas e mercadorias em todo o território brasileiro. Composto pelos modais rodoviário, ferroviário, aquaviário e aéreo federais, estaduais e municipais, seus objetivos são facilitar o deslocamento eficiente de cargas e passageiros entre os estados e regiões do país, promover a coesão territorial e o desenvolvimento econômico sustentável, atender aos grandes fluxos de mercadorias por meio de Corredores Logísticos Estratégicos (CLEs), e garantir a malha viária estratégica necessária à segurança do território nacional.

Corredores Logísticos Estratégicos (CLEs) são eixos que proporcionam investimentos e constituição de mercados, impulsionando o desenvolvimento econômico e social. Eles incluem um sistema viário composto por diferentes modais que facilitam o transporte eficiente de cargas e, consequentemente, de pessoas.

O Projeto "Corredores Logísticos Estratégicos", realizado pelo Ministério dos Transportes entre 2017 e 2020 (Brasil, 2024), em complemento à Lei nº 12.379, teve como objetivo apresentar uma visão panorâmica e diagnóstica da infraestrutura para o escoamento das principais cargas do país, além de abordar temas e locais estratégicos onde o Governo atua como promotor de infraestrutura, como o transporte de passageiros, integração e defesa nacional. O estudo identificou 10 (dez) CLEs no Brasil, como apresentado na Figura 2.

Traçando um paralelo entre as definições de ICT, apresentada no início deste estudo, e de CLE, pode-se afirmar que o SNV pode representar a ICT do Brasil.

Figura 2. CLEs do Brasil



Fonte: Brasil (2024).

2.4 Gestão e mitigação de riscos

A segurança das ICs pode ser definida como a redução do risco de invasões, ataques ou efeitos de desastres naturais ou antrópicos por intermédio da aplicação de meios físicos ou de medidas cibernéticas defensivas (Estados Unidos da América, 2019). Uma estratégia de segurança de ICs deve identificar quais elementos da infraestrutura são críticos para o seu funcionamento ou representam o perigo mais significativo para a vida e a propriedade, ainda que alguns elementos possam ser mais críticos do que outros (Moteff *et al.*, 2003).

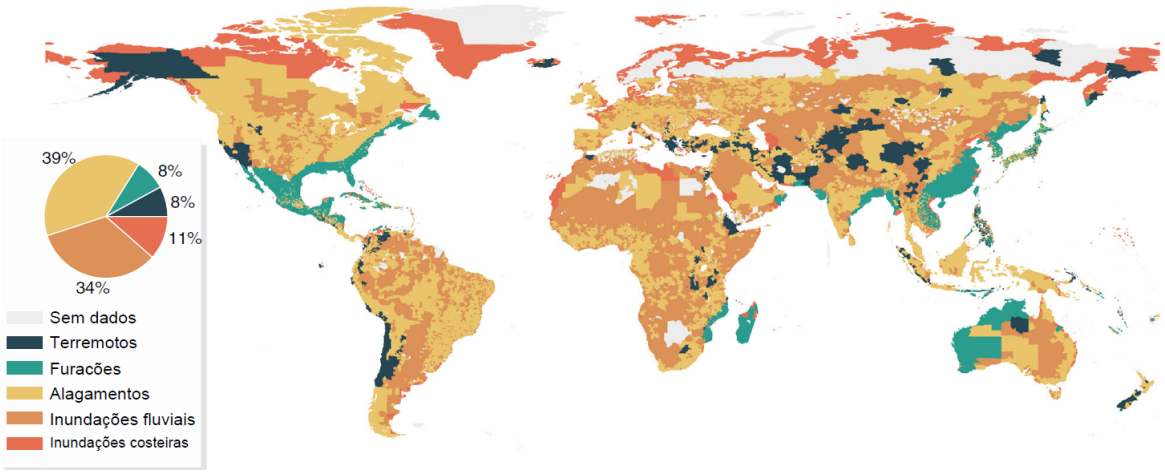
Mas como se define risco?

A CISA (Estados Unidos da América, 2019) refere-se a risco como o potencial de materialização de um resultado indesejado decorrente de um incidente, acidente ou evento determinado pela sua probabilidade e pelas consequências associadas. Enquanto gerenciamento de risco é o processo de identificar, analisar e comunicar, passando pela decisão de aceitar, evitar, transferir ou controlá-lo a um nível aceitável, envidando recursos nas ações destinadas a prevenir ou mitigar os efeitos das ameaças e perigos que têm maior probabilidade de causar resultados indesejados significativos em uma infraestrutura.

Moteff *et al.* (2003) explicam que o tamanho e a complexidade de algumas infraestruturas, a exemplo de rodovias e ferrovias de extensões continentais, podem tornar a identificação dos riscos a elementos individuais de uma IC uma tarefa complexa. Contudo, em levantamento realizado

por Koks *et al.* (2019), observou-se que alagamentos (39%) e inundações fluviais (34%) são os fatores com maiores níveis de risco predominante às infraestruturas de transportes na maioria dos países e regiões do planeta. Mais especificamente para o caso do Brasil, nota-se, conforme apresentado na Figura 3, que os riscos aos quais está sujeita a ICT nacional concentram-se integralmente nesses dois eventos de origem climática.

Figura 3. Indicação do risco predominante à Infraestrutura Crítica de Transporte em cada região



Fonte: Koks *et al.* (2019).

Mattsson e Jenelius (2015) também observaram que a interrupção de vias, o isolamento causado por inundações e a frequência das chuvas intensas têm impacto significativo no funcionamento das redes rodoviárias, bem como das ferroviárias, que são particularmente vulneráveis aos riscos naturais devido à falta de capacidade excedente[1], às limitadas possibilidades de redirecionamento de trens e à presença de linhas ferroviárias únicas.

Ainda de acordo com Koks *et al.* (2019), é possível mitigar em até 42% as estimativas de risco globais de todos os tipos de alagamentos e inundações com a execução de obras de adaptação dos parâmetros de drenagem rodoviária. Em outras palavras, adaptar o padrão das rodovias para resistir a chuvas intensas com um Período de Retorno (T_r)[2] duas vezes maior, de 100 anos em vez de 50 anos, por exemplo, poderia reduzir os riscos relacionados às chuvas intensas pela metade, resultando em uma diminuição estimada dos custos globais de manutenção entre 0,1% e 0,9%.

A gestão de riscos, combinada com a implementação de método lógico para estabelecer contextos, identificar, avaliar e tratar riscos de toda natureza de maneira sistêmica, desempenha um papel crucial na segurança da ICT, garantindo a capacidade máxima de cada medida de proteção e a continuidade das atividades de transporte e do fluxo logístico (Brasil, 2022).

1 Capacidade excedente: infraestrutura de suporte instalada e não utilizada, total ou parcialmente, disponível para compartilhamento (BRASIL, 2017a).

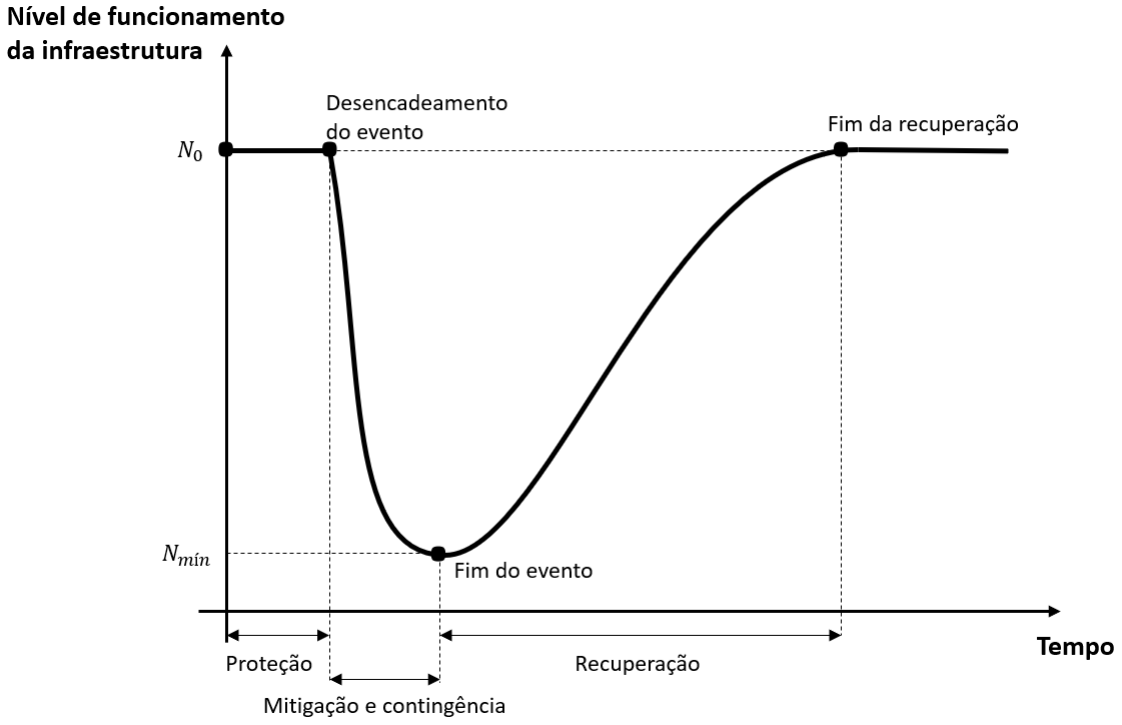
2 Período de retorno (T_r) é o intervalo de tempo médio em que um determinado evento de chuva é igualado ou superado pelo menos uma vez. Quanto menor o período de retorno, mais frequente e mais provável é o evento.

2.5 Resiliência e segurança da ICT brasileira

A OCDE (2019) narra que até meados dos anos 2000, as políticas e atividades relacionadas à segurança das ICs ao redor em todo o mundo eram focadas simplesmente na proteção de ativos. No entanto, devido ao crescente custo com a reparação de desastres ou ataques, a exemplo dos atentados terroristas em 11 de setembro de 2001 nos Estados Unidos, e aos ataques cibernéticos voltados às ICs, os governos passaram a direcionar seu foco não mais na proteção, mas na resiliência das estruturas.

Em momentos de crise, dedicar esforços exclusivamente às atividades de proteção pode não ser suficiente para garantir a segurança das infraestruturas. Nessas situações, é necessário implementar medidas de mitigação e contingência com o objetivo de recuperar o sistema do seu nível de funcionamento mínimo ao nível anterior ao evento de materialização dos riscos, dentro do menor tempo possível, considerando a gravidade da situação e a criticidade da estrutura (Figura 4). O equilíbrio entre as ações de proteção e gerenciamento de riscos é fundamental para o sucesso da atividade de segurança das infraestruturas críticas. (Brasil, 2022).

Figura 4. Alteração no nível de funcionamento de uma infraestrutura causada por evento ou ataque, e sua recuperação graças à resiliência



Fonte: Adaptado de Arrighi, Pregnolato e Castelli (2021).

No Brasil, a PNSIC (Brasil, 2018a) estabelece que a segurança das ICs consiste em um conjunto de medidas preventivas e reativas que têm como objetivo preservar ou restabelecer a prestação dos serviços relacionados a essas infraestruturas; ao mesmo tempo que a ENSIC (Brasil,

2020) destaca a importância da segurança das ICs como uma atividade fundamental para fortalecer a segurança e a resiliência dos setores estratégicos vitais para o funcionamento dos Estados, tanto individualmente quanto em conjunto.

Uma infraestrutura resiliente tem a capacidade de resistir e se recuperar rapidamente de interrupções, ataques intencionais, acidentes, ameaças ou incidentes naturais (Estados Unidos da América, 2019). Para Liu e Song (2020), resiliência refere-se à capacidade de se adaptar a condições em constante mudança, resistir e se recuperar no menor espaço de tempo de interrupções causadas por emergências. Argyroudis *et al.* (2020) definem ainda resiliência como a propriedade emergente ou os atributos que a infraestrutura possui que permitem-na suportar, reagir e/ou adaptar-se a uma ampla variedade de eventos perturbadores, ao mesmo tempo que mantém e/ou aprimora sua funcionalidade.

Como observado por Mattsson e Jenelius (2015) e por Koks *et al.* (2019), a resiliência da ICT está intimamente ligada, então, à sua capacidade de adaptar-se às consequências das chuvas intensas. Nos casos de construção rodoviária ou de manutenção de estradas vicinais, estima-se que adaptar o sistema de drenagem para uma frequência pluviométrica maior ou para reduzir pela metade os danos financeiros esperados, gere um impacto financeiro de aproximadamente 2% no orçamento. Todavia, para estradas pavimentadas existentes, redimensionar os parâmetros de chuva significaria reconstruir seções inteiras da rodovia apenas para substituir as tubulações de drenagem (Koks *et al.*, 2019).

2.6 O Sistema de Engenharia do Exército Brasileiro

Desde a Guerra do Paraguai, a Engenharia do Exército Brasileiro tem sido empregada em obras de ferrovias, linhas telegráficas estratégicas e em outros projetos de interesse do Estado. Embora as empresas privadas tenham ganhado cada vez mais espaço na construção de infraestruturas após o final do século XIX, a Engenharia Militar continuou desempenhando um papel importante em empreendimentos estratégicos, especialmente na construção de eixos rodoviários e ferroviários, fortificações permanentes e em trabalhos de mapeamento do território (Figueiredo *et al.*, 2014).

O Manual *A Engenharia nas Operações* (Brasil, 2018b, p. 2-1) define a Engenharia como a arma de apoio ao combate que tem como missão principal apoiar as operações conduzidas pelo Exército Brasileiro, por intermédio das atividades de mobilidade, contramobilidade e proteção, e de apoio geral de engenharia. Essas ações visam a multiplicar o poder de enfrentamento das forças amigas e a destruir, neutralizar ou diminuir o poder de combate inimigo, propiciando a conquista e manutenção dos objetivos estabelecidos.

Especificamente na função mobilidade, reúnem-se tarefas desenvolvidas para proporcionar o movimento contínuo e ininterrupto de uma força amiga ou dos próprios cidadãos, em tempos de paz, e é composta, além de outras ações mais voltadas ao exercício da atividade militar, de transposição de cursos de água, e de conservação e reparação de pistas e estradas. Dentro da missão de apoio geral de engenharia, a Engenharia realiza, por exemplo: construção de instalações logísticas; recuperação de áreas danificadas; construção, melhoramento e reparação de hidrovias, rodovias, ferrovias e aeródromos.

> Tem atuação na função logística engenharia definida como: 'Conjunto de atividades que são executadas, visando ao planejamento e à execução de obras e de serviços com o objetivo de obter e adequar a infraestrutura física e as instalações existentes às necessidades das forças (Brasil, 2018b, p. 2-1).

Ainda no Manual *A Engenharia nas Operações* (Brasil, 2018b, p. 2-1), cita-se que as operações da Engenharia em zonas construídas, a exemplo do ambiente urbano, são realizadas com o objetivo de contribuir com o desenvolvimento nacional em tempos de paz. Entre os fatores que influenciam a defesa dessas áreas estão o interesse em manter a posição, as possibilidades que a localidade oferece, e, antes de tudo isso, a situação da infraestrutura rodoviária ou ferroviária para que se possa chegar ao local de interesse, sendo o principal fator. Em tempos de guerra, têm o objetivo de manter o controle de parte ou de toda uma área para negá-la ao inimigo, e para garantir às forças amigas o controle total das ICs pelo uso do planejamento adequado.

O Departamento de Engenharia e Construção (DEC) é o órgão de direção setorial do Exército Brasileiro responsável por garantir e regular a utilização do Sistema de Engenharia do Exército Brasileiro (SEEx) em benefício do Estado Brasileiro. O DEC, por intermédio do SEEx, desempenha uma variedade de atividades que vão desde a manutenção da trafegabilidade de estradas vicinais até a montagem emergencial de pontes desmontáveis em situações de calamidade pública, abrangendo a coordenação e execução de obras e serviços de engenharia de infraestrutura física em todo o território nacional, em diferentes momentos e regiões, desde o Sul até a Amazônia (Brasil, 2021).

Dutra (2017) explica que o Sistema de Engenharia do Exército (SEEx) é o instrumento do DEC para articular-se estrategicamente em todo o território nacional, tanto em apoio às operações militares atribuídas à Força Terrestre quanto ao desenvolvimento nacional, com as atribuições de:

- executar as atividades relacionadas à análise, ao estudo de viabilidade técnica e ao controle de projetos de engenharia por meio do Sistema de Projetos de Engenharia (SPE);
- projetar, contratar e fiscalizar obras e serviços de engenharia diversos em organizações militares por meio do Sistema de Obras Militares (SOM);
- executar obras e serviços de engenharia de infraestrutura física em cooperação com outros órgãos governamentais por meio do Sistema de Obras de Cooperação (SOC);
- realizar a aquisição, controle do acervo e vida útil, emprego, descarga e alienação dos materiais de Engenharia por meio do Sistema de Material de Engenharia (SME); e
- preservar o Meio Ambiente e controlar o patrimônio imobiliário jurisdicionado ao Exército Brasileiro por meio do Sistema de Patrimônio Imobiliário e Meio Ambiente (SPIMA).

Em cooperação com o Ministério da Infraestrutura, o Departamento Nacional de Estradas de Ferro (DNEF), o Departamento Nacional de Estradas de Rodagem (DNER), e instituição sucessora, o Departamento Nacional de Infraestrutura de Transportes (DNIT) e outros órgãos federais, o SEEx executou diversas obras de grandes eixos rodoviários e ferroviários, além da construção de portos e aeroportos em todo o território nacional. No Norte e no Nordeste, entre as décadas de 1950 e 1970, executou obras de implantação e construção rodoviárias, como o início da implantação dos 4.918 km da BR-230, conhecida como Transamazônica,

e 1.114 km da BR-116, com o objetivo de estabelecer a conexão entre as principais cidades da região, de amenizar os impactos da seca devastadora no semiárido e consequentemente de promover o desenvolvimento regional.

Posteriormente na década de 1990, os esforços foram mais intensificados na conservação e restauração de rodovias federais, a exemplo da restauração de 196 km da BR-319 entre Porto Velho e divisa entre Amapá e Roraima. No setor ferroviário, o Sistema atuou em diversas obras de extrema importância, como: na implantação da estrada de ferro Paraná-Mato Grosso em 1901; na ligação de Uberlândia à Brasília e na construção de 60 km de ferrovia interligando Piripiri a Teresina na década de 1960. No ano de 1950, o 1º Batalhão Ferroviário foi responsável pela construção da ferrovia do Tronco Principal Sul, no trecho que abrangia desde o Rio Canoas até o Rio Pelotas (Figueiredo *et al.*, 2014).

Dutra (2017) explica que no início deste século houve um significativo aumento de recursos decorrente dos investimentos realizados e da diversificação de parceiros do Exército Brasileiro, especialmente do esforço despendido pelo DEC para estabelecer novas parcerias com outros órgãos governamentais. Isso possibilitou a recuperação de equipamentos e viaturas, assim como a retomada da capacitação do pessoal militar e civil após um hiato intelectual de décadas.

As consequências dessa decisão resultaram em benefícios significativos para o SEEx, que atualmente conta com tropas de engenharia treinadas e prontas para serem empregadas em missões em prol do desenvolvimento nacional, integrar Forças de Paz ou prestar apoio à Defesa Civil, além de resultar em um grandioso acervo de obras de infraestrutura de transporte para o Exército Brasileiro (Tabela 3).

Tabela 3. Acervo de obras de infraestrutura de transporte executadas pelo SEEx no período de 1901 a 2017

Acervo de obras de infraestrutura de transporte executadas pelo SEEx		
Descrição	**Unidade**	**Quantidade**
Rodovias (construção, pavimentação e rodovias vicinais)	km	26.900
Ferrovias	km	5.800
Aeroportos	un	13
Pontes e Viadutos	m	58.500
Túneis	m	47.500
Portos	un	3

Fonte: Dutra (2017).

Em setembro de 2020, o DEC e a Valec Engenharia, Construções e Ferrovias S.A., empresa pública vinculada ao Ministério da Infraestrutura com a função de construção e exploração de infraestrutura ferroviária, assinaram um Termo de Execução Descentralizada tendo como objeto a execução de 18,34 km da Ferrovia de Integração Oeste Leste (FIOL). A motivação para o instrumento passa pelo interesse recíproco em regime de colaboração mútua entre as partes envolvidas, com o objetivo de contribuir para um maior equilíbrio da matriz de transporte de carga do Brasil, o escoamento da produção e a melhoria da qualidade de vida da população (DEC, 2020). A parceria simboliza também a volta do SEEx às atividades de construção ferroviária.

3 A SEGURANÇA DA ICT PELO PRISMA DO SEEX

Nos Objetivos Nacionais de Defesa da PND, as ICs, entre elas a ICT por proporcionar a Capacidade de Mobilidade Estratégica (Brasil, 2023, p. 38), são apontadas como fatores de suporte às Forças Armadas para a realização da vigilância, controle e defesa do território (Brasil, 2023, p. 24), proporcionando ao Exército Brasileiro a capacidade de se fazer presente em todo território nacional (Brasil, 2023, p. 51).

Ao passo que a revisão da PND estabelece uma relação de dependência das Forças Armadas com a ICT, a revisão da END inverte essa relação, atribuindo de forma clara e objetiva ao Exército Brasileiro a responsabilidade pela segurança, especificamente pela proteção, das ICs lançando mão das atividades realizadas pelo SEEx:

> Decorrente da estratégia da presença, **o Exército** [...]. **Participará, ademais, da proteção integrada de Estruturas Críticas e da execução de obras de engenharia em todo o território nacional**, em proveito do desenvolvimento do País (Brasil, 2023, p. 54, grifo nosso).

E complementa a atribuição de responsabilidade às Forças Armadas de contribuir com a segurança da ICT na Estratégia de Fortalecimento do Poder Nacional, dentro do Objetivos Nacional de Garantir a soberania, o patrimônio nacional e a integridade territorial, e do Objetivo de Incrementar a projeção do Brasil no concerto das nações e sua inserção em processos decisórios internacionais:

> AED-2 **Contribuir para o incremento do nível de segurança das Estruturas Críticas** de sistemas de captação, tratamento e distribuição de água; geração e distribuição de energia elétrica; **transporte**; produção e distribuição de combustíveis; e comunicações, entre outros (Brasil, 2023, p. 63 e 73, grifo nosso).

Além das disposições legais presentes nas Políticas Nacional de Defesa e Estratégia Nacional de Defesa, a Lei Complementar nº 97 (Brasil, 1999) estabelece, em seu artigo 16º, a atribuição subsidiária geral das Forças Armadas de colaborar com o desenvolvimento nacional e a defesa civil. Da mesma forma, o artigo 17º, alínea A, estabelece a atribuição específica do Exército Brasileiro de cooperar com órgãos públicos federais, estaduais e municipais, bem como, em situações excepcionais, com empresas privadas, na execução de obras e serviços de engenharia.

O Plansic (Brasil, 2022), ao distribuir as responsabilidades entre os Ministérios para a elaboração dos Planos Setoriais de segurança de ICs, considerou o Ministério da Infraestrutura como o responsável por implementar as ações estratégicas e elaborar os planos relativos à ICT. No mesmo texto, de forma complementar, é aberta a possibilidade de que outros órgãos e entidades públicos e privados detentores de conhecimento na proteção de ICs participem da elaboração e desenvolvimento dos planos específicos.

Observando o que se colocou de forma literal nas PND/END (Brasil, 2023) sobre o papel do Exército Brasileiro na proteção e na segurança das ICs nacionais, pode-se classificar a

instituição como possuidora do conhecimento específico necessário a atuar com o Ministério da Infraestrutura no desempenho de suas atividades relacionadas à segurança da ICT.

4 CONSIDERAÇÕES FINAIS

Nenhuma das definições do que constitui uma IC, conforme constatado pela revisão bibliográfica, pode ser considerada rigorosa. A literatura apresenta certas limitações, porém oferece margem para interpretação quanto às infraestruturas que se enquadram nessa definição. Essencialmente, o desafio enfrentado pelos governos nacionais reside em identificar e minimizar o impacto esperado sobre as ICs diante de qualquer tipo de risco ou ameaça.

Para o caso de países que integram à OCDE, a exemplo dos EUA e de países da União Europeia, pelo fato de estarem mais sujeitos a ameaças de terrorismo, os instrumentos de segurança de ICs encontram-se em um maior nível de maturidade quando comparados ao do Brasil, inclusive com a participação de entidades vocacionadas exclusivamente às atividades de proteção e de gerenciamento de riscos, como a CISA nos EUA e o CPNI no Reino Unido.

Ao observar a ICT, nota-se que praticamente todos os países que passaram pelo levantamento acerca da classificação dos setores essenciais, definiram que o setor de transportes é considerado uma IC dado o papel fundamental que desempenha no funcionamento da cadeia logística de diversos serviços essenciais à sociedade. A sociedade, em qualquer nível, não conta com a infraestrutura de transportes, especialmente com a rede de estradas, apenas para a mobilidade diária e para o transporte de bens e serviços, mas também como um sistema auxiliar ao socorro e resgate de pessoas e de ativos, e ainda por permitir as ações emergenciais ou de reparação a outras infraestruturas atingidas por ações adversas.

A vastidão territorial do Brasil e a diversidade de suas atividades produtivas demandam uma infraestrutura eficiente e abrangente. O transporte de passageiros possibilita a mobilidade da força de trabalho e promove a integração entre as diferentes regiões, impulsionando inclusive o turismo, enquanto o transporte de cargas é responsável pela distribuição dos insumos necessários à produção e ao escoamento dos insumos e produtos, conectando produtores, indústrias e consumidores em um complexo sistema logístico.

Pelo prisma da gestão e mitigação de riscos, percebeu-se que o fenômeno climático das chuvas intensas é o responsável pela totalidade das ameaças predominantes às quais está sujeita a ICT brasileira. Ações com o intuito de aumentar a proteção e a resiliência das infraestruturas, como obras de adaptação dos parâmetros de drenagem, no entanto, podem reduzir em quase pela metade os riscos a alagamentos e inundações, resultando inclusive numa diminuição dos custos globais de manutenção em até 0,9%. Do ponto de vista da aplicação de medidas não estruturais[3], políticas públicas abrangentes podem também limitar o risco de interrupções nos serviços essenciais de transporte e aumentar a capacidade de se recuperar rapidamente após um impacto.

Os instrumentos legais para a defesa nacional, consolidados nos níveis político e estratégico por intermédios das PND/END (Brasil, 2023), abrem espaço para o Exército Brasileiro atuar

3 Medidas não estruturais são aquelas que não envolvem a execução de obras ou serviços de engenharia. Podem ser políticas públicas, como campanhas de conscientização, por exemplo.

na segurança da ICT por meio da utilização de mecanismos a nível tático que podem, inclusive, subsidiar a elaboração do Plano Setorial de transportes previsto no Plansic.

A atribuição complementar (Brasil, 1999) permitiu à instituição ainda, especificamente ao SEEx, a execução de obras e serviços de engenharia em todo o território nacional, inclusive lançando mão de parcerias com empresas privadas e outros órgãos governamentais, que desencadearam a construção de uma infraestrutura de transporte terrestre equivalente ao tamanho da malha ferroviária da Suíça (CIA, 2023a) e da malha rodoviária da Croácia (CIA, 2023b).

Sabendo que o DEC é o único órgão da administração pública federal capaz de realizar obras de infraestrutura por execução direta, e olhando o extenso acervo de obras bem sucedidas realizadas em mais de um século pelo SEEx, seria um equívoco estratégico para Pastas Ministeriais encarregadas da implantação, manutenção e desenvolvimento de infraestruturas de transportes, como o Ministério da Infraestrutura, não requisitarem o apoio do Exército Brasileiro, por intermédio do Ministério da Defesa, na participação no Plano Setorial da ICT.

Da análise da relação entre as Forças Armadas, mais especificamente o Exército Brasileiro, e a infraestrutura de transporte do Brasil nas PND/END (Brasil, 2023), percebe-se a existência de relação causal cíclica (Figura 5) entre as missões constitucionais e complementares da Força Terrestre e a segurança da ICT, pois, ao mesmo tempo que as Forças dependem da plena disponibilidade das redes rodoviárias e ferroviárias para ter assegurada a Capacidade de Mobilidade Estratégica, o Exército, por sua vez, deve proporcionar a segurança das estruturas críticas existentes, além de executar novas obras em todo o território brasileiro, colaborando com o desenvolvimento nacional e a defesa civil (Brasil, 1999).

Figura 5. Relação de causa e efeito cíclica entre a ICT e o Exército Brasileiro

Fonte: elaborado pelo autor.

Quando comparados os mecanismos de segurança de ICs brasileiros aos dos EUA e da União Europeia, nota-se que ainda há um longo caminho a ser trilhado para se alcançar um nível adequado de gerenciamento e mitigação de riscos. Ainda assim, a ausência de legislação a nível tático específica para a segurança da ICT não impediu que o Sistema de Engenharia do Exército

Brasileiro estivesse sempre capacitado a atuar projetando, executando e fiscalizando obras de construção e manutenção de infraestruturas de transporte em diversos ambientes e regiões.

Ainda que não esteja sujeita à iminência de ataques terroristas ou de inimigos, a sociedade brasileira precisa estar a par dos riscos aos quais está sujeita, principalmente aqueles relacionados às chuvas intensas, pois são as responsáveis pela totalidade das ameaças predominantes à ICT.

O presente artigo, mesmo que tenha aprofundado um assunto pouco abordado na literatura nacional, limitou-se a estudar as relações do SEEx com a segurança de tipos restritos de infraestruturas de transportes, a exemplo das estruturas físicas de rodovias e de ferrovias. Como mencionado na introdução, a ICT de um país pode englobar ainda as estruturas físicas de portos e de aeroportos e o sistema de transporte de passageiros. Isto posto, sugere-se que próximos estudos abordem a relação do SEEx com a segurança de outros ativos que compõem a ICT brasileira, e recomenda ainda que, após a elaboração do Plano Setorial de segurança para o setor de transporte, seja reavaliada a atuação do SEEx diante das metas estabelecidas. Recomenda-se ainda que seja estudada a atuação do SEEx na manutenção da integridade da IC do país, apresentando compilação de dados históricos e avaliação do desempenho do Sistema, preferencialmente recorrendo-se a métodos de análise socioeconômica de programas e projetos.

Por fim, conclui-se que o SEEx tem colaborado com a segurança da ICT brasileira de forma objetiva ao atuar no gerenciamento e mitigação dos riscos por meio da execução de obras e serviços de engenharia, proporcionando uma maior resiliência às infraestruturas físicas terrestres.

REFERÊNCIAS

ARGYROUDIS, Sotirios; MITOULIS, Stergios; HOFER, Lorenzo; ZANINI, Mariano; TUBALDI, Enrico; FRANGOPOL, Dan. Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. **Science of the Total Environment**, [*s. l.*], v. 714, 136854, 2020.

ARRIGHI, Chiara; PREGNOLATO, Maria; CASTELLI, Fabio. Indirect flood impacts and cascade risk across interdependent linear infrastructures. **Natural Hazards and Earth System Sciences**, [*s. l.*], n. 21, p. 1955-1969, 2021.

BRASIL. **Resolução nº 683, de 05 de outubro de 2017**. Aprova o Regulamento de Compartilhamento de Infraestrutura de Suporte à Prestação de Serviço de Telecomunicações. Brasília, DF: Presidência da República, 2017a.

BRASIL. **Decreto nº 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 22 nov. 2018a.

BRASIL. EXÉRCITO BRASILEIRO. **A Engenharia nas Operações**. EB70-MC-10.237. 1. ed. Brasília, DF: Ministério da Defesa, DF: Presidência da República, 2018b.

BRASIL. EXÉRCITO BRASILEIRO. **Regulamento do Departamento de Engenharia e Construção**. EB10-R-04.001. Brasília, DF: Ministério da Defesa, 2021.

BRASIL. EXÉRCITO BRASILEIRO. **Manual de Campanha - Operações**. EB70-MC-10.223. 5. ed. Brasília, DF: Ministério da Defesa, 2017b.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, DF: Presidência da República, 2008.

BRASIL. **Decreto nº 10.569, de 9 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 9 dez. 2020.

BRASIL. **Decreto nº 11.200, de 15 de setembro de 2022**. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 15 set. 2022.

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. Brasília, DF: Presidência da República, 9 jun. 1999.

BRASIL. **Lei nº 12.379, de 6 de janeiro de 2011**. Dispõe sobre o Sistema Nacional de Viação - SNV. Brasília, DF: Presidência da República, 6 jan. 2011.

BRASIL. MINISTÉRIO DOS TRANSPORTES. **Corredores Logísticos Estratégicos**. Brasília: Ministério dos Transportes. DF: Ministério dos Transportes, 2024. Disponível em: https://www.gov.br/transportes/pt-br/assuntos/PIT/politica-e-planejamento/cle. Acesso em 13 fev. 2025.

BRASIL. **Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END)**: encaminhadas, em 22 de julho de 2020, para apreciação do Congresso Nacional. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf. Acesso em: 6 jun. 2023.

CÂMARA aprova atualização da Política Nacional de Defesa. **Agência Câmara de Notícias**, Brasília, DF, 15 maio 2024. Disponível em: https://www.camara.leg.br/noticias/1062814-CAMARA-APROVA-ATUALIZACAO-DA-POLITICA-NACIONAL-DE-DEFESA. Acesso em: 4 fev. 2025.

CIA - CENTRAL INTELLIGENCE AGENCY. **Country Comparisons – Railways**. Disponível em: https://www.cia.gov/the-world-factbook/field/railways/country-comparison. Acesso em 24 jun. 2023a.

CIA - CENTRAL INTELLIGENCE AGENCY. **Country Comparisons – Roadways**. Disponível em: https://www.cia.gov/the-world-factbook/field/roadways/country-comparison. Acesso em 24 jun. 2023b.

DEC - DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO. **Termo de Execução Descentralizada - TED Nº 001/2020**. Brasília, DF, 08 set. 2020. Disponível em: http://www.dec.eb.mil.br/images/PERMANENTE/TED/SEI_MINFRA_-_2769928_-_TED_001-2020-assinado.pdf. Acesso em: 19 jun. 2023.

DUTRA, Antônio. **A institucionalização da participação do Sistema de Obras de Cooperação do Exército Brasileiro em serviços de infraestrutura no país – uma proposta**. 2017. 59 f. Trabalho de Conclusão de Curso – Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia, Rio de Janeiro, 2017.

ESTADOS UNIDOS DA AMÉRICA. Cybersecurity and Infrastructure Security Agency (CISA). **A Guide to Critical Infrastructure Security and Resilience**. Washington, DC, 2019.

ESTADOS UNIDOS DA AMÉRICA. Cybersecurity and Infrastructure Security Agency (CISA). **Infrastructure Security**. Disponível em: https://www.cisa.gov/infrastructure-security. Acesso em: 6 jun. 2023.

FIGUEIREDO, Washington; OLIVEIRA, Emerson; SANTANA, José; ALVES, Edmar. **A engenharia do exército na construção do desenvolvimento nacional**. Brasília, DF: Departamento de Engenharia e Construção, 2014. 294 p.

INTERNATIONAL STANDARDS ORGANIZATION (ISO). **ISO 3166**: codes for the representation of names of countries. 4. ed. Genebra: [*s. n.*], 2020.

KOKS, E.; ROZENBERG, J.; ZORN, C.; TARIVERDI, M.; VOUSDOUKAS, M.; FRASER, S.; HALL, J.; HALLEGATTE, S. A global multi-hazard risk analysis of road and railway. **Nature Communications**, [*s. l.*], v. 10, n. 2677, 2019.

LIU, Wei; SONG. Zhaoyang. Review of studies on the resilience of urban critical infrastructure networks. **Reliability Engineering and System Safety**, [*s. l.*], v. 2020, n. 193, 2019.

MATTSSON, Lars-Göran; JENELIUS, Erik. Vulnerability and resilience of transport systems – A discussion of recent research. **Transportation Research Part A**, [*s. l.*], v. 81, p 16-34, 2015.

MOTEFF, John; COPELAND, Claudia; FISCHER, John. Critical Infrastructures: **What Makes an Infrastructure Critical?** Congressional Research Service – The Library of Congress. EUA, 29 jan. 2003. Disponível em: https://irp.fas.org/crs/RL31556.pdf. Acesso em: 25 jun. 2023.

NATÁRIO, Rui; NUNES, Paulo. Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas. **Revista Militar**, Lisboa, n. 2547, p 249-286, 2014.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OCDE). **Good Governance for Critical Infrastructure Resilience**. OECD Reviews of Risk Management Policies. Paris: OECD Publishing, 2019

PAIVA, Iure. Política Nacional de Defesa e proteção da infraestrutura energética crítica no Brasil. **Austral: Revista Brasileira de Estratégia e Relações Internacionais**, [*s. l.*], v. 5, n. 10, 2016.

POLÍTICA Nacional de Defesa é aprovada no Senado e segue para Câmara. **Agência Senado**, Brasília, DF, 22 junho 2022. Disponível em: https://www12.senado.leg.br/noticias/noticias/materias/2022/06/02/politica-nacional-de-defesa-e-aprovada-no-senado-e-segue-para-camara. Acesso em: 25 jun. 2023.

REINO UNIDO. Centre for the Protection of National Infrastructure (CPNI). **Critical National Infrastructure**. Disponível em: https://www.cpni.gov.uk/critical-national-infrastructure-0. Acesso em: 6 jun. 2023.

ROCHA, Paulo Cesar. **A relação entre a gestão de riscos integrada em uma organização com infraestrutura crítica e as questões de Defesa Nacional**. 2019. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa) - Escola Superior de Guerra, Brasília, DF, 2019.