OBSERVATÓRIO MILITAR da Praia Vermelha
http://ompv.eceme.eb.mil.br/

A mobilização de competências e a geração de forças para a Defesa Nacional.

Rodrigo Carran Oliveira dos Santos
Cofundador da Vulcan Defense e especialista em Segurança da Informação, Governança e Gestão de Riscos Cibernéticos.
Primeiro-Tenente da Reserva de 2ª Classe (R/2) do Exército Brasileiro

1. Introdução

Uma das capacidades estratégicas mais caras a uma Nação é a sua capacidade de mobilizar-se para responder a uma crise. Imaginemos um cenário no qual um operador elétrico perde o controle sobre parte de sua rede de supervisão. Quase ao mesmo tempo, três hospitais de referência relatam indisponibilidade de sistemas de suporte à vida, um terminal portuário suspende a movimentação de contêineres e um fornecedor estrangeiro comunica, sem alarde, que o *firmware* de uma estrutura crítica não receberá mais atualizações.

Não há tropa cruzando as nossas fronteiras e não há declaração de guerra, entretanto, o país precisa, de forma urgente, reunir capacidades críticas. Engenheiros, operadores nacionais, pesquisadores, gestores, cientistas, criptógrafos, fabricantes e militares que nunca trabalharam juntos. Nesse momento, a pergunta que importa não diz respeito aos meios que o país possui, mas sim: quem convoca? Quem são os convocados? Com base em qual lista? Sob qual autoridade? E em quanto tempo? O país começou a tentar responder a essas perguntas em 2007, com a Lei nº 11.631, de 27 de dezembro de 2007, que criou o Sistema Nacional de Mobilização — o SINAMOB — regulamentado pelo Decreto nº 6.592/2008. Seu desenho permanece atual: um conjunto de órgãos, sob coordenação central do Ministério da Defesa, organizado em direções setoriais nas áreas política, econômica, social, psicológica, de segurança e inteligência, de defesa civil, científico-tecnológica e militar. A composição foi atualizada pelo Decreto nº 11.183/2022 para acompanhar a estrutura do Poder Executivo.

A lei permite ao SINAMOB requisitar de órgãos públicos, pessoas e entidades as informações necessárias às suas atividades e lhes confere prioridade absoluta durante a execução da Mobilização. Trata-se de instrumento aprovado pelo Congresso e regulamentado. Sua doutrina básica, porém, permanece a 1ª edição de 1987, aprovada pela Secretaria-Geral do Conselho de Segurança Nacional — anterior à Constituição, ao Ministério da Defesa e à Lei do SINAMOB. O Ministério da Defesa a registra como “em vigor (revisão)”.

Ao que parece, a lei e a estrutura foram atualizadas, porém o fundamento doutrinário ainda não. O desafio é transformar a resposta jurídica em capacidade comprovada, mas antes disso é preciso saber medi-la. Portanto, o Brasil não carece de base legal. Carece de prática recorrente, mensurável e capaz de alterar decisões, e este artigo se propõe a abrir esse diálogo e apontar caminhos que possam indicar possíveis soluções.

2. As primeiras iniciativas em mobilização nacional

Em outubro de 2024, a Escola Superior de Defesa sediou o 1º Exercício de Planejamento de Mobilização Nacional, promovido pela Chefia de Logística do Estado-Maior Conjunto das Forças Armadas, com representantes do SINAMOB e instituições convidadas. A despeito do mérito da iniciativa, dezesseis anos separaram a regulamentação do sistema de seu primeiro exercício integrado. O cenário foi o clássico: dois países fictícios em disputa por uma região rica em recursos hidrelétricos. Em agosto de 2025, nova edição, integrada à Operação ATLAS, confirmou a

continuidade; porém, novos avanços precisam ser incorporados, a exemplo dos cenários híbridos e assimétricos, reproduzindo formas de coerção capazes de produzir efeitos estratégicos, antes que sua autoria ou natureza jurídica estejam esclarecidas.

Entretanto, há boas práticas no Brasil que ensaiam crises tecnológicas. Desde 2018, o Exercício Guardião Cibernético (EGC), sob responsabilidade do Ministério da Defesa e coordenado pelo Exército Brasileiro, por meio do Comando de Defesa Cibernética (ComDCiber), simula ataques contra infraestruturas críticas. Em setembro de 2025, sua sétima edição reuniu 169 organizações e cerca de 750 participantes de vinte países. Em sua oitava edição, realizada de 21 a 25 de setembro de 2026, o EGC 8.0 reuniu cerca de 1.300 participantes, aproximadamente 300 organizações e representantes de 14 países, com atividades em Brasília e nos polos de Belém, Manaus, Recife, Curitiba, São Paulo e Rio de Janeiro. No polo fluminense, as atividades ocorreram na Firjan SENAI Digitech. Os cenários envolveram a resposta a incidentes, a continuidade de serviços essenciais e a coordenação entre instituições públicas, privadas e militares, incluindo exercícios relacionados ao setor nuclear. A amplitude dessa prática oferece um ambiente concreto para avaliar a prontidão e a articulação de capacidades estratégicas.

Em 2025, o Guardião Cibernético e o Exercício de Planejamento de Mobilização Nacional ocorreram na Escola Superior de Defesa. Até o levantamento documental realizado para este artigo, não foi identificado mecanismo público que estabeleça uma integração sistemática entre os resultados dos dois exercícios. A edição de 2026 do Guardião reforça a relevância dessa questão: multiplicam-se os participantes, os polos e os cenários de crise, mas ainda é necessário demonstrar como os aprendizados dessas simulações podem alimentar formalmente o planejamento de mobilização nacional.

O Guardião testa a resiliência e a coordenação dos operadores diante de ataques simulados; o exercício de mobilização avalia a convergência das capacidades do Estado diante de hipóteses estratégicas. Sem uma interface formal e verificável, não é possível assegurar que as carências identificadas em um ciclo orientem os documentos produzidos no outro. A pergunta central permanece: quem identifica, convoca e habilita as competências de que os operadores necessitam quando a crise excede sua capacidade instalada? A lacuna a investigar está na articulação entre exercícios. Acoplar ciclos que já possuem público e estrutura pode ser uma decisão de governança mais econômica do que criar novos instrumentos.

A lei define Mobilização Nacional como as atividades destinadas a capacitar o país para ações estratégicas de Defesa diante de agressão estrangeira. O Decreto nº 6.592/2008 inclui ameaças ou atos lesivos à soberania, ao povo ou às instituições, mesmo sem invasão. A Doutrina Militar de Defesa de 2025 incorpora a zona cinza: a faixa ambígua em que as fronteiras entre paz, crise e conflito armado perdem nitidez.

O conceito já está na doutrina, porém o importante é convertê-lo em gatilho de preparo. A agressão pode chegar como comprometimento da cadeia de software, interrupção de serviços essenciais, negativa de suporte a sistema homologado ou manipulação informacional. Essas hipóteses não produzem automaticamente a certeza jurídica necessária à Mobilização formal. Por isso, o SINAMOB precisa ser preparado e exercitado antes que o Estado discuta, sob pressão, se o limiar legal foi alcançado.

Não se propõe acionar fora da lei poderes reservados à Mobilização. Propõe-se cumprir o preparo contínuo, metódico e permanente previsto no regulamento, incorporando tecnologias e dependências que ganharam centralidade desde 2007. Como a Mobilização toca requisição, propriedade privada, dados pessoais e liberdade econômica, seus limites devem ser desenhados na normalidade, com transparência e supervisão.

3. A nova lógica da mobilização por competências

Nossa tradição institucional de mobilização é demográfica. O serviço militar obrigatório, o alistamento, a reserva: o país sabe, com razoável

eficiência, localizar e convocar pessoas em função de idade e de situação militar. É uma capacidade real, construída ao longo de gerações.

Mas a crise descrita no início não pede somente efetivo. Pede competência nominal e na maioria das vezes escassa: quem opera determinado sistema industrial, domina engenharia reversa de *firmware*, mantém uma linha nacional de produção ou já respondeu a incidente em tecnologia operacional. Não há evidência pública de cadastro nacional, intersetorial e periodicamente exercitado que permita localizar essas pessoas, confirmar sua disponibilidade e integrá-las a equipes prontas. Cadastros isolados não formam reserva de capacidade; aquilo que não foi integrado em paz dificilmente será improvisado sob crise.

Aqui está a lacuna central do ecossistema brasileiro de mobilização estratégica: temos reserva de efetivo e não temos reserva de capacidade. O ativo mais demorado de recompor não é uma plataforma e sim uma equipe que acumulou conhecimento, confiança e experiência operacional. Perder um profissional crítico custa anos que a Defesa pode não dispor.

Essa constatação corre o risco de permanecer retórica enquanto não houver um número que a torne verificável. Proponho uma métrica: o Tempo de Mobilização de Competência, ou TMC.

Defino o TMC como o intervalo entre o momento em que uma crise é caracterizada e o momento em que a equipe dotada das competências necessárias está constituída, autorizada e efetivamente operando sobre o problema. É um número, não um conceito, e decompõe-se em quatro parcelas mensuráveis: identificação, que responde a quem sabe fazer aquilo; localização, que responde ao lugar onde essa pessoa está e se está disponível; habilitação, que compreende vínculo, contrato, credenciamento de segurança e concessão de acesso; e integração, que vai da chegada da pessoa até a equipe operando de forma coordenada.

Minha hipótese, formada na prática de resposta a incidentes, é que a parcela dominante não é a identificação, mas a habilitação. Costuma-se saber quem sabe fazer; o que não se consegue é colocar essa pessoa dentro do perímetro, com instrumento contratual válido, credencial concedida e acesso liberado, dentro da janela em que a intervenção ainda importa. Seria uma falha administrativa com consequência estratégica. Mas trata-se de hipótese, não de dado — e é exatamente por isso que esse tempo precisa ser medido em vez de estimado. Um país que não conhece a decomposição do próprio TMC não sabe onde investir para reduzi-lo, e corre o risco de gastar em capacidade técnica quando o gargalo parece ser jurídico-administrativo.

Não há registro público de que o TMC tenha sido medido em qualquer exercício nacional. Proponho que o primeiro exercício híbrido do SINAMOB tenha como produto mínimo obrigatório esse número, decomposto nas quatro parcelas, por setor crítico. Um exercício que produza apenas isso já terá entregado mais do que qualquer diagnóstico narrativo, porque terá convertido uma preocupação em linha de base — e linha de base é o que permite estabelecer meta, cobrar prazo e justificar orçamento.

A experiência de participação no EGC 8.0, em setembro de 2026, no hub do Rio de Janeiro, representando a Vulcan Defense em atividades de controle da linha temporal de simulações e de gestão de crise, reforça essa reflexão. A observação das dinâmicas de coordenação nos cenários de Defesa e Nuclear evidenciou a utilidade de distinguir o tempo de reação técnica do tempo necessário para identificar, autorizar e integrar competências externas. Essa experiência fundamenta uma questão de pesquisa; não constitui, por si só, mensuração do Tempo de Mobilização de Competência (TMC) nem comprovação de integração formal com o SINAMOB.

4. Transformando norma em ação estratégica

Para converter arquitetura normativa em capacidade comprovada, as dimensões jurídica, humana, científico-industrial e operacional do SINAMOB precisam operar de forma integrada.

O primeiro movimento é construir o módulo que falta. No Subsistema Setorial de Mobilização Científico-Tecnológica, um módulo permanente de preparo tecnológico e cibernético deve estabelecer gatilhos de planejamento, alerta, exercício e coordenação anteriores à caracterização formal de agressão. A Mobilização e os poderes extraordinários continuariam submetidos à Constituição e à lei; antes da crise, porém, devem estar definidos quem avalia, recomenda e decide, sob qual evidência e controle.

Isso não duplica governança. A Política Nacional de Cibersegurança, de 2023, e a Estratégia Nacional de Cibersegurança, instituída pelo Decreto nº 12.573/2025 e dotada de eixo de soberania e governança, orientam a coordenação permanente. O Conselho Nacional de Cibersegurança (CNCiber) acompanha essa agenda; seu presidente é o representante do GSI/PR, órgão que também exerce a Secretaria-Executiva do colegiado. Coordenar segurança e resiliência na normalidade é função diferente de mobilizar capacidade sob crise. O módulo daria ao SINAMOB a interface técnica que lhe falta e ao Comitê um caminho institucional quando a resposta exceder a coordenação ordinária, preservada a competência de cada órgão.

O segundo movimento é criar uma Reserva Nacional de Competências Estratégicas: cadastro voluntário de civis e militares em cibersegurança, tecnologia operacional, criptografia, energia, telecomunicações, logística, materiais e saúde. Por ser um mapa de alvos humanos, sua proteção é condição de existência: finalidade, minimização, compartimentação setorial, acesso auditável e relatório de impacto. No tratamento exclusivamente destinado à defesa nacional ou à segurança do Estado, incidirá o regime do art. 4º, III, e §§ 1º a 4º da LGPD, sob tutela pública e legislação específica; nos demais, as bases e salvaguardas ordinárias.

O desafio é tornar esse cadastro um instrumento de vínculo permanente. O vínculo exige formação, exercícios, convocação previsível e contrapartida individual: certificação estatal, capacitação e remuneração ou compensação por disponibilidade e acionamento. A reserva só reduzirá o TMC se atacar a parcela dominante: credenciamento prévio, contratos de prontidão celebrados na normalidade — inclusive com empresas detentoras das competências e cessão temporária de especialistas — e acesso predefinido. Universidades, institutos federais e escolas militares formam a rede de preparação.

A reserva também deve reter talentos. Em 2024, o Conhecimento Brasil recebeu 2.572 propostas de cientistas brasileiros em 56 países; a demanda aproximou-se de R$ 2 bilhões. O Estado respondeu: contratou 599 projetos de atração e fixação, com R$ 604 milhões, e aprovou 640 redes, com R$ 228,5 milhões. O dado não demonstra inércia; revela capacidade dispersa, demanda superior à oferta e ausência de vínculo com missões de Defesa. Residências Tecnológicas de Defesa poderiam reunir pesquisadores, engenheiros e militares por doze a vinte e quatro meses, trabalhando sobre missão real, com bolsa competitiva, laboratório, carreira previsível e regras prévias de propriedade intelectual.

O terceiro movimento é mapear dependências críticas. O Currículo Lattes registra o que o País sabe fazer; não há registro equivalente daquilo que não sabe. Proponho um Balanço Nacional de Dependências Críticas, anual, com parte pública e parte classificada, respondendo: o que o Brasil não produz, quanto tempo levaria para produzir e qual linha nacional poderia assumir a encomenda. O balanço incluiria exercício de conversão industrial coerente com a Política Nacional da Base Industrial de Defesa (Decreto nº 11.169/2022): quais fábricas civis assumem produção de Defesa e em que prazo.

Há ainda um recorte ignorado: exigimos origem e rastreabilidade no aço, mas não no código. Alinhados à Estratégia Nacional de Cibersegurança, os editais de Defesa devem exigir inventário de componentes de software (SBOM) em padrão aberto, atestações de integridade da cadeia de desenvolvimento e condições nacionais de manutenção.

A patente só será capacidade nacional com protótipo, licenciamento, escala e usuário. O Balanço deve orientar uma Linha de Maturação Tecnológica de

Defesa, financiada por entregas — prova de conceito, teste operacional, licenciamento e produção — e executada por universidade, empresa, Forças Armadas e Base Industrial de Defesa. O objetivo é evitar que conhecimento financiado pelo Brasil só se torne capacidade depois de atravessar a fronteira.

O quarto movimento é realizar o ensaio que muda o orçamento. Basta acoplar os ciclos existentes: carências do Guardião alimentariam os documentos do SINAMOB, e as hipóteses de mobilização orientariam os cenários cibernéticos. O exercício integrado seria anual, alternando cenários e incluindo crise cibernética, energética, logística e informacional, com participação dos subsistemas e, sob regras adequadas, de operadores privados de infraestruturas críticas. Cada edição deveria medir e publicar o TMC e fazer seu relatório alimentar formalmente o planejamento e a proposta orçamentária do ciclo seguinte, com destino no plano plurianual e nas ações do Ministério da Defesa.

Um exercício agendado, porém, mede a melhor hipótese: credenciais providenciadas na véspera, contratos assinados na semana anterior, pessoas avisadas. Para conhecer o TMC real, a rotina anual precisa ser complementada por chamadas de prontidão sem aviso prévio, de duração curta e escopo limitado, que verifiquem se o vínculo, a credencial e o acesso funcionam dentro de poucas horas. Exercícios sem efeito sobre prioridade, plano ou recurso perdem eficiência; exercícios que produzem consequência são os instrumentos mais econômicos de aprendizado estratégico do Estado.

5. O papel das lideranças estratégicas

O verdadeiro exercício de soberania está em testar e medir o SINAMOB, que já tem órgão central, doutrina, subsistemas e uma cadência de simulações. A Política e a Estratégia Nacional de Defesa, aprovadas pelo Decreto nº 12.725/2025, já apontam essa direção: a AED-03 determina aprimorar o SINAMOB, e a AED-04, coordenar com os órgãos setoriais o atendimento dos requisitos de infraestruturas de interesse da Defesa. O que falta é definir o método de entrega: o responsável, o prazo, o indicador e a consequência. O TMC oferece o indicador; o restante depende de decisão.

Uma agenda inicial deve conter a definição do módulo tecnológico e cibernético; a publicação do protocolo de acoplamento com o Guardião Cibernético e a metodologia do Balanço; a estruturação da primeira chamada da Reserva, com credenciamento e instrumento contratual resolvidos; e a marcação dos próximos exercícios, que deverão devolver ao País o seu primeiro TMC.

A ameaça à soberania não está somente atrelada à violação do território; manifesta-se também quando um país descobre, no meio de uma crise, que mesmo com a lei, a doutrina, o sistema e as pessoas — nunca havia medido quanto tempo levaria para reuni-las.

Rio de Janeiro - RJ, 15 de outubro de 2026.

Referência:

BRASIL. Lei nº 11.631, de 27 de dezembro de 2007. Dispõe sobre a Mobilização Nacional e cria o Sistema Nacional de Mobilização — SINAMOB.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

BRASIL. Decreto nº 6.592, de 2 de outubro de 2008. Regulamenta o disposto na Lei nº 11.631, de 27 de dezembro de 2007.

BRASIL. Decreto nº 11.183, de 25 de agosto de 2022. Altera o Decreto nº 6.592/2008 e atualiza a composição e a organização do SINAMOB.

BRASIL. Secretaria-Geral do Conselho de Segurança Nacional. Doutrina Básica de Mobilização Nacional. 1ª edição. Brasília, DF, 1987. Aprovada pela Exposição de Motivos nº 006, de 14 de setembro de 1987. Registrada pelo Ministério da Defesa como em vigor (revisão).

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. MD51-M-04 Doutrina Militar de Defesa. 3ª edição, 2025.

BRASIL. Ministério da Defesa. Escola Superior de Defesa. 1º Exercício de Planejamento de Mobilização Nacional, realizado de 17 a 25 de outubro de 2024.

BRASIL. Ministério da Defesa. Escola Superior de Defesa. Exercício de Planejamento de Mobilização Nacional, realizado de 11 a 15 de agosto de 2025, integrante da Operação ATLAS 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. GSI/PR participa do 7º Exercício Guardião Cibernético, que reuniu 20 países. 3 out. 2025.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança.

BRASIL. Decreto nº 12.725, de 18 de novembro de 2025. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional.

BRASIL. Decreto nº 11.169, de 10 de agosto de 2022. Institui a Política Nacional da Base Industrial de Defesa.

BRASIL. Conselho Nacional de Desenvolvimento Científico e Tecnológico. Programa Conhecimento Brasil: atração, fixação e formação de redes com pesquisadores brasileiros no exterior, 2024-2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 5962:2021: Information technology — SPDX Specification V2.2.1. Geneva: ISO/IEC, 2021.

BRASIL. Ministério da Defesa. Exercício Guardião Cibernético 8.0 reúne cerca de 1.300 participantes em Brasília. Publicado em 21 set. 2026, atualizado em 25 set. 2026. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/exercicio-guardiao-cibernetico-8-0-reune-cerca-de-1-300-participantes-em-brasilia/. Acesso em: 14 out. 2026.

BRASIL. Departamento de Trânsito do Estado do Rio de Janeiro. Detran RJ participa do maior exercício cibernético do Hemisfério Sul. 25 set. 2026. Disponível em: https://detran.rj.gov.br/noticias/detran-rj-participa-do-maior-exercicio-cibernetico-do-hemisferio-sul.html. Acesso em: 14 out. 2026.

BRASIL. Comissão Nacional de Energia Nuclear. CNEN participa do Exercício Guardião Cibernético 8.0. 24 set. 2026. Disponível em: https://www.gov.br/cnen/pt-br/assunto/ultimas-noticias/cnen-participa-do-exercicio-guardiao-cibernetico-8.0. Acesso em: 14 out. 2026.

BRASIL. Centro Gestor e Operacional do Sistema de Proteção da Amazônia. Censipam participa da abertura do Exercício Guardião Cibernético 8.0. 22 set. 2026. Disponível em: https://www.gov.br/censipam/pt-br/central-de-conteudos/noticias/censipam-participa-da-abertura-do-exercicio-guardiao-cibernetico-8.0. Acesso em: 14 out. 2026.

BRASIL. Agência Nacional de Águas e Saneamento Básico. ANA participa do Exercício Guardião Cibernético 8.0 com foco na proteção do espaço cibernético brasileiro e infraestruturas críticas. set. 2026. Disponível em: https://www.gov.br/ana/pt-br/assuntos/noticias-e-eventos/noticias-periodo-eleitoral-2026/ana-participa-do-exercicio-guardiao-cibernetico-8-0-com-foco-na-protecao-do-espaco-cibernetico-brasileiro-e-infraestruturas-criticas. Acesso em: 14 out. 2026.