UNIVERSIDADE FEDERAL DA BAHIA
ESCOLA POLITÉCNICA
DEPARTAMENTO DE ENGENHARIA AMBIENTAL
CURSO DE ESPECIALIZAÇÃO EM SEGURANÇA DE BARRAGENS: ASPECTOS TÉCNICOS E LEGAIS – TURMA IV

LEONARDO DAVID CARVALHO DE QUEIROZ

A SEGURANÇA CIBERNÉTICA CONTRA OS RISCOS DE CIBERATAQUES ÀS INFRAESTRUTURAS CRÍTICAS DO SETOR ÁGUA

Salvador
2024

LEONARDO DAVID CARVALHO DE QUEIROZ

A SEGURANÇA CIBERNÉTICA CONTRA OS RISCOS DE CIBERATAQUES ÀS INFRAESTRUTURAS CRÍTICAS DO SETOR ÁGUA

Trabalho de Conclusão de Curso, no formato de artigo científico, apresentado ao Colegiado do Curso de Especialização em Segurança de Barragens: Aspectos Técnicos e Legais – Turma IV, da Universidade Federal da Bahia, como requisito parcial para a obtenção do Título de Especialista em Segurança de Barragens.

Orientador: Dr. Rogério de Abreu Menescal

Salvador
2024

LEONARDO DAVID CARVALHO DE QUEIROZ

A SEGURANÇA CIBERNÉTICA CONTRA OS RISCOS DE CIBERATAQUES ÀS INFRAESTRUTURAS CRÍTICAS DO SETOR ÁGUA

Trabalho de Conclusão de Curso apresentado ao Colegiado do Curso de Especialização em Segurança de Barragens: Aspectos Técnicos e Legais – Turma IV, da Universidade Federal da Bahia, como requisito parcial para a obtenção do Título de Especialista em Segurança de Barragens.

Aprovado com média: _____

Banca examinadora

_____
Rogério de Abreu Menescal / Doutor em Recursos hídricos - ANA
Agência Nacional de Águas e Saneamento Básico – ANA

_____
Fabiano Costa de Almeida / Mestre em Sensoriamento Remoto – INPE
Agência Nacional de Águas e Saneamento Básico – ANA

_____
Yvonilde Dantas P Medeiros / Doutora em Hidrologia - Newcastle University
Universidade Federal da Bahia – UFBA

Salvador, ____ de _____ de 2024.

A SEGURANÇA CIBERNÉTICA CONTRA OS RISCOS DE CIBERATAQUES ÀS INFRAESTRUTURAS CRÍTICAS DO SETOR ÁGUA

RESUMO

A era da informação trouxe uma conectividade digital e produtividade econômica sem precedentes, mas também introduziu novas vulnerabilidades às relações humanas. À medida que nossa dependência da tecnologia cresce, também cresce a necessidade de medidas vigorosas de segurança cibernética, particularmente para a proteção das infraestruturas críticas do país.
Este artigo procura evidenciar a importância das infraestruturas críticas para a defesa nacional, como Barragens e Estações de Tratamento de Água, sua relação de interdependência com as outras infraestruturas estratégicas e as principais documentações governamentais vigentes sobre a segurança e a defesa cibernéticas acerca do tema.
Por fim, procura-se alertar sobre o desafio de implementação de políticas de proteção dos sistemas de infraestruturas críticas contra ameaças de ciberataques, o necessário estímulo do governo para com os empreendedores de barragens e concessionárias de abastecimento de água, em investimento para capacitação de pessoal e novas tecnologias, a fim de garantir a resiliência e a confiabilidade destes sistemas após um potencial ataque.

Palavras-chave: infraestruturas críticas; espaço cibernético; segurança cibernética; setor água; barragens; estações de tratamento de água; ataque cibernético; defesa cibernética.

ABSTRACT

The information age has brought unprecedented digital connectivity and economic productivity, but it has also introduced new vulnerabilities to human relationships. As our dependence on technology grows, so does the need for vigorous cybersecurity measures, particularly to protect the nation's critical infrastructure.
This article seeks to highlight the importance of critical infrastructures for national defense, such as Dams and Water Treatment Stations, their interdependent relationship with other strategic infrastructures and the main current government documentation on cyber security and defense on the topic.
Finally, we seek to raise awareness about the challenge of implementing policies to protect critical infrastructure systems against threats of cyberattacks, the necessary stimulus and support from the government towards entrepreneurs of dams and water supply concessionaires, in investment for training of personnel and new technologies, in order to guarantee the resilience and reliability of these systems after a potential attack.

Keywords: critical infrastructures; cyber space; cybersecurity; water sector; dams; water treatment stations; cyberattack; cyber defense.

1. INTRODUÇÃO

O mundo atual está cada vez mais digital e amplamente interconectado. É incontestável que as tecnologias têm se tornado cada vez mais presentes em todos os aspectos da vida humana, impactado e afetado a sociedade, a cultura, o modo como vivemos e interagimos com o mundo. O setor de sistemas automatizados, por exemplo, vem ganhando maior visibilidade e a sua utilização está em constante avanço.

Nos últimos anos, os serviços baseados em novas tecnologias vêm trazendo inúmeros benefícios aos usuários, mas também ampliando em muito a complexidade e a diversidade dos ambientes virtuais. Percebe-se, com isso, o aumento de vulnerabilidades e ameaças de segurança cibernética no mundo digital, onde os atacantes não respeitam fronteiras e, na maioria das vezes, suas invasões em sistemas de uso pessoal ou institucional sequer são notadas.

O espaço cibernético tem sido definido como um domínio global dentro do ambiente da informação que surge da interconexão das redes de dispositivos digitais interligados no planeta, incluindo Internet, redes de telecomunicações, sistemas de computadores incorporados, processadores e controladores. O ciberespaço não se refere apenas à infraestrutura material da comunicação digital, mas também ao universo de informações que ela abriga. Escondidos sob códigos de programação, os cibercriminosos se valem do anonimato – ao menos para a maioria dos usuários de recursos digitais – e da onipresença dos dispositivos eletrônicos na vida das pessoas para agirem.

Por não existirem fronteiras claramente definidas no espaço virtual, há dificuldade em se identificar e atribuir responsabilidades quando da ocorrência de ataques cibernéticos. Como todos estão sujeitos à legislação e à soberania de um Estado, os governos têm buscado evoluir suas normas e práticas internas para resguardar seus sistemas e sua população contra essas ameaças.

Geralmente, os ataques podem ser dissimulados ou assumidos e podem trazer impactos físicos ou não, que variam desde desfiguração de websites, perdas financeiras, parada de um serviço ou ainda a indisponibilização de uma infraestrutura crítica para o país. No Brasil, consideram-se Infraestruturas Críticas, as instalações, serviços e bens que se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional. Os serviços prestados por essas infraestruturas (energia, telecomunicações, finanças, transporte,

águas e outros) também compartilham do espaço cibernético e alguns deles suportam a própria existência. Esses serviços possuem dimensão estratégica, pois são essenciais para cidadãos, organizações e para o Estado, uma vez que desempenham papel tanto para a segurança e soberania nacional como para a integração e o desenvolvimento econômico sustentável do País. Dessa forma, problemas no fornecimento desses serviços podem acarretar transtornos e prejuízos ao próprio Estado, à sociedade, à população e ao meio ambiente.

Assim, sem haver a pretensão de esgotar o tema, o presente artigo propõe apresentar sua relevância e verificar se os empreendedores, órgãos e entidades governamentais que operam infraestruturas críticas do setor água, como barragens e plantas de tratamento, estão conscientes dos riscos associados a ciberataques e adotam boas práticas de segurança cibernética.

2. METODOLOGIA

O método de abordagem empregado à realização do trabalho foi a pesquisa bibliográfica, em que realizou-se um levantamento de material e obras com dados já analisados e publicados, como livros, artigos científicos, página de *web sites*, para entender e conhecer melhor o tema em estudo, sendo dividido em 3 (três) partes: em um primeiro momento, buscou-se identificar o conceito de infraestruturas críticas e sua interdependência com a área prioritária águas, a fim de demonstrar a relevância do assunto; em seguida, abordou-se a conceituação de cibersegurança e defesa cibernética, apresentando casos reais de ataques em infraestruturas hídricas no exterior; na terceira parte, é descrito um levantamento da política nacional acerca do tema, com os principais normativos relacionados à segurança cibernética; e por fim, nas considerações finais, buscou-se alertar os atores envolvidos sobre a importância de investimento e treinamento profissional para a proteção das Infraestruturas Críticas brasileiras do Setor Água.

3. INFRAESTRUTURAS CRÍTICAS

De acordo à Portaria nº 45 GSI/PR de 2009, em seu art. 2º, § 2º, consideram-se Infraestruturas Críticas, no Brasil, as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

O art. 3º da referida portaria elenca, entre os incisos I e V, as áreas prioritárias das infraestruturas que estão relacionadas à energia, à água, à rede de transporte, às telecomunicações e às finanças, sem prejuízo de outras que porventura vierem a ser definidas.

Nesse contexto, pode-se comparar a interdependência das infraestruturas críticas a um 'centro nervoso' que alimenta a sociedade, prestando serviços indispensáveis aos cidadãos e catalisando o crescimento econômico e o desenvolvimento. Esta rede vital abrange barragens, hidrelétricas, sistemas de transporte, redes de telecomunicações de ponta, pilares financeiros, estações de tratamento de água e instalações de saúde, as quais constituem a estrutura da nossa existência na Era da Informação.

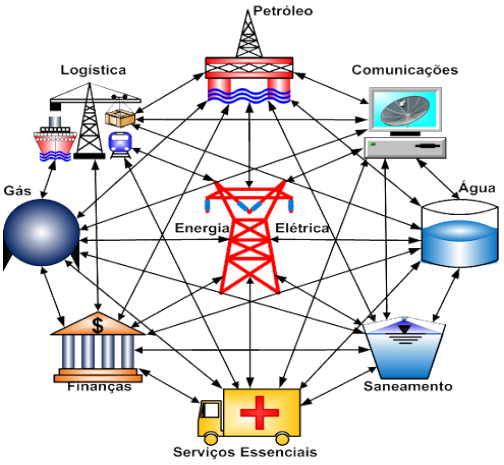

Figura 1: Esquema de interdependência de uma rede de infraestruturas críticas.
Fonte: http://www.tecnix.com.br/Infra/default.htm

A infraestrutura crítica precisa ser fiscalizada por um conjunto de normas regulamentares rigorosas, concebidas para fortalecer a sua segurança, resiliência e confiabilidade constante. Por outro lado, os esforços despendidos na proteção das Infraestruturas Críticas não podem ser vistos como garantia de segurança plena, pois a maioria destes sistemas indispensáveis são suscetíveis a uma infinidade de ameaças e falhas: ataques cibernéticos traiçoeiros, ataques físicos implacáveis, desastres naturais impiedosos e, lamentavelmente, os erros humanos.

3.1 BREVE HISTÓRICO

Há mais de duas décadas, o ataque de 11 de setembro de 2001 marcou não apenas um ponto de virada na geopolítica mundial, mas também teve impactos profundos na segurança cibernética. Primeiramente, na resposta aos atentados às Torres Gêmeas, em que os Estados Unidos alteraram suas regras de migração e de controles em aeroportos, articularam um discurso antiterrorismo e implementaram uma política específica governamental de proteção às infraestruturas críticas.

Em outubro de 2007, a maior exposição global do Brasil, face aos grandes eventos internacionais, fez com que a Câmara de Relações Exteriores e Defesa Nacional – CREDEN, submetesse ao Presidente da República a proposta de inclusão dos assuntos relacionados a segurança de infraestruturas críticas e a segurança da informação às suas competências. Essa mesma Resolução instituiu um Grupo Técnico de Segurança de Infraestruturas Críticas - GTSIC para propor medidas e ações de segurança para as infraestruturas críticas dos setores de energia, transporte, água e telecomunicações.

3.2 IMPORTÂNCIA ESTRATÉGICA E A SEGURANÇA CIBERNÉTICA DAS INFRAESTRUTURAS CRÍTICAS

Serviços essenciais, tais como energia, transportes, comunicação, finanças, águas, dentre outros, imprescindíveis e fundamentais na integração e desenvolvimento econômico sustentável do país, possuem importância estratégica para o Estado, segurança e soberania nacional. Dessa forma, observa-se que são infraestruturas que necessitam de segurança que garanta seu funcionamento contínuo e ininterrupto.

Segundo (Pederson et al., 2006), seja através de ligação direta, proximidade geográfica, ou relações cibernéticas, é inquestionável que as infraestruturas críticas não estão isoladas e que as suas interações criam uma complexa rede de relações, dependências e interdependências que extravasam o âmbito das infraestruturas críticas para afetar toda a sociedade. Nesse sentido, as relações de interdependência são uma intricada estrutura de múltiplos níveis onde as influências se fazem sentir em todos os setores da sociedade e do Estado, do domínio público ao privado, e do âmbito regional à escala global.

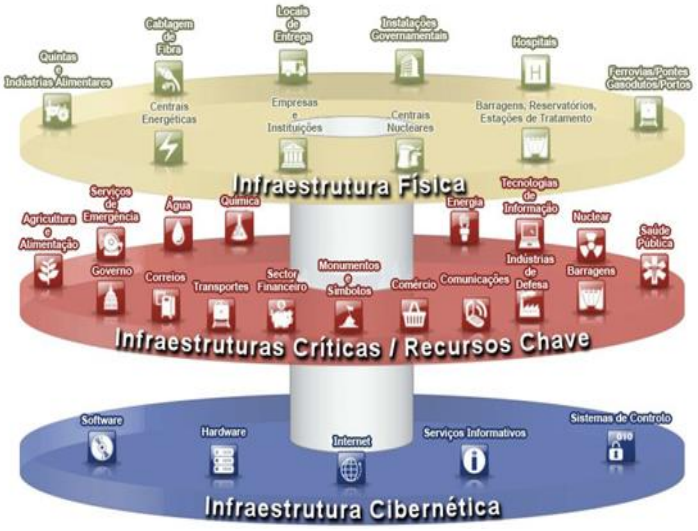

Figura 2: A Infraestrutura Cibernética como alicerce das outras infraestruturas.
Fonte: Adaptado de Beggs (2010)

Conforme consta no Anexo do Decreto nº 10.569 de 2020, define-se segurança das infraestruturas críticas como o conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados a essas infraestruturas.

Tal segurança inicia-se pela compreensão dos tipos e níveis de risco que as envolvem. Ao analisarmos os riscos de uma infraestrutura crítica, levamos em conta as ameaças reais e potenciais com base em vários fatores, seja no potencial de periculosidade ou capacidade danosa do evento adverso, seja nas vulnerabilidades relativas aos sistemas de proteção pessoal, dos processos e operações que possam ser alvos de ataques que, porventura, possam interromper a continuidade do serviço.

Ao pensarmos que os investimentos em infraestruturas estratégicas são fundamentais para o desenvolvimento nacional, torna-se imperioso que a segurança, efetiva ou preventiva, receba também a mesma atenção. Danos às estruturas e aos sistemas críticos podem acarretar sérias dificuldades sociais e econômicas. Essas estruturas sustentam economias, governos e sociedades.

Deve-se ter capacidade de responder a possíveis ataques, desastres e acidentes, caso contrário, esses eventos podem atuar como multiplicadores de riscos, aumentando ainda mais a gravidade da situação. Dito isso, o investimento na segurança das infraestruturas críticas minimiza os custos financeiros, sociais e políticos de possíveis ataques. Assim, cabe à administração pública desempenhar um

papel crucial na promoção da resiliência dessas infraestruturas, estimulando, por exemplo, a adoção de medidas de redução de riscos.

Desse modo, a atividade de segurança de infraestruturas críticas foi inserida no rol de competências do CREDEN, conforme o Decreto Federal nº 9.819, de 3 de junho de 2019. Essa medida deu destaque de que este assunto tem necessidade de acompanhamento permanente e estudo aprofundado em âmbito institucional.

3.3 BARRAGENS: DEFINIÇÃO E IMPORTÂNCIA PARA OS DIVERSOS USOS

As barragens são consideradas infraestruturas críticas de extrema importância para o desenvolvimento do ser humano desde a antiguidade. Construídas para suprir suas necessidades básicas e, atualmente, os crescentes padrões de vida. Por armazenarem grandes massas de água, são consideradas como fonte de um perigo potencial para a população que vive na região de jusante dessas estruturas, incluindo possíveis impactos adversos para a vida, propriedade e o meio-ambiente.

De acordo com a Lei 14.066/20, que alterou a Lei nº 12.334, de 20 de setembro de 2010, que estabeleceu a Política Nacional de Segurança de Barragens (PNSB), as barragens são qualquer estrutura em um curso permanente ou temporário de água para fins de contenção ou acumulação de substâncias líquidas ou de misturas de líquidos e sólidos, compreendendo o barramento e as estruturas associadas.

Já a Resolução Federal CNRH 37/04 define as barragens como uma estrutura construída transversalmente em um corpo de água, dotada de mecanismos de controle com a finalidade de obter a elevação do seu nível de água ou de criar um reservatório de acumulação de água ou de regularização de vazões.

Essas estruturas podem ter tamanhos variados, desde pequenos maciços de terra, usados para atender atividades ligadas à agropecuária, recreação e demandas domésticas, até enormes estruturas de concreto ou de aterro, utilizadas como reservatórios de água para abastecimento público, geração de hidroeletricidade, usos para fins industriais, retenção de rejeitos de mineração e navegação. As barragens contribuem também para a mitigação de eventos extremos como no controle de inundações e na manutenção hídrica e captação de água nos períodos prolongados de seca, os quais têm se intensificado, possivelmente em decorrência das mudanças climáticas globais.

É interessante ressaltar a importância das barragens que formam reservatórios de água para a sociedade e para as comunidades no entorno dela, contudo, são inúmeros os impactos adversos devido a eventuais interrupções de suas atividades.

No caso de uma suspensão da geração hidrelétrica, além de ocasionar o caos nas cidades afetadas e paralisar atividades industriais que dependem diretamente dessa energia, essas usinas deixam de recolher tributos que beneficiariam os municípios, que são considerados como royalties da energia elétrica.

Quando determinada barragem é o principal reservatório de abastecimento de uma região, a paralisação de suas atividades traz impactos negativos em vários aspectos, desde o hídrico, passando pelo econômico e o social. O prejuízo é verificado especialmente para o abastecimento humano, a agricultura irrigada e os envolvidos com a pesca artesanal e de subsistência, ainda mais se a paralisação ocorrer em períodos de seca. Pode-se mencionar também impactos adversos nas atividades como o lazer, o turismo, a navegação e as indústrias que dependem da qualidade da água. Ou seja, existe toda uma cadeia afetada devido à súbita insegurança hídrica.

Figura 3: Usina de Itaipu, maior do mundo em potência instalada.
Fonte: Itaipu (2023)

Nota-se que, em nível mundial, o crescimento da população está causando contínuo aumento na demanda por água, alimentos, energia, minerais e controle de secas e inundações. A possibilidade de ruptura ou de uma invasão desautorizada nos sistemas de acionamento das comportas, por exemplo, resultará em uma liberação descontrolada ou catastrófica de água acumulada, representando um grande risco potencial para vidas humanas, perdas materiais e impactos econômico-financeiros.

Essas estruturas exigem monitoramento periódico e tecnologias eficientes para garantir a segurança geral. Para isso, diversos parâmetros devem ser considerados para garantir a operação e manutenção de uma barragem, tais como topografia, geologia, natureza das fundações, sismicidade do local, condições climáticas locais, entre outros.

O território brasileiro possui um vasto potencial hidrológico, que possibilita a construção de barragens para a geração de energia e abastecimento. Pontua-se que muitas barragens e represas hidrelétricas já são controladas por meio de diferentes tipos de redes de computadores, com ou sem fio, e essas redes de controle estão conectadas à internet. Uma falha na defesa cibernética poderia chegar aos controladores lógicos que comandam equipamentos de monitoramento automatizado do sistema de instrumentação básica de uma barragem ou que fazem o maquinário elétrico abrir ou fechar as comportas, por exemplo.

Um ataque cibernético contra hipotéticas barragens a montante de um mesmo rio, poderia liberar um volume de água que aumentasse abruptamente as vazões nas barragens a jusante. Com a súbita sobrecarga, as barragens a jusante correriam o risco de romperem com o fluxo d'água. Isso poderia gerar um efeito cascata, literalmente, por todo o sistema fluvial, resultando em uma inundação catastrófica.

O modo objetivo de enquadrar o problema em termos de segurança cibernética seria considerar a perda de função e a interrupção na geração de eletricidade, ignorando os possíveis impactos ambientais nas regiões afetadas. Isso é especialmente preocupante em locais onde há grande densidade populacional e de indústrias ao longo de um rio. Caso o ataque cibernético ocorra durante chuvas torrenciais, por exemplo, quando as barragens já estiverem sobrecarregadas, qualquer aumento rápido no nível de água poderá desencadear colapsos sucessivos.

Nesse contexto, muitas vidas e propriedades seriam perdidas, bem como uma perda crítica na capacidade hidrelétrica. Os efeitos ambientais podem ser drásticos e de longo prazo: os recursos de água doce podem ser contaminados; ecossistemas inteiros podem ser destruídos; agentes tóxicos podem ser liberados; e o solo pode sofrer remoção por erosão. Cardumes podem ser dizimados, assim como a indústria pesqueira que deles dependem. Os efeitos de curto e longo prazo seriam consideráveis, e os esforços de restauração poderiam ser caros demais para o município e para o próprio país. Os danos ambientais seriam permanentes.

3.4 ESTAÇÃO DE TRATAMENTO DE ÁGUA – ETA

A falta de coleta e tratamento de esgotos bem como a disposição inadequada de resíduos sólidos, é uma das maiores causas da poluição dos mananciais subterrâneos e dos cursos d'água, tornando a água imprópria para consumo direto. As estações de tratamento têm papel fundamental na potabilização da água a ser distribuída para a população, minimizando os riscos à saúde pública decorrentes do consumo de água com qualidade imprópria.

Diversas são as tecnologias que podem ser empregadas no tratamento da água visando sua purificação, sendo, no Brasil, o tratamento convencional e a filtração direta as mais empregadas, seguidas da filtração lenta, da flotação e da separação por membrana, presentes em um menor número de estações. O tratamento convencional predomina no país, contemplando cerca de 69% da água distribuída (IBGE, 2010), devido, principalmente, às características da água bruta, que é influenciada fortemente pela variação sazonal, demandando um processo de tratamento que é considerado mais robusto em função do maior número de barreiras presentes.

Numa ETA ocorre a captação da água bruta e acontece a transformação em água potável ao consumo humano, por meio das operações unitárias e etapas convencionais como a coagulação, floculação, decantação, filtração e desinfecção. Da qual ao fim desse processo de purificação é gerado um resíduo de partículas sólidas, rico em matéria orgânica e elementos químicos, com grande potencial de contaminação ambiental, nominado de lodo.

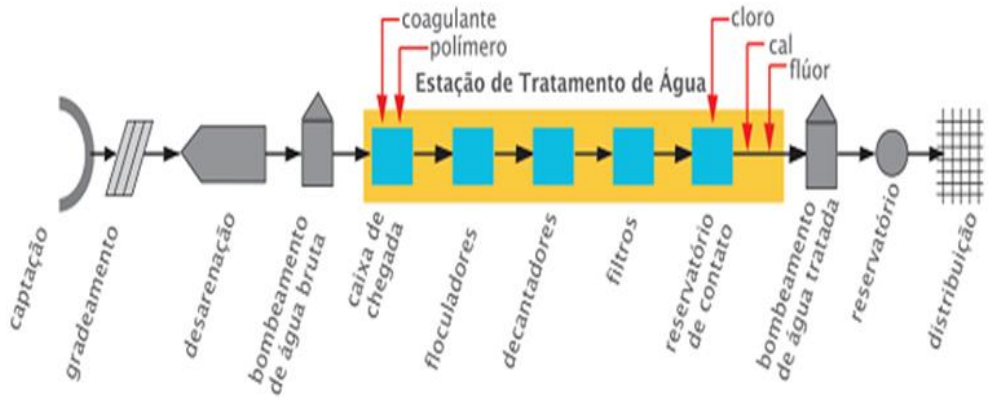

Figura 4: Fluxograma simplificado das etapas de tratamento convencional.
Fonte: CEDAE, 2023

As etapas que constituem o tratamento convencional são, no geral: coagulação, floculação, decantação, filtração, desinfecção e fluoretação. Esses processos visam, de modo geral, a remover sólidos suspensos e dissolvidos na água, além da inativação de microrganismos e são desenvolvidos em série, de forma que o desempenho de uma determinada etapa está intimamente relacionado ao desempenho da etapa anterior.

Ressalta-se que, para uma maior segurança cibernética nas atividades das estações de tratamento de água, é necessário proteger o acesso remoto aos sistemas automatizados de dosagem de produtos químicos, por exemplo, onde os cibercriminosos podem alterar a quantidade de substâncias e compostos de tratamento de água para níveis tóxicos.

Identificou-se que esses atacantes procuram agir no sistema da câmara de mistura a rápida, logo na chegada da água bruta à ETA, onde são adicionados coagulantes tipo sulfato de alumínio e cal hidratada. Igualmente, na etapa de desinfecção após a filtragem, podem acessar o comando das válvulas dosadoras para alterar deliberadamente a quantidade da soda cáustica, elevando a alcalinidade total e desestabilizar o pH da água, aumentando sua acidez e comprometendo a qualidade e potabilidade da água.

4. CIBERSEGURANÇA E DEFESA CIBERNÉTICA

4.1 CONCEITOS E DEFINIÇÕES

Com intuito de nivelar o entendimento sobre os principais termos relacionados à temática de segurança cibernética de infraestruturas críticas e consequentemente deste artigo, será apresentada uma breve descrição destes termos.

Cibersegurança é a proteção de sistemas de computador contra roubo ou danos ao hardware, software ou dados eletrônicos, bem como a interrupção ou desorientação dos serviços que fornecem (pt.wikipedia.org/wiki/Seguranca_de_comptadores). O campo está crescendo em importância devido à crescente dependência de sistemas computadores, internet e redes sem fio, como bluetooth e wi-fi, e devido ao crescimento de dispositivos "inteligentes", incluindo smartphones, televisores e vários dispositivos pequenos que constituem a internet das coisas. Devido à sua complexidade, tanto em termos de política quanto de tecnologia, é também um dos maiores desafios do mundo contemporâneo.

Nessa linha de entendimento, (BRASIL, 2021) conceitua segurança cibernética como as ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

De acordo com o Glossário das Forças Armadas (MD35-G-01, 2015), Defesa Cibernética é definida como o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente.

No âmbito militar, Carvalho (2011) corrobora que, a defesa cibernética constitui-se de atuações de defesa, de exploração e de ofensividade, ocorridas no espaço cibernético. O intuito dessas operações é a proteção dos sistemas de informações, levantamento de informações para fins de inteligência, bem como a neutralização dos recursos dos adversários, ou seja, uma guerra cibernética propriamente dita.

Nesse sentido, nota-se que a segurança das infraestruturas críticas é uma preocupação constante, não apenas para as Forças Armadas, mas também para a sociedade em geral. De forma sintética, pode ser entendida como um arcabouço de medidas, preventivas e reativas contra ameaças cibernéticas, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas.

Importante observar que a segurança das infraestruturas críticas se faz relevante, tanto para garantir a continuidade das operações em setores essenciais para o país, quanto pela sua transversalidade setorial, dado que um evento adverso que impacte negativamente um setor específico pode induzir danos colaterais a outros setores interdependentes. Ilustrativamente, um ataque perpetrado contra uma barragem para geração de energia hidrelétrica pode acarretar consequências de alto impacto, por exemplo, para uma estação de tratamento de água ou para uma infraestrutura de telecomunicações que dependem da energia dessa usina que, por sua vez, podem afetar as instalações bancárias, atingindo o sistema financeiro, e em forma de cascata, no limite, trazer caos a um país.

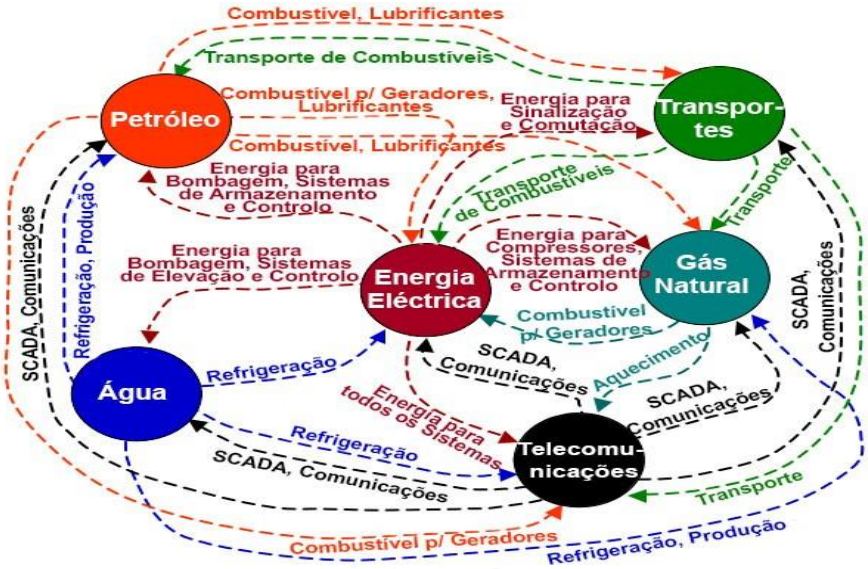

Figura 5: Ilustração sobre a complexidade da rede de dependências e interdependências existentes nas Infraestruturas Críticas.
Fonte: Kelly, T. K. (2001).

Nota-se na Figura 5, que as relações de interdependência das infraestruturas críticas são uma intricada estrutura de múltiplos níveis onde as influências se fazem sentir em todos os setores da sociedade e do Estado, do domínio público ao privado, e do âmbito regional à escala global.

Ressalta-se que a essa concepção de interdependência passaram a ser associados os conceitos de resiliência e risco. Para uma infraestrutura crítica ser resiliente, ela deve possuir a capacidade de manter funções críticas e absorver o impacto em caso de crise ou interrupção, ser capaz de responder e gerenciar uma crise, com habilidade adaptativa e flexibilidade para redirecionar recursos e ativos, além de ter a capacidade de retornar às operações normais da forma mais rápida e eficiente possível.

4.2 INFRAESTRUTURAS HÍDRICAS, NA MIRA DOS CIBERATAQUES

O ano de 2020 não apenas marcou um ponto de virada em todo o mundo, devido à crise global da saúde, devido a pandemia do coronavírus, mas será lembrado como um ano em que a transformação digital nos tornou mais conectados.

O trabalho remoto, a falta de mobilidade, o aumento das videochamadas e a necessidade de isolamento para conter a propagação do vírus, ampliaram a vulnerabilidade dos sistemas favorecendo um aumento nas tentativas de invasões.

Desta forma, acendeu-se um alerta em que precauções extremas foram necessárias para garantir a continuidade dos negócios e serviços essenciais aos

cidadãos, como a integridade e segurança das infraestruturas críticas necessárias ao tratamento, armazenamento e distribuição de água para abastecimento público, com qualidade e quantidade suficientes.

Ainda, de acordo com a Diretiva Europeia 2008/114/CE de 8 de dezembro de 2008 (Jornal Oficial da União Europeia, Vol. L 345/77), entende-se por infraestrutura crítica “o elemento, sistema ou parte dele localizado nos Estados membros que é essencial para a manutenção das funções sociais vitais, saúde, integridade física, segurança e o bem-estar social e econômico da população e cuja perturbação ou destruição afetaria gravemente um Estado Membro por não poder manter essas funções”.

Dentro dessa definição, os serviços relacionados à água são uma das áreas estratégicas que são alvo de ataques cibernéticos e, levando-se em conta que a água também é um fator estratégico nos conflitos armados, a preocupação do setor é mais do que justificada. Embora não seja uma infraestrutura tão atacada quanto outras concessionárias, um ataque fracassado ao abastecimento de água de Israel em 2020 e o ataque a uma estação de tratamento de água na Flórida em 2021, levantou a preocupação de um setor vulnerável devido, precisamente, à sua importância dentro do desenvolvimento econômico e social de uma região.

4.2.1 Principais tipos de ataques cibernéticos

Um ataque cibernético é qualquer tipo de manobra ofensiva para invadir um computador e, ano após ano, tem-se registrado um aumento no número de ataques cibernéticos em infraestruturas críticas do setor água.

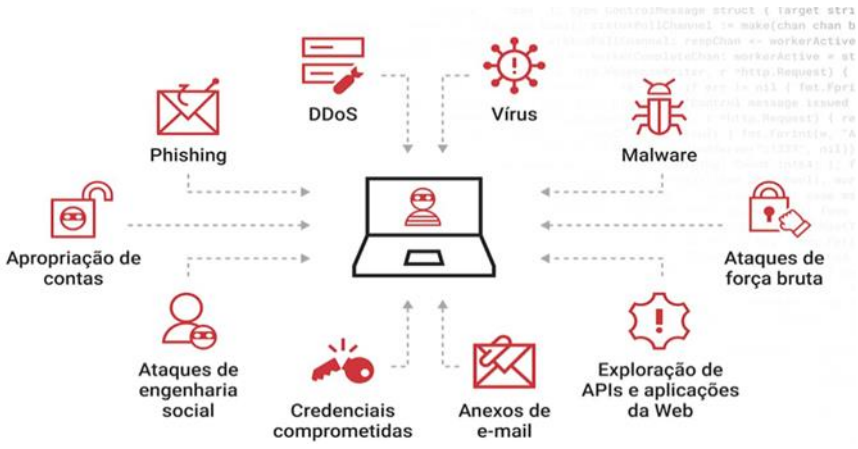

Figura 6: Tipos de vetores mais comuns de ataque.
Fonte: https://www.akamai.com/pt/glossary/what-is-attack-vector

Entre as principais ameaças cibernéticas enfrentadas pelas infraestruturas críticas do setor água, estão:

• ransomware, um software malicioso usado para extorsão por meio de sequestro de dados e de informações digitais usando a criptografia;

• phishing, um tipo de ciberataque que persuade as pessoas a tomar uma ação que dá a um atacante acesso ao seu dispositivo, contas ou informações pessoais;

• DDoS, ataque distribuído de negação de serviço, tentativa maliciosa de interromper o tráfego normal de um servidor, serviço ou rede ao sobrecarregar o alvo ou sua infraestrutura com uma inundação de tráfego da internet;

• vulnerabilidade de software, como falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede;

• vírus ou malware, qualquer código ou programa malicioso que infecta a máquina;

• Defacement, caracterizado como a desfiguração de página, que consiste em alterar o conteúdo de um website. Este tipo de ataque é muito utilizado por hacktivistas para promover algum tipo de ideologia;

• erro humano, em que o comportamento e as ações dos usuários são geralmente o elo mais fraco da cadeia de cibersegurança, principalmente com a maior vulnerabilidade proporcionada pela conectividade remota.

4.2.2 Registros de ciberataques a infraestruturas críticas do setor água

O primeiro ataque cibernético registrado em uma infraestrutura do setor água ocorreu no ano de 2000. O evento foi um ataque intencional e direcionado por um ex-funcionário da Maroochy Water Services com conhecimento do sistema de controle industrial, que assumiu o controle do sistema da empresa prestadora de serviços de abastecimento de água e esgotamento sanitário onde trabalhava e causou uma descarga significativa de esgoto em parques e rios no Condado de Maroochy, Queensland, Austrália.

Em 2013, a Bowman Avenue Dam foi alvo de hackers iranianos, que invadiram o sistema SCADA (Supervisory Control and Data Acquisition) da barragem que abastece parte da população novaiorquina, explorando uma conexão de modem celular suscetível, que conectava a barragem à internet. Embora existam várias teorias por trás da intenção do ataque, por muita sorte, os hackers não poderiam causar nenhum dano naquele momento porque a comporta havia sido desconectada manualmente para manutenção de rotina. O atacante conseguiu obter acesso remoto

a informações sobre o estado e operação da barragem, incluindo informações sobre os níveis e temperatura da água, e o estado da comporta, que é responsável por controlar os níveis de água e vazões. Este ataque, mesmo contra um alvo tão pequeno, foi um exemplo da vulnerabilidade da infraestrutura e um sinal de que atacantes estrangeiros poderiam operar sistemas críticos remotamente e potencialmente causar estragos na nação.

Em janeiro de 2015, foi registrada invasão em uma estação de tratamento de água na cidade de São Francisco, Estados Unidos, onde o invasor obteve acesso às credenciais da conta de TeamViewer de um ex-funcionário que trabalhou na ETA. O hacker tentou alterar as rotinas de tratamento de água que atende parte da área da Baía de São Francisco. Após conseguir acesso ao sistema, o criminoso desconhecido deletou os programas que o prestador de serviços usava para a dosagem e controle do tratamento de purificação de água para a companhia de abastecimento público.

Em 2021, um hacker invadiu a rede de computadores de uma concessionária de água na cidade de Oldsmar, no estado da Flórida, Estados Unidos, e tentou contaminá-la aumentando significativamente a dosagem de um composto químico para tratamento. O invasor obteve acesso ao sistema de tratamento de água e aumentou o nível de hidróxido de sódio para níveis perigosos para o consumo humano. Felizmente, os funcionários da estação de tratamento de água conseguiram reduzir a concentração da substância perigosa imediatamente, e todas as correções foram feitas para que ninguém corresse perigo. O ataque ao sistema informatizado foi percebido por um técnico que se surpreendeu quando o cursor do mouse se moveu remotamente e procurou ativar o comando que regula a quantidade de hidróxido de sódio para tratamento da água. Esse evento alertou as empresas estatais a fortalecerem a segurança cibernética de suas instalações.

No final de 2023, foi registrada tentativa de invasão a duas instalações públicas de tratamento de água no estado da Pensilvânia, EUA, onde hackers conseguiram penetrar no sistema de uma ETA e desativaram remotamente um controlador para alterar os parâmetros de uma das variáveis do tratamento. A denúncia ao FBI foi feita pela Pennsylvania Water Action Response Network (PaWARN), que enviou um e-mail para seus membros informando que dois sistemas de água foram “violados ciberneticamente”. Segundo a mensagem, os hackers instalaram uma web shell nas redes corporativas para acesso remoto a elas, que incluem o monitoramento computadorizado dos níveis de cloro e pH da água, na tentativa de alterarem os níveis

de concentração dos produtos químicos utilizados no tratamento. Felizmente, o ataque foi detectado e interrompido, e o FBI iniciou uma investigação.

Da breve análise dos ciberataques acima apresentados, conclui-se que, em sua maioria, a invasão se dá por intermédio do uso de engenharia social, onde usuários são manipulados para compartilhar informações privadas e expor dados particulares ou organizacionais, espalhar infecções por malware ou dar acesso a sistemas restritos. Nesse sentido, a engenharia social é atraente para os cibercriminosos, pois permite que eles acessem redes digitais, dispositivos e contas sem ter que fazer o difícil trabalho técnico de superar firewalls, software antivírus e outros controles de segurança cibernética.

4.3 CIBERSEGURANÇA - ÁREA PRIORITÁRIA ÁGUA

No Setor Água, especificamente, processos como represamento para abastecimento público, irrigação, tratamento de água ou controle de qualidade, são impensáveis hoje em dia sem o uso das Tecnologias da Informação, uma vez que esses processos são monitorados por meio da captura de informações do ambiente físico por meio de diferentes instrumentos e sensores, a fim de medir parâmetros e atuar no referido ambiente em resposta a determinados eventos.

Num país em que grande parte do território é sistematicamente assolado por longos períodos de seca e de enchentes, este é um setor verdadeiramente crítico para a saúde pública e para a vida econômica, sendo imprescindível proteger a população da suspensão de abastecimento e eventuais contaminações. Uma perturbação grave do abastecimento de água acarretaria consequências imediatas no funcionamento de outros setores, bem como na qualidade de vida dos cidadãos. Um ataque por contaminação poderia causar inúmeras vítimas.

Recentemente, a Agência Nacional de Águas e Saneamento Básico (ANA), sofreu um ataque cibernético que prontamente foi detectado pela Superintendência de Tecnologia da Informação da entidade que, por precaução, desabilitou a operação dos serviços de dados das bacias hidrográficas localizadas em todo o Brasil, afetando o trabalho de monitoramento dos rios do Rio Grande do Sul.

Foto 7: Cais Mauá, Porto Alegre, régua automática conectada à internet.
Grupo RBS (2023)

Os principais incidentes ocorridos nos últimos anos demonstram que um elo fraco na cadeia de abastecimento tem sido a maneira para penetrar no coração das infraestruturas críticas. No Brasil, nota-se que a maioria das infraestruturas hídricas são gerenciadas por concessionárias estaduais, autarquias municipais e prestadores de serviços que não tem, muitas vezes, incorporada uma cultura de cibersegurança de suas instalações, com pessoal constantemente capacitado em defesa e segurança cibernética.

É valido lembrar que a pandemia do coronavírus aumentou drasticamente a dependência de sistemas digitais, levando muitas organizações a serem mais abertas e expostas e, em alguns casos, expor a vulnerabilidade de seus sistemas.

Desde o início da pandemia, as concessionárias e prestadores de serviços tiveram que se adaptar a um novo cenário cheio de incertezas em que nos tornou muito mais conscientes da importância da gestão da água e do papel que desempenha na inovação e digitalização. A crise hídrica global e o impacto das mudanças climáticas exigem o uso racional dos recursos hídricos e, para isso, as empresas devem adotar tecnologias capazes de responder aos desafios e reduzir não apenas a pegada hídrica, mas também energética e de carbono.

Esse processo de digitalização e transformação de processos colocou todos os negócios na mira dos cibercriminosos. Cenários de crise como os mencionados anteriormente ou o agora causado pelo conflito entre a Rússia e a Ucrânia, trazem consigo um aumento nos riscos de ataques e incidentes de segurança cibernética em

uma guerra direcionada tanto aos participantes diretos, quanto aos atores que apoiam algum dos lados, e isso acontece tanto no campo físico quanto no ciberespaço.

Segundo o relatório de riscos do Fórum Econômico Mundial - FEM (World Economic Forum, Global Risks Perception Survey 2019–2020), ataques cibernéticos e comprometimento de infraestruturas de informação estão entre os 10 maiores riscos globais em termos de impacto. Esses riscos foram consideravelmente ampliados com a pandemia. A Covid-19 não só resultou em uma acelerada digitalização de empresas e serviços, mas na criação de uma nova superfície de ataques e vulnerabilidades.

Nesse sentido, os ataques cibernéticos também representam um enorme risco para o valor das empresas e, em última análise, para a estabilidade da sociedade. Assim, a segurança cibernética no setor de água tornou-se transcendental e as empresas devem gerenciar a segurança cibernética como parte de sua estratégia corporativa, social e ambiental. De fato, o FEM alerta que o risco cibernético é o risco de sustentabilidade mais imediato e material do ponto de vista financeiro que as organizações enfrentam hoje.

O impacto de um ciberataque e as suas consequências nas infraestruturas hídricas dependerá de vários fatores, sendo especialmente relevante o downtime, em que os sistemas ficam temporariamente inativos, que pode ter grandes repercussões para os cidadãos, ou o efeito dominó devido às interdependências entre as diversas infraestruturas críticas. Porém, à medida que os ativos operacionais estão conectados uns aos outros, são necessários componentes e sistemas de controle mais resilientes diante de ataques cibernéticos.

5. NORMATIVOS RELACIONADOS À SEGURANÇA CIBERNÉTICA - BRASIL

5.1 POLÍTICA NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

Em novembro de 2018, foi publicado o Decreto nº 9.573, que aprovou a Política Nacional de Segurança de Infraestruturas Críticas - PNSIC. Em seu art. 13, a PNSIC delegou à CREDEN a elaboração da Estratégia Nacional de Segurança de Infraestruturas Críticas e do Plano Nacional de Segurança de Infraestruturas Críticas, no prazo de dois anos da data de publicação da PNSIC.

A PNSIC define infraestruturas críticas como instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da

sociedade. Da mesma forma, caracteriza a segurança das infraestruturas críticas como um conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas.

Foram, ainda, definidos três instrumentos para a implementação da PNSIC. Assim, em dezembro de 2020, foi publicada, por meio do Decreto nº 10.569, a Estratégia Nacional de Segurança de Infraestruturas Críticas – ENSIC e, em setembro de 2022, através do Decreto nº 11.200, o Plano Nacional de Segurança de Infraestruturas Críticas - PLANSIC e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas - SIDSIC.

5.2 POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO

A Política Nacional de Segurança da Informação - PNSI foi instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional. Nessa política, a segurança da informação abrange em seu arcabouço a segurança cibernética, a defesa cibernética, bem como a segurança física e a proteção de dados organizacionais (BRASIL, 2018b).

A PNSI passou a caracterizar a Segurança de Infraestruturas Críticas como uma atividade de Estado, sinalizando à sociedade brasileira a prioridade que o Governo brasileiro atribui ao tema no âmbito da segurança institucional. Contém ainda as orientações indispensáveis ao esforço conjunto a ser desenvolvido pelos órgãos e entidades dos setores público e privado no que diz respeito à atividade de segurança de infraestruturas críticas.

Tendo em vista essa abrangência, a PNSI definiu como instrumentos a Estratégia Nacional de Segurança da Informação - ENSI e os planos nacionais. A ENSI deverá conter as ações estratégicas e os objetivos relacionados à segurança da informação, e construída em módulos contemplando a Segurança Cibernética, a Defesa Cibernética, a Segurança das Infraestruturas Críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados (BRASIL, 2018b).

5.3 ESTRATÉGIA NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

A Estratégia Nacional de Segurança de Infraestruturas Críticas - ENSIC, aprovada por meio do Decreto n° 10.569, de 9 de dezembro de 2020, consolida os

conceitos e identifica os principais desafios para a atividade de segurança de infraestruturas críticas, definindo eixos estruturantes e objetivos estratégicos, de forma a criar as melhores condições para que o País possa se antecipar às ameaças e aproveitar as oportunidades de aprimoramento da segurança de infraestruturas críticas. Dessa forma, a ENSIC serve de orientação tática e de referência para as ações estratégicas elaboradas para o PLANSIC.

Considerando a Segurança Cibernética como a área mais crítica a ser abordada, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) elencou a E-Ciber como o primeiro módulo da ENSIC a ser elaborado. A E-Ciber traz a orientação do Governo Federal à sociedade sobre as ações pretendidas na área de segurança cibernética, apresentando os seguintes objetivos estratégicos: tornar o Brasil mais próspero e confiável no ambiente digital; aumentar a resiliência brasileira às ameaças cibernéticas; e fortalecer a atuação brasileira em segurança cibernética no cenário internacional (BRASIL, 2020b).

Já as ações estratégicas estabelecidas são: fortalecer as ações de governança cibernética; estabelecer um modelo centralizado de governança no âmbito nacional; promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade; elevar o nível de proteção do Governo; elevar o nível de proteção das infraestruturas críticas nacionais; aprimorar o arcabouço legal sobre segurança cibernética; incentivar a concepção de soluções inovadoras em segurança cibernética; ampliar a cooperação internacional do Brasil em segurança cibernética; ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade; e elevar o nível de maturidade da sociedade em segurança cibernética (BRASIL, 2020b).

Dentre estas ações, destacam-se: a elevação do nível de proteção das infraestruturas críticas nacionais; o aprimoramento do arcabouço legal, o qual deve estar em constante atualização, em razão da extrema velocidade com que os normativos se tornam obsoletos; e a elevação do nível de maturidade dos empreendedores de barragens, dos prestadores de serviços e da sociedade em segurança cibernética, uma vez que, na maioria das vezes, os ataques são perpetrados por meio de engenharia social.

A E-Ciber foi aprovada pelo Decreto nº 10.222, de 05 de fevereiro de 2020, conforme disposto no inciso I do art. 6º do decreto que instituiu a PNSIC, e assevera que, no atual cenário de ameaças cibernéticas, é provável que as organizações

experimentem o mesmo tipo de ataque, o que ressalta a importância das informações sobre o fato, sobre o tratamento realizado e sobre as lições aprendidas.

Um exemplo de ação colaborativa é o Exercício Guardião Cibernético - EGC, organizado anualmente pelo Comando de Defesa Cibernética, em parceria com o Gabinete de Segurança Institucional da Presidência da República. É o maior exercício de defesa cibernética do Hemisfério Sul, o qual tem por objetivo criar um ambiente realista onde as infraestruturas críticas participantes precisam proteger seus sistemas de Tecnologia da Informação de ataques cibernéticos, contribuindo para o crescimento da resiliência cibernética das infraestruturas críticas do Brasil.

Figura 8: Chamamento Público do Exercício Guardião Cibernético 4.0
Fonte: Exército Brasileiro (MD/Brasil, 2022).

A atividade consiste em treinamento de ações de proteção cibernética, por meio da cooperação entre Forças Armadas, órgãos parceiros e representantes das infraestruturas críticas, ao adotar técnicas virtuais de simulação e práticas de gestão de incidentes. O exercício emprega gabinetes de crise das áreas de tecnologia da informação e comunicação, de comunicação social, jurídica e da alta administração dos participantes, que são levados a apresentar soluções para os eventos cibernéticos com impacto nas organizações, incluindo o nível decisório-gerencial (gestão de crise) e o nível técnico (resposta a incidentes) das empresas e de órgãos de governo. (BRASIL, 2020a).

A E-Ciber, dentre suas ações estratégicas, busca elevar o nível de proteção das infraestruturas críticas, de modo a aumentar sua resiliência, através da promoção de interação entre as agências reguladoras de infraestruturas críticas para tratar de temas relativos à segurança cibernética, bem como incentivar a participação dessas infraestruturas críticas em exercícios cibernéticos.

No Brasil, a gestão sobre as ações no espaço cibernético é dividida em quatro níveis: i) o político, coordenado pela Presidência da República, que abrange a administração federal e os órgãos decisórios de caráter público, responsável pela segurança cibernética; ii) o estratégico, coordenado pelo Ministério da Defesa, Estado maior e conjunto de Comando das Forças Armadas, responsável pela defesa cibernética; e os níveis iii) operacional e iv) tático, sob a coordenação exclusiva das forças armadas, responsável em caso de guerra cibernética. Os níveis podem ser representados conforme a Figura 9.

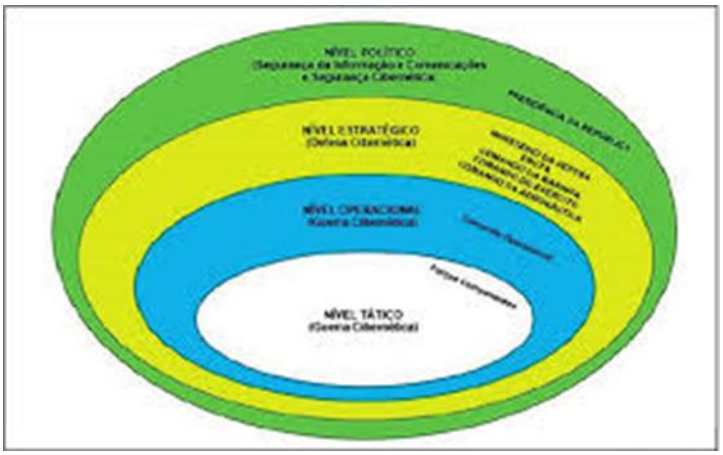

Figura 9 - Níveis de atuação do Setor Cibernético
Fonte: Doutrina Militar de Defesa Cibernética (2014, p. 17).

5.4 PLANO NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

O planejamento institucional constitui valioso instrumento de ação governamental, voltado para coordenar e articular a atuação de órgãos e entidades envolvidos na atividade de segurança das infraestruturas críticas. Assim, o PLANSIC, aprovado por meio do Decreto nº 11.200, de 15 de setembro de 2022, objetiva transmitir orientações gerais, estimular as parcerias entre os diversos órgãos e entidades envolvidos na atividade, atribuir responsabilidades e apresentar os fundamentos básicos para a elaboração dos planos setoriais de segurança de infraestruturas críticas do País.

Seu conteúdo define as áreas prioritárias de aplicação, prevê o envolvimento dos Estados, do Distrito Federal, dos Municípios e da sociedade e destaca a gestão de riscos e o estudo de interdependência. Ademais, reúne um conjunto de ações estratégicas, com respectivas metas e prazos, elaboradas com o objetivo de

estabelecer e organizar responsabilidades na implementação da Política Nacional de Segurança de Infraestruturas Críticas.

Um dos eixos estruturantes do PLANSIC é o de “envolver, nos exercícios Guardião Cibernético, setores abordados em Segurança de Infraestruturas Críticas, com meta de envolver os diversos setores de infraestruturas críticas na realização dos EGC a cada ano” (BRASIL, 2022b).

Quadro 1 - Setores de Segurança de Infraestruturas Críticas

ÁREA PRIORITÁRIA	SETOR
Águas	Barragens
	Abastecimento Urbano de Águas
Energia	Energia Elétrica
	Petróleo, Gás Natural e Biocombustíveis
Transporte	Terrestre
	Aéreo
	Aquaviário
Comunicações	Telecomunicações
	Radiodifusão
	Serviços Postais
Finanças	Finanças
Biossegurança e Bioproteção	Biossegurança e Bioproteção
Defesa	Defesa

Fonte: Adaptado de (BRASIL, 2022b).

6. CONSIDERAÇÕES FINAIS

As nações alicerçadas no conhecimento estão numa fase de transição para uma situação de total dependência das tecnologias de informação, sem qualquer hipótese de retrocesso para os antigos processos e modos de funcionamento. Na base desta mudança estão as Infraestruturas Críticas, que sustentam a nossa defesa nacional, o nosso desenvolvimento econômico e a nossa qualidade de vida e que, por isso mesmo, já são consideradas à luz da Era Digital.

Nesse sentido, o debate sobre a segurança cibernética das Infraestruturas Críticas, principalmente as relacionadas ao setor água, como barragens e estações de tratamento, tem como ponto central questões de segurança nacional e saúde pública. O Brasil tem adotado diversas políticas e estratégias para garantir a segurança cibernética do país, como a PNSI, a PNSIC, a E-Ciber, o PLANSIC, bem como os exercícios de treinamento, com simulação construtiva e virtual.

Com a grande transformação tecnológica presenciada no mundo nos últimos anos, que elevou a interdependência e a interação entre os sistemas dessas infraestruturas estratégicas, a necessidade de mantê-las em perfeito funcionamento conduz a uma necessária cooperação entre os diversos atores, principalmente o governo, uma vez que todos dependem da indústria da água para economia, saúde, segurança e alimentação; defendê-la das ameaças cibernéticas é essencial.

Os empreendedores de barragens, os prestadores de serviços de abastecimento de água e esgotamento sanitário, devem tomar medidas proativas para proteger seus sistemas e dados contra ataques cibernéticos, constituindo processos de segurança cibernética de suas plantas, com uma análise periódica de acordo com a evolução tecnológica, sendo necessário envolver as entidades reguladoras infranacionais e organizações públicas e privadas para uma parceria no sentido de aperfeiçoar procedimentos, atualizar sistemas e frameworks de segurança, ofertar capacitação contínua e treinamento aos colaboradores.

Apesar de muitas entidades ainda não terem amadurecido uma cultura sobre a relevância do assunto, é preciso adotar uma política de investimentos em benefício da segurança cibernética, gerenciamento de riscos e de ações contra esses incidentes. O planejamento orçamentário adequado para a política de segurança cibernética interna poderá ser um meio de se estruturar e prevenir possíveis ataques nessas organizações.

Outrossim, a fim de se opor aos impactos de possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou mesmo aqueles que permitam seu pronto restabelecimento.

Por todo o exposto, reforça-se a necessidade de uma atuação conjunta em prol da segurança cibernética das infraestruturas críticas do setor água. Para tanto, considera-se de suma importância a criação de um ambiente colaborativo, do qual participem a administração pública em cada esfera do governo, o setor privado, a academia e a sociedade em geral, na tentativa de compartilharem mais informações entre si sobre essas ameaças, a fim de proteger contra a ação de cibercriminosos as infraestruturas críticas, tão vitais para a existência e crescimento do Estado brasileiro.

REFERÊNCIAS

Agência Nacional das Águas (Brasil). Relatório de segurança de barragens 2022/Agência Nacional de Águas. – Brasília: ANA, Disponível em: <https://www.snisb.gov.br/portal-snisb/documentos-e-capacitacoes/rsb?id=121>. Acesso em: 30 de Mar. de 2024

Alves Junior, Sérgio A. G. Políticas Nacionais de Segurança Cibernética: o regulador das Telecomunicações – Brasil, Estados Unidos, União Internacional das Telecomunicações (UIT). Brasília: UnB, 2011.

Ataques a estações de tratamento de água nos EUA, 2021. Disponível em: <https://www.cisoadvisor.com.br/ataques-a-estacoes-de-tratamento-de-agua-nos-eua/>. Acesso em: 17 jan. 2024.

Aumento do Risco para a Natureza: Porque é que a crise que afeta a natureza é importante para os negócios e a economia, 2020. Disponível em: <https://www3.weforum.org/docs/WEF_New_Nature_Economy_Report_2020_PR.pdf>. Acesso em: 18 jan. 2024.

Beggs, P. (2010). Securing the Nation's Critical Cyber Infrastructure. *California Information Security Office Meeeting*. Department of Homeland Security.

BRASIL. (2004) Resolução CNRH Nº 37 de 26 de março de 2004. Estabelece diretrizes para a outorga de recursos hídricos para a implantação de barragens em corpos de água de domínio dos Estados, do Distrito Federal ou da União.

BRASIL. (2015) Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018: versão 1.0 / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. – Brasília: Presidência da República. Gabinete de Segurança Institucional.

BRASIL. (2015) Glossário das Forças Armadas. 5. ed. MD35-G-01, EMCFA, Ministério da Defesa, DF.

BRASIL. (2016) Decreto nº 8.793 de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Decreto/D8793.htm>. Acesso em: 6 fev. 2024.

BRASIL. (2016) Política Nacional de Defesa, Ministério da Defesa, DF, 2016a.

BRASIL. (2018) Decreto nº 9.573 de 22 de novembro de 2018. Aprova a Política Nacional de Segurança das Infraestruturas Críticas. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>. Acesso em: 30 de Nov. 2023.

BRASIL. (2018) Decreto nº 9.637 de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm>. Acesso em: 6 fev. 2024.

BRASIL. (2018) Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados – LGPD, DF: Congresso Nacional.

BRASIL. (2020) Lei 14.066 de 30 de setembro de 2020. Estabelece a Política Nacional de Segurança de Barragens, DF: Congresso Nacional.

BRASIL. (2020) Decreto nº 10.222 de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm>. Acesso em 31 jan.2024.

BRASIL. (2020) Doutrina de Operações Conjuntas. 2.ed. MD30-M-01, Ministério da Defesa, Brasília, DF, 2020b.

BRASIL. (2020) Portaria Normativa nº 3781 GM/MD de 17 de novembro de 2020. Cria o Sistema Militar de Defesa Cibernética e dá outras providências. Ministério da Defesa, DF, 2020a.

BRASIL. (2020) Política Nacional de Defesa e Estratégia Nacional de Defesa. Ministério da Defesa, Brasília, DF, 2020c.

BRASIL. (2020) Decreto nº 10.569 de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Disponível em: <https://www.planalto.gov.br/cCivil_03/_Ato2019-2022/2020/Decreto/D10569.htm>. Acesso em: 31 jan. 2024.

BRASIL. (2021) Decreto 10.748 de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Política Nacional de Segurança de Barragens, DF: Congresso Nacional.

BRASIL. (2022) Decreto nº 11.200 de 15 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Crítica. Disponível em: <https://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2022/Decreto/D11200.htm>. Acesso em: 18 abr. 2024.

CARVALHO, P.S.M. O Setor Cibernético nas Forças Armadas Brasileiras. In: Desafios Estratégicos para a Segurança e Defesa Cibernética. 1ª. Ed. Brasília: Presidência da República, 2011, p. 13-34.

CASTRO, Carmen Maria Barros de. Ponto 1 – A Qualidade da Água / Ponto – 2 Introdução ao Tratamento da Água. Porto Alegre: Gráfica UFRGS, 2008a.

Chamamento Público do Exercício Guardião Cibernético 4.0, 2022. Disponível em:<https://www2.eb.mil.br/web/guest/todos-os-avisos/-/asset_publisher/nElT00TY refc/content/chamamento-publico-do-exercicio-guardiao-cibernetico-4-0>.26/03/24.

Ciberguerra: A segurança das infraestruturas hídricas, 2022. Disponível em: <https://tratamentodeagua.com.br/ciberguerra-seguranca-infraestruturas-hidricas/>. Acesso em: 02 abr. 2024.

Desafios e impacto da cibersegurança nas infraestruturas críticas, 2023. Disponível em: <https://tiinside.com.br/31/08/2023/desafios-e-impacto-da-cibersegur anca-nas-infraestruturas-criticas/>. Acesso em: 02 abr. 2024.

Distribuidora de água de Brasília confirma invasão, 2014. Disponível em: <https://www.cisoadvisor.com.br/distribuidora-de-agua-de-brasilia-confirma-invasao/>. Acesso em: 17 jan. 2024.

HENRIQUES, Henrique de Queiroz. Os desafios da capacitação de recursos humanos para a Defesa Cibernética. Observatório Militar da Praia Vermelha, Escola de Comando e Estado Maior do Exército, Rio de Janeiro, 2021.

Infraestrutura crítica, 2023. Disponível em: <https://pt.wikipedia.org/wiki/ Infraestru tura_cr%C3%ADtica>. Acesso em: 30 jan. 2024.

Instituto Brasileiro de Geografia e Estatística (IBGE). Sinopse do Censo Demográfico 2010. Rio de Janeiro: IBGE, 2010. Disponível em <https://www.ibge.gov.br/censo 2010/apps/sinopse/index.php>. Acesso em: 19 mar. 2024.

Itaipu Binacional, 2023. Disponível em: <https://www.itaipu.gov.br/energia /barragem>. Acesso em: 23 jan. 2024.

Jornal Oficial da União Europeia, (Vol. L 345/77). DIRECTIVA 2008/114/CE DO CONSELHO de 8 de Dezembro de 2008 relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri= CELEX:32008L0114>. Acesso em: 23 jan. 2024.

Kelly, T. K. (2001). Infrastructure Interdependencies. *A Workshop on Electricity Security and Survivability*. Carnegie Mellon University.

MANDARINO JUNIOR, Raphael, and Claudia Canongia (Org.). 2010. Livro Verde: Segurança Cibernética do Brasil. Departamento de Segurança da Informação e Comunicações. Brasília: GSIPR/SE/DSIC. Ministério da Defesa. 2012a. Estratégia Nacional de Defesa - END. Brasília. Disponível em: <https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf>. Acesso: 18 mar. 2024.

Pederson, P., Dudenhoeffer, D., Hartley, S., & Permann, M. (2006). *Critical Infrastructure Interdependency Modeling: A Survey of US and International Research*. Idaho National Laboratory.

Por que definir e proteger infraestruturas críticas sistemicamente importantes é tão vital, 2022. Disponível em: <https://www.weforum.org/agenda/2022/05/securing-systemically-important-critical-infrastructure/>. Acesso em: 18 jan. 2024.

Possível ataque hacker a sistema da ANA afeta trabalho de monitoramento de rios no RS, 2023. Disponível em: <https://gauchazh.clicrbs.com.br/geral/noticia/2023/09/possivel-ataque-hacker-a-sistema-da-ana-afeta-trabalho-de-monitoramento-de-rios-no-rs-cln5g290j003a015 nuy6wgt5a.html>. Acesso em: 10 out. 2023.

São Francisco registra invasão em tratamento de água, 2021. Disponível em: <https://www.cisoadvisor.com.br/sao-francisco-registra-invasao-em-tratamento-de-agua/>. Acesso em: 18 jan. 2024.

Segurança de computadores, 2024. Disponível em: <https://pt.wikipedia.org/wiki/Seguran%C3%A7a_de_computadores>. Acesso em: 30 jan. 2024.

Segurança de infraestruturas críticas, 2022. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas-sic>. Acesso em: 30 jan. 2024.

SILVA, Walbery N de Lima e. Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa Nacional. Brasília, 2019.