ANÁLISE DE ESTRATÉGIAS DE SEGURANÇA FÍSICA EM INSTALAÇÕES NUCLEARES UTILIZANDO REDES BAYESIANAS DE DECISÃO

Eduardo Mateus Sirtuli

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Nuclear, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia Nuclear.

Orientadora: Andressa dos Santos Nicolau

Rio de Janeiro

Maio de 2026

ANÁLISE DE ESTRATÉGIAS DE SEGURANÇA FÍSICA EM INSTALAÇÕES NUCLEARES UTILIZANDO REDES BAYESIANAS DE DECISÃO

Eduardo Mateus Sirtuli

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA NUCLEAR.

Orientador: Andressa dos Santos Nicolau

Aprovado por: Prof[a]. Andressa dos Santos Nicolau
Prof. Alan Miranda Monteiro de Lima
Prof. Cláudio Márcio do Nascimento Abreu Pereira

RIO DE JANEIRO, RJ – BRASIL
MAIO DE 2026

Sirtuli, Eduardo Mateus

Análise de estratégias de segurança física em instalações nucleares utilizando redes bayesianas de decisão / Eduardo Mateus Sirtuli. – Rio de Janeiro: UFRJ/COPPE, 2026.

XII, 119 p.: il.; 29,7cm

Orientadora: Andressa dos Santos Nicolau

Dissertação (Mestrado) – UFRJ/COPPE/Programa de Engenharia Nuclear, 2026.

Referência Bibliográfica: p. 113 –119.

1. Segurança nuclear. 2. Sistema de proteção física. 3. Redes bayesianas de decisão. 4. Diagramas de influência. I. Nicolau, Andressa dos Santos. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia Nuclear. III. Título.

AGRADECIMENTOS

A professora Andressa dos Santos Nicolau pela oportunidade concedida e por sua orientação ao longo desta jornada.

Aos meus pais, Lindomar e Margarete, os quais amo muito e agradeço todos os dias por tê-los como pais.

A minha namorada Sarah pelo incentivo e pelo apoio durante os momentos de dificuldade.

Aos meu gatos, Dom, Aurora, Donna e Mia, pela companhia durante a escrita da dissertação, incluindo as sonecas sobre o teclado.

E a todos os demais que direta ou indiretamente me ajudaram a realizar este trabalho.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

ANÁLISE DE ESTRATÉGIAS DE SEGURANÇA FÍSICA EM INSTALAÇÕES NUCLEARES UTILIZANDO REDES BAYESIANAS DE DECISÃO

Eduardo Mateus Sirtuli

Maio/2026

Orientadora: Andressa dos Santos Nicolau

Programa: Engenharia Nuclear

O presente trabalho propõe uma metodologia de apoio à decisão baseada em Redes Bayesianas de Decisão, estruturadas na forma de Diagramas de Influência com Memória Limitada (LIMID), para a análise e otimização de estratégias de proteção física em instalações nucleares. A metodologia foi aplicada a um estudo de caso representativo de uma instalação nuclear inserida em uma base naval hipotética, caracterizada por múltiplos modos de acesso ao alvo e pela presença de material nuclear sensível, que permitiu comparar diferentes combinações de medidas de proteção física, e utilizando o critério de utilidade esperada, como base para a seleção das estratégias mais custo-efetivas. Os resultados indicaram que a eficácia global das estratégias de segurança não depende apenas do desempenho técnico isolado de cada medida, mas de sua integração ao sistema como um todo e da relação entre ganhos de desempenho e custos associados. A análise de sensibilidade demonstrou a robustez da metodologia proposta frente as variações nos principais parâmetros do modelo. Conclui-se que o uso de Redes Bayesianas de Decisão constitui uma ferramenta promissora para o apoio à tomada de decisão estratégica em proteção física de instalações nucleares, permitindo incorporar de forma estruturada critérios de custo-benefício.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

ANALYSIS OF PHYSICAL SECURITY STRATEGIES IN NUCLEAR FACILITIES USING BAYESIAN DECISION NETWORKS

Eduardo Mateus Sirtuli

May/2026

Advisor: Andressa dos Santos Nicolau

Department: Nuclear Engineering

This work proposes a decision support methodology based on Bayesian Decision Networks, structured as Limited Memory Influence Diagrams (LIMID), for the analysis and optimization of physical protection strategies in nuclear facilities. The methodology was applied to a representative case study of a nuclear installation located within a hypothetical naval base, characterized by multiple access paths to the target and the presence of sensitive nuclear material. The developed model enabled the comparison of different combinations of physical protection measures under conditions of uncertainty, using the expected utility criterion as the basis for selecting the most cost-effective strategies. The results indicated that the overall effectiveness of security strategies depends not only on the isolated technical performance of each measure but on their integration within the system as a whole and on the relationship between performance gains and associated costs. Sensitivity analysis demonstrated the robustness of the propose methodology with respect to variations in the main model parameters. It is concluded that the use of Bayesian Decision Networks constitutes a promising tool for strategic decision support in the physical protection of nuclear facilities, allowing the structured incorporation of cost-benefit criteria

SUMÁRIO

1 INTRODUÇÃO.....1
2 FUNDAMENTAÇÃO TEÓRICA.....5
2.1 Sistemas de Proteção Fisica.....5
2.2 Projeto e Avaliação de um Sistema de Proteção Física.....7
2.2.1 Análise Sistêmica da Vulnerabilidade à Intrusão.....8
2.2.2 Estimativa da Interrupção da Sequência de Ações do Adversário.....9
2.2.3 Análise Sistemática da Efetividade da Proteção Física.....10
2.2.4 Utilização de Redes Bayesianas.....10
2.3 Redes Bayesianas.....14
2.3.1 Teorema de Bayes.....16
2.3.2 Diagramas de Influência de Memória Limitada (LIMIDs).....17
2.4 Histórico de ataques contra instalações nucleares.....20
3 METODOLOGIA.....35
3.1 Desenvolvimento do trabalho.....35
3.2 Modelo conceitual de decisão em proteção física.....37
3.2.1 Hipóteses de modelagem.....39
3.3 Construção do modelo aplicado.....41
3.4 Caracterização da ameaça.....43
3.5 Fontes de dados e atribuição de probabilidades.....48
3.6 Procedimento de avaliação das alternativas de decisão.....49
3.7 Limitações do Estudo.....50
4 APLICAÇÃO DA METODOLOGIA EM UM ESTUDO DE CASO.....52
4.1 Caracterização do estudo de caso.....52
4.2 Construção do modelo para o estudo de caso.....57
4.2.1 Ameaça.....57
4.2.2 Detecção.....58
4.2.3 Resposta.....64
4.2.4 Atraso.....66
4.2.5 Neutralização.....68
4.2.6 Danos.....73
4.2.7 Utilidade Total.....80
4.2.8 Estrutura da rede bayesiana de decisão aplicada ao estudo de caso.....81

5 RESULTADOS E DISCUSSÃO.....83
5.1 Análise comparativa das estratégias em condições de incerteza.....83
5.2 Análise de sensibilidade.....86
5.3 Análise por Cenários de Acesso.....89
5.3.1 Avaliação com Ajuste das Probabilidades de Acesso.....91
5.4 Análise por Cenários de Meios Empregados.....93
5.5 Análise em Função do Alvo do Ataque.....95
5.6 Análise de Sensibilidade dos Parâmetros de Neutralização.....98
5.6.1 Ameaças Terrestres e Aquáticas.....98
5.6.2 Ameaças Aéreas.....100
5.7 Avaliação do Impacto do *insider* no Desempenho do Modelo.....102
5.8 Análise de Sensibilidade dos Valores Atribuídos aos Danos.....105
5.9 Síntese dos resultados.....107
6 CONCLUSÃO E TRABALHOS FUTUROS.....109
REFERÊNCIAS.....113

LISTA DE FIGURA

Figura 1: Exemplo de rede bayesiana (MILLIAM *et al.* , 2010).....15
Figura 2 - Exemplo de um LIMID.....19
Figura 3 - Modelo de apoio à decisão para seleção de estratégias de proteção física em instalações nucleares.....38
Figura 4 - Exemplo de detalhamento da Ameaça.....41
Figura 5: Alternativas de detecção e medidas já implementadas no sistema.....42
Figura 6 - Representação esquemática da instalação nuclear hipotética e das zonas de proteção física consideradas no estudo de caso (SANTOS, 2024).....53
Figura 7 - Área Vigiada (SANTOS, 2024).....55
Figura 8 - Área Vital (SANTOS, 2024).....56
Figura 9 - Estrutura da rede bayesiana de decisão aplicada ao estudo de caso.....82
Figura 10 - Análise de sensibilidade global do modelo em relação à utilidade total.....87
Figura 11 - Distribuição dos danos por cenário de acesso.....90
Figura 12 - Comparação entre utilidade e probabilidade de neutralização por tipo de área….96
Figura 13 - Distribuição dos principais níveis de dano por área.....97
Figura 14 - Probabilidade de Liberação de material nuclear por área.....97
Figura 15 - Comparação entre utilidade e probabilidade de neutralização para cenários de neutralização.....99
Figura 16 - Comparação entre utilidades do sistemas de detecção/neutralização de VANT para diferentes parâmetros.....100
Figura 17 - Comparação da utilidade das estratégias em função da probabilidade de neutralização do sistema *jammer*.....101
Figura 18 - Impacto da ameaça interna na utilidade por vetor de acesso.....103
Figura 19 - Sensibilidade da utilidade e da neutralização ao impacto da ameaça interna….104

LISTA DE TABELAS

Tabela 1 - Probabilidade de Rinite dado Alergia e Gato (MILLIAM, E *et al.* , 2010).....16
Tabela 2 - Históricos de ataques contra instalações nucleares.....22
Tabela 3 - Nós que representam a ameaça.....58
Tabela 4 - Nós da função de Detecção.....62
Tabela 5 - Estimativa de custo da Equipe de Resposta reforçada.....65
Tabela 6 - Nós da função de Resposta.....66
Tabela 7 - Nós da função de Atraso.....67
Tabela 8 - Tabela de Probabilidade Condicional do nó Atraso Efetivo em função do alvo e das alternativas de obstáculos.....68
Tabela 9 - Nó de Neutralização.....69
Tabela 10 - Fatores associados ao atraso da força de resposta.....71
Tabela 11 - Probabilidades de Neutralização (Sim/Não) condicionadas aos níveis de Atraso, aos Meios empregados e ao Tamanho do Grupo adversário para a Força de Resposta Básica 72
Tabela 12 - Probabilidades de Neutralização (Sim/Não) condicionadas aos níveis de Atraso, aos Meios empregados e ao Tamanho do Grupo adversário para a Força de Resposta Reforçada.....72
Tabela 13 - Nós de Dano.....76
Tabela 14 - Exemplos de eventos técnicos associados à liberação de material nuclear em piscinas de combustível irradiado.....77
Tabela 15 - Tabela de Probabilidade Condicional do nó Dano para a Área Vital.....78
Tabela 16 - Tabela de Probabilidade Condicional do nó Dano para a Área Protegida.....79
Tabela 17 - Tabela de Probabilidade Condicional do nó Dano para a Área Vigiada.....79
Tabela 18 - Tabela de Probabilidade Condicional do nó Dano para a Área Vital no acesso aéreo.....80
Tabela 19 - Estratégias com as maiores utilidades esperadas no cenário sem evidências.....83
Tabela 20 - Estratégias com as menores utilidades esperadas no cenário sem evidências.....85
Tabela 21 - Estratégias ótimas por cenário de acesso.....89
Tabela 22 - Principais estratégias no cenário com aumento do acesso aéreo.....92
Tabela 23 - Principais estratégias no cenário com diminuição do acesso aéreo.....93
Tabela 24 - Estratégias ótimas por tipo de meios empregados pelo inimigo.....94
Tabela 25 - Cenários paramétricos adotados para a neutralização.....98

Tabela 26 - Estratégias ótimas e desempenho do modelo em função da presença de ameaça interna.....102
Tabela 27 - Impacto da variação dos valores de dano na utilidade e na estratégia ótima.....105

LISTA DE SIGLAS

AIEA - Agência Internacional de Energia Atômica

BNH – Base Naval Hipotética

CAS - Central de Alarmes de Segurança

CCTV - Closed-Circuit Television

CME – Complexo de Manutenção Especializada

CNEN – Comissão Nacional de Engenharia Nuclear

DI - Diagramas de Influência

EASI - Estimate of Adversary Sequence Interruption

LIMID - Limited Memory Influence Diagrams

PI – Probabilidade de Interrupção

PN – Probabilidade de Neutralização

RN - Redes Bayesianas

SAPE - Systematic Analysis of physical Protection Effectiveness

SAVI - System Analysis of Vulnerability to Intrusion

SPF – Sistema de Proteção Física

TPC – Tabela de Probabilidade Condicional

VDM - Video Detection Motion

1 INTRODUÇÃO

Pouco depois dos experimentos nucleares de 1942 no Stagg Field, em Chicago, Enrico Fermi expressou uma preocupação que persiste sempre que a segurança dos reatores é discutida: “O público pode não aceitar uma fonte de energia que esteja associada a grandes quantidades de radioatividade e que produza um explosivo nuclear, o qual poderia cair em mãos hostis” (FERGUSON, SETTLE, 2012). A afirmação de Enrico Fermi destaca a importância de equilibrar os benefícios da tecnologia nuclear com a responsabilidade de gerenciar seus riscos potenciais.

Deste então, uso pacífico da energia nuclear se expandiu ao redor do mundo, e, à medida que o volume de materiais nucleares e seu transporte internacional aumentaram, cresceram também as preocupações com a proteção desses materiais contra grupos terroristas e outros atores mal intecionados (KIM,KANG, 2012). Dessa forma, usinas nucleares, reatores de pesquisa civis, algumas instalações de combustível naval, plantas de enriquecimento de urânio e instalações de fabricação de combustível podem ser vulneráveis a ataques que caso ultrapassem as barreiras de projeto poderiam levar a uma contaminação radioativa generalizada (FERGUSON, SETTLE, 2012).

A ameaça de ataque pode se manifestar de diferentes formas: ações terrestres, semelhantes a operações de comando, direcionadas a equipamentos que caso sejam danificados podem resultar no derretimento do núcleo de um reator ou na liberação em larga escala de material radioativo. Além de ataques externos, como o choque de uma aeronave contra uma usina nuclear, um ataque cibernético, entreoutros(FERGUSON, SETTLE, 2012).

A segurança nuclear vai além da prevenção de acidentes em usinas nucleares, incluindo também a proteção contra roubo, contrabando e uso indevido de materiais radioativos para a fabricação de armas nucleares. Além disso, a gestão adequada de resíduos nucleares, a utilização de tecnologias avançadas de monitoramento, a implementação de normas rigorosas e a colaboração internacional são aspectos essenciais para assegurar um ambiente nuclear seguro e controlado (SANTOS, 2024).

Nesse contexto, a crescente complexidade das ameaças e a necessidade de garantir a eficácia dos Sistemas de Proteção Física (SPF) impulsionaram o desenvolvimento de diferentes metodologias de análise ao longo do tempo. A avaliação desses sistemas não é trivial, pois envolve múltiplas variáveis, como as capacidades do adversário, os meios de

ataque disponíveis, os tempos de resposta e a eficácia das medidas de proteção implementadas. Assim, diversas abordagens foram propostas na literatura com o objetivo de apoiar a tomada de decisão e aprimorar o desempenho desses sistemas.

Entre os métodos clássicos, destaca-se o *Estimate of Adversary Sequence Interruption* (EASI), amplamente utilizado para estimar a probabilidade de interrupção de um adversário ao longo de um caminho de ataque, integrando elementos de detecção, atraso e resposta (ANDIWIJAYAKUSUMA, 2022). Nesse sentido, SANTOS (2024) aplicou o método EASI na análise de uma base naval hipotética, evidenciando sua utilidade na avaliação da eficácia de barreiras e tempos de resposta, embora sua abordagem baseada em caminho único apresente limitações em cenários mais complexos. Outro método relevante é o *System Analysis of Vulnerability to Intrusion* (SAVI), que utiliza Diagramas de Sequência do Adversário para identificar caminhos mais vulneráveis, mas simplifica a dinâmica real ao considerar, de forma predominantemente linear, as possíveis estratégias de ataque (MATTER, 1988; ZOU *et al.*, 2018). Como evolução dessas abordagens, o *Systematic Analysis of Physical Protection Effectiveness* (SAPE) incorpora modelos bidimensionais e algoritmos heurísticos para uma análise mais abrangente, ainda que com maior custo computacional (JANG *et al.*, 2009).

Paralelamente, métodos como Redes Bayesianas (JENSEN; NIELSEN, 2007), que permitem modelar incertezas e interdependências entre variáveis, sendo aplicadas em diferentes contextos, como instalações industriais, portos, redes de transporte e segurança marítima (IANINI *et al.*, 2023; ARGENTI *et al.*, 2018; MARRONI *et al.*, 2024; WANG; WU; YUEN, 2023; MOHSENDOKHT *et al.*, 2025; HOU *et al.*, 2025). Além disso, abordagens baseadas em Diagramas de Influência (JENSEN; NIELSEN, 2007) têm sido utilizadas para classificar ameaças, avaliar consequências e otimizar a alocação de recursos de proteção (GRACE; RENJITH, 2021; MISURI *et al.*, 2019).

Diante da evolução das metodologias de análise de Sistemas de Proteção Física para instalações nucleares e das limitações observadas nos métodos tradicionais, como SAPE, SAVI e EASI, especialmente no que se refere à ausência de um processo estruturado de tomada de decisão. O objetivo principal deste trabalho é otimizar a alocação de medidas de segurança e respostas a emergências em uma base naval hipotética que armazena material nuclear, de forma a maximizar a eficácia dessas

medidas enquanto minimiza os custos associados. Para alcançar esse objetivo, foi utilizada uma metodologia que combina a modelagem probabilística das Redes Bayesianas com a capacidade de tomada de decisão sequencial dos *Limited Memory Influence Diagrams* (LIMID) (IANINI *et al.*, 2023), a qual permite uma avaliação quantitativa dos riscos e dos danos potenciais decorrentes de atos mal-intencionados.

De modo, para aplicar a metodologia proposta será utilizado um modelo de uma base naval hipotética, considerando a disposição dos prédios com material nuclear e seu sistema preliminar de proteção física, desenvolvido por Santos (2024). Em seguida, serão postulados cenários de ataque e estratégias de defesas a fim de avaliar como as vulnerabilidades específicas podem influenciar as escolhas dos atacantes. Além disso, serão avaliadas quais são as medidas de segurança mais eficazes para mitigar esses riscos, obedecendo os requisitos impostos pelas normas brasileiras da CNEN e internacional da AIEA.

Destaca-se que a base naval, assim como os cenários propostos, são tratados de forma inteiramente hipotética, embora plausíveis e alinhados com a realidade e as demandas específicas do setor nuclear no que diz respeito à segurança física.

Nesse sentido, a motivação deste trabalho fundamenta-se no fato das instalações nucleares apresentarem riscos significativos devido ao potencial de impactos ambientais de longo prazo, contaminação em larga escala e possíveis implicações geopolíticas, por isso é necessário otimizar a segurança dessas instalações a fim de proteger vidas humanas, o meio ambiente e os ativos estratégicos do país.

Além disso, em um cenário onde orçamentos para segurança são limitados, a alocação eficiente de recursos é crucial, este estudo busca fornecer uma abordagem que permita maximizar a eficácia das medidas de segurança enquanto minimiza os custos, garantindo que os recursos sejam utilizados da melhor forma possível.

Cabe ressaltar que, a necessidade de combinar diferentes tipos de informações e a necessidade de levar em conta as interações mútuas entre os parâmetros exigem o uso de modelos adequados para fornecer aos proprietários das instalações uma avaliação mais realista possível, nesse contexto, a utilização de Redes Bayesianas (RN) e Diagramas de Influência de Memória Limitada (LIMID) representa uma abordagem inovadora para a avaliação de riscos e a tomada de decisões em segurança física

Em resumo, a motivação para este trabalho abrange desde a proteção de vidas e do meio ambiente, até a otimização de recursos e a inovação em metodologias de segurança e resposta a emergências. Esses fatores combinados justificam a importância e a relevância do estudo proposto.

Para atingir esses objetivos, o presente trabalho está organizado em seis capítulos, tais como segue.

O Capítulo 1 apresenta a contextualização do tema, os objetivos do estudo e a motivação para a aplicação de metodologias probabilísticas no apoio à decisão em proteção física de instalações nucleares.

O Capítulo 2 aborda os principais conceitos relacionados à proteção física de instalações nucleares, os métodos tradicionais de avaliação de sistemas de proteção física e os fundamentos das redes bayesianas e dos diagramas de influência, bem como o procedimento de revisão da literatura adotado neste trabalho.

No Capítulo 3 é descrita a metodologia proposta, incluindo o desenvolvimento do modelo conceitual de decisão, a formulação do modelo bayesiano de decisão na forma de Diagramas de Influência com Memória Limitada (LIMID), a definição das variáveis e seus estados, a parametrização das probabilidades condicionais e o procedimento de avaliação das alternativas de decisão.

O Capítulo 4 apresenta a aplicação da metodologia a um estudo de caso representativo de uma instalação nuclear inserida em uma base naval hipotética, incluindo a caracterização da instalação e a construção do modelo específico para o cenário analisado.

O Capítulo 5 discute os resultados obtidos, apresentando a análise comparativa das estratégias de proteção física sob condições de incerteza, bem como a análise de sensibilidade dos principais parâmetros do modelo.

Por fim, o Capítulo 6 apresenta as conclusões do trabalho e as perspectivas para estudos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 SISTEMAS DE PROTEÇÃO FISICA

O Sistema de Proteção Física (SPF) em instalações nucleares é um sistema integrado de medidas de detecção, atraso e resposta, e deve ser eficaz contra remoção não autorizada e sabotagem referente a material radioativo. Ele deve incluir pessoas, procedimentos e equipamentos para fornecer defesa em profundidade, com uma abordagem graduada, a fim de enfrentar a variedade de ameaças identificadas na declaração de ameaças aplicável e proteger tanto contra remoção não autorizada quanto contra sabotagem (IAEA, 2025).

No contexto da proteção física de instalações nucleares, conforem a IAEA,-*(2025), o Sistema de Proteção Física (SPF) é tradicionalmente estruturada a partir de quatro funções fundamentais: dissuasão, detecção, atraso e resposta, que são apresentadas nas subseções a seguir.

A dissuasão é alcançada se potenciais adversários considerarem uma instalação como um alvo pouco atraente e decidirem não atacá-la porque estimam que sua probabilidade de sucesso é muito baixa ou os riscos para si mesmos são muito altos

Projetistas de SPF podem adotar a metodologia de prevenção de crimes através do *design* ambiental, que utiliza elementos como iluminação, visibilidade e controle de acesso para desencorajar atividades maliciosas. Além disso, o uso estratégico de guardas e forças de resposta, como patrulhas aleatórias, posições fortificadas, postos de vigilância e veículos blindados, pode reforçar a dissuasão. A presença reforçada em situações específicas, como protestos pacíficos que poderiam ser explorados por adversários, também aumenta a capacidade de detecção, atraso e resposta, fortalecendo a segurança geral da instalação

A detecção em um SPF começa com a identificação de atividades suspeitas ou não autorizadas (por sensores, controle de acesso ou relatos) e termina com a avaliação que confirma se há uma ameaça real. O objetivo é detectar o mais cedo possível, utilizando medidas como alarmes, tecnologias de avaliação e controle de acesso.

O sistema de detecção de intrusão gera alarmes avaliados por um operador para identificar ameaças à segurança nuclear e depende da capacidade de sensoriamento e da avaliação dos alarmes. O sistema inclui sensores internos/externos, câmeras (CCTV),

controle de acesso e pessoal treinado, devendo detectar tentativas de remoção ou sabotagem de material nuclear conforme a avaliação de ameaças .

O projetista do sistema precisa conhecer as características da instalação e as tecnologias de detecção, incluindo suas limitações, para garantir eficácia contra as ameaças.

A probabilidade de detecção depende de fatores como a área coberta, o design do sensor, as condições de instalação, a sensibilidade ajustada, as condições climáticas e ambientais, e o estado do equipamento. Também pode variar significativamente com as capacidades do adversário. Nenhum sensor é 100% eficaz, mas a probabilidade de alarmes falsos ou incômodos deve ser minimizada, enquanto a probabilidade de detecção deve ser maximizada.

O atraso é uma função do SPF que busca retardar o progresso de um adversário em direção a um alvo, proporcionando mais tempo para uma resposta eficaz. Embora o atraso possa ocorrer antes da detecção, apenas o atraso após a primeira detecção de uma ação adversária auxilia na resposta. Ele é geralmente proporcionado por barreiras físicas, mas também pode ser reforçado por guardas ou forças de resposta. Todas as barreiras podem ser superadas, mas a função do atraso é ganhar tempo para que as medidas de resposta sejam acionadas antes que o adversário complete o ato malicioso

A resposta é a função do SPF que visa interromper e neutralizar um adversário, impedindo a conclusão de um ato malicioso. Um incidente de segurança física em instalações nucleares pode envolver uma força de reação composta por agentes internos, como guardas, ou externos, como polícia local, bombeiros e até a polícia federal.

A equipe de segurança (guardas e força de resposta) tem como funções: controle de acesso, patrulhas, avaliação de alarmes, resposta rápida e comunicação com a Central de Alarmes de Segurança (CAS). A força de resposta deve estar preparada para se mover, comunicar e neutralizar adversários, conforme a avaliação de ameaças.

Os fatores que influenciam no sucesso da força de reação são os equipamentos, qualificação e treinamentos, descrimanados a abaixo.

Equipamentos: Incluem veículos (blindados, aéreos, aquáticos), armas, sistemas de comunicação e tecnologias para consciência situacional (ex.: drones e sistemas de rastreamento de pessoal). Equipamentos de proteção, como postos blindados e veículos

armados, são essenciais para garantir a segurança da equipe e reduzir o tempo de resposta.

Qualificação: Guardas e equipes de resposta devem atender a requisitos mínimos de saúde, aptidão física, proficiência com armas, conhecimento de procedimentos e habilidades de comunicação.

Treinamento: deve ser baseado em cenários realistas, refletindo as capacidades dos adversários. Inclui exercícios de mesa, simulações de resposta e testes de força contra força, focados em conhecimento de procedimentos, planos de resposta, proficiência com armas (inclusive em condições de pouca luz), uso de força não letal e rastreamento de adversários.

2.2 PROJETO E AVALIAÇÃO DE UM SISTEMA DE PROTEÇÃO FÍSICA

Conforme a IAEA (2025), o processo de projeto e avaliação de um SPF deve ser sistemático e, preferencialmente, utilizar uma abordagem de engenharia de sistemas. A engenharia de sistemas é uma metodologia aplicada para projetar e construir sistemas complexos, envolvendo processos como:

- Definição de Requisitos: Estabelecer as necessidades e objetivos do SPF com base na análise de ameaças e nos ativos a serem protegidos.
- Projeto do Sistema: Desenvolver medidas integradas de detecção, atraso e resposta, alinhadas aos requisitos definidos.
- Avaliação do Projeto: Testar e analisar a eficácia do SPF contra cenários de ataque, identificando pontos fracos e oportunidades de melhoria.

O projeto de uma instalação nuclear deve levar em consideração os padrões de *safety* e *security*, ambos fundamentais e complementares para garantir o uso seguro, controlado e confiável da energia nuclear.

De modo geral, *security* (segurança física) está relacionado a ações intencionais que possam causar ou ameaçar danos a indivíduos, propriedades, sociedade ou ao meio ambiente, enquanto *safety* (segurança nuclear) refere-se à prevenção de consequências prejudiciais decorrentes da exposição à radiação, independentemente de sua causa (IAEA, 2022).

O *safety* envolve um conjunto de medidas técnicas e organizacionais baseadas no princípio da defesa em profundidade, incluindo a prevenção de acidentes, o monitoramento contínuo das operações, a implementação de sistemas de segurança para garantir o resfriamento do combustível nuclear e evitar a liberação de material radioativo, bem como o desenvolvimento de planos de emergência para lidar com eventos extremos (FERGURSON, SETTLE, 2012).

Por outro lado, o *security* abrange a prevenção, detecção e resposta a atos maliciosos, como roubo, sabotagem, acesso não autorizado e transferência ilegal de materiais nucleares ou radioativos. Dessa forma, embora ambos os conceitos estejam inter-relacionados e contribuam para a segurança global das instalações nucleares, a principal distinção entre eles reside na intencionalidade: eventos associados ao *safety* são, em geral, não intencionais, enquanto aqueles relacionados ao *security* resultam de ações deliberadas com objetivos específicos (IAEA, 2022).

A análise da eficácia de um Sistema de Proteção Física (SPF) é crucial para garantir que ele atenda aos seus objetivos de proteger ativos críticos, como uma base naval com material nuclear, e não é uma tarefa simples devido às características da instalação e às capacidades do adversário. É necessário prever a quantidade e a qualidade do adversário, sua capacidade, conhecimento, equipamentos, entre outros.

Devido à essa complexidade do SPF, técnicas de modelagem computacional são geralmente necessárias para a análise. Existem vários métodos e abordagens para realizar essa análise, cada um com suas vantagens e aplicações específicas. Alguns dos métodos explorados pela literatura são apresentaos a seguir.

2.2.1 Análise Sistêmica da Vulnerabilidade à Intrusão

Proposto por Matter (1988), o *System Analysis of Vulnerability to Intrusion* (SAVI), traduzido como Análise Sistêmica da Vulnerabilidade à Intrusão, é um programa computacional utilizado para avaliar a eficácia de um Sistema de Proteção Física (SPF). Ele determina os caminhos mais vulneráveis em um Diagrama de Sequência do Adversário (DSA), que serve como medida de eficácia. A análise com o SAVI começa com a identificação de um alvo e a construção de um DSA específico para o local. Em seguida, as características da ameaça devem ser especificadas,

incluindo o tempo de implantação da força de resposta, os valores de atraso e detecção para cada elemento de proteção no DSA. Todas essas informações são usadas como entrada para o código SAVI, que calcula a probabilidade de interrupção do adversário para cada caminho no DSA.

A abordagem unidimensional do SAVI ignora a complexidade do mundo real, onde o adversário pode explorar múltiplos caminhos ou estratégias baseadas na geografia do local (ZOU *et al.*, 2018) . Por exemplo, um adversário pode contornar um sensor se souber que ele está mal posicionado, algo que uma análise unidimensional não captura.

2.2.2 Estimativa da Interrupção da Sequência de Ações do Adversário

Desenvolvido por GARCIA (2008), o *Estimate of Adversary Sequence Interruption* (EASI), traduzido como Estimativa da Interrupção da Sequência de Ações do Adversário, examina a sequência de ações do adversário em um caminho de ataque e estima a probabilidade de uma equipe de resposta neutralizar os adversários antes que eles concluam sua missão de ataque. O EASI se destaca por integrar de forma eficiente os aspectos de detecção, atraso e resposta, oferecendo uma visão clara do tempo necessário para interromper um adversário. Essa abordagem é especialmente valiosa em instalações nucleares, pois permite avaliar a eficácia de barreiras, sensores e tempos de resposta em cenários de intrusão externa, que são críticos para a segurança dessas instalações (SANTOS, 2024).

Pelos motivos citados, esse método é amplamente utilizado na análise dos sistemas de proteção física de instalações nucleares, vale destacar o trabalho de SANTOS (2024), que consistiu na análise do SPF de uma base naval hipotética.

Uma das principais limitações do EASI é que ele se baseia em uma análise de caminho único, ou seja, avalia a probabilidade de interrupção do adversário para um único caminho de ataque, isso pode ser adequado para instalações nucleares simples e de pequeno porte, mas se torna insuficiente para instalações maiores e mais complexas, onde os adversários podem ter múltiplos caminhos ou estratégias de ataque (ANDIWIJAYAKUSUMA, 2022).

2.2.3 Análise Sistemática da Efetividade da Proteção Física

Desenvolvido por JANG *et al.* (2009), Systematic Analysis of Physical Protection Effectiveness (SAPE), traduzido como Análise Sistemática da Efetividade da Proteção Física, é uma evolução dos códigos de avaliação anteriores, que utilizam um modelo simples chamado diagrama de sequência do adversário. Ele usa um mapa bidimensional e um algoritmo heurístico generalizado ara analisar o sistema de proteção física, esse código foi aplicado a diversas instalações e avaliado quanto à sua viabilidade ao ser testado em diferentes contextos

Diferentemente de abordagens mais simplificadas, como aquelas baseadas em caminhos únicos, o SAPE considera a possibilidade de exploração de diversas rotas pelo adversário, o que implica na análise de um grande número de combinações entre elementos de detecção, atraso e resposta. Esse aumento na complexidade do modelo resulta em maior demanda por processamento computacional e tempo de execução, especialmente em cenários com elevada granularidade espacial ou grande quantidade de componentes de segurança. Além disso, estudos indicam que métodos baseados em avaliação exaustiva de caminhos e algoritmos heurísticos, como o SAPE, podem enfrentar dificuldades de escalabilidade quando aplicados a instalações extensas ou altamente complexas, limitando sua aplicabilidade prática em análises em tempo real ou em processos iterativos de otimização (GARCIA, 2008; ZOU *et al.*, 2018). Dessa forma, embora o SAPE represente um avanço em relação a métodos mais simplificados, seu custo computacional elevado constitui um fator limitante, incentivando a busca por abordagens alternativas mais eficientes e flexíveis.

2.2.4 Utilização de Redes Bayesianas

Uma alternativa à esse métodos mais tradicionais é a utilização de redes bayesianas, as quais permitem modelar a incerteza e as interdependências entre variáveis, proporcionando uma abordagem mais flexível e abrangente para analisar cenários complexos e avaliar a capacidade dos sistemas em mitigar ameaças.

Ao longo dos anos, as Redes Bayesianas têm sido cada vez mais adotadas no campo da segurança de infraestruturas críticas, como industrias químicas, instalações de

petróleo e gás, portos e redes ferroviárias, devido à sua capacidade de prever a probabilidade de variáveis desconhecidas ou de atualizar a probabilidade de variáveis conhecidas (IANINI *et al.*, 2023).

KANG e KOH (2017) propuseram uma abordagem baseada em Redes Bayesianas para calcular a probabilidade de detecção de comportamentos anormais e identificar caminhos vulneráveis em usinas nucleares, utilizando informações sobre pontos cegos das câmeras de vigilância.

ARGENTI *et al.*, (2018) utilizou redes Bayesianas para avaliar as vulnerabilidades de instalações químicas a ataques intencionais com o desenvolvimento uma abordagem quantitativa para a avaliação probabilística da vulnerabilidade a ataques externos. Essa rede permitiu representar as interações entre o fatores de impacto de um ataque e as medidas de proteção das unidades de processo, possibilitando determinar os resultados finais de um ataque. Uma análise detalhada dos sistemas de proteção, com base em dados de desempenho fornecidos por especialistas, ajudou a calcular as probabilidades de forma mais precisa.

ZHU *et al.* (2020), estudaram o uso redes bayesianas para modelar e análisar riscos de ataques terroristas com armas químicas e produtos industriais tóxicos.

Ataques envolvendo o uso de dispositivos de dispersão radiológica, popularmente conhecidos como bombas sujas, foram estudados por TANG *et al.* (2019) com a utilização de uma Rede Bayesiana, o que permitiu examinar o impacto de fatores como o horário do ataque, localização, campos de vento, tamanho da bomba suja, resposta de emergência e abordagens de defesa sobre as vítimas, tanto do impacto direto da explosão quanto dos cânceres causados pela radiação.

WALL e AGRAFIOTIS (2021) propuseram e avaliaram uma arquitetura de Rede Bayesiana para detectar ameaças internas, combinando dados de rede com aspectos comportamentais. O Modelo incorporou características específicas baseadas em teorias sobre ameaças internas, permitindo que os analistas considerassem também dados comportamentais, quando disponíveis.

CARLESS, REDUS e DRYDEN (2021) estimaram os riscos associados à introdução de energia nuclear em países emergentes, como a probabilidade de desvio de material nuclear para fins militares, roubo por atores não estatais e uso indevido de

tecnologia nuclear, com a utilização de Redes Bayesianas e o julgamento de especialistas.)

GRACE ee RENJITH (2021) propuseram um método para classificar possíveis ameaças e priorizar as medidas de proteção a serem implementadas, utilizando uma abordagem probabilística com diagramas de influência para representar diferentes categorias de ameaças e tipos de armas, como nucleares, biológicas e explosivos

IANINI *et al.* (2023) utilizou redes bayesianas para avaliar a probabilidade de sucesso de ataques à segurança física em instalações *offshore* de petróleo e gás. O estudo considerou múltiplas estratégias de intervenção de segurança (tanto preventivas quanto mitigativas) e utilizou redes bayesianas para modelar as dependências probabilísticas e atualizar as probabilidades com base em novos dados, enquanto o modelo EASI forneceu a base para avaliar a interrupção do ataque com base no tempo restante da tarefa do adversário e o tempo de resposta e calcular as tabelas de probabilidade condicional para os nós de intervenção.

WANG, WU e YUEN (2023) propuseram um método de quatro etapas para estudar a resiliência de portos, identificando e classificando os principais distúrbios que os afetam. Eles desenvolveram um modelo de avaliação de resiliência portuária usando Redes Bayesianas, categorizando estratégias de resiliência em preparação e resposta.

MARRONI *et al.* (2024) desenvolveu uma metodologia para avaliar perdas econômicas causadas por ataques intencionais a instalações industriais, utilizando Redes Bayesianas para considerar fatores como cenários de intrusão e interdependências. Ele demonstrou que ataques bem-sucedidos podem causar danos significativos a pessoas e perdas econômicas relevantes e que, além disso, a análise conjunta de barreiras de segurança e proteção melhora a precisão na estimativa de perdas de ativos.

HOU *et al.* (2025) propôs um método para alocar recursos defensivos de forma otimizada em redes ferroviárias, que são altamente vulneráveis a ataques intencionais, ele utilizou um modelo de rede bayesiana e considerou a importância das estações e as diferentes preferências dos atacantes.

MOHSENDOKHT *et al.* (2025) desenvolveu um método inovador para análise de riscos de segurança marítima, focando em ataques terroristas marítimos, que podem ocorrer tanto em alto mar quanto em portos, os autores treinaram um modelo de Rede

Bayesiana Orientada a Dados para identificar fatores-chave, analisar interdependências e prever probabilidades de diferentes cenários terroristas.

Dentro desse contexto, tem destaque o método desenvolvido por MISURI *et al.* (2019), que utiliza redes bayesianas para otimização da segurança física em estruturas criticas. O modelo consiste em duas decisões sequenciais. A primeira decisão diz respeito as medidas de segurança dentro das instalações da infraestrutura crítica antes que um ataque ocorra, enquanto a segunda decisão descreve as possíveis respostas de segurança que os defensores podem adotar caso um ataque seja realizado, o que torna o processo de tomada de decisão dinâmico, pois o defensor terá a oportunidade de adaptar sua estratégia de acordo com os resultados do ataque.

Essa abordagem permite levar outros fatores em consideração, pois ao considerar os adversários como tomadores de decisão racionais, ela analisa a possibilidade deles redirecionarem sua atenção para alvos mais vulneráveis como reação ao fortalecimento dos sistemas de segurança.

Uma limitação dessa abordagem é a mesma dos métodos tradicionais baseados em cenários. O modelo é construído considerando um conjunto fixo e predeterminado de cenários para adversários e características de ataques. Dessa forma, ele não consegue levar em conta adversários inovadores, que podem planejar novos tipos de ataques, definir alvos não tradicionais ou desenvolver tecnologias imprevisíveis.

As dependências probabilísticas devem ser determinadas pelo defensor, sendo que a maior parte das probabilidades precisa ser estimada diretamente a partir do julgamento de especialistas, enquanto as preferências dos adversários entre diferentes tipos de cenários podem ser avaliadas usando a abordagem baseada no conhecimento da inteligência sobre os possíveis grupos adversários e suas preferências entre diferentes ações, considerando que eles são racionais e tentariam maximizar a utilidade esperada de seu ataque.

Por fim, vale ressaltar que as Redes Bayesianas têm limitações: os resultados refletem um momento específico, exigindo atualizações frequentes devido a mudanças tecnológicas e políticas. Além disso, como dependem de julgamentos subjetivos de especialistas, estão sujeitas a vieses humanos, o que requer um design cuidadoso para minimizar esses vieses. (CARLESS, REDUS, DRYDEN, 2021).

2.3 REDES BAYESIANAS

As redes bayesianas são modelos gráficos probabilísticos baseados no Teorema de Bayes, uma ferramenta fundamental na teoria das probabilidades que permite atualizar nossas crenças (probabilidades) sobre um evento com base em novas evidências (MISURI *et al.*, 2019). Essas redes são amplamente utilizadas para elicição de conhecimento e raciocínio sob incerteza, sendo representadas por um grafo acíclico direcionado que modela as dependências entre variáveis aleatórias.

Uma rede bayesiana é um modelo gráfico probabilístico que utiliza o Teorema de Bayes para representar dependências condicionais entre variáveis e permitir a realização de inferências sob incerteza. Estruturalmente, consiste em um grafo acíclico direcionado, no qual os nós representam variáveis aleatórias e os arcos indicam relações de dependência entre elas. Esse tipo de modelo é amplamente reconhecido como uma das principais ferramentas para representação e análise de conhecimento incerto em sistemas complexos, permitindo tanto a incorporação de conhecimento especializado quanto a utilização de dados para atualização das probabilidades associadas (WANG *et al.*, 2025).

A principal propriedade das Redes Bayesianas é a independência condicional. De forma geral, essa propriedade estabelece que cada variável do modelo depende apenas das variáveis que a influenciam diretamente, denominadas seus nós pais. Assim, uma vez conhecidos os valores dessas variáveis, as demais variáveis do modelo tornam-se irrelevantes para a determinação da sua probabilidade (WANG, *et al.*, 2025). Como consequência, a distribuição conjunta de probabilidade pode ser obtida a partir de probabilidades menores e mais simples, associadas a cada variável e às variáveis que a influenciam diretamente. Em vez de calcular a probabilidade de todas as variáveis simultaneamente, o modelo permite decompor esse cálculo em termos condicionais locais, reduzindo significativamente a complexidade do problema, conforme a Equação (1).

$$P(E_1, E_2, \ldots, E_n) = \prod_{i=1}^{n} P(E_i | pais(E_i)) \qquad \text{Eq (1)}$$

A figura 1 (MILLIAM *et al.*, 2010).representa um exemplo simplicado de uma rede bayesiana com seis variaveis. Na rede, os nós Gato, Alergia e Resfriado são considerados nós raiz, pois não possuem pais. Isso significa que suas probabilidades são definidas de forma independente, representadas por distribuições marginais. Esses nós funcionam como causas iniciais no modelo, influenciando outras variáveis, mas não sendo influenciados por nenhuma dentro da estrutura apresentada (POURRET, 2008).

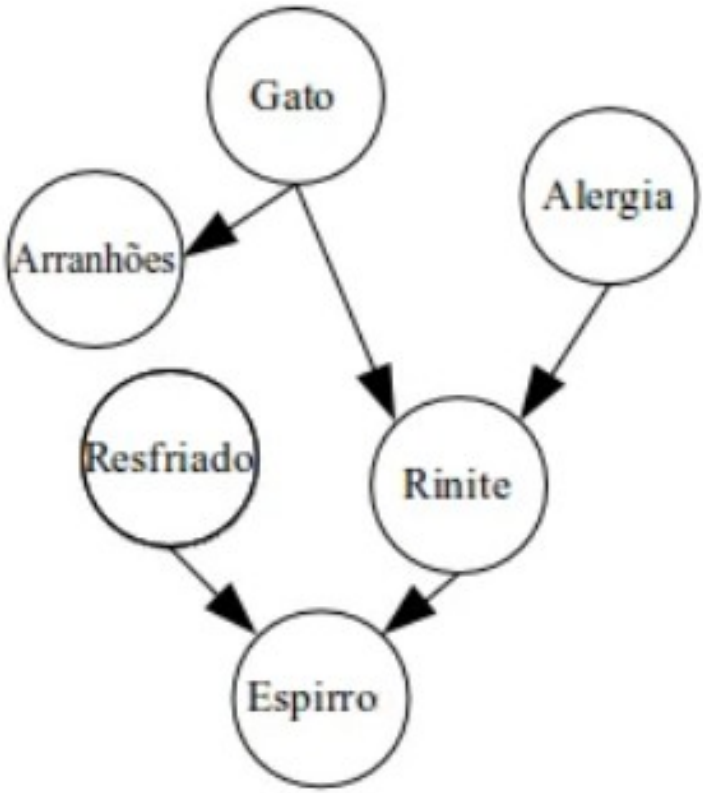

Figura 1: Exemplo de rede bayesiana (MILLIAM *et al.* , 2010)

O nó Arranhões é um no filho, pois possui como pai o nó Gato, indicando que a ocorrência de arranhões depende diretamente da presença ou contato com um gato. Já o nó Rinite possui dois pais, Gato e Alergia, o que significa que sua probabilidade depende da combinação dessas duas variáveis. Por fim, o nó Espirro é influenciado por dois pais, Rinite e Resfriado. Isso indica que o espirro pode ser consequência tanto de uma rinite quanto de um resfriado, ou da interação entre ambos. Dessa forma, o modelo

captura diferentes caminhos causais que levam ao mesmo sintoma, permitindo análises mais realistas e completas.

Cada uma dessas variáveis é definida por um conjunto de estados possíveis, que representam os valores que ela pode assumir (BAYESFUSION, 2024). Por exemplo, a variável “Rinite” possui dois estados: “Verdadeiro”, indicando a presença da condição, e “Falso”, indicando sua ausência. Esses estados são mutuamente exclusivos, uma vez que apenas um pode ocorrer em determinado momento, e conjuntamente exaustivos, por contemplarem todas as possibilidades relevantes para a variável.

Uma vez definidos os estados, associa-se a cada nó uma Tabela de Probabilidade Condicional (TPC), responsável por descrever quantitativamente o comportamento da variável. Essas tabelas especificam as probabilidades de ocorrência de cada estado, podendo ser independentes, no caso de nós raiz, ou condicionadas aos estados dos nós pais (POURRET, 2008). Dessa forma, as TPCs traduzem numericamente as relações qualitativas representadas pelo grafo, sendo fundamentais para o funcionamento da rede bayesiana como ferramenta de apoio à decisão e análise probabilística.

Por exemplo, a Tabela 1 apresenta a Tabela de Probabilidade Condicional da variável “Rinite”, que possui como pais as variáveis “Alergia” e “Gato”.

Tabela 1 - Probabilidade de Rinite dado Alergia e Gato (MILLIAM, E *et al.* , 2010)

Alergia	**Gato**	**P(Rinite = V)**	**P(Rinite = F)**
V	V	0,99	0,01
V	F	0,8	0,2
F	V	0,10	0,9
F	F	0,005	0,995

2.3.1 Teorema de Bayes

O Teorema de Bayes é um princípio da teoria das probabilidades que permite atualizar a probabilidade de uma hipótese à medida que novas evidências são incorporadas. Ele estabelece uma relação entre a probabilidade inicial de um evento (probabilidade a priori) e a probabilidade condicionada à observação de determinados dados (probabilidade a posteriori), considerando também a verossimilhança dessas

evidências. Dessa forma, o teorema fornece um mecanismo formal para a revisão de probabilidades diante de novas informações, sendo amplamente aplicado em contextos que envolvem incerteza, como análise de riscos, diagnóstico e previsão. (DEGROOT, M; SCHERVISH,M., 2012).

O Teorema de Bayes é definido pelas equações (2) e (3). A equação (2) permite calcular a probabilidade condicional de um evento E, dado que o evento F ocorreu:

$$P(E|F)=\frac{P(F|E)\cdot P(E)}{P(F)} \quad \text{Eq (2)}$$

onde:

- P(E | F): Probabilidade de *E* dado *F* (probabilidade posterior).
- P(F | E): Probabilidade de *F* dado *E* (verossimilhança).
- P(E): Probabilidade a priori de *E*.
- P(F): Probabilidade marginal de F.

A equação 3 generaliza o Teorema de Bayes para casos em que há múltiplos eventos $E_1,E_2,\ldots,E_n$:

$$P(E_i|F)=\frac{P(F|E_i)\cdot P(E_i)}{\sum_{j=1}^{n} P(F|E_j)\cdot P(E_j)} \quad \text{Eq. (3)}$$

2.3.2 Diagramas de Influência de Memória Limitada (LIMIDs)

Diagramas de Influência (DIs) representam uma sofisticação das Redes Bayesianas (BNs) ,eles são uma estrutura intuitiva para formular problemas conforme percebidos pelos tomadores de decisão e para incorporar o conhecimento de especialistas (SHACHTER, 1986)

Os DIs têm a mesma estrutura das BNs, mas incluem dois tipos adicionais de nós: nós de decisão e nós de utilidade. Os nós de decisão correspondem às escolhas (alternativas de decisão) disponíveis para o tomador de decisão, enquanto os nós de utilidade são nós cujos valores, que são números (não probabilidades), representam as

preferências do tomador de decisão em relação ao resultado de cada alternativa de decisão (MISURI *et al.*, 2019).

Diagramas de Influência de Memória Limitada (daqui em diante, LIMIDs) são generalizações dos diagramas de influência que permitem a tomada de decisão com informação limitada, como no caso de decisões simultâneas, controladores com memória limitada e agentes cooperativos que não se comunicam (MAUÁ, 2012).

A Figura 2, adaptada de Misuri *et al.* (2019), apresenta a representação de um problema de segurança nacional por meio de um Diagrama de Influência com Memória Limitada (LIMID), no qual diferentes tipos de nós são utilizados para modelar, de forma integrada, as incertezas do cenário, as alternativas de decisão e as consequências associadas. É possível observar que a representação gráfica do LIMID na Figura 2 possui diferentes tipos de nós: chance, decisão e utilidade (BAYESFUSION, 2024).

Os nós de chance, representados por formas ovaladas, correspondem às variáveis incertas do sistema, ou seja, aquelas que não estão sob controle direto do tomador de decisão. No contexto da figura 2, exemplos incluem os nós probabilidade de chuva, previsão do tempo e nuvens escuras.

Os nós de decisão, representados por retângulos, correspondem às variáveis sobre as quais o tomador de decisão possui controle. Esses nós representam as alternativas disponíveis, sendo definidos por um conjunto discreto de ações possíveis. Na Figura 2, o nó “Levar Guarda-chuva” é um exemplo desse tipo, pois representa as ações que podem ser adotadas para mitigar ou responder às ameaças identificadas.

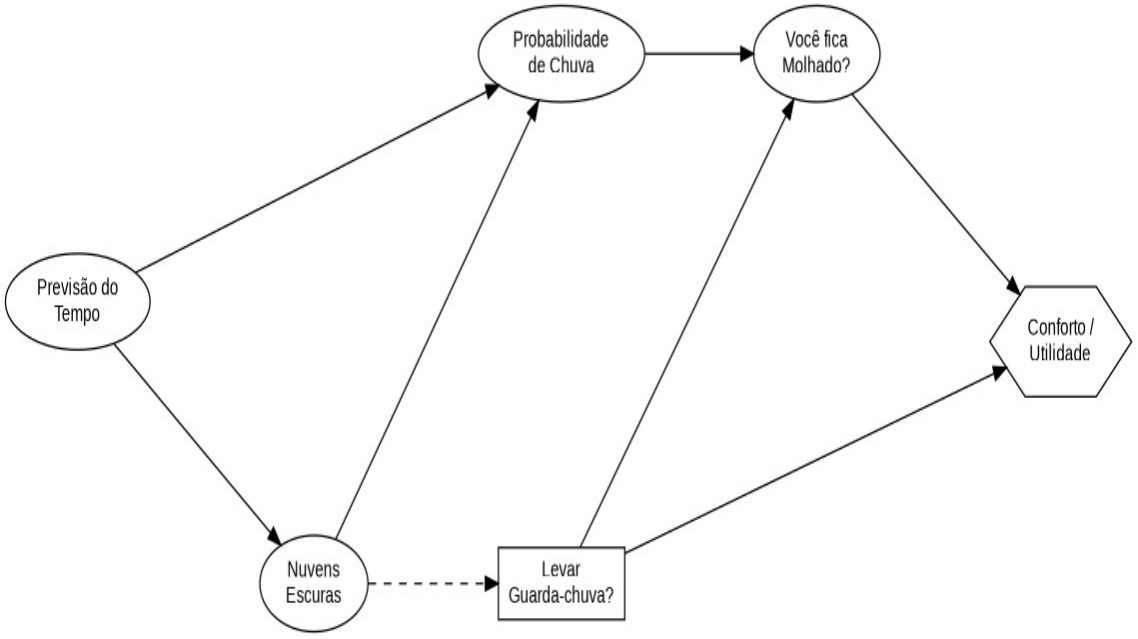

Figura 2 - Exemplo de um LIMID

A decisão representa nesse grafo envolve uma troca:

- Levar o guarda-chuva reduz o risco de ficar molhado, mas gera o custo de carregar algo que pode ser inútil.
- Não levar o guarda-chuva evita esse inconveniente, mas aumenta o risco de sofrer uma consequência pior caso chova.

Já os nós de valor, representados por hexágonos, expressam os objetivos do modelo e permitem avaliar os resultados das decisões. Esses nós não representam incerteza nem decisão, mas sim a forma como os resultados são avaliados. No caso da figura, o nó “Conforto/Utilidade” sintetiza os impactos finais do cenário, incorporando os efeitos combinados das variáveis anteriores e permitindo comparar diferentes alternativas de decisão com base em sua utilidade.

No contexto dos LIMIDs, cada possível escolha em um nó de decisão é chamada de política, enquanto a combinação de escolhas ao longo de múltiplos nós de decisão constitui uma estratégia. A solução do modelo consiste em identificar a política ou estratégia que maximiza a utilidade esperada, permitindo selecionar, de forma estruturada, a melhor alternativa diante das incertezas do sistema. A equação 4 é utilizada para calcular essa utilidade:

$$UE(d)=\sum_{c} U(c,d)\cdot P(c) \quad \text{Eq.(4)}$$

onde:

- EU(d): utilidade esperada associada à decisão d;
- d: alternativa de decisão considerada pelo tomador de decisão;
- c: possível estado da natureza ou consequência incerta relevante para a decisão;
- U(c,d): utilidade obtida quando a decisão d é adotada e ocorre o estado c;
- P(c): probabilidade de ocorrência do estado c;

Embora o cálculo exato dessas probabilidades possa se tornar computacionalmente complexo em redes de grande dimensão, existem algoritmos capazes de fornecer soluções exatas ou aproximadas de forma eficiente. Esses métodos estão implementados em diferentes ferramentas computacionais, amplamente utilizadas para modelagem e inferência em redes bayesianas. No presente trabalho, as redes foram modeladas e avaliadas com o auxílio do software GeNIe.

2.4 HISTÓRICO DE ATAQUES CONTRA INSTALAÇÕES NUCLEARES

A definição das combinações de atributos utilizadas neste trabalho não foi realizada de forma arbitrária. Para subsidiar a construção dos cenários analisados, foi elaborado um levantamento de eventos históricos envolvendo ataques, tentativas de sabotagem e incidentes de segurança em instalações nucleares.

Dessa forma, o conjunto de alternativas e cenários analisados permite explorar, de maneira sistemática, o impacto das decisões estratégicas de segurança sobre a probabilidade de neutralização do adversário, os danos potenciais e a utilidade total associada a cada estratégia, fornecendo subsídios objetivos para a comparação entre diferentes opções de proteção física no contexto da instalação nuclear considerada.

A Tabela 2 apresenta um histórico de casos documentados na literatura envolvendo ataques ou tentativas de ataque a instalações nucleares ou a infraestruturas associadas, cujas informações foram compiladas a partir de diferentes fontes abertas, incluindo relatórios técnicos, bases institucionais e registros jornalísticos, como World Institute for Nuclear Security (2020), Nuclear Regulatory Commission (1981), OECD

Nuclear Energy Agency (2022), U.S. Department of Energy Office of Scientific and Technical Information (2015), Bellona Foundation (2002), Washington Post (1979; 1985), Los Angeles Times (1985; 1986; 1987), El País (1979; 2004), Le Monde (1982).

Tabela 2 - Históricos de ataques contra instalações nucleares

Ano	Local	Descrição
1973	Atucha Nuclear Power Plant, Lima, Argentina	Cerca de 15 integrantes do Ejército Revolucionario del Pueblo (ERP) invadiram o canteiro de obras da instalação, explorando a limitada segurança típica desse estágio, realizaram o roubo de armamentos e deixaram mensagens de cunho político com objetivo de propaganda
1975	Brennilis Nuclear Power Plant, Monts d'Arree, France	Ocorreram duas explosões dentro da instalação que causaram danos leves a uma turbina e destruíram um circuito telefônico interno, sem provocar vítimas ou liberação radiológica, sendo o evento associado a um ato de sabotagem de baixa intensidade, com impacto operacional limitado, mas que evidenciou vulnerabilidades em sistemas auxiliares da planta
1977	Lemoniz Nuclear Power Plant, Lemoniz, Spain	15 integrantes da organização separatista ETA invadiram o canteiro da usina como parte de ações de cunho político contra o projeto nuclear, explorando vulnerabilidades típicas dessa fase e buscando principalmente demonstrar capacidade operacional e pressionar o governo, sem registro de liberação radiológica, mas evidenciando riscos associados à segurança física de instalações nucleares em contextos de conflito interno.
1977	U.S. 42nd Field Artillery Brigade at Giessen, Geissen, West Germany	Integrantes da organização extremista Red Army Faction (RAF) realizaram um ataque com explosivos contra instalações de armazenamento de combustível, detonando bombas em tanques e causando danos materiais significativos, sem vítimas fatais, caracterizando uma ação de sabotagem com motivação política voltada a atingir infraestrutura militar e gerar impacto simbólico durante o período de tensão da Guerra Fria
1977	Trojan Nuclear Power Plant, Ranier, Oregon, U.S.A.	Um artefato explosivo foi detonado nas proximidades do centro de visitantes da instalação, causando danos materiais limitados e sem registro de vítimas ou liberação radiológica, sendo o incidente caracterizado como um ato de sabotagem de baixa intensidade com provável motivação política, que

		evidenciou a vulnerabilidade de áreas periféricas e de acesso público em instalações nucleares.
1978	Lemoniz Nuclear Power Plant, Lemoniz, Spain	A organização separatista ETA realizou um atentado ao posicionar um artefato explosivo no prédio do reator da usina, ainda em construção, cuja detonação destruiu parte da estrutura, resultou na morte de dois operários e provocou a paralisação das obras por semanas
1979	Lemoniz Nuclear Power Plant, Lemoniz, Spain	Dois integrantes da organização separatista ETA instalaram um artefato explosivo na área da turbina da usina, ainda em construção, cuja detonação causou danos significativos à infraestrutura, sem liberação radiológica, caracterizando mais um ato de sabotagem com motivação política que contribuiu para atrasos adicionais, aumento dos custos do projeto e reforço das medidas de segurança no complexo.
1979	Equipos Nucleares facility, Maliano, Spain	Cinco integrantes da organização separatista ETA realizaram um ataque coordenado durante a madrugada, no qual detonaram artefatos explosivos que danificaram galpões de fabricação e escritórios administrativos, ao mesmo tempo em que sequestraram temporariamente cerca de 10 guardas da instalação, sem registro de vítimas fatais, caracterizando uma ação de sabotagem com impacto operacional relevante e forte conotação política.
1979	Kaiseraugst Nuclear Power Plant, Kaiseraugst Switzerland	Um artefato explosivo foi detonado em um dos prédios da instalação, ainda em fase de projeto e construção, causando danos materiais localizados, sem registro de vítimas ou liberação radiológica, caracterizando um ato de sabotagem de baixa intensidade associado ao contexto de oposição ao programa nuclear no país e evidenciando vulnerabilidades em áreas não operacionais da planta.
1979	Surry Nuclear Power Plant, Surry, Virginia, U.S.A.	Funcionários da própria instalação estiveram envolvidos em um incidente no qual soda cáustica foi deliberadamente introduzida em elementos combustíveis, sem causar liberação radiológica ou danos graves à operação, caracterizando um caso de ameaça interna (*insider*) com potencial de impacto significativo, mas que resultou apenas em consequências operacionais limitadas e reforçou a importância de controles de acesso e monitoramento de pessoal em instalações nucleares.
1979	Gösgen Nuclear Power Plant	Um ato de sabotagem atingiu um mastro de aço de aproximadamente 110 metros utilizado para medições

	Plant, Däniken, Switzerland	meteorológicas, localizado fora do perímetro cercado, mas próximo ao sistema de transformadores e barramentos de 400 kV, cuja ancoragem foi destruída por explosivos por volta da 1h30 da manhã, fazendo com que a estrutura caísse sobre a infraestrutura elétrica e causasse danos significativos; como consequência, a usina precisou ser desconectada da rede e desligada
1981	Nine Mile Point Nuclear Power Plant, Oswego, New York, U.S.A.	Em julho de 1981, a área de processamento de resíduos radioativos da usina (radwaste building) foi intencionalmente alagada, levando à queda de tambores contendo resíduos contaminados e à liberação de água radioativa no subsolo. Mais tarde, parte dessa água teve de ser lançada no Lago Ontário por saturação dos tanques de contenção.
1982	Superphenix Fast-Breeder Reactor, Creys-Malville, France	O reator rápido Superphénix, ainda em construção em Creys-Malville, França, foi alvo de um ataque realizado por militantes do grupo Action Directe, que dispararam foguetes antitanque a partir da margem oposta do rio Ródano; um dos projéteis atingiu o edifício do reator, perfurando uma parede de aproximadamente 40 cm sem alcançar a contenção interna, causando danos estruturais significativos, atrasando o cronograma da obra e levando ao reforço das medidas de segurança nuclear no país, com prejuízos estimados em cerca de 50 milhões de francos franceses (aproximadamente R$ 100 milhões em valores atuais).
1982	Salem Nuclear Power Plant, Salem, New Jersey, U.S.A.	Autoridades norte-americanas investigaram um possível caso de sabotagem na usina nuclear de Salem, em Lower Alloways Creek (Nova Jersey). Um operador encontrou duas válvulas fechadas em um gerador a diesel de emergência, que haviam sido verificadas abertas apenas cinco horas antes. O fechamento não afetou a operação da planta, que continuou em plena capacidade, mas levantou suspeitas porque, uma semana antes, a NRC e o FBI já haviam sido acionados para investigar a perda de energia em um painel de controle, causada por um interruptor manualmente desligado, o que levara ao desligamento preventivo do reator.
1982	Koeberg Nuclear Power	Após uma série de incidentes de segurança naquele ano, um militante da ANC conseguiu burlar os

	Station, Cape Town, South Africa	controles reforçados e instalar explosivos dentro da instalação. As bombas explodiram entre 18 e 19 de dezembro, danificandoprédios do reator e áreas de controle, mas sem causar vítimas.
1983	Hardt Barracks, Schwäbisch Gmünd, West Germany	Quatro indivíduos invadiram a base militar e danificaram um caminhão utilizado para o lançamento de mísseis, em uma ação de sabotagem com provável motivação política no contexto das tensões da Guerra Fria, causando prejuízos materiais sem registro de vítimas e evidenciando vulnerabilidades em instalações militares estratégicas.
1984	Minuteman ICBM silo, Higginsville, Missouri, U.S.A.	Em 12 de novembro de 1984 um grupo de ativistas antinucleares invadiu o perímetro de um silo Minuteman (N-05) (usada para lançar misseis intercontinentais) perto de Higginsville, Missouri, cortou a cerca, subiu ao tampão do silo e o danificou usando marretas e um martelo-pneumático, deixando uma faixa e reivindicando o ato como protesto contra armas nucleares.
1985	Palo Verde Nuclear Power Plant, Wintersburg, Arizona, U.S.A.	Em 11 de julho de 1985, foi relatado pela imprensa que a usina nuclear ainda em construção (unidade 1 ainda não comercial) teve uma queda drástica de pressão no sistema de refrigeração depois que alguém “manipulou” quatro conjuntos de válvulas de água
1985	Bataan Nuclear Power Plant, Bataan, Philippines	26 torres de transmissão associadas à infraestrutura da usina foram derrubadas em um ato de sabotagem, causando interrupções significativas no sistema elétrico e prejuízos materiais relevantes, sem registro de vítimas ou liberação radiológica.
1986	Palo Verde Nuclear Power Plant, Wintersburg, Arizona, U.S.A.	Na noite de 14 de maio de 1986, pelo menos três indivíduos escalaram torres de transmissão de alta tensão (> 100 ft) que levavam energia à usina, desmontaram ou danificaram os condutores e provocaram falha nas linhas que sustentavam a alimentação elétrica da planta nuclear.
1987	Sandia National Laboratories, Livermore, California, U.S.A.	Em 29 de novembro de 1987: uma bomba explodiu no estacionamento da instalação, destruindo dois carros e quebrando janelas de um laboratório próximo.
1992	Chepetsky Metallurgical Plant,	Pelo menos 12 pessoas, incluindo funcionários da instalação e membros da segurança, roubaram uma quantidade considerável de urânio (identificado como urânio natural e empobrecido), desviando cerca de

	Glazov, Russia	4% da “perda de inventário permitida” a cada mês, durante vários meses. Eles contrabandeavam o material após acumular uma quantidade significativa. O Serviço Federal de Segurança da Rússia (FSB) apreendeu pelo menos parte (possivelmente todo) o material roubado. Verificações de inventário posteriores revelaram que um total de 300 quilos de urânio estava faltando na instalação.
1992	Ignalina Nuclear Power Plant, Visaginas, Lithuania	O técnico interno e programador de software Oleg Savchuck foi preso ao tentar introduzir um vírus no sistema de computadores da Usina Nuclear de Ignalina. A usina também sofreu uma pane no sistema de resfriamento do primeiro reator, mas a conexão entre os dois incidentes não foi confirmada.
1992	Ignalina Nuclear Power Plant, Visaginas, Lithuania	Um conjunto de combustível de LEU de 280 kg, contendo 100 kg de LEU, foi amarrado sob a carroceria de um ônibus em serviço e contrabandeado com sucesso para fora da instalação, com auxilio de fucionários.
1991	Udmurtia, Russia	Um homem preso por contrabandear 2,5 kg de urânio para a Polônia admitiu já ter contrabandeado 3 kg e disse fazer parte de um grupo maior que planejava roubar um total de 100 kg de urânio-238 de uma “fábrica” em Udmúrtia, na Rússia, e contrabandeá-lo para a Polônia
1992	Luch Scientific Production Association, Podolsk, Russia	Em 1992, um engenheiro da Luch, identificado em fontes como Leonid Smirnov, desviou pequenas quantidades diárias de urânio altamente enriquecido (HEU ~90%), abaixo do limiar de detecção contábil, acumulando cerca de 1,5 kg ao longo de alguns meses. O furto só foi descoberto quando a polícia o abordou por outro motivo e encontrou HEU em sua posse; o material foi recuperado e o caso passou a ser referência clássica de sabotagem/roubo por *insider* em instalações nucleares pós-soviéticas.
1992	Borne-Sulinowo garrison, Borne Sulinowo, Poland	Dois contêineres de Césio-137 (Cs-137) foram roubados da antiga guarnição soviética de Borne-Sulinowo, na Polônia. Os autores do furto eram soldados designados para guardar o local e dois fazendeiros locais. Após 12 dias de buscas, foi encontrado um contêiner contendo 88 kg de material e um segundo contêiner com 35 kg de material não identificado.

1993	Three Mile Island Nuclear Power Plant, Londonderry Township, Pennsylvania, U.S.A.	O incidente ocorreu em 7 de fevereiro de 1993, quando um homem de 31 anos, em estado de depressão, invadiu de carro a usina nuclear de Three Mile Island (Pensilvânia, EUA). Ele dirigiu o veículo da mãe, um Plymouth 1984, através do portão de segurança, derrubou a cerca de área protegida e arrombou uma porta de rolo, parando cerca de 20 metros dentro do prédio da turbina. Após sair do carro, ele desceu uma escada e se escondeu em uma área escura sob o condensador. A usina continuou operando em plena potência, enquanto os operadores monitoravam atentamente os instrumentos para detectar qualquer sinal de sabotagem. Os guardas assumiram posições defensivas e trancaram todas as portas por controle computadorizado, o que aumentou a segurança, mas também atrasou a chegada de equipes externas. Cerca de quatro horas depois, o intruso foi encontrado enrolado em posição fetal, desorientado, e preso.
1993	Andreeva Guba Technical Base, Kola Peninsula, Russia	Pelo menos três pessoas internas (dois militares e pelo menos um guarda de segurança) conspiraram, em pelo menos uma ocasião, para roubar entre 1,8 kg e 3,6 kg de urânio altamente enriquecido (~35% HEU) provenientes de dois conjuntos de combustível de reator naval. Os guardas responsáveis pelo posto de alarme teriam cooperado com o roubo. O material foi posteriormente recuperado, e os culpados condenados a penas de 4 a 5 anos de prisão. Os condenados alegaram ter atuado sob ordens de dois oficiais, mas os oficiais negaram as acusações e foram absolvidos.
1993	Elektrostal plant, Moscow Oblast, Russia	Relatórios indicaram que guardas da instalação desligavam temporariamente o sistema de segurança em troca de 1.000 rublos. Outro relatório do mesmo período apontou que 3,05 kg de urânio altamente enriquecido (HEU) haviam sido roubados da instalação. Um material que pode ter sido o mesmo desaparecido desse local foi encontrado em São Petersburgo em junho de 1994.
1993	Severomorsk Naval Yard, Severomorsk, Russia	Um oficial naval russo e pelo menos dois comparsas roubaram 4 kg de urânio enriquecido (20% U-235) de uma área pouco vigiada da base. O oficial foi posteriormente preso, mas sua pena foi suspensa em troca de entregar os dois cúmplices, que foram então condenados a três anos em um campo de trabalhos forçados.

1993	Zlatoust-36 Instrument Plant, Chelyabinsk, Russia	Funcionários da filial de Orel do Instituto de Pesquisa e Desenvolvimento de Instrumentação de Moscou foram presos ao tentar vender 75 gramas de plutônio, que haviam contrabandeado para fora da instalação.
1994	SS-25 ICBM site, Barnaul, Siberia, Russia	Em um armazem de mísseis balísticos intercontinentais SS-25 em Barnaul, na Sibéria, um soldado russo abriu fogo com uma submetralhadora contra sua própria unidade, matando o comandante e outros dois militares, enquanto os demais não puderam reagir imediatamente devido ao risco de disparar na direção do sistema estratégico SS-25 ICBM, tendo o agressor se refugiado em um veículo blindado e se rendido após cerca de três horas de negociação.
1996	Russian Naval Base, Sovetskaya Gavan, Russia	Três empregados internos roubam varetas de combustível contendo ≈7 kg de HEU; parte do material (≈2,5 kg) é posteriormente apreendida em Kaliningrado.
1996	Y-12 National Security Complex, Oak Ridge, Tennessee, U.S.A.	No complexo nuclear Y-12 National Security Complex, o funcionário de limpeza Charles Stevens Roddy tentou subtrair de um barril de resíduos um dispositivo que continha, em parte, urânio empobrecido e estava identificado como “material secreto” e “radioativo”, sendo interceptado ao acionar o sistema de detecção radiológica na saída de funcionários; Roddy alegou que pretendia utilizar o objeto como peso de papel, mas, após investigação, foram encontrados em sua residência computadores furtados da cooperativa de crédito da instalação, caracterizando um caso de ameaça interna (*insider*) envolvendo tentativa de desvio de material sensível
1997	Kursk Nuclear Power Plant, Kursk Oblast, Russia	Cinco homens desarmados invadiram a Kursk Nuclear Power Plant, inicialmente suspeitos de ligação com grupos ambientalistas, embora posteriormente tenha se indicado motivação predominantemente criminosa, conseguindo alcançar a área do gerador da instalação com a intenção de desabilitar o reator e assumir o controle da sala de comando, mas sem possuir capacidade técnica ou meios para concretizar a ação, não havendo registro de danos significativos ou liberação radiológica
2000	Tokaimura, Japan JCO	O indivíduo Tatsufumi Oshiba foi preso após plantar um artefato explosivo improvisado nas proximidades da instalação de processamento de urânio da JCO Co. em Tokaimura, Japão, o qual não

	Uranium Processing Plant	chegou a detonar devido ao temporizador não ter sido ativado; durante a investigação, confessou ainda planos adicionais de atacar a mesma instalação, motivado por indignação em relação ao acidente nuclear de Tokaimura
2000	Nuclear research facility, Research Institute of Physics, Rostov-na-Donu, Russia	Uma bomba acionada remotamente explodiu em uma instalação de pesquisa nuclear em Rostov-on-Don, ferindo duas pessoas, sendo inicialmente divulgados rumores de altas vítimas e liberação de radiação, posteriormente desmentidos pelas autoridades, que indicaram que não havia mais atividades nucleares em curso no local no momento do ataque; o incidente é considerado resultado de disputas entre grupos criminosos, caracterizando um ato de violência com motivação não ideológica e sem impacto radiológico.
2000	Mühleberg Nuclear Power Plant, Mühleberg, Switzerland	Um ativista antinuclear conseguiu pousar um parapente motorizado (parafoil) sobre o teto do edifício do reator, em uma ação de caráter demonstrativo que não causou danos ou liberação radiológica, mas evidenciou vulnerabilidades relacionadas à proteção contra ameaças aéreas de baixa altitude em instalações nucleares.
2002	Koeberg Nuclear Power Station, Cape Town, South Africa	Três homens e três mulheres se aproximaram da instalação em botes infláveis, escalaram o muro de proteção e invadiram a usina, onde penduraram uma grande faixa com os dizeres “Fora as armas nucleares da África”, em uma ação de protesto de caráter simbólico que não causou danos ou liberação radiológica, mas evidenciou vulnerabilidades nos sistemas de segurança física e controle de acesso.
2002	Sizewell B Nuclear Power Plant, Suffolk, England	Cerca de 50 ativistas invadiram a Sizewell Nuclear Power Station, no Reino Unido, entrando sem oposição pelo portão principal e também pela cerca perimetral, permanecendo dentro da área de segurança por aproximadamente 25 minutos antes de serem abordados por apenas dois vigilantes, declarando que a ação tinha como objetivo protestar contra os planos do governo de construir novas usinas nucleares, sem causar danos ou liberação radiológica, mas evidenciando falhas significativas nos sistemas de controle de acesso e resposta.

2008	Dera Ghazi Khan, Punjab, Pakistan Dera Ghazi Khan Conversion Facility	Combatentes separatistas balúchis realizaram um ataque com morteiros contra instalações associadas à Baghalchur Uranium Mine, atingindo prédios de apoio e uma cafeteria sem causar danos diretos a estruturas nucleares sensíveis, além de provocar um incêndio em uma área de vegetação próxima que levou cerca de 10 horas para ser controlado; um dos relatos indica que o alvo específico era um local de resíduos ligado à mina, caracterizando uma ação de cunho insurgente com impacto material limitado, mas potencial de risco à infraestrutura associada ao ciclo do combustível nuclear.
2007	Pelindaba Nuclear Research Facility, Pelindaba, South Africa	Em 2007, na Pelindaba Nuclear Facility, na África do Sul, oito homens organizados em duas equipes coordenaram um ataque ao perímetro da instalação durante a noite, conseguindo violar cercas eletrificadas, desativar alarmes, cortar comunicações e inutilizar câmeras de segurança sem resposta imediata, permitindo que quatro invasores penetrassem profundamente na área protegida e alcançassem o centro de controle de emergência, onde um funcionário foi baleado, enquanto a equipe de segurança levou cerca de 24 minutos para reagir; os intrusos permaneceram aproximadamente 45 minutos dentro do perímetro antes de fugir sem serem interceptados, evidenciando falhas graves nos sistemas de detecção e resposta da instalação.
2010	Kleine Brogel Airbase, Kleine Brogel, Belgium	Um grupo de ativistas pela paz invadiu a Kleine Brogel Air Base, na Bélgica, ao escalar as cercas de proteção e posicionar faixas em abrigos associados ao armazenamento de armas nucleares dos EUA, em uma ação de caráter simbólico, sendo posteriormente afirmado pelo Ministério da Defesa belga que os manifestantes não tiveram acesso a áreas sensíveis e que o bunker em questão estava vazio, não havendo danos ou riscos diretos, mas evidenciando vulnerabilidades no controle de acesso.
2011	Cofrentes Nuclear Power Plant, Cofrentes, Spain	Cerca de 20 ativistas do Greenpeace escalaram uma torre de resfriamento da Cofrentes Nuclear Power Plant, na Espanha, onde penduraram faixas em protesto contra a renovação da licença de operação da usina, em uma ação de caráter demonstrativo que não colocou em risco componentes vitais da instalação,

		conforme indicado pelas autoridades, mas evidenciou vulnerabilidades no controle de acesso a estruturas externas.
2011	Nogent Nuclear Power Plant, Nogent-sur-Seine, France	Nove ativistas do Greenpeace contornaram a segurança externa da Nogent-sur-Seine Nuclear Power Plant, na França, sendo imediatamente detectados e acompanhados pela equipe de segurança, conseguindo escalar o edifício do reator para exibir faixas criticando a segurança da energia nuclear; sete foram rapidamente detidos e os outros dois foram localizados e presos posteriormente após se esconderem no local, caracterizando uma ação de protesto sem danos ou liberação radiológica, mas que evidenciou vulnerabilidades no controle de acesso inicial.
2012	Bugey Nuclear Power Station, Bugey, France	Um ativista do Greenpeace utilizando um parapente motorizado lançou um sinalizador de fumaça sobre o telhado de um edifício da Bugey Nuclear Power Plant, na França, antes de pousar e ser detido pelas autoridades no local, em uma ação deliberadamente planejada para demonstrar a vulnerabilidade de instalações nucleares a ameaças aéreas, sem causar danos ou liberação radiológica.
2012	Ringhals Nuclear Power Plant, Väröbacka, Sweden	Cerca de 20 ativistas do Greenpeace violaram o perímetro de segurança da Cattenom Nuclear Power Plant, na França, e circularam de bicicleta pelo interior da instalação, permanecendo no local por cerca de 40 minutos até a chegada da polícia, que efetuou a prisão de 16 indivíduos, em uma ação de protesto sem danos ou liberação radiológica, mas que evidenciou falhas relevantes nos sistemas de detecção e resposta.
2012	Forsmark Nuclear Power Plant, Forsmark, Sweden	Cerca de 50 ativistas do Greenpeace escalaram as cercas perimetrais da Tricastin Nuclear Power Plant, na França, conseguindo acessar a instalação antes da chegada da polícia, que respondeu em cerca de 15 minutos e efetuou a prisão de todos os invasores, em uma ação de protesto sem danos ou liberação radiológica, mas que evidenciou vulnerabilidades no controle de acesso físico ao perímetro.
2012	Y-12 National Security Complex, Oak Ridge, Tennessee U.S.A	Uma freira de 82 anos e dois outros ativistas do movimento Plowshares Movement invadiram o Y-12 National Security Complex, nos EUA, ao atravessar sucessivas cercas utilizando alicates de corte e acessar a área que abriga urânio altamente enriquecido (HEU), onde realizaram atos de vandalismo,

		permanecendo no local por cerca de duas horas sem serem interceptados devido a falhas na cultura de segurança e em sistemas tecnológicos de detecção, evidenciando vulnerabilidades graves na proteção de material nuclear sensível.
2012	Minhas Air Force Base, Kamra, Pakistan	Militantes afiliados ao Tehrik-i-Taliban Pakistan realizaram um ataque à Minhas Air Force Base, no Paquistão, supostamente associada ao armazenamento de ogivas nucleares, utilizando uniformes da força aérea e armamento pesado, incluindo fuzis automáticos, RPGs e coletes suicidas; enquanto parte do grupo permaneceu do lado externo disparando foguetes, outros escalaram o muro e enfrentaram as forças de segurança por cerca de cinco horas, sem conseguir acessar materiais nucleares, caracterizando um ataque coordenado de alta intensidade que evidenciou a resiliência das camadas internas de proteção.
2013	Watts Bar Nuclear Power Plant, Rhea County, Tennessee U.S.A.	Um indivíduo aproximou-se de barco da Watts Bar Nuclear Plant, nos EUA, e conseguiu acessar uma área restrita da instalação onde se encontra um reator nuclear, efetuando diversos disparos com arma de fogo contra um vigilante de segurança antes de fugir novamente pelo rio, sem registro de liberação radiológica, caracterizando um ataque armado de baixa escala que evidenciou vulnerabilidades no controle de acesso por via aquática.
2014	Oskarshamn Nuclear Power Plant, Oskarshamn, Sweden	Cerca de 20 ativistas do Greenpeace utilizaram escadas para transpor três cercas perimetrais da Fessenheim Nuclear Power Plant, na França, conseguindo acessar a instalação, onde seis deles escalaram até o telhado do edifício do reator e exibiram uma faixa, em uma ação de protesto sem danos ou liberação radiológica, mas que evidenciou vulnerabilidades nos sistemas de segurança física e controle de acesso.
2014	Fessenheim Nuclear Power Plant, Fessenheim, France	Cerca de 60 ativistas do Greenpeace, provenientes de 14 países, invadiram a Fessenheim Nuclear Power Plant, na França, onde escalaram o edifício do reator e exibiram uma faixa com a mensagem “Stop

		Risking Europe”, sendo posteriormente removidos por forças de segurança com apoio de helicópteros, sem causar impacto na operação da usina, conforme informado pelas autoridades, mas evidenciando vulnerabilidades no controle de acesso e resposta a intrusões.
2014	August 5, 2014, Doel, Belgium	Em 5 de agosto de 2014, na Doel Nuclear Power Plant, na Bélgica, um ato aparente de sabotagem envolveu a liberação de óleo para um tanque subterrâneo, provocando o superaquecimento e a parada da turbina da unidade Doel 4, sem liberação radiológica, mas resultando em interrupção prolongada da operação e prejuízos significativos, sendo considerado um caso relevante de possível ameaça interna (*insider*).
2014	France and Belgium	Ao longo de setembro e outubro de 2014, ao menos 13 usinas nucleares na França foram sobrevoadas em pelo menos 15 ocasiões distintas por drones remotamente operados, incluindo múltiplos incidentes no mesmo dia, sem identificação ou captura dos responsáveis, evidenciando vulnerabilidades persistentes relacionadas a ameaças aéreas de baixa altitude; posteriormente, um evento de características semelhantes também foi registrado na Doel Nuclear Power Plant, na Bélgica, sem danos ou liberação radiológica, mas com relevante impacto na percepção de segurança dessas instalações.
2014	Tamil Nadu, India Madras Nuclear Power Plant	Um policial da Central Industrial Security Force abriu fogo com sua arma de serviço dentro de uma instalação nuclear na Índia, matando três pessoas e ferindo outras duas antes de se render, caracterizando um grave caso de ameaça interna (*insider*) com uso de armamento oficial e impacto direto sobre o pessoal da instalação.

2021	Iran Centrifuge Assembly Center (ICAC) – Karaj	Um drone, aparentemente lançado de dentro do próprio território iraniano e a curta distância do alvo, conseguiu atingir uma instalação nuclear no país, segundo fonte iraniana citada em relatórios, embora não haja confirmação sobre danos causados, o que é consistente com outros incidentes recentes em que ataques ou projéteis próximos a instalações nucleares não resultaram em impactos significativos às estruturas principais
2024	Zaporizhzhia Nuclear Power Plant (Ucrânia)	Ataques com drones atingiram a Unidade 6 da Zaporizhzhia Nuclear Power Plant, na Ucrânia, resultando em vítimas, embora sem evidências de danos a sistemas críticos de segurança nuclear ou proteção física; inspetores da International Atomic Energy Agency presentes no local confirmaram os impactos das detonações, que aparentemente tiveram como alvo equipamentos de vigilância e comunicação, evidenciando a vulnerabilidade desses sistemas auxiliares a ataques com drones.
2025	Khmelnytskyi Nuclear Power Plant	Observadores da International Atomic Energy Agency relataram aumento de atividades militares nas proximidades da Khmelnytskyi Nuclear Power Plant, incluindo nove ocorrências de atividade de drones e disparos de armas de fogo em diferentes distâncias da instalação em 9 de setembro, sem registro de danos diretos à usina, mas evidenciando o ambiente de risco elevado no entorno de instalações nucleares em zonas de conflito.
2025	Chernobyl Nuclear Power Plant (Ucrânia)	Um drone atingiu o invólucro de contenção conhecido como “New Safe Confinement” da Unidade 4 da Chernobyl Nuclear Power Plant, causando incêndio e perfuração da cobertura, sem indicação de liberação radiológica significativa, mas evidenciando a vulnerabilidade de estruturas de confinamento a impactos de sistemas aéreos não tripulados.

3 METODOLOGIA

3.1 DESENVOLVIMENTO DO TRABALHO

Para o desenvolvimento deste trabalho, considera-se como estudo de caso uma instalação nuclear hipotética, inserida em um complexo naval representativo, destinada a apoiar atividades associadas à operação e manutenção de meios navais com propulsão nuclear. A utilização de um estudo de caso tem como objetivo demonstrar a aplicabilidade da metodologia proposta, não se tratando de um projeto executivo de um Sistema de Proteção Física (SPF), no qual seriam definidos o posicionamento físico, o dimensionamento e as especificações técnicas dos elementos de segurança, mas de uma análise conceitual destinada a apoiar a tomada de decisão.

A estrutura metodológica adotada neste trabalho é inspirada na abordagem baseada em redes bayesianas de decisão proposta por Misuri *et al.* (2018), que utilizaram Diagramas de Influência com Memória Limitada (LIMID) para apoiar a seleção de estratégias de segurança em infraestruturas críticas sob condições de incerteza. No presente estudo, essa abordagem é adaptada ao contexto da proteção física de instalações nucleares e fundamenta-se nos princípios de detecção, atraso e resposta, que constituem a base dos sistemas de proteção física em profundidade, conforme estabelecido nas recomendações internacionais da Agência Internacional de Energia Atômica (IAEA, 2011).

Diferentemente de abordagens tradicionais de análise de proteção física, como o EASI, o SAVI e o SAPE, que são voltadas principalmente para a avaliação do desempenho do sistema, o presente trabalho incorpora explicitamente o processo de tomada de decisão por meio de Redes Bayesianas de Decisão, estruturadas como Limited Memory Influence Diagrams (LIMID).

Nessas abordagens tradicionais, a análise é centrada na estimativa de probabilidades de sucesso ou interrupção de ataques, não sendo considerada, de forma estruturada, a escolha entre diferentes alternativas de proteção. Por outro lado, o modelo proposto permite representar decisões e avaliar suas consequências, possibilitando a comparação entre diferentes estratégias com base na utilidade esperada a fim de determinar a estratégia com o melhor custo-beneficio.

A partir do modelo proposto por Misuri *et al.* (2019), este trabalho introduz adaptações voltadas ao contexto da segurança física nuclear. O modelo foi estruturado segundo a lógica de detecção, atraso e resposta, amplamente utilizada na área de proteção física nuclear. Para isso, foram introduzidos no modelo de redes bayesianas nós específicos que representam explicitamente esses elementos, incluindo nós de decisão associados à detecção e ao atraso. Essa abordagem permite avaliar, de forma mais direta, o impacto das medidas de proteção na eficácia do sistema, além de consolidar o modelo como uma ferramenta de apoio à decisão no contexto da segurança física nuclear.

Adicionalmente, o modelo foi desenvolvido utilizando terminologia e conceitos compatíveis com o domínio da segurança física nuclear, o que contribui para sua maior aderência a aplicações práticas nesse contexto.

O desenvolvimento do trabalho é estruturado em etapas metodológicas complementares, na primeira etapa, realiza-se a caracterização do problema de proteção física, incluindo a descrição geral da instalação nuclear considerada, a identificação dos principais ativos a serem protegidos e a definição do contexto de ameaça. Nessa etapa, o alvo principal é assumido como a área vital da instalação, em consonância com diretrizes internacionais de proteção física nuclear. O objetivo dessa fase é estabelecer o escopo do modelo e as premissas adotadas para a análise.

Na segunda etapa, procede-se à formulação do problema de decisão, sob a perspectiva do defensor, representado pelo gestor responsável pela segurança física da instalação. São consideradas explicitamente três decisões estratégicas, ambas tomadas previamente à ocorrência de um ataque:

- a seleção de medidas de segurança voltadas à detecção.
- a seleção de medidas de barreiras físicas associadas ao atraso do adversário.
- a seleção de medidas de resposta que influenciam na neutralização do adversário.

Na terceira etapa, é desenvolvida a estrutura do modelo bayesiano de decisão, por meio da definição dos nós de decisão, nós aleatórios e nós de utilidade, bem como das relações de dependência causal entre eles. O modelo incorpora elementos relacionados às medidas de segurança, às características da ameaça, aos mecanismos de detecção e atraso, à comunicação e à atuação da força de reação, além das

consequências associadas a um ataque bem-sucedido ou interrompido. As incertezas inerentes a cada um desses elementos são representadas por meio de tabelas de probabilidade condicional, construídas com base em literatura especializada, referências técnicas e julgamento especializado.

Na quarta etapa, o modelo é utilizado para a avaliação de diferentes estratégias de segurança física, definidas como combinações das medidas de detecção e de barreiras físicas consideradas. Para cada estratégia, calcula-se a utilidade esperada, levando em conta os custos associados às medidas adotadas e os impactos decorrentes das possíveis consequências de um ataque. A comparação entre as estratégias permite identificar aquelas que apresentam melhor desempenho sob a ótica do custo-beneficio.

Por fim, os resultados obtidos são analisados de forma a avaliar a aplicabilidade da metodologia proposta como ferramenta de apoio à decisão em proteção física de instalações nucleares, bem como discutir suas limitações e possibilidades de adaptação a outros contextos e tipos de instalações.

3.2 MODELO CONCEITUAL DE DECISÃO EM PROTEÇÃO FÍSICA

O modelo desenvolvido neste trabalho é estruturado como um Diagrama de Influência com Memória Limitada (LIMID), utilizado para analisar problemas de decisão em que existem diferentes alternativas possíveis, resultados incertos e consequências associadas. Esse tipo de modelo é adequado para o contexto da proteção física de instalações nucleares, no qual não se conhece previamente o comportamento do adversário e o desempenho das medidas de segurança pode variar conforme o cenário considerado.

O modelo adotado neste trabalho é apresentado na Figura 3. A estrutura do modelo está organizada a partir das três funções fundamentais da proteção física: detecção, atraso e resposta , que são representadas por nós de chance.

No contexto da proteção física nuclear, essas funções podem ser associadas a diferentes tipos de medidas. A detecção compreende sistemas e procedimentos voltados à identificação da ameaça, como sistemas de vigilância por vídeo (CCTV), sensores de movimento, sensores perimetrais, radares, sistemas de detecção de intrusão e monitoramento por operadores. O atraso está relacionado a barreiras físicas e estruturais

que dificultam a progressão do adversário, incluindo cercas, muros, portas reforçadas, sistemas de controle de acesso e estruturas de proteção. Por sua vez, a resposta envolve os meios empregados para neutralizar a ameaça após sua identificação, tais como equipes de segurança, forças de reação, protocolos operacionais e recursos táticos disponíveis para contenção do adversário.

As decisões do defensor são modeladas por meio dos nós de decisão: Alternativas de Detecção, Alternativas de Barreiras e Alternativas de Resposta, os quais influenciam diretamente o desempenho dessas funções. Em particular, as alternativas de detecção afetam a probabilidade de identificação da ameaça, enquanto as alternativas de barreiras impactam o atraso imposto ao adversário e as alternativas de resposta determinam a capacidade de reação do sistema. Cada uma dessas alternativas está associada a custos específicos, representados por nós de utilidade no modelo, permitindo incorporar o impacto econômico das decisões adotadas.

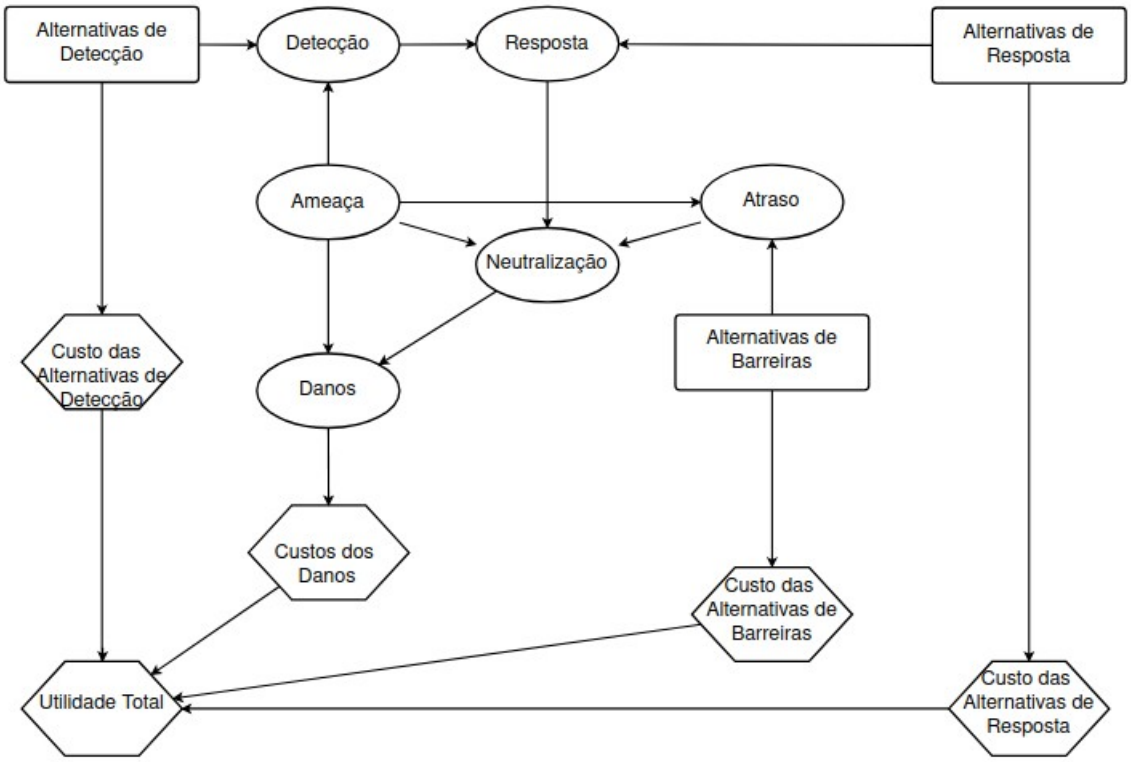

Figura 3 - Modelo de apoio à decisão para seleção de estratégias de proteção física em instalações nucleares

As variáveis Ameaça, Neutralização e Danos são representadas por nós de chance. A variável Ameaça representa as características do adversário e influencia simultaneamente a detecção, a neutralização e os danos, refletindo o papel central do comportamento adversário no modelo. A partir da interação entre detecção, atraso e resposta, define-se a variável Neutralização, que representa a capacidade do sistema de impedir o sucesso do ataque. Caso a neutralização não seja totalmente bem-sucedida , a variável Danos é impactada, sendo posteriormente associada a um custo por meio do nó Custos dos Danos.

A variável Utilidade Total, representada por um nó de utilitade, agrega os custos das alternativas implementadas e os custos decorrentes dos danos. Por meio desse nó, o modelo permite comparar as diferentes combinações de alternativas, avaliando seu desempenho de forma integrada sob a ótica da utilidade esperada. A estratégia ótima é definida como aquela que apresenta o maior valor de utilidade total entre as alternativas consideradas.

3.2.1 Hipóteses de modelagem

A formulação do modelo de decisão apresentado neste trabalho baseia-se em um conjunto de hipóteses de modelagem adotadas de forma explícita, com o objetivo de delimitar o escopo da análise, garantir coerência lógica à estrutura do modelo e assegurar sua aderência ao contexto da proteção física de instalações nucleares. Essas hipóteses refletem recomendações normativas, evidências observadas em dados históricos e práticas consolidadas na literatura especializada, sendo compatíveis com o caráter estratégico e de apoio à decisão da metodologia proposta.

- Hipótese H1 – Independência entre as decisões do defensor e a escolha do alvo e da forma de acesso: Assume-se que a seleção de medidas de proteção física pelo defensor não altera de forma direta a escolha do alvo nem da forma de acesso pelo adversário, no nível de abstração adotado. Embora se reconheça que em determinados contextos adversários possam adaptar suas ações em resposta às medidas de segurança, a introdução explícita dessa dinâmica exigiria hipóteses adicionais sobre percepção, racionalidade e capacidade adaptativa do adversário,

as quais não são diretamente observáveis nem facilmente sustentáveis por dados empíricos no contexto nuclear. Assim, a escolha do alvo e da forma de acesso é tratada como externa às decisões estratégicas de proteção física avaliadas no modelo.

- Hipótese H2 – Decisões estratégicas prévias à ocorrência do ataque: As decisões representadas no modelo correspondem a escolhas estratégicas realizadas previamente à ocorrência de um ataque, no âmbito do planejamento e do dimensionamento do Sistema de Proteção Física. O modelo não representa decisões adaptativas em tempo real, nem interações dinâmicas contínuas entre defensor e adversário durante a execução do ataque, concentrando-se na avaliação comparativa de estratégias de proteção definidas a priori.

- Hipótese H3 – Foco no desempenho do sistema de proteção física: As medidas de proteção física avaliadas no modelo influenciam diretamente o desempenho das funções de detecção, atraso e resposta, bem como as probabilidades associadas à neutralização e aos danos resultantes. Não se busca, entretanto, modelar explicitamente mudanças no comportamento do adversário decorrentes da presença dessas medidas, mas sim avaliar como diferentes configurações do sistema de proteção física afetam os resultados esperados frente a cenários de ameaça considerados plausíveis.

As hipóteses acima não implicam a negação da possibilidade de adaptação do adversário, mas representam uma delimitação consciente do escopo do modelo, compatível com seu caráter estratégico e com o objetivo de apoiar a tomada de decisão em proteção física nuclear. Em aplicações futuras ou em contextos distintos, essas hipóteses podem ser revistas ou relaxadas, permitindo a incorporação de níveis adicionais de complexidade conforme a disponibilidade de dados e os objetivos da análise.

3.3 CONSTRUÇÃO DO MODELO APLICADO

O modelo conceitual apresentado na Seção 3.2 representa a estrutura lógica do problema de decisão em proteção física, de forma abstrata e independente de uma instalação específica. Para que esse modelo possa ser utilizado em análises práticas, é necessária a construção de um modelo aplicado, no qual a estrutura conceitual é traduzida em uma rede bayesiana concreta, construída a partir das características da instalação analisada, das informações disponíveis e das escolhas de modelagem do decisor.

Na aplicação prática do modelo, os nós conceituais, como detecção, atraso, resposta, ameaça, por exemplo, podem ser desdobrados em conjuntos de variáveis que descrevem diferentes condições operacionais e fatores de desempenho associados a cada um deles de forma detalhada. Por exemplo, a variável Ameaça, pode ser decomposta em motivação, intenções, armas, formas de acesso, presença de *insiders* e tamanho do grupo, conforme ilustrado na Figura 4.

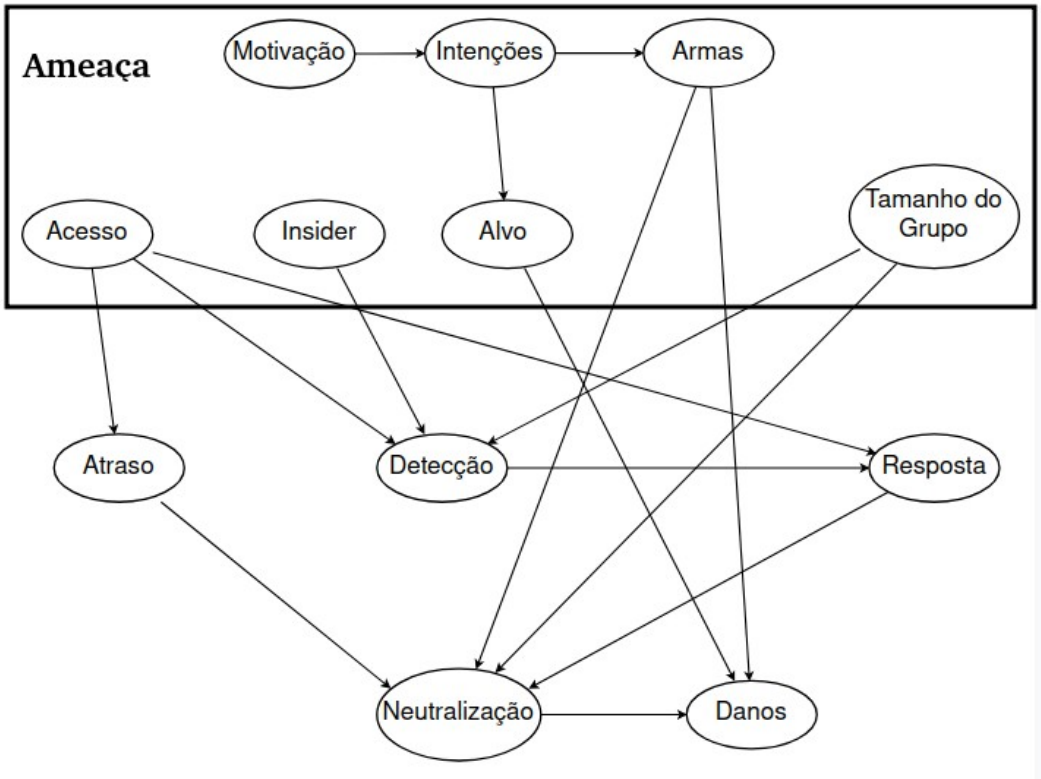

Figura 4 - Exemplo de detalhamento da Ameaça

Esse detalhamento permite caracterizar de forma mais realista o comportamento do adversário e influencia o desempenho das funções de proteção física de forma separada. Em especial, esses fatores impactam as variáveis de detecção, atraso e resposta, refletindo como diferentes perfis de ameaça afetam a eficácia do sistema. Como consequência, influenciam também a neutralização do adversário e os danos resultantes.

A definição das variáveis incluídas no modelo aplicado e o grau de detalhamento adotado não são únicos nem fixos, dependem do contexto da instalação, do nível de informação disponível e das necessidades do processo decisório. Dessa forma, o modelo conceitual atua como um guia estruturante, assegurando coerência lógica, enquanto a rede bayesiana construída reflete escolhas específicas de modelagem.

Vale ressaltar que medidas de proteção física previamente implantadas, como a presença de vigias ou determinadas barreiras físicas, não são tratadas como alternativas a serem escolhidas, mas como características do cenário. Essas condições influenciam o desempenho da detecção e do atraso, mas não fazem parte do conjunto de alternativas comparadas pelo modelo. A Figura 5 apresenta um exemplo da modelagem da função de detecção. Nesse caso, considera-se que o sistema já possui elementos preexistentes, como a presença de vigias, que influenciam diretamente o desempenho da detecção. A partir dessa base, o decisor deve selecionar entre diferentes alternativas adicionais, câmeras ou patrulha, com o objetivo de aumentar a eficiência do sistema.

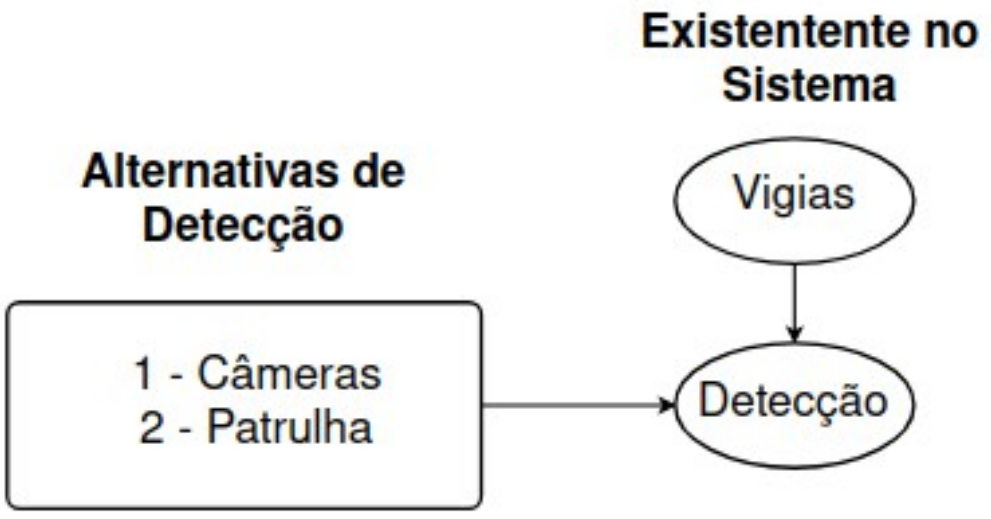

Figura 5: Alternativas de detecção e medidas já implementadas no sistema

Na construção do modelo aplicado, o decisor possui a flexibilidade de definir os estados das variáveis de acordo com as características específicas da instalação analisada. Essa adaptação é importante para garantir que o modelo represente de forma adequada o contexto real do problema. Como exemplo, a variável “via de acesso” pode, em uma configuração geral, assumir três estados: água, ar e terra. No entanto, para uma instalação localizada em região sem acesso por via aquática, essa variável pode ser simplificada para apenas dois estados (ar e terra), sem prejuízo à representatividade do modelo.

Destaca-se que a definição do número de estados das variáveis impacta diretamente a complexidade do modelo, especialmente no que se refere às tabelas de probabilidade condicional. De modo geral, o número de combinações possíveis em uma tabela cresce de forma multiplicativa com o número de estados dos nós pais, consequentemente, a inclusão de muitos estados pode tornar a modelagem mais trabalhosa, aumentando o esforço necessário para a definição das probabilidades e a interpretação dos resultados.

3.4 CARACTERIZAÇÃO DA AMEAÇA

A caracterização da ameaça adotada neste trabalho baseia-se nas definições de Ameaças Base de Projeto e Declarações Representativas de Ameaça (IAEA, 2021). A partir desse referencial, os eventos foram categorizados segundo atributos relevantes do adversário, incluindo sua motivação, intenção, composição do grupo, capacidades operacionais, eventual presença de ameaça interna (*insider*) e a via de acesso empregada.

A motivação pode ser compreendida como o fator que orienta sua intenção, uma vez que representa o fator subjacente que orienta seus objetivos e decisões ao longo da ação. Nesse sentido, é possível classificar as motivações em:

- Financeira: associada à obtenção de ganhos econômicos, como roubo ou tráfico ilícito de material nuclear;
- Ideológica: relacionada à defesa de crenças, valores ou causas, frequentemente vinculada a ações de caráter simbólico ou demonstrativo;

- Política, voltada à obtenção de efeitos estratégicos, como pressão sobre governos ou desestabilização institucional; e
- Pessoal: geralmente associada a indivíduos com vínculos internos ou conhecimento da instalação, podendo envolver insatisfação, vingança ou interesses particulares.

A intenção está diretamente relacionada ao propósito operacional do ataque, ela influencia diretamente a escolha dos meios empregados pelo adversário, incluindo o tipo de armamento ou recursos utilizados, bem como a seleção do alvo. Ela foi dividida nas seguintes categorias:

- Sabotagem: envolve a degradação ou destruição de estruturas e sistemas críticos, visando causar danos significativos ou comprometer a segurança da instalação;
- Roubo: está associado à subtração de materiais nucleares ou radioativos, geralmente com fins ilícitos; e
- Disrupção: refere-se à interrupção ou comprometimento das operações, sem necessariamente implicar destruição física relevante.

O tamanho do grupo adversário foi classificado em individual, pequeno grupo e grande grupo.

- Individual: refere-se a ações conduzidas por um único agente, geralmente associadas a limitações operacionais e menor capacidade de coordenação.
- Pequeno grupo, definido como composto por dois a quatro indivíduos, representa um nível intermediário de organização, permitindo divisão básica de tarefas e execução coordenada de ações.
- Grande grupo: com cinco ou mais integrantes, caracteriza operações mais complexas, com maior capacidade de planejamento, coordenação simultânea e potencial de enfrentamento às forças de segurança.

Esse limite foi estabelecido com base no conhecimento especialista de uma organização da força de segurança nuclear, que opera em equipes compostas por quatro militares, de modo que grupos adversários com efetivo superior a esse número passam a

apresentar potencial vantagem numérica inicial, o que pode impactar diretamente a dinâmica de neutralização.

Os meios empregados pelo adversário foram classificados em quatro categorias: uso de explosivos, uso de armas, uso combinado de explosivos e armas, e ausência de meios ofensivos (nada).

Explosivos: associado a intenções de sabotagem e à produção de danos estruturais relevantes;

- Armas de fogo: relacionado a ações de invasão, coerção ou enfrentamento direto com forças de segurança;
- Combinação de explosivos e armas: representa um nível mais elevado de capacidade operacional, permitindo tanto o engajamento direto quanto a destruição de infraestruturas críticas; e
- Ausência de meios ofensivos: abrange situações em que o adversário não emprega meios ofensivos diretos, sendo frequentemente associada a ações de protesto, invasões não violentas ou ataques dependentes de acesso interno, como sabotagens.

A presença de ameaça interna (*insider*) foi tratada como uma variável binária, classificada nas categorias “sim” ou “não”, indicando, respectivamente, a participação ou não de indivíduos com acesso autorizado à instalação ou conhecimento privilegiado de seus sistemas e rotinas. A inclusão dessa variável permite capturar situações em que o adversário se beneficia de informações internas, facilitação de acesso ou manipulação de sistemas, impactando diretamente a probabilidade de sucesso do ataque.

A área atingida nos ataques foi classificada com base na estrutura de segurança física das instalações nucleares, distinguindo-se : Área Protegida, Área Vigiada e Área Vital.

- Área Protegida: corresponde à região mantida sob proteção contínua, delimitada por barreiras físicas e com acessos rigorosamente controlados, podendo englobar uma ou mais áreas vitais ou, em alguns casos, toda a instalação nuclear quando não há segregação interna;

- Área Vigiada: situa-se externamente à área protegida, sendo igualmente cercada e sinalizada, porém com foco em vigilância e controle de aproximação, funcionando como uma zona de amortecimento; e
- Área Vital: constitui o nível mais sensível da instalação, localizada no interior da área protegida e composta por estruturas que abrigam equipamentos essenciais e/ou material nuclear, sendo protegida por barreiras físicas robustas, como paredes, teto e piso, projetadas para impedir acessos não autorizados e mitigar ações adversas.

A via de acesso utilizada pelo adversário foi classificada em três categorias: terrestre, aquática e aérea, representando os principais vetores pelos quais uma instalação nuclear pode ser abordada.

- Acesso terrestre: corresponde ao vetor mais comum, associado a invasões pelo perímetro físico da instalação ou por vias de acesso convencionais;
- Acesso aquático: refere-se a aproximações por rios, lagos ou mar, sendo particularmente relevante para instalações localizadas em áreas costeiras ou próximas a corpos d’água; e
- Acesso aéreo: envolve o uso de meios como drones, aeronaves leves ou outros dispositivos capazes de ultrapassar barreiras físicas, representando um vetor de difícil detecção e crescente relevância no contexto atual.

Ressalta-se que nem todos os atributos de ameaça discutidos na literatura são explicitamente representados como variáveis independentes no modelo. Optou-se por uma representação agregada da ameaça, capaz de capturar seus efeitos relevantes sobre o desempenho do sistema de proteção física, evitando um nível de detalhamento incompatível com o caráter estratégico e de apoio à decisão do modelo. No presente modelo, o conceito de alvo é tratado como parte da caracterização da ameaça, representando a área ou o ativo de interesse do adversário, e não como uma variável associada à configuração da instalação.

A partir dos atributos definidos, motivação, intenção, tamanho do grupo, capacidades (meios empregados), presença de ameaça interna e via de acesso, procedeu-se à análise de eventos históricos selecionados, os quais foram sistematicamente

classificados segundo esses critérios, servindo com base para a construção das Tabelas de Probabilidade Condicional relacionadas a ameaça.

A partir do histórico é possível perceber que em geral , casos classificados como disrupção social ou política, associados a ações de protesto e ativismo, como as conduzidas por organizações ambientais, caracterizam-se predominantemente por ações não violentas, sem o emprego de armas ou explosivos, tendo como objetivo principal chamar atenção pública ou interromper temporariamente atividades da instalação.

Por outro lado, eventos de sabotagem correspondem a ações voltadas à destruição ou comprometimento de partes específicas da infraestrutura, podendo envolver o uso de explosivos ou a danificação deliberada de equipamentos críticos, com o intuito de prejudicar o funcionamento da instalação.

Já os episódios de roubo de material nuclear observados historicamente apresentam forte associação com a participação de ameaças internas (*insider*s), explorando acessos legítimos e conhecimentos operacionais, sendo geralmente conduzidos sem o uso de armamentos pesados ou explosivos, de forma a minimizar a detecção durante a subtração do material.

Cabe ressaltar que, embora os cenários associados ao acesso aéreo apresentem, de forma geral, baixa frequência histórica nos dados analisados, observa-se um aumento recente na utilização de veículos aéreos não tripulados (drones) em incidentes e tentativas de ataque contra infraestruturas críticas e instalações sensíveis. Esse aumento está associado à maior disponibilidade comercial de drones, à redução de custos, ao avanço de capacidades autônomas e à facilidade de adaptação desses meios para fins maliciosos. Dessa forma, apesar de classificados como cenários de baixa frequência histórica, os cenários de acesso aéreo são considerados relevantes, apresentando potencial de crescimento nos próximos anos.

A partir dessa base de eventos classificados, foram definidos os estados das variáveis associadas à ameaça no modelo bayesiano, bem como as distribuições de probabilidade relativas entre esses estados.

Ressalta-se que essa parametrização possui caráter ilustrativo e estratégico, sendo empregada com o objetivo de demonstrar a aplicabilidade do modelo bayesiano de decisão na integração de múltiplos fatores de ameaça, podendo ser ajustada em

aplicações reais a partir de avaliações locais de risco, dados de inteligência e julgamento de especialistas.

3.5 FONTES DE DADOS E ATRIBUIÇÃO DE PROBABILIDADES

Inicialmente, ressalta-se a limitada disponibilidade de dados abertos e sistematizados sobre esses aspectos, em especial em razão de restrições de sigilo inerentes à área de proteção física nuclear. Adicionalmente, reconhece-se que as probabilidades dependem fortemente das características específicas de cada instalação, de seus procedimentos operacionais e das capacidades da força de resposta local.

As probabilidades usadas neste trabalho associadas às características da ameaça são fundamentadas em dados históricos de ataques e incidentes envolvendo instalações nucleares, apresentadas na Seção 3.4. Esses dados foram utilizados para orientar a definição dos estados das variáveis e na construção das Tabelas de Probabilidade Condicional.

A literatura especializada, como o trabalho de ARGENTI, *et al.* (2018), lista uma série de dados que permitem a construção de Tabelas de Probabilidade Condicional para as probabilidades relacionadas às funções de detecção, atraso e resposta, as quais foram usadas neste modelo.

Para as variáveis associadas à função de neutralização podem ser utilizadas funções que calculam a probabilidade de neutralização em função do poder de combate da força de reação e da força inimiga, como o método descrito por SNELL (2013).

Em relação aos possíveis danos, é possível utilizar dados históricos de eventos semelhantes em conjunto com a opinião de especialista, para construir as Tabelas de Probabilidade Condicional da distruição de danos e da na determinação dos custos gerados.

Cabe ressaltar que caso o modelo proposto seja utilizado em uma instalação real em que não existam informações disponíveis sobre alguma variável da planta, os dados podem ser obtidos com os especialista da instalação através de métodos de elicitação, descrito por ARGENTI, *et al.* (2018). Essa abordagem pode ser empregada em modelos de segurança física, especialmente em contextos nos quais a disponibilidade de dados empíricos é limitada.

3.6 PROCEDIMENTO DE AVALIAÇÃO DAS ALTERNATIVAS DE DECISÃO

Após a definição dos nós, seus estados e suas respectivas Tabelas de Probabilidade Condicional, a estrutura do modelo é implementada no software GeNIe (BAYESFUSION, 2024), o qual é utilizado para a construção do diagrama de influência e para a realização dos cálculos probabilísticos e da utilidade esperada. Essa implementação computacional permite a avaliação consistente das alternativas de decisão, bem como a realização de análises de sensibilidade e simulações de diferentes cenários.

O objetivo é utilizar a estrutura do diagrama de influência para comparar diferentes combinações de alternativas associadas às funções de detecção, atraso e resposta, sob condições de incerteza, a partir do critério de utilidade esperada.

Para cada combinação de alternativas de decisão, o modelo calcula a distribuição de probabilidades dos possíveis resultados, considerando a interação entre as características da ameaça, o desempenho do sistema de proteção física e os efeitos das decisões adotadas.

A utilidade esperada de cada combinação de alternativas é obtida nó de utilidade total pela ponderação dos possíveis resultados pelas suas respectivas probabilidades, permitindo a comparação objetiva entre diferentes estratégias de proteção física. A combinação de alternativas que apresenta o melhor custo-benefício é aquela que resulta no maior valor de utilidade esperada, sendo, portanto, considerada a estratégia ótima no âmbito do modelo.

No cálculo da utilidade total, foram atribuídos pesos unitários (peso igual a 1) aos diferentes componentes considerados, de modo que os custos associados às medidas de proteção e os custos decorrentes dos danos fossem agregados de forma direta, sem priorização relativa entre esses termos. Essa escolha foi feita para evitar introduzir mais subjetividade na análise, já que a definição de pesos diferentes exigiria critérios adicionais que podem variar conforme o decisor. Assim, ao utilizar pesos iguais, a comparação entre as alternativas é feita de forma mais direta e transparente, baseada apenas nos custos e nas consequências estimadas. Além disso, o modelo permanece flexível, permitindo a inclusão de pesos diferentes no futuro, caso seja necessário representar preferências específicas.

Ressalta-se que o modelo não impõe uma única solução ótima de forma determinística, mas fornece ao decisor uma base estruturada para a comparação de alternativas sob incerteza. Essa abordagem permite identificar estratégias mais eficientes em termos de custo-benefício, bem como analisar compromissos entre níveis de proteção, custos de implementação e consequências potenciais de um ataque.

Por fim, o procedimento adotado reforça o caráter do modelo como ferramenta de apoio à decisão estratégica, permitindo que diferentes conjuntos de alternativas sejam avaliados de forma consistente e transparente, e que os parâmetros do modelo sejam ajustados conforme as características específicas da instalação e as preferências do decisor.

3.7 LIMITAÇÕES DO ESTUDO

Apesar da metodologia proposta apresentar uma estrutura coerente para o apoio à decisão estratégica em proteção física de instalações nucleares, algumas limitações devem ser explicitadas, decorrentes tanto das hipóteses de modelagem adotadas quanto da natureza dos dados e do nível de abstração empregado.

Uma primeira limitação refere-se às hipóteses utilizadas na formulação do modelo de decisão. Em particular, assumiu-se que as decisões estratégicas do defensor não influenciam diretamente a escolha do alvo nem da forma de acesso pelo adversário, bem como que as alternativas de proteção física são definidas previamente à ocorrência de um ataque, não sendo consideradas decisões adaptativas em tempo real. Essas hipóteses são compatíveis com o caráter estratégico da análise e permitem manter a complexidade do modelo em níveis gerenciáveis, porém não representam explicitamente possíveis processos de adaptação dinâmica do adversário frente ao fortalecimento das medidas de segurança.

Outra limitação relevante está associada à atribuição das probabilidades condicionais do modelo bayesiano. Em razão da escassez de dados públicos sistematizados sobre o desempenho de sistemas de proteção física, especialmente no que se refere às funções de atraso, neutralização e danos decorrentes de um ataque, optou-se por utilizar valores representativos coerentes com a literatura e com o comportamento esperado do sistema. Tais probabilidades foram empregadas com o

objetivo de demonstrar o funcionamento do modelo e permitir a comparação entre alternativas de decisão, não devendo ser interpretadas como estimativas absolutas de desempenho em situações reais. Em aplicações práticas, esses parâmetros devem ser ajustados por especialistas diretamente envolvidos na proteção da instalação analisada.

Adicionalmente, o estudo de caso considerado possui caráter inteiramente hipotético e funcional, não correspondendo a uma instalação real nem a um projeto executivo de Sistema de Proteção Física. A caracterização da instalação foi realizada apenas no nível de detalhamento necessário para a aplicação estratégica do modelo de decisão, sem a especificação de *layouts* físicos, tempos de deslocamento precisos ou características técnicas individuais de sensores e barreiras. Essa abordagem é adequada ao objetivo do trabalho, mas limita a extrapolação direta dos resultados para contextos reais sem a devida adaptação do modelo.

Outra limitação decorre da representação agregada da ameaça adotada no modelo. Embora fundamentada em eventos históricos e em diretrizes normativas de segurança nuclear, a caracterização da ameaça não contempla a totalidade de possíveis comportamentos adversários nem a emergência de táticas inovadoras ou tecnologias futuras. Os cenários considerados representam um conjunto plausível e coerente de situações adversas, porém não esgotam o universo de ameaças potenciais.

Por fim, ressalta-se que o modelo proposto concentra-se na avaliação comparativa de estratégias de proteção física sob incerteza, não tendo como objetivo a previsão determinística de eventos específicos nem a simulação detalhada de confrontos reais. Sua principal contribuição reside no apoio estruturado à tomada de decisão estratégica, permitindo analisar compromissos entre custos, níveis de proteção e consequências esperadas.

Apesar dessas limitações, entende-se que o modelo desenvolvido constitui uma ferramenta flexível e robusta para o apoio à decisão em proteção física nuclear, podendo ser aprimorado e adaptado conforme a disponibilidade de dados mais detalhados e as necessidades específicas de diferentes instalações.

4 APLICAÇÃO DA METODOLOGIA EM UM ESTUDO DE CASO

4.1 CARACTERIZAÇÃO DO ESTUDO DE CASO

O estudo de caso adotado neste trabalho consiste em uma instalação nuclear hipotética inserida em um complexo naval localizado em região litorânea, destinada a apoiar atividades associadas à operação e manutenção de meios navais com propulsão nuclear. A escolha desse tipo de instalação tem como objetivo ilustrar a aplicação do modelo de decisão proposto em um contexto caracterizado por elevado interesse estratégico, presença de material nuclear sensível e necessidade de elevados níveis de proteção física.

A instalação considerada não representa uma base real e não corresponde a um projeto executivo de segurança física. Sua caracterização é intencionalmente genérica e funcional, sendo definida apenas no nível de detalhe necessário para a aplicação do modelo bayesiano de decisão. Dessa forma, não são especificados *layouts* físicos, dimensões exatas ou posicionamentos detalhados de estruturas, uma vez que tais informações não são requeridas para a análise estratégica conduzida neste trabalho.

Do ponto de vista funcional, a instalação hipotética possui uma área destinada a atividades de manutenção especializada envolvendo material nuclear armazenado nas piscinas de elementos combustíveis, onde permanecem antes de sua instalação nos meios navais e após sua remoção. Essa área é caracterizada como a área vital do complexo, cujo acesso não autorizado ou eventual sabotagem pode resultar em consequências significativas para a segurança nuclear, o que justifica sua priorização no modelo de proteção física. Além disso, a instalação inclui áreas de apoio operacional e administrativas.

Situações envolvendo submarinos nucleares atracados no complexo naval não foram consideradas no escopo do modelo, em razão de apresentarem camadas adicionais de proteção física, configurações operacionais distintas e por não permanecerem de forma contínua na instalação analisada.

O complexo naval no qual a instalação está inserida apresenta múltiplos modos potenciais de acesso ao alvo, incluindo acessos terrestres e marítimos, refletindo um cenário típico de instalações localizadas em ambiente costeiro. Essa característica é

relevante para a modelagem da ameaça, uma vez que influencia as possíveis rotas de aproximação do adversário, os meios empregados e o desempenho esperado das funções de detecção e atraso.

A Figura 6 apresenta uma representação esquemática da configuração funcional da instalação hipotética (SANTOS, 2024), considerada como estudo de caso, destacando as diferentes zonas de proteção física, área externa, área protegida, área vigiada e área vital, bem como a disposição das principais edificações e acessos terrestres e marítimos. Ressalta-se que a figura possui caráter ilustrativo, não representando uma instalação real, sendo apresentada apenas para facilitar a compreensão da estrutura adotada no modelo.

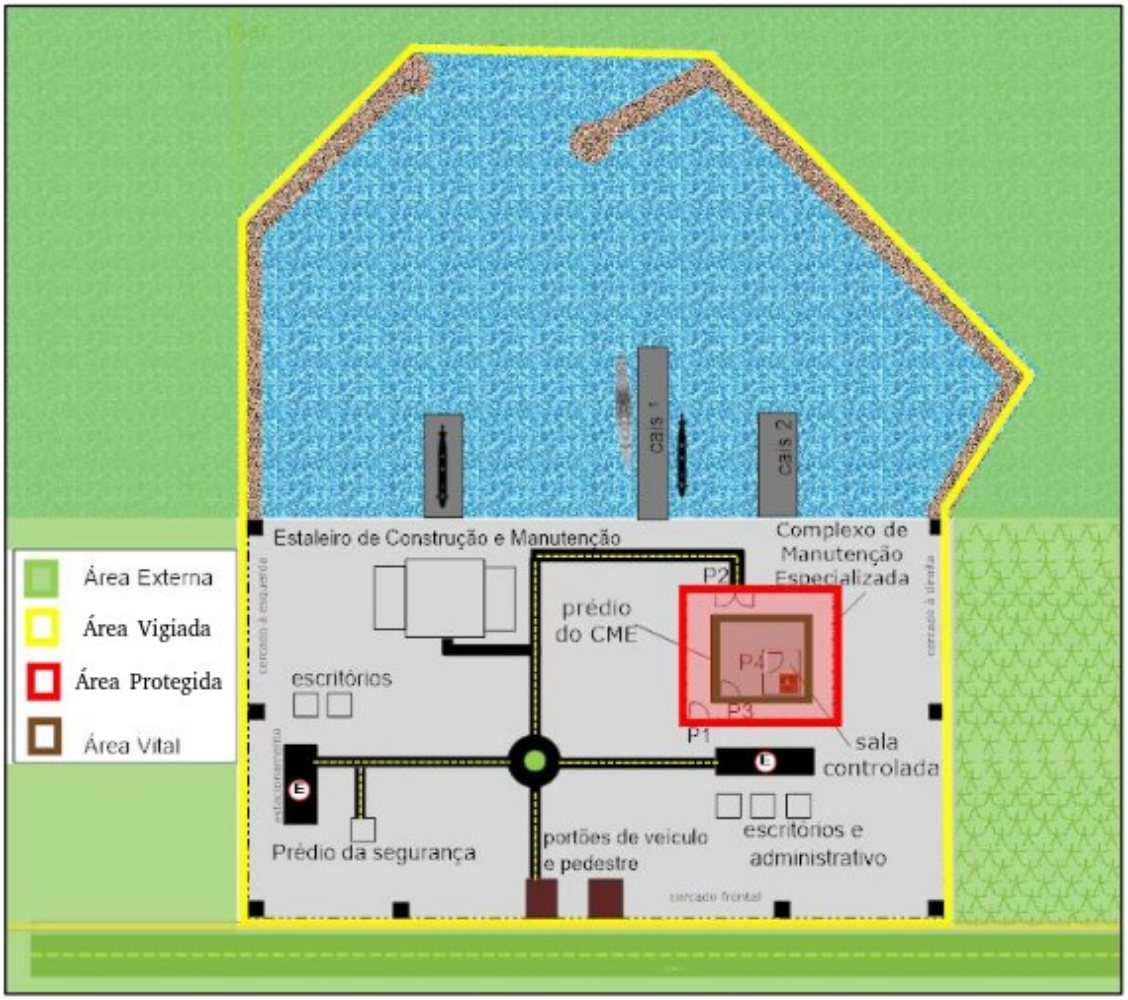

Figura 6 - Representação esquemática da instalação nuclear hipotética e das zonas de proteção física consideradas no estudo de caso (SANTOS, 2024)

A Base Naval Hipotética (BNH) é composta por diferentes edificações com funções operacionais, técnicas e administrativas, organizadas de forma a apoiar as atividades de manutenção de meios navais de propulsão nuclear e garantir a segurança do complexo.

O Estaleiro de Construção e Manutenção (EsCoMa) é responsável pelas atividades de construção, manutenção e reparo das embarcações navais, incluindo docas secas, oficinas especializadas e áreas de armazenamento de materiais e suprimentos. Trata-se de uma infraestrutura essencial para o funcionamento da frota, caracterizada por intensa atividade operacional.

No interior do Complexo de Manutenção Especializada (CME) encontram-se diferentes tipos de material nuclear de interesse do ponto de vista da proteção física. Durante as operações de reabastecimento dos reatores das embarcações de propulsão nuclear, o combustível novo é armazenado temporariamente no CME. Esse combustível consiste, em geral, em urânio enriquecido (U-235), com níveis de enriquecimento superiores aos utilizados em reatores comerciais, podendo atingir valores da ordem de até 20%. Em razão de sua composição e potencial de uso indevido para fins não pacíficos, esse material apresenta elevado grau de atratividade para agentes mal-intencionados.

Para fins de caracterização do estudo de caso, considerou-se um inventário típico de de dióxido de urânio (UO_2) distribuídos nos elementos combustíveis de um reator naval de médio porte, o que o enquadra como material nuclear de Categoria I, conforme a classificação estabelecida pela Comissão Nacional de Energia Nuclear (CNEN, 2019a).

Além do combustível novo, o CME abriga o combustível nuclear irradiado, removido dos reatores durante as operações de carga/manutenção. Embora não seja mais empregado diretamente na propulsão naval, esse material ainda contém quantidades significativas de material físsil, incluindo urânio residual e plutônio gerado durante a operação do reator, tornando-se também um alvo de interesse para fins ilícitos. O combustível irradiado é armazenado nas piscinas de decaimento do complexo, sendo classificado como material nuclear de Categoria II, segundo a CNEN (2019a).

O prédio da segurança atua como centro de comando e controle das operações de proteção física da base, abrigando sistemas de vigilância, coordenação de resposta a emergências e as equipes de segurança armada.

Além dessas estruturas, o complexo inclui prédios administrativos e escritórios técnicos, responsáveis pelas atividades de gestão, planejamento e suporte operacional, bem como guaritas distribuídas em pontos estratégicos do perímetro, responsáveis pela vigilância local e controle de acessos.

A classificação das áreas de segurança é estabelecida de acordo com a criticidade e vulnerabilidade de cada região da instalação. Uma vez identificados os alvos no item anterior, é possível estabelecer a categorização das zonas de segurança em três níveis principais:

- Área vigiada: compreende toda a área da BNH (Figura 6)
- Área protegida : compreende todo o cercado do CME (Figura 7); e
- Área vital : compreende todo o prédio do CME (Figura 8).

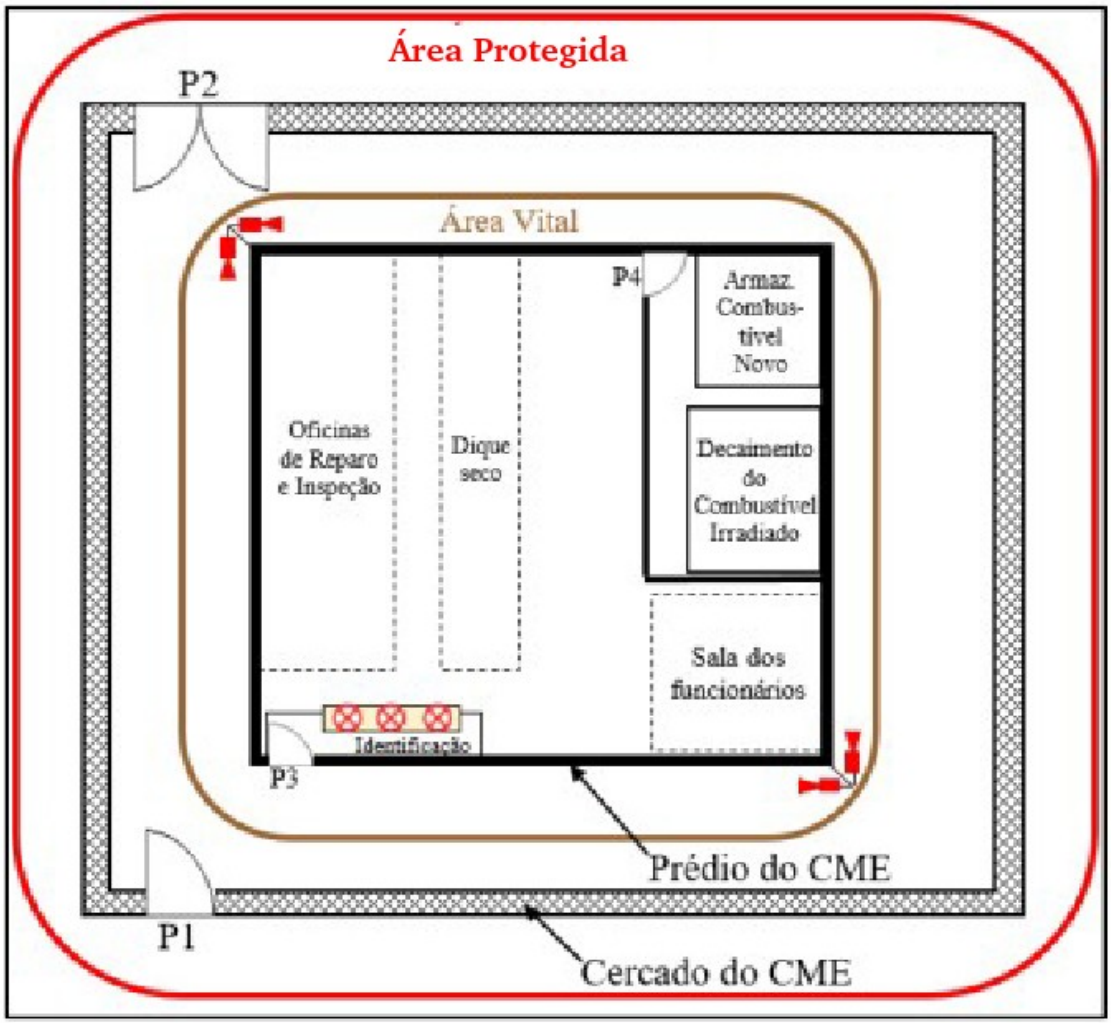

Figura 7 - Área Vigiada (SANTOS, 2024)

Figura 8 - Área Vital (SANTOS, 2024)

Admite-se a existência de um sistema de proteção física composto por múltiplas camadas, incluindo medidas de detecção, barreiras físicas e uma força de resposta dedicada à segurança da instalação. Algumas dessas medidas são consideradas como condições já existentes do cenário, enquanto outras são tratadas como alternativas de decisão a serem avaliadas pelo modelo, conforme descrito no Capítulo 3. A presença de pessoal autorizado, atividades operacionais contínuas e rotinas administrativas também é assumida, refletindo a complexidade inerente ao ambiente de operação da instalação.

4.2 CONSTRUÇÃO DO MODELO PARA O ESTUDO DE CASO

Nesta seção descreve-se o processo de parametrização do modelo bayesiano aplicado ao estudo de caso da Base Naval Hipotética. A parametrização consiste na atribuição dos estados das variáveis, das probabilidades condicionais e dos valores de custo associados às alternativas de decisão e às consequências consideradas, permitindo a execução das análises e a obtenção dos resultados apresentados no capítulo seguinte.

A parametrização do modelo foi realizada de forma coerente com a estrutura conceitual apresentada no Capítulo 3 e com as definições estabelecidas nas seções anteriores deste capítulo. Os cenários de ameaça considerados no estudo de caso são definidos a partir da combinação dos atributos descritos na Seção 3.4, incluindo intenções, capacidades, tamanho do grupo, formas de acesso e alvo pretendido.

4.2.1 Ameaça

Com base na classificação dos casos históricos apresentada na Seção 3.4 a ameaça foi representada por meio dos nós de chance, seus respectivos estados e pais, apresentados na Tabela 3 .

Os nós motivação do adversário tamanho de grupo e presença de ameaça interna foram definidos como nó raiz, porque representam às capacidades e à organização do adversário prévias ao ataque. O nó via de acesso foi considerada como uma característica da instalação.

Foi assumido que a motivação do adversário atua como nó pai da variável intenção do adversário, por representar o fator que direciona o tipo de ação a ser realizada. Por sua vez, a intenção foi modelada como nó pai das variáveis alvo pretendido e meios empregados, uma vez que o objetivo da ação influencia diretamente tanto a escolha do alvo quanto os recursos utilizados. Dessa forma, estabelece-se uma relação causal em que a motivação condiciona a intenção, e esta, por sua vez, orienta as decisões operacionais do adversário.

As tabelas de probabilidade condicional desses nós foram construídas a partir dos dados históricos.

Tabela 3 - Nós que representam a ameaça

Nó	**Estados**	**Pais**
Motivação do Adversário	Ideológica Política Pessoal Financeira	NA
Inteção do Adversário	Disrupção Roubo Sabotagem	Motivação do Adversário
Via de Acesso	Água Ar Terra	NA
Meios Empregados	Armas Explosivos Armas e Explosivos Nada	Intenção do Adversário
Alvo	Vital Protegida Vigiada	Intenção do Adversário
Presença de *insider*	Sim Não	NA
Tamanho do Grupo	Individual Pequeno Grupo Grande Grupo	NA

4.2.2 Detecção

O cenário base da instalação já contempla nós para meios permanentes de detecção: Vigilância por vídeo convencional, patrulhas de segurança e postos fixos de vigilância. Esses elementos constituem camadas iniciais do sistema de proteção física e

foram incorporados ao modelo como condições do ambiente, permanecendo constantes ao longo das análises realizadas.

No modelo aplicado ao estudo de caso, foi assumido que o decisor deve escolher entre estratégias adicionais para complementar as que já existem no sistema, sendo elas divididas em dois grupos, Alternativas de detecção para acesso terrestre/aquático e Alternativas de detecção e neutralização para acesso aéreo.

As alternativas de detecção para acesso terrestre/aquatico são o Radar subaquático e o Sistema de detecção de movimento por vídeo , descritos a seguir:

- Radar subaquático: Destina-se à identificação de aproximações não autorizadas por vias marítimas ou submersas, ampliando a capacidade de detecção de ameaças provenientes do ambiente aquático. O custo de implementação dessa medida foi estimado em R$ 7.000.000,00. (*NATIONAL HOMELAND SECURITY KNOWLEDGEBASE*, 2009).

- Sistema de detecção de movimento por vídeo (*Video Detection Motion* - VDM): consiste no aprimoramento da vigilância por vídeo existente por meio da incorporação de algoritmos de análise automática de imagens, capazes de identificar eventos relevantes, como movimento, intrusão, permanência indevida e comportamentos anômalos. Diferentemente da simples observação humana, o VDM permite a detecção contínua e automatizada de eventos, reduzindo falhas associadas à fadiga dos operadores e aumentando a probabilidade de detecção em áreas já monitoradas. Além disso, esses sistemas podem ser integrados a centros de comando e controle, possibilitando geração de alertas em tempo real e apoio à tomada de decisão. O custo de implementação, considerado que a instalação possui 40 câmeras já instaladas, foi estimado em R$ 1.000.000,00 (DIGITAL SECURITY GUARD, 2025).

As alternativas de detecção para o acesso terrestre/aquatico são o Sistema baseado em radiofrequência (*jammer)* e o Sistema híbrido de defesa anti-drone, descritos a seguir:

- Sistema anti-drone baseado em radiofrequência (RF) e interferência eletrônica: Destina-se à detecção e neutralização de veículos aéreos não tripulados por meio da identificação de sinais de comunicação entre o drone e seu operador, seguida da aplicação de interferência eletrônica (jamming) para interromper esse enlace. Essa abordagem amplia a capacidade de proteção da instalação ao permitir a atuação ativa contra drones comerciais amplamente disponíveis, sendo atualmente uma das soluções mais difundidas para proteção de infraestruturas críticas. No entanto, sua eficácia pode ser reduzida em cenários envolvendo drones autônomos ou que operam sem dependência de comunicação por radiofrequência. O custo de implementação dessa medida foi estimado em R$ 6.000.000,00 (CHAARI,2025; DEDRONE, 2022; DRONESHIELD, 2020).

- Sistema híbrido de defesa anti-drone (multissensor com neutralização física): Destina-se à detecção, rastreamento e neutralização de veículos aéreos não tripulados por meio da integração de múltiplos sensores, como radiofrequência, radar de baixa altitude e sistemas eletro-ópticos, associados a meios ativos de neutralização física, como drones interceptadores ou sistemas cinéticos. Essa abordagem amplia significativamente a capacidade de resposta da instalação ao permitir a atuação contra diferentes tipos de ameaças, incluindo drones autônomos ou resistentes a interferência eletrônica, aumentando a robustez do sistema frente à evolução tecnológica dos vetores aéreos. O custo de implementação dessa medida foi estimado em R$ 9.000.000,00, considerando a necessidade de integração de sensores e meios ativos de resposta (CHAARI, 2025; DEDRONE, 2022).

As probabilidades associadas para patrulhas, vigias e vídeo foram extraídas e adaptadas do estudo de ARGENTI *et al.* (2018), que apresenta valores de referência para o desempenho desses mecanismos em diferentes contextos operacionais, as quais possibilitaram as construções das Tabelas de Probabilidade Condicionais.

No caso de sistemas de detecção e interdição de veículos aéreos não tripulados, materiais técnicos de fabricantes indicam que soluções baseadas em sensores de radiofrequência e interferência eletrônica podem alcançar taxas de detecção superiores a

85% e níveis de sucesso de neutralização superiores a 80% contra drones comerciais em cenários controlados. No entanto, tais sistemas apresentam limitações frente a drones autônomos ou que não dependem de comunicação por radiofrequência (DRONESHIELD, 2020; DEDRONE, 2022; CHAARI, 2025). Com base nesses dados, adotou-se no modelo um valor de 0,7 para o sucesso da neutralização dos drones nessa alternativa.

Por sua vez, sistemas híbridos, que combinam múltiplos sensores (como radiofrequência, radar e meios eletro-ópticos) com mecanismos de neutralização física, apresentam maior robustez operacional, sendo capazes de atuar contra diferentes tipos de drones, inclusive aqueles imunes à interferência eletrônica. Materiais técnicos e estudos recentes indicam que a integração de múltiplas camadas de detecção e resposta contribui para o aumento da eficácia global desses sistemas (DEDRONE, 2022; CHAARI, 2025). Com base nesses dados, adotou-se no modelo um valor de 0,85 para o sucesso da neutralização dos drones nessa alternativa.

De forma análoga, sistemas de detecção subaquática, como sonares ativos empregados na proteção de instalações sensíveis, apresentam elevada capacidade de detecção de alvos submersos em ambientes monitorados, embora seu desempenho dependa de fatores como condições acústicas, ruído ambiental e características do alvo. Estudos sobre sistemas de vigilância subaquática indicam que tais tecnologias apresentam altas taxas de detecção em ambientes controlados, especialmente quando operando em redes integradas de sensores (NATO, 2017). Com base nessa evidência qualitativa, adotou-se no modelo o valor de 0,85 como representativo da probabilidade de detecção desse tipo de sistema.

A tabela 4 apresenta os nós relacionados a função de detecção, seus estados e pais.

Tabela 4 - Nós da função de Detecção

Nó	**Estados**	**Pais**
Detecção de Movimento por Vídeo	Sim Não	Atenção do Operador Alternativas de Detecção Condições Meterológicas Cobertura das câmeras Manutenção *insider* Tamanho do Grupo
Atenção do Operador	Alta Baixa	NA
Cobertura das Câmeras	Completa Incompleta	NA
Condições Metereológicas	Boas Ruins	NA
Manutenção	Satisfatória Insatisfátoria	NA
Alternativas de Detecção para Detecção de acesso Terrestre/ Aquátic (Nó de Decisão)	Nenhuma VDM Radar Subáquatico	NA
Custos das Alternativas para Detecção de acesso Terrestre/ Aquático (Nó de Utilidade)	Nenhuma = 0 VDM = 600.000 Radar Subáquatico= 7.000.000	Alternativas de Detecção de acesso Terrestre/Aquático Via de Acesso
Detecção por Patrulha	Sim Não	Presença da Patrulha Nível de Treinamento
Deteção por Vigia	Sim Não	Nível de Treinamento
Detecção por Radar Subaquatico	Sim	Alternativas de Detecção

	Não	*insider*
Detecção Global	Precoce Tardia Não Detecado	Detecção de Movimento por vídeo Detecção por Vigia Detecção por Patrulha Detecção por Radar Subáquatico
Alternativas de Detecção para Detecção de acesso aéreo (Nó de Decisão)	Nenhuma *jammer* Hibrido	NA
Custos das Alternativas para Detecção de acesso aéreo(Nó de Utilidade)	Nenhuma = 0 *jammer* = 6.000.000 Hibrido= 7.000.000	Alternativas de Detecção Detecção de acesso aéreo Via de Acesso
Detecção e Neutralização do VANT	Sim Não	Alternativas de Detecção de acesso aéreo *insider*

Foram adotadas algumas premissas na modelagem da função de detecção a fim de simplicar o construção das tabelas de probabilidade, definidas a seguir:

1) Os meios permanentes de detecção da instalação (vigilância por vídeo convencional, patrulhas e vigias) são considerados eficazes principalmente para acessos terrestres e marítimos de superfície, não contribuindo de forma significativa para a detecção de ameaças provenientes do acesso aéreo por drones.

2) Embora seja possível que vigias ou patrulhas visualizem um drone em determinadas situações, assume-se que tal detecção ocorreria em estágio muito próximo ao alvo, com tempo insuficiente para uma resposta eficaz, motivo pelo qual seu efeito prático foi desconsiderado no modelo.

3) A detecção de ameaças aéreas é tratada predominantemente como dependente da adoção de sistemas específicos antidrone, representados como alternativas de decisão no modelo bayesiano.

4) A alternativa VDM (*Video Detection Motion*) não foi representada por um novo nó de detecção independente, pois sua função no modelo não é criar um meio adicional autônomo de vigilância, mas sim aperfeiçoar o desempenho do sistema de vigilância por vídeo já existente. Dessa forma, sua adoção foi modelada como um fator que eleva a probabilidade de detecção no nó de detecção por vídeo, em razão das vantagens associadas à análise automática de imagens, como identificação contínua de movimento, geração de alertas em tempo real e redução de falhas decorrentes da observação exclusivamente humana.

5) A variável presença de *insider* foi modelada como nó pai dos sistemas de detecção, uma vez que a atuação de um agente interno pode comprometer direta ou indiretamente o desempenho desses sistemas, por meio de ações como sabotagem, desativação de equipamentos, omissão deliberada na vigilância ou facilitação de acessos indevidos. Esse efeito foi representado no modelo como uma redução estimada de 20% na probabilidade de detecção. Ressalta-se que esse valor constitui uma aproximação inicial, sendo posteriormente avaliado por meio de análise de sensibilidade, a fim de verificar a robustez dos resultados frente a diferentes níveis de degradação.

6) O nó Detecção Global foi modelado com lógica do tipo “OU” (OR), de modo que a detecção por qualquer um dos meios considerados é suficiente para caracterizar sua ocorrência. Com o objetivo de representar a oportunidade temporal da detecção, o nó foi estruturado em três estados: precoce, tardia e não detectado. Os sistemas de antidrone, radar subaquático e vigilância fixa (vigias), foram associados predominantemente ao estado de detecção precoce, por sua capacidade de identificar a ameaça ainda nos limites da instalação ou antes de sua violação. Já meios como câmeras e patrulhas móveis foram modelados com distribuições probabilísticas entre detecção precoce e tardia, refletindo suas limitações operacionais. Para as câmeras, foi adotada uma distribuição de 0,9 para detecção precoce e 0,1 para detecção tardia, enquanto para as patrulhas foram considerados valores de 0,7 e 0,3, respectivamente, baseados em parâmetros de referência apresentados em GARCIA(2008).

4.2.3 Resposta

No estudo de caso, foram consideradas duas estratégias de resposta como alternativas de decisão do defensor: uma estratégia básica e uma estratégia reforçada.

A estratégia de resposta básica corresponde à configuração padrão da força de segurança da instalação, composta por um efetivo de oito operadores por turno, operando de forma contínua. Essa configuração é tratada como condição de referência do cenário, não sendo associado custo adicional a essa alternativa no nó de utilidade do modelo.

A estratégia de resposta reforçada corresponde ao aumento do efetivo da força de reação para doze operadores por turno. Ressalta-se que a definição do efetivo reforçado considerou a organização tática usual da força, estruturada em equipes de quatro operadores. Dessa forma, a configuração básica corresponde a dois grupos operacionais, enquanto a configuração reforçada permite a formação de três grupos, possibilitando maior flexibilidade de emprego, atuação simultânea em múltiplos setores e incremento da capacidade de resposta.

Os custos associados à estratégia de resposta reforçada, apresentados na Tabela 5, foram definidos contemplando investimentos em meios materiais.

Tabela 5 - Estimativa de custo da Equipe de Resposta reforçada

Item	**Descrição**	**Valor (R$)**
Viatura dedicada	Aquisição (amortização), manutenção e operação	200.000
Equipamentos táticos	Equipamentos individuais, meios de proteção, armamento institucional e demais recursos operacionais	200.000
Total anual		400.000

Na função de resposta, optou-se por uma modelagem mais agregada, representando a capacidade de reação da força de segurança por meio do nó Alternativas de Resposta, que representa as configurações possíveis da força de resposta (básica e reforçada). Essa abordagem permite capturar, de forma simplificada, o impacto das diferentes estratégias. A Tabela 6 apresenta os nós considerados na função de resposta.

Tabela 6 - Nós da função de Resposta

Nó	Estados	Pais
Alternativas de Resposta (Nó de Decisão)	Básica Reforçada	NA
Custos da Reposta (Nó de Utilidade)	Básica = 0 Reforçada= 400.000	Alternativas de Resposta

Nos cenários de ameaça aérea por drones, a neutralização foi modelada como independente da força de resposta terrestre, sendo atribuída exclusivamente ao sistema antidrone. Essa escolha reflete a baixa efetividade operacional de meios terrestres convencionais frente a ameaças aéreas de pequena dimensão e alta mobilidade, além da maior adequação de sistemas especializados para esse tipo de interdição.

4.2.4 Atraso

Foram consideradas três estratégias de atraso como alternativas de decisão do defensor:

- Nenhuma barreira adicional, que representa a configuração atual do sistema de proteção física, já contemplando as barreiras e obstáculos existentes na instalação, sem acréscimo de medidas estruturais.
- Portas reforçadas nos edifícios da área protegida (Alternativa 1): consistindo no fortalecimento dos acessos críticos por meio de portas de maior resistência física, capazes de impor maior tempo de violação ao adversário em tentativas de invasão direta às estruturas sensíveis. O custo de implementação para duas portas foi estimado em R$ 400.000 (CIS SHOW HARDWARE,2025).
- Portas reforçadas nos edifícios da área vital e protegida (Alternativa 2): com custo de implementação para duas portas foi estimado em R$ 800.000 (CIS SHOW HARDWARE,2025).

A Tabela 7 apresenta os nós considerados na função de resposta.

Tabela 7 - Nós da função de Atraso

Nó	**Estados**	**Pais**
Alternativas de Obstáculos (Nó de Decisão)	Nenhuma Portas Reforçadas na Area Vital Portas Reforças da Area Vital e Protegida	NA
Custos das Alternativas de Obstáculos (Nó de Utilidade)	Nenhuma = 0 Portas Reforçadas na Area Protegida= 400.000 Portas Reforças da Area Vital e Protegida=800.000	Alternativas de Obstáculos
Atraso Efetivo	Baixo Médio Alto	Alternativas de Obstáculos Alvo

As premissas adotadas na modelagem da função de atraso, são apresentadas a seguir:

1) As barreiras físicas já existentes na instalação são consideradas parte integrante do cenário base de proteção física e não são explicitamente modeladas como variáveis individuais, estando incorporadas à alternativa de decisão sem reforços adicionais (“Nenhuma”)

2) As estratégias de atraso consideradas no modelo representam reforços estruturais incrementais sobre o sistema atual, com impacto principal na ampliação do tempo disponível para a atuação da força de resposta.

3) O nó Atraso Efetivo tem como pais as alternativas de obstáculos e o alvo, pois a eficácia das medidas de atraso varia conforme a região da instalação, podendo uma mesma alternativa gerar diferentes níveis de atraso dependendo do alvo considerado.

Para a construção da Tabela de Probabilidade Condicional do nó Atraso Efetivo, foram utilizados os tempos de atraso obtidos a partir dos diferentes caminhos de progressão do adversário na instalação, com base nos dados apresentados por Santos (2024). Para cada combinação entre alternativa de obstáculos e alvo, foram considerados os respectivos tempos de atraso associados aos caminhos possíveis, a partir dos quais se construiu a distribuição de probabilidade do nó.

Em seguida, os tempos obtidos foram discretizados em três estados qualitativos: baixo, para tempos de até 150 s; médio, para tempos entre 150 s e 300 s; e alto, para tempos superiores a 300 s. Essa divisão foi definida de forma a refletir agrupamentos naturais dos dados, permitindo diferenciar cenários de baixa, média e alta resistência à progressão do adversário.

Dessa forma, a distribuição de probabilidade do nó Atraso Efetivo foi construída diretamente para todos os cenários analisados, em função do alvo e da estratégia de obstáculos considerada. Os valores correspondentes são apresentados na Tabela 8.

Tabela 8 - Tabela de Probabilidade Condicional do nó Atraso Efetivo em função do alvo e das alternativas de obstáculos

Alternativa	**Nenhuma**			**Alternativa 1**			**Alternativa 2**		
Área	**Vig.**	**Prot.**	**Vit.**	**Vig.**	**Prot.**	**Vit.**	**Vig.**	**Prot.**	**Vit.**
Baixo	0,31	0,09	0,06	0,31	0,04	0,02	0,31	0,04	0,01
Médio	0,69	0,63	0,36	0,69	0,45	0,23	0,69	0,45	0,11
Alto	0,00	0,28	0,59	0,00	0,51	0,74	0,00	0,51	0,87

4.2.5 Neutralização

O nó de Neutralização representa a capacidade da força de resposta em conter ou derrotar o adversário após sua detecção e durante seu avanço no interior da instalação. Esse nó expressa, portanto, o resultado operacional do engajamento entre a força de segurança e o adversário, sendo diretamente influenciado tanto pelas características da ameaça quanto pelo desempenho do sistema de proteção física. Os estados do nó foram definidos como “Sim” (quando a neutralização do adversário é bem-sucedida) e “Não”

(quando o adversário não é neutralizado). A Tabela 9 apresenta os estados do nó e seus pais

Tabela 9 - Nó de Neutralização

Nó	**Estados**	**Pais**
Neutralização	Sim Não	Alternativas de Resposta Atraso Efetivo Detecção Global de acesso Terrestre/ Aquático Tamanho do Grupo Meios Empregados

A formulação adotada para a probabilidade de neutralização foi proposta no presente trabalho, sendo baseada nas hipóteses apresentadas por Snell (2013), que relacionam a probabilidade de neutralização à razão entre as capacidades relativas da força de reação e do adversário, considerando o número de indivíduos, a eficácia dos meios empregados e e os tempos associados do caminho do adversário e do de chegada da força de reação.

Com base nessas hipóteses, foi assumido que a capacidade efetiva de combate de cada lado pode ser representada pelo produto entre o número de combatentes e um fator de eficácia associado aos meios utilizados. Adicionalmente, adotou-se uma relação não linear entre essas capacidades, inspirada em modelos clássicos de combate, como as leis quadráticas de LANCHESTER (1956).

Foi introduzido um fator de atraso, denotado por f_A, que representa o atraso imposto ao adversário pelas barreiras físicas do sistema de proteção. Esse atraso amplia a janela temporal disponível para a atuação da força de resposta, de modo que valores mais elevados de f_A estão associados a maiores probabilidades de neutralização. em consonância com as hipóteses apresentadas por SNELL (2013).

De forma análoga, foi introduzido um fator associado à detecção, denotado por f_D, que representa o efeito da oportunidade temporal da detecção sobre a efetividade da resposta. Esse fator assume valor igual a 1 para a detecção precoce, valores reduzidos para a detecção tardia e valor igual a 0 na ausência de detecção, refletindo a inexistência de acionamento oportuno da força de resposta. Essa abordagem está em consonância com as hipóteses apresentadas por SNELL (2013)

Dessa forma, foi proposta a Equação (5) para a probabilidade de neutralização:

$$PN = \frac{(A_R \cdot C_R)^2}{(A_R \cdot C_R)^2 + (A_I \cdot C_I)^2} \times f_D \times f_A \quad \text{Eq (5)}$$

onde:

A_R e C_R representam, respectivamente, o fator de eficácia do armamento e o número de combatentes na da força de resposta;

A_I e C_I representam, respectivamente, o fator de eficácia do armamento e o número de combatentes na do inimgo;

f_D representa o efeito da detecção; e

f_A representa o efeito atraso;

Para fins de simplificação do modelo, foi assumido que a força de resposta está sempre armada. Essa hipótese baseia-se no fato de que, em cenários de proteção de instalações sensíveis, a força de segurança é permanentemente equipada com armamento adequado para pronta resposta a ameaças.

Dessa forma, o fator de eficácia associado à força de resposta foi considerado constante, assumindo valor equivalente ao de armamento do tipo fuzil, adotado como referência neste trabalho. Tal escolha permite reduzir a complexidade do modelo, ao eliminar variações desnecessárias, sem prejuízo da representatividade do cenário analisado. Por outro lado, para o adversário, foram considerados dois estados: sem armamento e armado com fuzil, de modo a capturar diferentes níveis de ameaça. Essa simplificação tem como objetivo reduzir a complexidade do modelo, mantendo sua capacidade de avaliar comparativamente o impacto dos diferentes perfis adversários sobre a neutralização.

Os valores atribuídos ao fator de eficácia do armamento foram definidos com base nas relações de equivalência apresentadas por SNELL (2013), segundo as quais combatentes com armamento superior podem ser representados como múltiplos de combatentes com armamento inferior. Com base nessas relações, foi adotada uma escala relativa de eficácia, na qual o valor A_R=1,0 foi atribuído ao uso de fuzil, considerado equivalente ao rifle utilizado na referência. O valor A_R=0,1 foi atribuído à condição sem armamento, representando uma capacidade de combate significativamente inferior, de forma a preservar a diferença de ordens de grandeza entre os níveis de eficácia.

Os fatores associados ao atraso foram propostos no presente trabalho, a partir da categorização previamente estabelecida para o nó Atraso Efetivo, com base na variações observada por Santos (2024) para diferentes configurações de barreiras físicas, embora os valores adotados constituam uma adaptação paramétrica voltada à operacionalização do modelo.sendo utilizados como coeficientes de ajuste da probabilidade de neutralização e apresentados na Tabela 10.

Tabela 10 - Fatores associados ao atraso da força de resposta

Categoria de atraso	**f_D**
Baixo	0,6
Médio	0,8
Alto	1,0

O nó Tamanho do Grupo foi definido de forma discreta, com três estados: individual, pequeno e grande. Para fins de aplicação da Equação (5), foi necessário associar valores numéricos a cada uma dessas categorias. Assim, foram adotados os seguintes valores representativos: 1 combatente para o estado individual, 4 combatentes para o estado pequeno e 8 combatentes para o estado grande, baseado nos casos históricos.

Além disso, foi assumido que, na ausência de detecção do adversário, não há possibilidade de neutralização. Dessa forma, para o estado “Não detectado” do nó Detecção Global, a probabilidade de neutralização foi considerada nula, independentemente dos demais fatores do modelo.

A partir da formulação apresentada e dos parâmetros definidos, foi construída a Tabela de Probabilidade Condicionaldo nó Neutralização, a qual estabelece a probabilidade de ocorrência dos seus estados (“Sim” e “Não”) para cada combinação dos estados dos nós pais. Os valores da CPT foram obtidos a partir da Equação (5), aplicada às diferentes combinações dos parâmetros associados à força de resposta, ao adversário e ao fator de atraso, conforme os estados definidos no modelo. As Tabelas 11 e 12, apresentam os dados para as duas alternativas de resposta, Básica e Reforçada, respectivamente, para uma detecção precoce. Para a detecção tardia, esses valores foram multiplicados por um fator (f_D) de 0,8.

Tabela 11 - Probabilidades de Neutralização (Sim/Não) condicionadas aos níveis de Atraso, aos Meios empregados e ao Tamanho do Grupo adversário para a Força de Resposta Básica

Atraso	**Alto**						**Médio**						**Baixo**					
Meios	**Nada**			**Armas**			**Nada**			**Armas**			**Nada**			**Armas**		
Grupo	**Ind.**	**Peq.**	**Gra.**	**Ind.**	**Peq.**	**Gra.**	**Ind.**	**Peq.**	**Gra.**	**Ind.**	**Peq.**	**Gra.**	**Ind.**	**Peq.**	**Gra.**	**Ind.**	**Peq.**	**Gra.**
Sim	0,999	0,999	0,996	0,985	0,800	0,500	0,799	0,799	0,796	0,788	0,640	0,400	0,599	0,599	0,597	0,591	0,480	0,300
Não	0,001	0,001	0,004	0,015	0,200	0,500	0,201	0,201	0,204	0,212	0,360	0,600	0,401	0,401	0,403	0,409	0,520	0,700

Tabela 12 - Probabilidades de Neutralização (Sim/Não) condicionadas aos níveis de Atraso, aos Meios empregados e ao Tamanho do Grupo adversário para a Força de Resposta Reforçada

Atraso	**Alto**						**Médio**						**Baixo**					
Meios	**Nada**			**Armas**			**Nada**			**Armas**			**Nada**			**Armas**		
Grupo	**Ind.**	**Peq.**	**Gra.**	**Ind.**	**Peq.**	**Gra.**	**Ind.**	**Peq.**	**Gra.**	**Ind.**	**Peq.**	**Gra.**	**Ind.**	**Peq.**	**Gra.**	**Ind.**	**Peq.**	**Gra.**
Sim	0,999	0,999	0,996	0,993	0,900	0,692	0,799	0,799	0,796	0,794	0,720	0,554	0,599	0,599	0,597	0,596	0,540	0,415
Não	0,001	0,001	0,004	0,007	0,100	0,308	0,201	0,201	0,204	0,206	0,280	0,446	0,401	0,401	0,403	0,404	0,460	0,585

Para ameaças envolvendo veículos aéreos não tripulados, considerou-se que a neutralização é realizada pelo próprio sistema antidrone, e não pela força de resposta convencional, em função da necessidade de reação rápida e do emprego de tecnologias específicas, como interferência por radiofrequência. Dessa forma, a probabilidade de neutralização foi modelada de forma independente da resposta terrestre, sendo diferenciada conforme a alternativa de defesa adotada. Para sistemas baseados em interferência eletrônica (RF), foi adotado o valor de 0,7, refletindo limitações frente a drones autônomos ou não dependentes de comunicação. Já para sistemas híbridos, que combinam múltiplos sensores com meios de neutralização física, foi adotado o valor de 0,85, representando o ganho de eficácia associado à atuação em múltiplas camadas. Esses valores foram definidos com base em materiais técnicos de fabricantes de sistemas C-UAS, como Dedrone e DroneShield.

Ressalta-se que os valores adotados para os fatores de eficácia e atraso possuem caráter paramétrico e baseado nos estudos de SNELL (2013), sendo utilizados com o objetivo de demonstrar a aplicabilidade do modelo de decisão proposto na comparação entre estratégias de proteção física. Assim como nas demais variáveis do modelo, esses parâmetros podem ser ajustados em aplicações reais a partir de dados operacionais, exercícios de simulação e julgamento de especialistas.

4.2.6 Danos

Os impactos decorrentes de um evento adverso foram representados por meio de cinco estados discretos de dano, definidos de forma a capturar níveis progressivos de severidade das consequências sobre a instalação nuclear analisada. Esses estados compreendem:

- Sem Dano: corresponde a situações em que o evento adverso não resulta em impactos relevantes sobre a instalação, podendo incluir, por exemplo, tentativas frustradas, invasões sem sucesso ou ações interrompidas pela atuação eficaz do sistema de proteção física.
- Dano Estrutural: refere-se a impactos físicos localizados na instalação, que não comprometem de forma significativa sua operação ou integridade funcional.

Incluem-se nessa categoria danos a estruturas secundárias, sistemas auxiliares ou áreas periféricas.

- Subtração de Material Nuclear: representa eventos nos quais ocorre a perda ou desvio de material nuclear, sem que haja, necessariamente, danos físicos à infraestrutura da instalação. Essa categoria foi introduzida com o objetivo de capturar consequências associadas à falha dos sistemas de proteção física, distinguindo-se dos danos estruturais e refletindo implicações relevantes do ponto de vista da segurança nuclear
- Dano Crítico: corresponde a situações em que há comprometimento significativo da operação ou da integridade da instalação, podendo envolver a degradação de sistemas essenciais, paralisação de atividades ou prejuízos relevantes à infraestrutura.
- Liberação de Material Nuclear: representa a consequência mais severa considerada no modelo, caracterizada pela liberação de material radioativo para o ambiente, ainda que em diferentes magnitudes, implicando riscos à segurança radiológica e ao entorno da instalação.

Os custos associados a cada estado foram definidos de forma agregada, representando ordens de grandeza compatíveis com os impactos esperados em uma instalação nuclear de interesse estratégico. Esses valores não correspondem a estimativas orçamentárias reais, mas sim a custos-base utilizados para fins comparativos no modelo bayesiano de decisão, permitindo refletir o aumento relativo das consequências à medida que a gravidade do evento se intensifica.

Para o estado Sem Dano, o custo foi assumido como nulo para fins de simplificação do modelo, podendo alternativamente ser representado por um valor simbólico negativo de pequena magnitude, de modo a refletir a existência de um custo mínimo de acionamento.

O estado de Subtração de Material Nuclear foi considerada a perda do potencial energético associado ao material desviado. Considerando que um elemento combustível de um reator do tipo PWR pode gerar aproximadamente 200 milhões de kWh ao longo de sua vida útil (IAEA, 2019), adotou-se como referência o valor de R$ 0,60 por kWh, resultando em um custo estimado da ordem de R$ 120 milhões por elemento combustível. .

O estado de Dano Estrutural contempla custos relacionados a reparos civis e de instalações, substituição de equipamentos danificados, interrupções operacionais de curta duração (dias a semanas), bem como despesas associadas a perícias técnicas e avaliações de segurança. Esse nível de dano foi representado por um custo-base de R$ 30 milhões, refletindo impactos significativos, porém localizados e reversíveis no curto prazo, como os ocorridos em Brows Ferry em 1975 (ASSOCIATED PRESS, 1986).

O estado de Dano Crítico abrange danos a sistemas essenciais da instalação, tais como acessos controlados, sistemas de energia de emergência, instrumentação nuclear e componentes do sistema de proteção física, além de paralisações prolongadas das atividades (semanas a meses), processos de recuperação operacional e eventual recertificação de segurança. Para esse nível, foi adotado um custo-base de R$ 700 milhões, representando consequências severas para a continuidade das operações e para a segurança da instalação, usando como base o Incidente de Forsmark (SVERIGES RADIO, 2006)

Por fim, o estado de Liberação de material nuclear inclui custos associados à resposta radiológica de emergência, operações de descontaminação ambiental e estrutural, gerenciamento de rejeitos radioativos, evacuações locais limitadas, investigações técnicas e legais, paralisações prolongadas das atividades, bem como impactos reputacionais e institucionais. Esse cenário foi representado por um custo-base de R$ 1 trilhão, como os ocorridos em Fukushima (REUTERS, 2016). Ressalta-se que esse valor representa um cenário extremo de impacto, incorporando não apenas custos diretos de resposta e descontaminação, mas também efeitos econômicos, sociais e institucionais de larga escala.

Ressalta-se que esses custos não têm a finalidade de reproduzir prejuízos reais de forma precisa, mas sim de fornecer uma base consistente para a comparação relativa entre estratégias de proteção física no âmbito do modelo bayesiano de decisão. Adicionalmente, conforme apresentado no capítulo de resultados, foram realizadas análises de sensibilidade variando os valores associados aos danos, a fim de avaliar o impacto dessas premissas sobre a estratégia ótima selecionada pelo modelo.

Com base nessas definiçãos , foi criado nó Dano, responsável por representar as consequências decorrentes de um evento adverso sobre a instalação analisada. A ocorrência de cada estado de dano foi condicionada a três variáveis principais: a

neutralização do adversário, que representa a eficácia da resposta do sistema de proteção física; o alvo atingido, classificado em área vigiada, protegida ou vital, refletindo a criticidade dos ativos envolvidos e os meios empregados no ataque, representados pelas categorias armas, explosivos, combinação de armas e explosivos ou ausência de meios, indicando o potencial destrutivo da ação adversa. A Tabela 13 apresenta a estrutura do nó Dano, incluindo seus estados e as variáveis parentais consideradas no modelo.

Tabela 13 - Nós de Dano

Nó	**Estados**	**Pais**
Danos	Sem Danos Subtração de material nuclear Danos Estruturais Danos Críticos Liberação de Material Nuclear	Neutralização de acesso Terrestre/Aquático Detecção/Neutralização de acesso aéreo Alvo Meios
Custos dos Danos (Nó de utilidade)	Sem Danos = 0 Subtração de material nuclear= 120 x 10^6 Danos Estruturais= 30 x 10^6 Danos Críticos=700 x10^6 Liberação de Material Nuclear = 1 x 10^9	Danos

A Tabela de Probabilidade Condicional do nó Dano foi construída com base na frequência relativa observada nos eventos históricos analisados, os quais foram previamente classificados segundo os estados de consequência definidos no modelo. Considerando as limitações inerentes à base de dados, em especial o número reduzido de observações e a presença de estados não observados, foi aplicada a técnica de suavização de Laplace , conforme apresentado na literatura de aprendizado de máquina (MANNING; RAGHAVAN; SCHÜTZE, 2008), com o objetivo de evitar probabilidades nulas e distribuições determinísticas. Adicionalmente, foram incorporadas premissas

estruturais ao modelo, dentre as quais se destaca a consideração de que a subtração de material nuclear ocorre exclusivamente em cenários envolvendo área vital, por ser a região onde se encontra o material nuclear de interesse no contexto analisado.

No que se refere ao estado Liberação de Material Nuclear, devido à sua baixa representatividade na base histórica utilizada, adotou-se uma abordagem complementar baseada em dados da literatura técnica. Assim, foram utilizados como referência os estudos apresentados no relatório NUREG-1738 (2001) e no trabalho de Alvarez *et al.* (2003), os quais discutem cenários de perda de resfriamento e drenagem de piscinas de combustível.

A Tabela 14 apresenta exemplos de cenários e suas respectivas ordens de grandeza de probabilidade, os quais foram utilizados como referência conceitual para a definição do estado de liberação de material nuclear no presente estudo.

Tabela 14 - Exemplos de eventos técnicos associados à liberação de material nuclear em piscinas de combustível irradiado

Evento	**Probabilidade de liberação**
Drenagem da piscina por válvulas e tubulação	$1{,}00 \times 10^{-5}$
Queda de aeronave sobre a piscina de combustível irradiado	$2{,}00 \times 10^{-8}$
Perda de energia externa	$1{,}00 \times 10^{-7}$
Perda do sistema refrigerante	$1{,}00 \times 10^{-8}$
Queda de cask (contenção de combustível)	$2{,}00 \times 10^{-7}$
Incêndio	$1{,}00 \times 10^{-8}$

Após a análise dos cenários técnicos apresentados na Tabela 14, foram adotadas ordens de grandeza representativas para a probabilidade de ocorrência de Liberação de Material Nuclear no modelo. Para cenários envolvendo área vital, foi considerado o menor valor, 1×10−5, tomando como referência o evento de drenagem da piscina por válvulas e tubulações, por representar um dos mecanismos com maior probabilidade relativa dentre os analisados.

Para as áreas protegida e vigiada, foi adotado o valor de $1\times10-7$, associado a cenários de perda de alimentação elétrica externa, os quais podem ser desencadeados por ações de sabotagem em sistemas localizados fora da área vital. Essa escolha reflete a possibilidade de ocorrência de efeitos indiretos, nos quais a degradação de sistemas de suporte pode levar, ainda que com baixa probabilidade, a condições favoráveis à liberação de material nuclear.

Para situações em que há emprego simultâneo de armas e explosivos, adotou-se a equivalência com o estado “Explosivos”, uma vez que o potencial de dano é dominado por esse tipo de meio

A Tabela 15, 16 e 17 sintetizam os resultados do processo de modelagem descrito anteriormente, para as Áreas Vital, Protegida e Vigiada, respectivamente, incorporando tanto as frequências observadas nos eventos históricos quanto os ajustes realizados por meio de suavização de Laplace e da incorporação de premissas estruturais e dados da literatura técnica.

Tabela 15 - Tabela de Probabilidade Condicional do nó Dano para a Área Vital

Meio	**Explosivos**	**Armas**	**Explosivos_Armas**	**Nada**
Sem Dano	0,0714285	0,2499988	0,0714285	0,3749998
Subtração de Material Nuclear	0,0714285	0,2499988	0,0714285	0,5249997
Dano Estrutural	0,3571423	0,2499988	0,3571423	0,0750000
Dano Crítico	0,4999907	0,2499937	0,4999907	0,0249905
Liberação de material nuclear	1×10^{-5}	1×10^{-5}	1×10^{-5}	1×10^{-5}

Tabela 16 - Tabela de Probabilidade Condicional do nó Dano para a Área Protegida

Meio	Explosivos	Armas	Explosivos_Armas	Nada
Sem Dano	0,0434783	0,6363636	0,0434783	0,7894737
Subtração de Material Nuclear	0,0000000	0,0000000	0,0000000	0,0000000
Dano Estrutural	0,9130435	0,2727273	0,9130435	0,1578947
Dano Crítico	0,0434782	0,0909090	0,0434782	0,0526315
Liberação de material nuclear	1×10^{-7}	1×10^{-7}	1×10^{-7}	1×10^{-7}

Tabela 17 - Tabela de Probabilidade Condicional do nó Dano para a Área Vigiada

Meio	Explosivos	Armas	Explosivos_Armas	Nada
Sem Dano	0,0909091	0,7142857	0,0909091	0,7647059
Subtração de Material Nuclear	0,0000000	0,0000000	0,0000000	0,0000000
Dano Estrutural	0,8181818	0,1428571	0,8181818	0,1764706
Dano Crítico	0,0909090	0,1428571	0,0909090	0,0588234
Liberação de material nuclear	1×10^{-7}	1×10^{-7}	1×10^{-7}	1×10^{-7}

Adicionalmente, foram impostas restrições estruturais ao vetor aéreo. O uso exclusivo de armas leves por drones foi considerado equivalente ao estado “Nenhum”, por não representar impacto relevante. A subtração de material foi considerada implausível, com probabilidade fixada em zero e redistribuição da massa entre os demais estados. A Tabelas 18, apresenta os ajustes realizados para os danos causados por um ataque por drone na área vital.

Tabela 18 - Tabela de Probabilidade Condicional do nó Dano para a Área Vital no acesso aéreo

Meio	**Explosivos**	**Armas**	**Explosivos_Armas**	**Nada**
Sem Dano	0,0769	0,7894	0,0769	0,7894
Subtração de Material Nuclear	0	0	0	0
Dano Estrutural	0,3846	0,1578	0,3846	0,1578
Dano Crítico	0,5384	0,05261	0,5384	0,05261
Liberação de material nuclear	1×10^{-5}	1×10^{-5}	1×10^{-5}	1×10^{-5}

4.2.7 Utilidade Total

O nó de utilidade total do modelo foi definido de forma a agregar os custos associados às alternativas de decisão de proteção física e às consequências decorrentes dos diferentes estados de dano. Especificamente, esse nó recebe como entradas os custos das medidas de detecção, atraso e resposta consideradas no estudo de caso, bem como os custos-base associados aos estados de dano.

A combinação desses componentes foi realizada por meio de uma soma ponderada, na qual foram adotados pesos unitários para todos os termos de custo. Essa escolha se justifica pelo fato de todos os elementos de utilidade serem expressos na mesma unidade monetária (reais), permitindo sua agregação direta sem a necessidade de normalização ou atribuição de importâncias relativas artificiais.

Os custos foram representados por valores negativos no modelo, de modo que a utilidade total também assume valores negativos, sendo sua magnitude proporcional ao custo global da estratégia. Assim, a utilidade total expressa o custo esperado de cada alternativa de proteção física, considerando tanto os investimentos em segurança quanto os impactos de possíveis eventos adversos, sendo a melhor estratégia aquela que apresenta o maior valor de utilidade total (ou seja, o menor custo esperado).

4.2.8 Estrutura da rede bayesiana de decisão aplicada ao estudo de caso

A Figura 9 apresenta a estrutura do modelo aplicado no estudo de caso, construída a partir das premissas e relações previamente definidas. Nela, são representados os nós do sistema, incluindo as variáveis associadas à caracterização da ameaça, às alternativas de detecção, atraso e resposta, bem como aos possíveis danos e custos envolvidos.

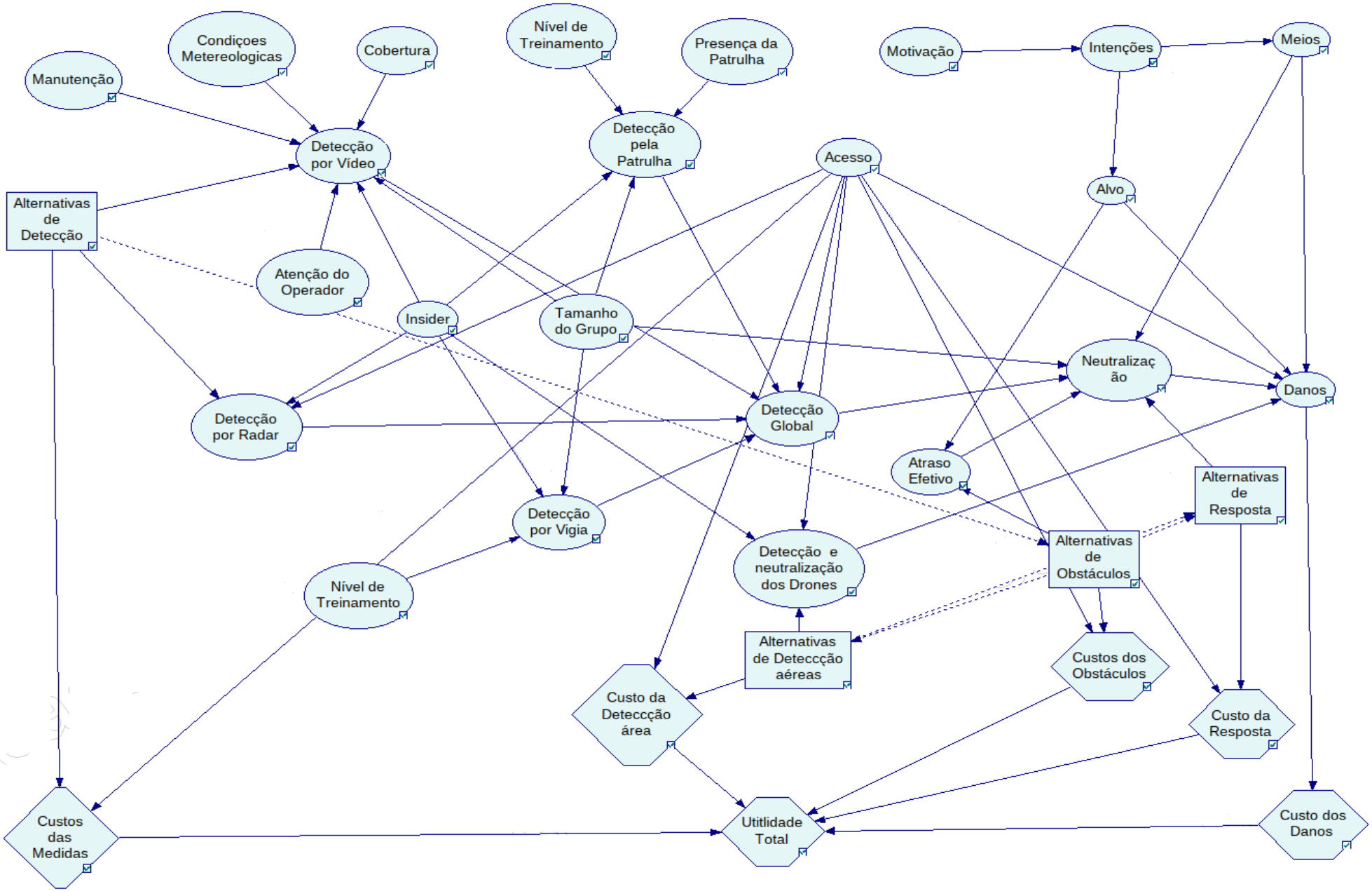

Figura 9 - Estrutura da rede bayesiana de decisão aplicada ao estudo de caso

5 RESULTADOS E DISCUSSÃO

5.1 ANÁLISE COMPARATIVA DAS ESTRATÉGIAS EM CONDIÇÕES DE INCERTEZA

Nesta seção são apresentados os resultados do modelo, obtidos na ausência de qualquer evidência específica sobre o cenário de ataque. Nessa configuração, o sistema opera sob condições de máxima incerteza, avaliando as alternativas de decisão exclusivamente com base nas distribuições a priori e nos custos associados. A Tabela 19 apresenta as melhores estratégias e suas respectivas utilidades esperadas.

Tabela 19 - Estratégias com as maiores utilidades esperadas no cenário sem evidências

Detecção para acesso aéreo	**Resposta**	**Detecção para acesso terrestre/ aquático**	**Alt. de Obstáculos**	**Utilidade**	**Investimento**
Hibrido	Reforçada	VDM	Portas Reforçadas nas Áreas Protegida e Vital	-22,35	R$ 11.200.000,00
Hibrido	Reforçada	Nenhuma	Portas Reforçadas nas Áreas Protegida e Vital	-22,53	R$ 10.200.000,00
Hibrido	Reforçada	VDM	Portas Reforçadas na Área Protegida	-23,88	R$ 10.800.000,00
Hibrido	Reforçada	Nenhuma	Portas Reforçadas na Área Protegida	-24,04	R$ 9.800.000,00
jammer	Reforçada	VDM	Portas	-24,91	R$ 8.200.000,00

			Reforçadas nas Áreas Protegida e Vital		

Observa-se que o sistema híbrido está presente na melhor estratégia mesmo apresentando um custo aproximadamente 50% superior ao sistema baseado em interferência eletrônica. Esse resultado indica que o ganho de eficácia proporcionado por essa alternativa na neutralização de veículos aéreos não tripulados é suficiente para compensar o aumento de custo, reduzindo de forma mais significativa os impactos associados aos eventos adversos. Dessa forma, embora mais oneroso, o sistema híbrido apresenta melhor custo-benefício no contexto do modelo, pois sua maior capacidade de neutralização de veículos aéreos não tripulados contribui para a redução do custo esperado total, justificando sua seleção na estratégia de melhor desempenho.

Adicionalmente, verifica-se que a força de resposta reforçada está presente em todas as estratégias analisadas, o que evidencia sua relevância no modelo, esse comportamento indica que o aumento da capacidade de reação contribui de forma consistente para a redução dos impactos associados aos eventos adversos, sendo um fator determinante na composição das melhores alternativas.

No que se refere às estratégias de detecção terrestre/aquática, observa-se uma maior variabilidade entre as alternativas, inclusive com a presença da opção “nenhuma” entre as melhores estratégias. Esse resultado pode ser explicado pelo fato de o modelo já considerar a existência de capacidades básicas de detecção no sistema, reduzindo o ganho marginal associado a investimentos adicionais nesse domínio, especialmente quando comparado às medidas voltadas à neutralização de drones.

Em relação aos valores de utilidade, observa-se que as diferenças entre as melhores estratégias são relativamente pequenas, indicando que múltiplas combinações podem apresentar desempenhos semelhantes. No entanto, ao se analisar o investimento necessário, torna-se evidente que estratégias mais caras não necessariamente resultam em melhor custo-benefício, reforçando a importância da análise conjunta entre desempenho e custo.

Nesse contexto,por exemplo, considerando um cenário hipotético com restrição orçamentária, no qual os investimentos não poderiam ultrapassar R$ 10.000.000,00, a estratégia correspondente à quarta melhor alternativa seria a opção mais adequada. Esse

exemplo reforça a importância da incorporação de restrições práticas na análise, evidenciando que a solução ótima do ponto de vista teórico nem sempre seria a mais viável sob limitações reais.

De forma geral, os resultados indicam que as variáveis relacionadas à neutralização de drones e à capacidade de resposta exercem maior influência sobre o desempenho do sistema, enquanto investimentos adicionais em detecção apresentam retornos marginais menores no cenário analisado.

De forma complementar, a Tabela 20 apresenta as estratégias de pior desempenho, permitindo evidenciar que a adoção de determinadas medidas, especialmente aquelas associadas a elevado custo e baixo ganho operacional, pode resultar em desempenho inferior até mesmo quando comparada à ausência de investimentos adicionais.

Tabela 20 - Estratégias com as menores utilidades esperadas no cenário sem evidências

Detecção para acesso aéreo	**Resposta**	**Detecção para acesso terrestre/ aquático**	**Alt. de Obstáculos**	**Utilidade**	**Investimento**
Nenhuma	Básica	Nenhuma	Nenhuma	-47,32	R$ 0,00
Nenhuma	Reforçada	Radar Subaquático	Nenhuma	-48,47	R$ 7.400.000,00
Nenhuma	Básica	Radar Subaquático	Portas Reforçadas nas Áreas Protegida e Vital	-48,66	R$ 7.800.000,00
Nenhuma	Básica	Radar Subaquático	Portas Reforçadas na Área Protegida	-50,13	R$ 7.400.000,00
Nenhuma	Básica	Radar Subaquático	Nenhuma	-52,91	R$ 7.000.000,00

Observa-se, a partir da análise das piores estratégias, que a alternativa na qual nenhuma medida adicional é implementada apresenta desempenho superior a outras combinações que incluem investimentos em detecção, em especial o radar subaquático. Esse resultado indica que, no cenário analisado, o ganho proporcionado por essa tecnologia não é suficientemente expressivo para compensar seu elevado custo de implementação.

Por fim , ao se comparar a melhor estratégia identificada, com utilidade de -22,35, com a alternativa na qual nenhuma medida adicional é implementada, cuja utilidade é de -47,32, observa-se uma diferença significativa no desempenho do sistema, esse resultado evidencia que a adoção de medidas de proteção adequadas pode reduzir substancialmente o custo esperado, praticamente pela metade, reforçando o impacto positivo das decisões de investimento em segurança física.

5.2 ANÁLISE DE SENSIBILIDADE

Com o objetivo de identificar as variáveis de maior influência sobre o desempenho do modelo, realizou-se uma análise de sensibilidade global, cujos resultados são apresentados na Figura 10. Nessa representação, quanto mais intensa a coloração, maior a influência exercida. Ressalta-se que essa análise é realizada por meio do software GeNIe, que permite a avaliação do impacto das variáveis do modelo sobre o resultado final.

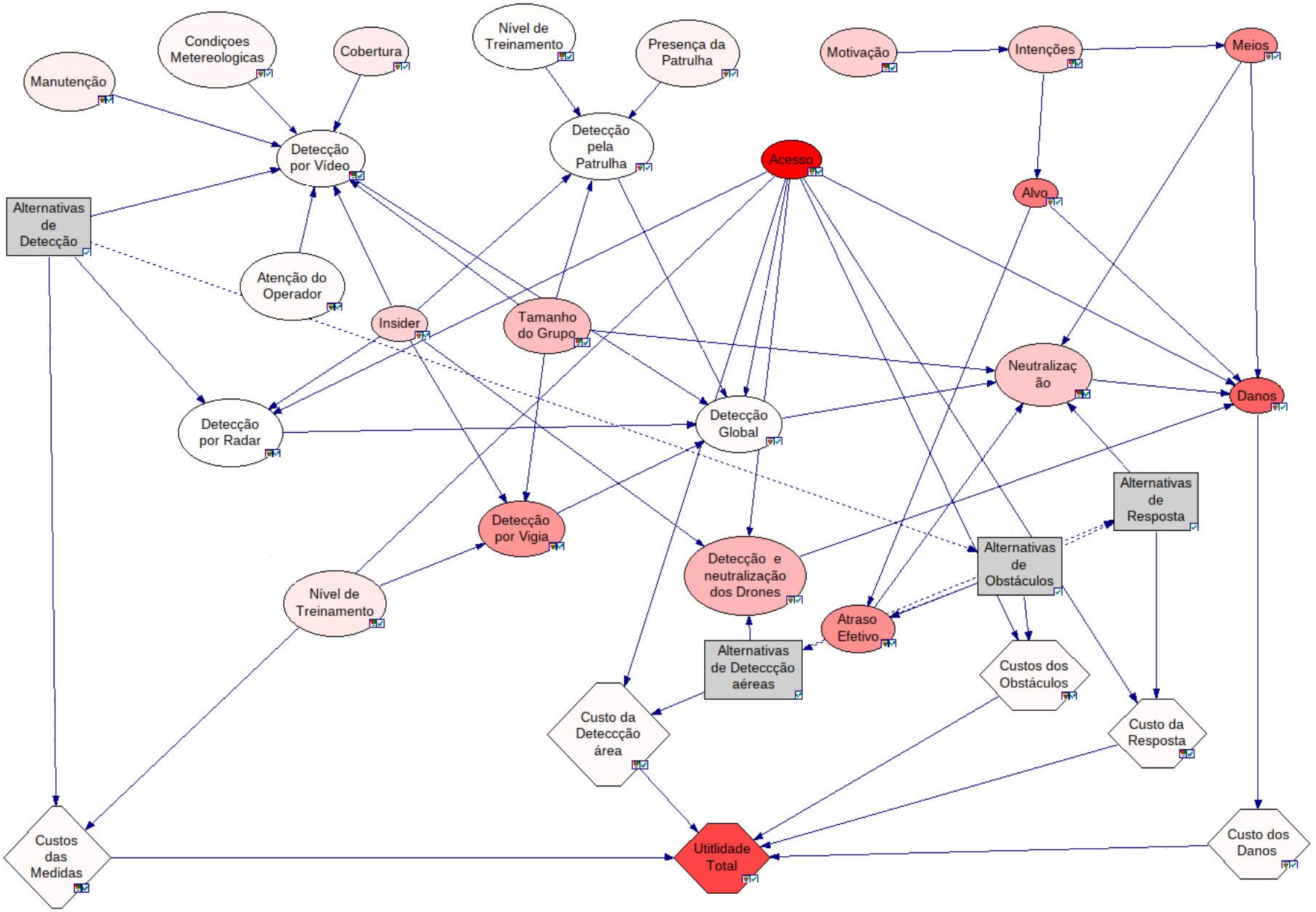

Figura 10 - Análise de sensibilidade global do modelo em relação à utilidade total

Observa-se que o nó “Acesso” apresenta elevado grau de sensibilidade, evidenciado pela maior intensidade de coloração na Figura 10, indicando forte influência sobre a utilidade total. Esse comportamento pode ser explicado pelo fato de que o tipo de acesso define o vetor de ataque (terrestre, aquático ou aéreo), influenciando diretamente o desempenho das medidas de detecção, atraso e neutralização. Dessa forma, variações nesse nó resultam em mudanças significativas no comportamento do modelo, afetando simultaneamente múltiplas variáveis e, consequentemente, o resultado final. Esse resultado evidencia que a caracterização do vetor de acesso constitui um dos fatores mais críticos na avaliação das estratégias de proteção física.

O nó “Utilidade Total” apresenta elevada intensidade de coloração, o que é esperado por se tratar da variável de saída do modelo. Sua sensibilidade decorre do fato de agregar, de forma ponderada, os custos das medidas de proteção e os impactos dos eventos adversos. Nesse contexto, os pesos atribuídos aos componentes da utilidade influenciam diretamente o resultado final, ao definirem a contribuição relativa de cada fator.

Os nós “Danos”, “Meios”, “Alvo” e “Tamanho do grupo” também apresentam elevada sensibilidade, uma vez que esses elementos estão diretamente associados à caracterização do ataque e às suas consequências. Em particular, o nó “Meios” influencia o potencial destrutivo da ação adversária, enquanto o nó “Alvo” define a relevância e vulnerabilidade da área atingida, impactando diretamente o nível de dano gerado. Por sua vez, o nó “Danos” atua como variável diretamente ligada à função utilidade, sendo responsável por traduzir os efeitos do ataque em perdas no modelo. Por fim, o nó “Tamanho do Grupo” exerce influência significativa ao afetar simultaneamente a capacidade de detecção e a probabilidade de neutralização, uma vez que grupos maiores tendem a ser mais facilmente detectados, porém também apresentam maior capacidade de resistência à resposta, alterando de forma relevante o desfecho do confronto.

Destaca-se ainda o comportamento do nó “Detecção por Vigia”, que apresenta nível de sensibilidade relativamente elevado. Esse resultado pode ser explicado pelo fato de que, no modelo, a detecção realizada pelo vigia ocorre de forma precoce quando bem-sucedida e apresenta elevada probabilidade de ocorrência em condições de atenção

elevada. Dessa forma, pequenas variações nesse nó impactam diretamente a capacidade de antecipação da resposta, influenciando de maneira significativa o resultado final. Por outro lado, o nó “Detecção Global” apresenta menor intensidade de coloração, indicando que, apesar de representar a integração das diferentes fontes de detecção, sua variação isolada produz impacto mais limitado na utilidade total, possivelmente em função da redundância já existente entre os mecanismos de detecção considerados no modelo.

Os nós de decisão aparecem em coloração neutra na análise de sensibilidade, uma vez que não representam variáveis probabilísticas, mas sim escolhas controladas pelo decisor.

5.3 ANÁLISE POR CENÁRIOS DE ACESSO

Considerando que o nó “Acesso” apresentou elevada influência sobre a utilidade total na análise de sensibilidade, realizou-se uma análise por cenários de acesso, com o objetivo de avaliar o comportamento das estratégias de proteção quando o vetor de ataque é previamente definido. Para isso, foram considerados separadamente os cenários de acesso terrestre, aéreo e aquático, permitindo identificar como a escolha da estratégia ótima varia em função da natureza da ameaça. A Tabela 21 apresenta as estratégias ótimas para cada cenário de acesso considerado, bem como os respectivos valores de utilidade e probabilidade de neutralização da ameaça.

Tabela 21 - Estratégias ótimas por cenário de acesso

Acesso	**Melhor Estratégia**	**Utilidade**	**Neutralização da ameaça**
Ar	Hibrido	-32,79	0,80
Água	VDM + Portas Reforçadas na área Vital e Protegida+ Força de Resposta Reforçada	-20,99	0,84
Terra	VDM + Portas Reforçadas na área Vital e Protegida+ Força de Resposta Reforçada	-19,83	0,85

No cenário aéreo, a estratégia ótima também coincide com aquela obtida no cenário sem evidência, sendo composta pelo sistema híbrido. Esse resultado indica que, mesmo na condição de incerteza, o modelo já favorecia essa alternativa para lidar com a ameaça aérea. Já nos cenários terrestre e aquático, a estratégia ótima permanece baseada na combinação de detecção por vídeo, medidas de atraso e reforço da capacidade de resposta, evidenciando maior estabilidade dessas soluções frente à definição do vetor de acesso.

Destaca-se ainda que, no cenário aquático, embora o radar subaquático apresente maior probabilidade de neutralização (0,85) quando comparado ao VDM, este último apresenta maior utilidade, em razão do elevado custo associado ao radar.

Adicionalmente, observa-se que o cenário aéreo apresenta o pior desempenho em termos de utilidade, mesmo com níveis elevados de neutralização. Esse comportamento pode ser melhor compreendido ao se analisar a distribuição dos danos para cada estratégia, apresentado na Figura 11.

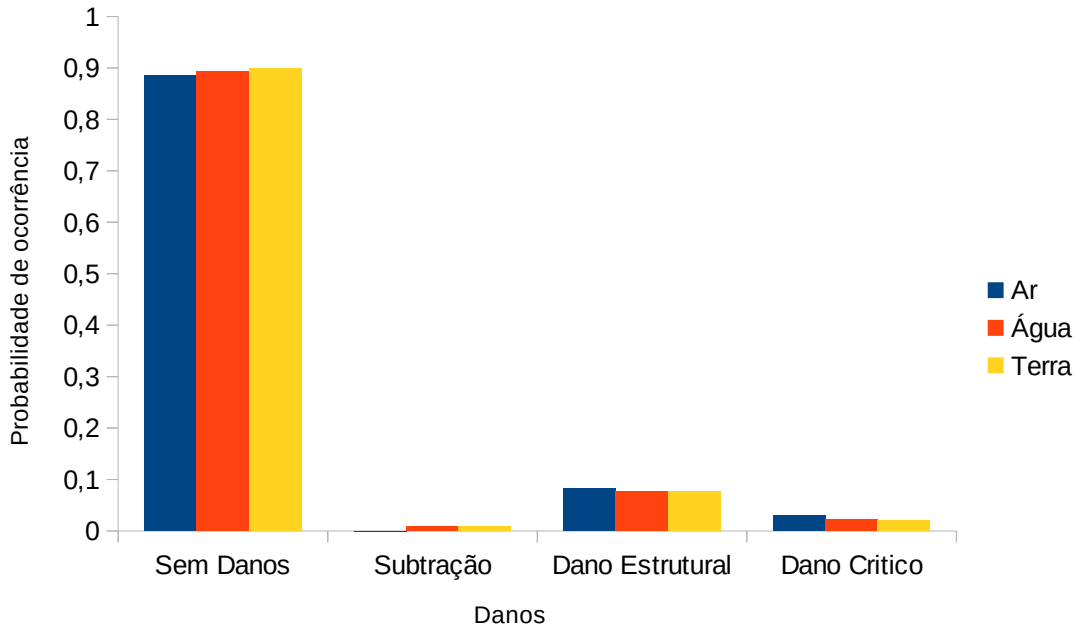

Figura 11 - Distribuição dos danos por cenário de acesso

Verifica-se que, no cenário aéreo, a probabilidade de ocorrência de situações sem danos relevantes é inferior à observada nos cenários terrestre e aquático, ao passo que as probabilidades associadas a danos estruturais e críticos são mais elevadas. Esse

resultado pode ser explicado pela menor redundância das medidas de proteção associadas ao vetor aéreo no modelo, uma vez que a mitigação da ameaça depende predominantemente da capacidade do sistema anti-drone. Em contraste, nos cenários terrestre e aquático, a presença de múltiplas camadas de defesa, como detecção, atraso e resposta, caracteriza uma arquitetura em camadas (defesa em profundidade), contribuindo para uma redução mais eficaz dos danos e, consequentemente, para melhores resultados em termos de utilidade.

De forma geral, os resultados indicam que a definição do vetor de acesso não altera a estratégia ótima, evidenciando sua robustez frente à variação do tipo de ameaça. Ainda assim, a análise permite identificar diferenças no desempenho e na distribuição dos danos entre os cenários, destacando a superioridade de estratégias baseadas em múltiplas camadas de defesa.

5.3.1 Avaliação com Ajuste das Probabilidades de Acesso

Embora a distribuição de probabilidades do nó “Acesso” tenha sido inicialmente definida com base em dados históricos, foram identificadas possíveis limitações quanto à representatividade de determinados vetores de ataque no contexto analisado. Em particular, o acesso aéreo, em função da crescente utilização de veículos aéreos não tripulados.

Para a construção do cenário prospectivo com maior relevância do vetor aéreo, foi adotada uma nova distribuição de probabilidades para o nó “Acesso”, na qual a probabilidade do acesso aéreo foi elevada de 0,192 para 0,35, enquanto o acesso terrestre foi reduzido de 0,78 para 0,63, mantendo-se o acesso aquático em 0,02. Essa configuração foi definida com o objetivo de representar um cenário no qual a ameaça aérea assume maior frequência relativa, permitindo avaliar o impacto dessa alteração na escolha das estratégias ótimas e no desempenho do modelo. A Tabela 22 apresenta as principais estratégias no cenário com aumento da probabilidade do acesso aéreo.

Tabela 22 - Principais estratégias no cenário com aumento do acesso aéreo

Detecção Terrestre/ Aquática	**Atraso**	**Detecção Aérea**	**Resposta**	**Utilidade**
VDM	Portas Reforçadas nas Áreas Protegida e Vital	Hibrido	Reforçada	-24,39
Nenhuma	Portas Reforçadas nas Áreas Protegida e Vital	Hibrido	Reforçada	-24,54
VDM	Portas Reforçadas na Área Protegida	Hibrido	Reforçada	-25,63
Nenhuma	Portas Reforçadas na Área Protegida	Hibrido	Reforçada	-25,76
VDM	Nenhuma	Hibrido	Reforçada	-27,87

Os resultados indicam que a estratégia ótima permanece inalterada, mantendo o sistema híbrido, o que já era esperado. No entanto, com o aumento da probabilidade do acesso aéreo, todas as cinco melhores estratégias passam a incluir essa alternativa, com a exclusão de soluções baseadas em *jammer*, evidenciando maior exigência do modelo por medidas mais robustas. Além disso, observa-se redução nos valores de utilidade, refletindo o aumento do custo esperado e tornando o cenário mais oneroso.

Adicionalmente, foi considerada uma análise complementar para um cenário em que o vetor aéreo apresenta menor relevância, sob a hipótese de que os adversários mais prováveis não possuam capacidade significativa de empregar veículos aéreos não tripulados. Para isso, foi adotada uma nova distribuição para o nó “Acesso”, na qual a probabilidade do acesso aéreo foi reduzida de 0,192 para 0,05, enquanto o acesso terrestre foi elevado para 0,92 e o aquático para 0,03, com o objetivo de avaliar o impacto dessa hipótese no comportamento do modelo. A Tabela 23 apresenta as principais estratégias com essa modificação.

Tabela 23 - Principais estratégias no cenário com diminuição do acesso aéreo

Detecção Terrestre/Aquática	**Atraso**	**Detecção Aérea**	**Resposta**	**Utilidade**
VDM	Portas Reforçadas nas Áreas Protegida e Vital	Hibrido	Reforçada	-24,39
Nenhuma	Portas Reforçadas nas Áreas Protegida e Vital	Hibrido	Reforçada	-24,54
VDM	Portas Reforçadas nas Áreas Protegida e Vital	*Jammer*	Reforçada	-25,63
Nenhuma	Portas Reforçadas nas Áreas Protegida e Vital	*Jammer*	Reforçada	-25,76
VDM	Portas Reforçadas na Área Protegida	Hibrido	Reforçada	-27,87

Os resultados indicam que, com a redução da probabilidade do vetor aéreo, há melhora nos valores de utilidade das estratégias, refletindo a diminuição do custo esperado associado a esse tipo de ameaça. Nesse cenário, observa-se uma alteração na composição das melhores alternativas, com o reaparecimento de estratégias baseadas em interferência eletrônica (*jammer*) entre as cinco melhores opções. Esse comportamento indica que, ao reduzir a relevância do acesso aéreo, o modelo passa a aceitar soluções menos robustas e de menor custo, uma vez que a necessidade de sistemas mais avançados de neutralização de veículos aéreos não tripulados se torna menos crítica.

5.4 ANÁLISE POR CENÁRIOS DE MEIOS EMPREGADOS

Considerando que o nó “Meios” apresentou elevada influência sobre a utilidade total na análise de sensibilidade, realizou-se uma análise por cenários de meios empregados, com o objetivo de avaliar o comportamento das estratégias de proteção em função do tipo de recurso utilizado pelo adversário. Para isso, foram considerados separadamente os principais tipos de meios definidos no modelo, permitindo verificar

como a escolha da estratégia ótima varia de acordo com o potencial ofensivo da ameaça, os dados são apresentados na Tabela 24.

Tabela 24 - Estratégias ótimas por tipo de meios empregados pelo inimigo

Meios	**Alternativa**	**Utilidade**	**Neutralização**
Explosivos	VDM + Portas Reforçadas na área Vital e Protegida+ Força de Resposta Reforçada+Hibrido	-22,61	0,71
Armas	VDM + Portas Reforçadas na área Vital e Protegida+ Força de Resposta Reforçada+Hibrido	-28,59	0,61
Armas e Explosivos	VDM + Portas Reforçadas na área Vital e Protegida+ Força de Resposta Reforçada+Hibrido	-45,06	0,61
Nada	Nenhuma + Portas Reforçadas na área Vital e Protegida+ Força de Resposta Básica+Hibrido	-9,07	0,72

Os resultados indicam que a estratégia ótima permanece inalterada nos cenários em que há emprego de meios ofensivos, mantendo a combinação baseada em VDM, medidas de atraso e força de resposta reforçada. Entretanto, observa-se que o cenário com emprego exclusivo de armas apresenta menor utilidade quando comparado ao uso de explosivos, apesar de gerar menores níveis de dano. Esse comportamento pode ser explicado pela maior dificuldade de neutralização de adversários armados, o que aumenta a probabilidade de sucesso da ação adversária e, consequentemente, o custo esperado.

No cenário em que há combinação de armas e explosivos, verifica-se o pior desempenho entre os casos analisados, refletindo o efeito combinado de alto potencial destrutivo e maior resistência à neutralização. Por outro lado, no cenário em que não há emprego de meios ofensivos, a estratégia ótima passa a exigir menor nível de resposta e detecção, apresentando melhor utilidade.

Esses resultados evidenciam que o tipo de meio empregado pelo adversário influencia não apenas o nível de dano esperado, mas também a dificuldade de neutralização, sendo ambos determinantes para a escolha da estratégia ótima.

5.5 ANÁLISE EM FUNÇÃO DO ALVO DO ATAQUE

Considerando que o nó “Alvo” apresentou elevada influência sobre a utilidade total na análise de sensibilidade, realizou-se uma análise por cenários de alvo, com o objetivo de avaliar como a área atingida pelo ataque influencia a escolha das estratégias de proteção. Foram considerados separadamente os diferentes tipos de áreas definidos no modelo, permitindo analisar variações no desempenho das alternativas em função da criticidade do alvo.

Os resultados indicam que a escolha da estratégia ótima varia conforme o tipo de área considerada, refletindo diferenças na criticidade e no nível de controle associado a cada alvo. Em todos os cenários analisados, observa-se a manutenção do sistema híbrido e da força de resposta reforçada como elementos centrais da estratégia, evidenciando sua importância para a neutralização da ameaça.

No caso da área vigiada, não se verifica a necessidade de adoção de medidas adicionais de detecção, sendo a estratégia composta essencialmente por ações de resposta e mitigação. De forma semelhante, na área protegida, a detecção adicional também não se mostra necessária; entretanto, observa-se o incremento de medidas de atraso, com a adoção de portas reforçadas, visando aumentar o tempo disponível para a atuação da força de resposta.

Já no cenário de área vital, além do reforço das medidas de atraso, verifica-se a incorporação do VDM como alternativa de detecção, indicando a necessidade de maior capacidade de antecipação da ameaça em função da criticidade do alvo. Esse comportamento evidencia que, à medida que a importância da área aumenta, o modelo passa a exigir estratégias mais completas, combinando detecção, atraso e resposta de forma mais intensiva.

A Figura 12 apresenta a comparação dos valores de utilidade e neutralização das melhores estratégias para os diferentes cenários de alvo, evidenciando o impacto da área atingida no desempenho das estratégias de proteção.

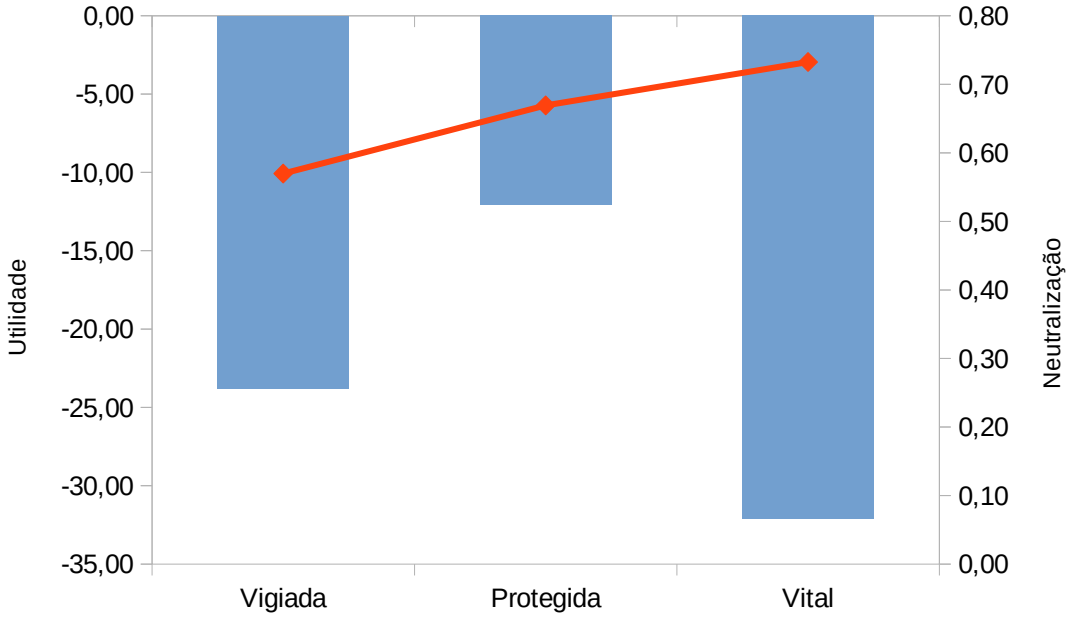

Figura 12 - Comparação entre utilidade e probabilidade de neutralização por tipo de área

Um aspecto relevante observado é que a utilidade associada ao cenário de área vigiada apresenta valores inferiores aos da área protegida, o que, à primeira vista, pode parecer contraintuitivo. Esse comportamento pode ser explicado pela menor probabilidade de neutralização nesse tipo de área, que permite maior liberdade de ação ao adversário. Adicionalmente, no contexto do modelo, ações realizadas em áreas vigiadas podem possibilitar a ocorrência de danos críticos por meios indiretos, como a interrupção da alimentação externa de energia. Dessa forma, mesmo não sendo a área mais sensível em termos estruturais, a menor capacidade de resposta associada a esse cenário aumenta a probabilidade de sucesso da ação adversária, elevando o risco de consequências mais severas. Esse comportamento pode ser melhor compreendido por meio da análise da distribuição dos níveis de dano em cada cenário, conforme apresentado nas Figura 13 e 14.

Observa-se que a área vital apresenta menor probabilidade de ocorrência de danos quando comparada às demais áreas, o que pode ser explicado pela maior probabilidade de neutralização nesse cenário. No entanto, os danos que ocorrem nessa área tendem a ser mais severos, incluindo subtração de material, danos críticos e, ainda que com baixa probabilidade, a possibilidade de liberação de material nuclear. Dessa forma, embora os eventos sejam menos frequentes, seu impacto é significativamente

maior, o que resulta em valores de utilidade substancialmente inferiores. Como consequência, a utilidade associada à área vital é aproximadamente duas vezes menor que a da área vigiada e cerca de quatro vezes menor que a da área protegida.

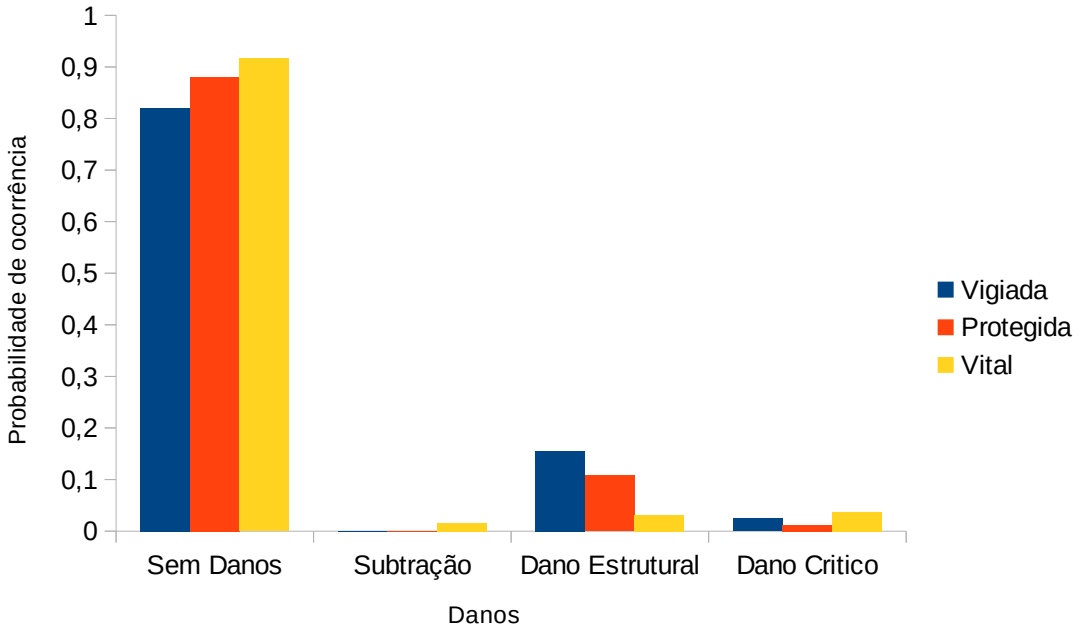

Figura 13 - Distribuição dos principais níveis de dano por área

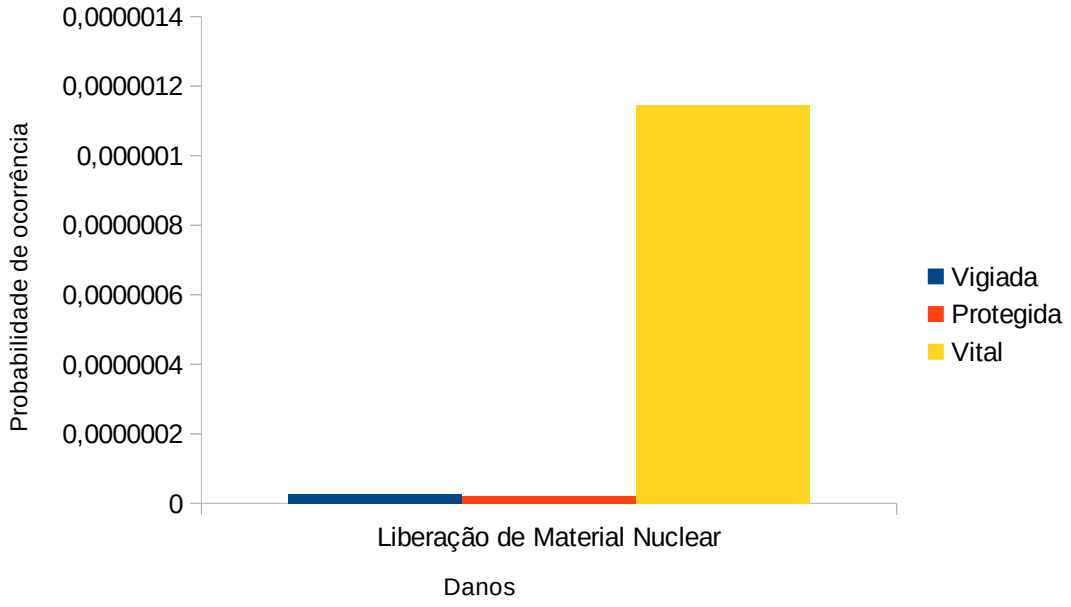

Figura 14 - Probabilidade de Liberação de material nuclear por área

5.6 ANÁLISE DE SENSIBILIDADE DOS PARÂMETROS DE NEUTRALIZAÇÃO

5.6.1 Ameaças Terrestres e Aquáticas

Considerando que a probabilidade de neutralização da ameaça desempenha papel central no desempenho do modelo, foi realizada uma análise complementar com o objetivo de avaliar a sensibilidade dos resultados aos parâmetros adotados para sua modelagem..

Para a realização da análise de sensibilidade paramétrica, foram considerados três cenários para os fatores utilizados na modelagem da neutralização: um cenário-base, correspondente aos valores originalmente adotados; um cenário conservador, no qual se reduziu a efetividade associada ao atraso e à detecção; e um cenário favorável, no qual esses fatores foram elevados dentro de limites compatíveis com a lógica do modelo, conforme apresentado na Tabela 25.

Tabela 25 - Cenários paramétricos adotados para a neutralização

Cenário	**Atraso (f_A)**			**Detecção (f_D)**	
	Baixo	**Médio**	**Alto**	**Precoce**	**Tardia**
Consevador	0,5	0,7	0,9	0,9	0,7
Base	0,6	0,8	1,0	1,0	0,8
Favorável	0,7	0,9	1,0	1,0	0,9

Os resultados indicam que a variação dos parâmetros de neutralização impacta diretamente, tanto a probabilidade de neutralização, quanto os valores de utilidade das estratégias analisadas. Como esperado, o cenário de baixa efetividade apresenta menor probabilidade de neutralização, resultando em maior custo esperado e, consequentemente, pior valor de utilidade. Em contrapartida, no cenário de alta efetividade, observa-se aumento da neutralização e melhoria da utilidade.

No que se refere às estratégias ótimas, observa-se que os cenários base e de alta efetividade apresentam a mesma configuração, caracterizada pela combinação de VDM, portas reforçadas na área vital e protegida e resposta reforçada. Já no cenário de baixa efetividade, a estratégia ótima não inclui medidas adicionais de detecção, sendo

composta apenas por medidas de atraso e reforço da resposta. Destaca-se ainda que, no cenário de baixa efetividade, a estratégia que incorpora detecção adicional apresenta maior probabilidade de neutralização (0,677), porém o custo associado à sua implementação não compensa essa melhoria, resultando em utilidade inferior.

A Figura 15 apresenta a comparação entre os valores de utilidade e as probabilidades de neutralização para a melhor estratégia em cada cenário analisado, permitindo visualizar de forma integrada o impacto da variação dos parâmetros de neutralização no desempenho do modelo.

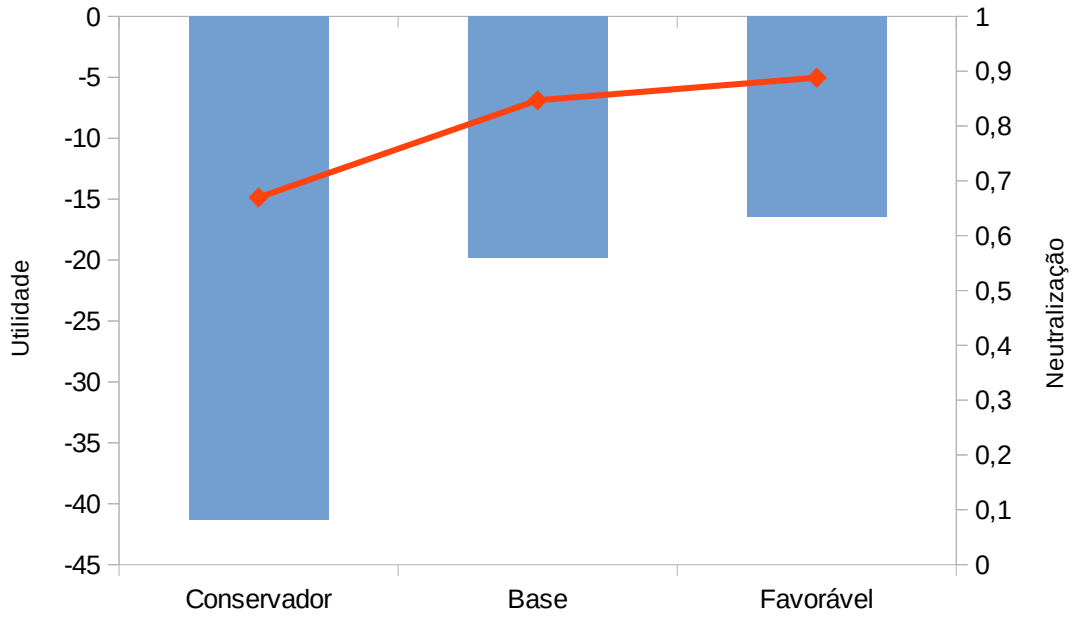

Figura 15 - Comparação entre utilidade e probabilidade de neutralização para cenários de neutralização

A passagem do cenário conservador para o cenário base gera uma melhora significativa na neutralização e na utilidade. Já a mudança do cenário base para o favorável traz ganhos menores, indicando que, à medida que o sistema melhora, cada avanço adicional tem um impacto menor. Esse comportamento evidencia que a influência da neutralização sobre o desempenho do modelo depende da sua parametrização, sendo necessário avaliar cuidadosamente os valores adotados para cada instalação em função de suas condições operacionais.

5.6.2 Ameaças Aéreas

Considerando as particularidades do vetor aéreo, foi realizada uma análise específica da sensibilidade dos parâmetros de neutralização de ameaças aéreas, com o objetivo de avaliar o impacto da variação desses parâmetros no desempenho do modelo. Diferentemente das ameaças terrestres e aquáticas, a neutralização de veículos aéreos não tripulados é realizada por sistemas dedicados, o que implica uma modelagem distinta da probabilidade de neutralização.

CHAARI (2025) indica superioridade relativa de sistemas híbridos em relação a soluções baseadas exclusivamente em interferência eletrônica, mas não fornece valores pontuais de eficácia. Dessa forma, optou-se por realizar uma análise de sensibilidade paramétrica com três cenários: conservador, base e favorável. Para o sistema *jammer*, adotaram-se os valores 0,60, 0,70 e 0,80, enquanto para o sistema híbrido foram adotados 0,75, 0,85 e 0,90, preservando-se, em todos os casos, a relação de maior efetividade do sistema híbrido. A Figura 16 apresenta os resultados.

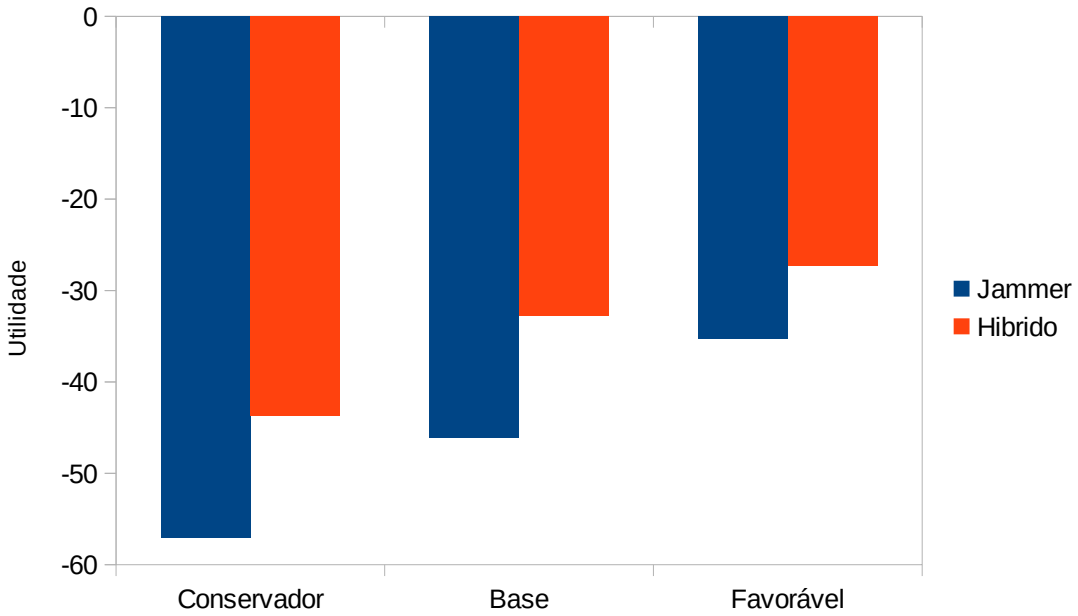

Figura 16 - Comparação entre utilidades do sistemas de detecção/neutralização de VANT para diferentes parâmetros

Os resultados indicam que, nos cenários conservador, base e favorável considerados, a estratégia ótima permanece inalterada, mantendo a preferência pelo

sistema híbrido. Isso sugere que, dentro da faixa de valores testada, o modelo apresenta estabilidade na escolha da alternativa de neutralização aérea.

A Figura 17 apresenta a variação da utilidade das estratégias baseadas em sistema *jammer* e sistema híbrido em função da probabilidade de neutralização atribuída ao *jammer*, permitindo avaliar o impacto dessa variação na escolha da estratégia ótima. Destaca-se que a probabilidade de neutralização do sistema híbrido foi mantida constante em 0,85 ao longo da análise.

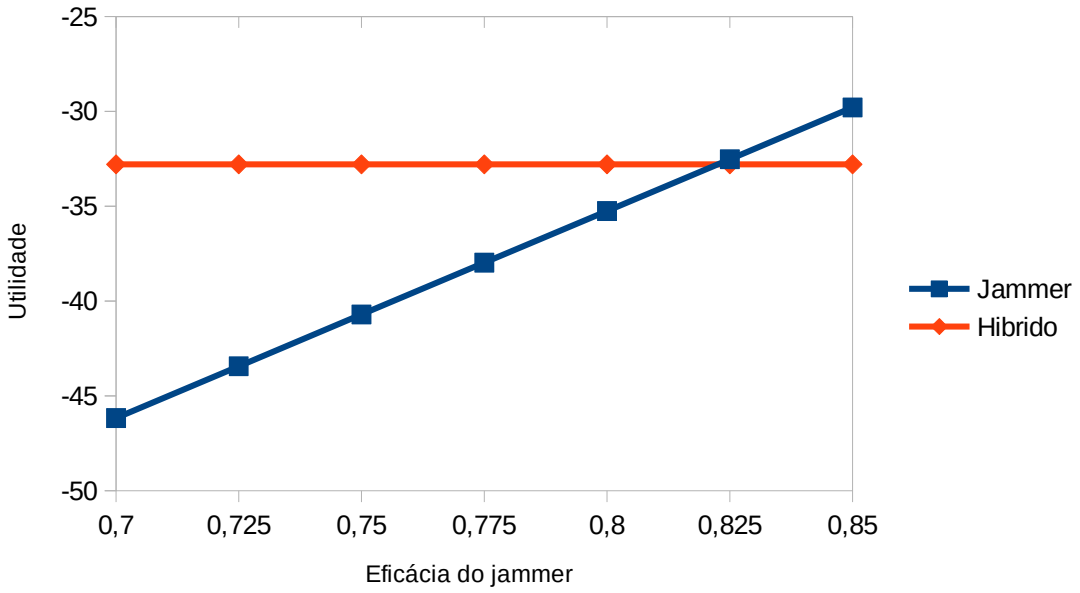

Figura 17 - Comparação da utilidade das estratégias em função da probabilidade de neutralização do sistema *jammer*

O resultado evidencia a existência de um limiar de decisão entre as alternativas, a superação do desempenho do sistema híbrido pelo *jammer* ocorre apenas para valores próximos ao limite superior considerado, indicando que essa transição depende de níveis de eficácia potencialmente elevados para o *jammer*.

Esse resultado sugere que, dentro de faixas de valores plausíveis, a estratégia baseada no sistema híbrido tende a permanecer como a alternativa de melhor desempenho. Dessa forma, a escolha do sistema híbrido mostra-se robusta em relação às incertezas associadas à parametrização da neutralização aérea.

5.7 AVALIAÇÃO DO IMPACTO DO *INSIDER* NO DESEMPENHO DO MODELO

Nesta seção é analisado o impacto da variável *insider* sobre o desempenho do sistema de proteção física e sobre os resultados de utilidade esperada das estratégias consideradas. Diferentemente das análises anteriores, nas quais o foco esteve na comparação entre alternativas de detecção, barreiras físicas e níveis de resposta, aqui o objetivo é avaliar como a presença de um agente interno altera o comportamento do sistema, em especial no que diz respeito às probabilidades de detecção, interdição, neutralização e aos danos resultantes.

A variável *insider* foi modelada como um fator que afeta diretamente os mecanismos de detecção, refletindo a possibilidade de degradação deliberada ou inadvertida do desempenho do sistema por parte de um indivíduo autorizado. Essa degradação se propaga ao longo da cadeia causal, influenciando as probabilidades de neutralização e, em última instância, a distribuição dos danos e a utilidade total.

‘ A Tabela 26 apresenta a utilidade esperada e a neutralização da melhor estratégia quando o estado da variável *insider* é alterado de “não” para “sim”.

Tabela 26 - Estratégias ótimas e desempenho do modelo em função da presença de ameaça interna

Insider	**Alternativa**	**Utilidade**	**Neutralização**
Sem evidência	VDM + Portas Reforçadas na área Vital e Protegida+ Força de Resposta Reforçada+Hibrido	-22,35	0,68
Sim	VDM + Portas Reforçadas na área Vital e Protegida+ Força de Resposta Reforçada+Hibrido	-27,16	0,67
Não	Nenhuma + Portas Reforçadas na área Vital e Protegida+ Força de Resposta Reforçada+Hibrido	-19,61	0,69

Os resultados indicam que a presença de ameaça interna exerce impacto direto sobre a escolha da estratégia ótima e sobre o desempenho do modelo. No cenário sem a

presença de *insider*, observa-se que não há necessidade de adoção de medidas adicionais de detecção, uma vez que os sistemas já existentes apresentam desempenho suficiente para a identificação da ameaça, não sendo afetados por fatores internos.

Por outro lado, na presença de ameaça interna, verifica-se a necessidade de incorporação de medidas adicionais de proteção, com o objetivo de aumentar a redundância do sistema. Esse comportamento pode ser explicado pelo fato de que a atuação de um *insider* reduz a eficácia das camadas tradicionais de detecção e controle, exigindo estratégias mais robustas para compensar essa vulnerabilidade.

A Figura 18 apresenta a variação da utilidade das melhores estratégias para os diferentes vetores de acesso, considerando os cenários sem evidência, com presença de ameaça interna e com ausência de ameaça interna. A análise permite comparar o impacto da ameaça interna no desempenho das estratégias de proteção em cada vetor, evidenciando diferenças na sensibilidade do modelo em função do tipo de acesso

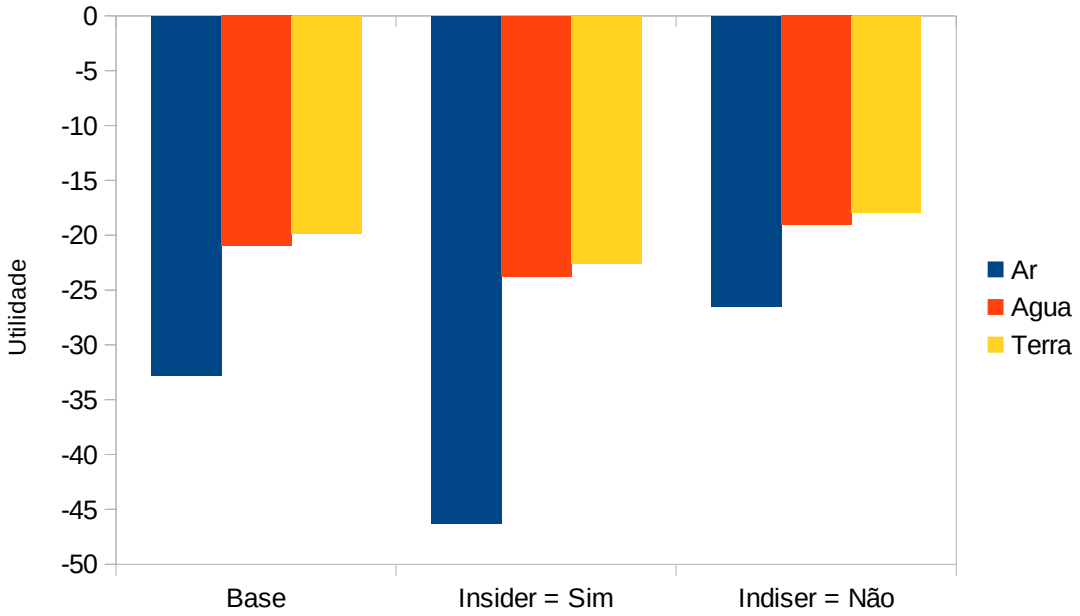

Figura 18 - Impacto da ameaça interna na utilidade por vetor de acesso

Destaca-se que o cenário aéreo é o mais sensível à presença de *insider*, apresentando uma redução expressiva da utilidade quando comparado ao cenário sem ameaça interna, com variação próxima ao dobro. Esse comportamento pode ser

explicado pela menor presença de camadas redundantes de proteção no vetor aéreo, tornando o sistema mais vulnerável à atuação de agentes internos.

Nos cenários terrestre e aquático, embora também se observe degradação da utilidade na presença de ameaça interna, o impacto é menos acentuado, o que sugere maior robustez desses vetores em função da existência de múltiplas camadas de detecção, atraso e resposta. Dessa forma, os resultados evidenciam que a ausência de redundância no acesso aéreo amplia a sensibilidade do modelo à presença de ameaça interna.

Adicionalmente, foi realizada uma análise de sensibilidade com o objetivo de avaliar o impacto da variação do parâmetro associado à ameaça interna. Ressalta-se que o valor de 20% corresponde ao adotado nas análises anteriores, sendo considerado como cenário base.

A Figura 19 apresenta a variação da utilidade e da probabilidade de neutralização em função do impacto atribuído à ameaça interna, considerando os cenários conservador (30%), base (20%) e favorável (10%). A análise permite avaliar a sensibilidade do modelo a esse parâmetro, tomando como referência a melhor estratégia identificada em cada cenário.

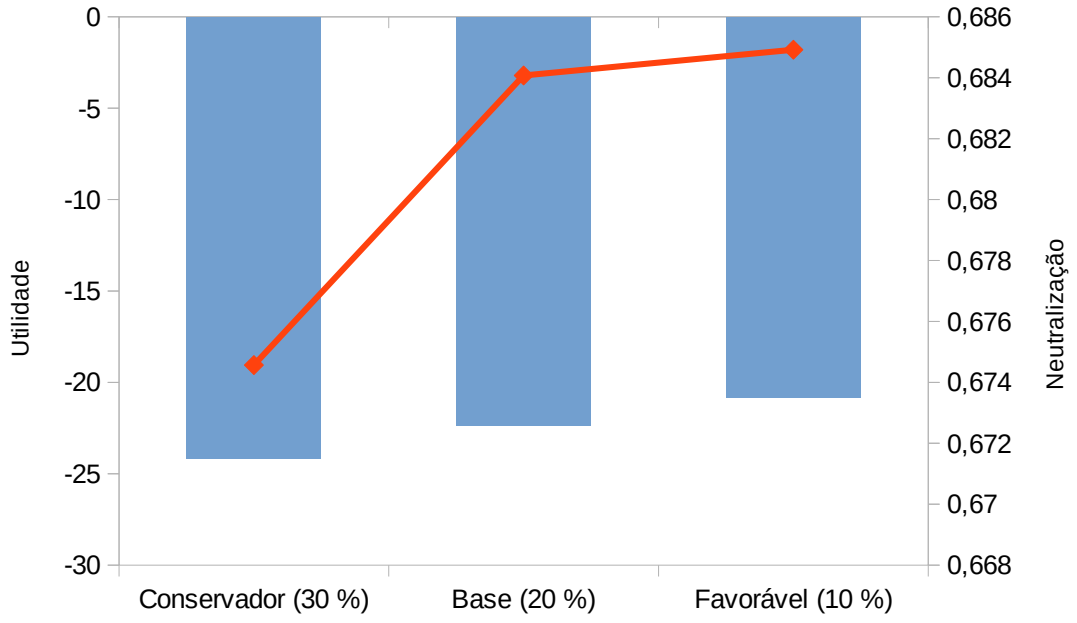

Figura 19 - Sensibilidade da utilidade e da neutralização ao impacto da ameaça interna

Os resultados indicam que a redução do impacto da ameaça interna está associada a uma melhoria progressiva da utilidade, acompanhada por um aumento na probabilidade de neutralização. Observa-se que a transição do cenário conservador para o base promove um ganho mais expressivo, enquanto a melhoria do cenário base para o favorável é mais discreta, evidenciando um comportamento não linear do modelo em relação a esse parâmetro.

No que se refere às estratégias ótimas, verifica-se que, nos cenários conservador e base, mantém-se a combinação composta por VDM, portas reforçadas nas áreas vital e protegida, força de resposta reforçada e sistema híbrido, indicando a necessidade de múltiplas camadas de proteção para mitigar os efeitos da ameaça interna. Por outro lado, no cenário favorável, observa-se que não há necessidade de adoção de medidas adicionais de detecção, resultado que se mostra consistente com o comportamento previamente identificado no cenário sem presença de ameaça interna.

5.8 ANÁLISE DE SENSIBILIDADE DOS VALORES ATRIBUÍDOS AOS DANOS

Foi realizada uma análise de sensibilidade com o objetivo de avaliar o impacto da variação dos valores atribuídos ao custo dos danos no desempenho do modelo. Considerando que esses valores foram definidos com base em casos históricos e estimativas representativas, buscou-se verificar em que medida alterações nessa parametrização influenciam a utilidade total e a escolha das estratégias ótimas. Para isso, foram considerados diferentes cenários de redução dos valores associados aos danos, além do cenário base previamente adotado.

Tabela 27 - Impacto da variação dos valores de dano na utilidade e na estratégia ótima

Cenário	**Estratégia**	**Utilidade**
Redução 90%	Nenhuma + Nenhuma + Força de Resposta Reforçada + Jammer	-4,1506
Redução 80%	Nenhuma + Portas Reforçadas na Área Protegida + Força de Resposta Reforçada + Jammer	-6,4890

Cenário	Estratégia	Utilidade
Redução 70%	Nenhuma + Portas Reforçadas na Área Protegida + Força de Resposta Reforçada + Híbrido	-8,6472
Redução 50%	Nenhuma + Portas Reforçadas na Área Protegida + Força de Resposta Reforçada + Híbrido	-12,6135
Redução 40%	Nenhuma + Portas Reforçadas na Área Protegida + Força de Resposta Reforçada + Híbrido	-14,5967
Redução 30%	Nenhuma + Portas Reforçadas na Área Protegida + Força de Resposta Reforçada + Híbrido	-16,5799
Base	VDM + Portas Reforçadas na Área Vital e Protegida + Força de Resposta Reforçada + Híbrido	-22,2500

Os resultados indicam que o aumento dos valores atribuídos aos danos não altera a estratégia ótima identificada no modelo. Esse comportamento pode ser explicado pelo fato de que, na configuração base, as estratégias selecionadas já priorizam níveis elevados de neutralização, de modo que o aumento da severidade das consequências reforça a necessidade dessas mesmas medidas, sem modificar a escolha ótima.

Por outro lado, a redução dos valores de dano leva à alteração das estratégias ótimas, com a adoção de soluções menos complexas e com menor nível de investimento. Esse resultado é coerente, uma vez que a diminuição da severidade das consequências reduz o benefício associado à implementação de medidas adicionais de proteção, tornando seu custo relativamente mais elevado em termos de custo-benefício.

Adicionalmente, foi observado que as variações nos custos associados à liberação de material nuclear não influenciam a escolha da estratégia ótima. Esse comportamento decorre da baixa probabilidade de ocorrência desse evento no modelo, fazendo com que sua contribuição para a utilidade total seja limitada, mesmo quando são considerados valores elevados de custo.

5.9 SÍNTESE DOS RESULTADOS

Os resultados obtidos evidenciam que o desempenho do modelo é fortemente influenciado pela interação entre a probabilidade de neutralização, o vetor de acesso, os meios empregados pelo adversário, o tipo de alvo e a presença de ameaça interna, sendo esses fatores determinantes para a escolha das estratégias ótimas e para os valores de utilidade esperada.

Na análise em condições de incerteza, observou-se que estratégias baseadas no sistema híbrido de neutralização de ameaças aéreas e na força de resposta reforçada apresentam melhor desempenho, mesmo quando associadas a custos mais elevados, evidenciando que ganhos de eficácia podem compensar aumentos de investimento. Além disso, verificou-se que investimentos adicionais em detecção apresentam retornos marginais reduzidos, quando comparados às melhorias na neutralização e na capacidade de resposta.

A análise por cenários de acesso indicou que a estratégia ótima permanece inalterada frente à definição do vetor de ataque, evidenciando robustez estrutural do modelo. Entretanto, o desempenho varia entre os cenários, sendo o vetor aéreo o mais crítico, em função da menor presença de camadas redundantes de proteção, o que resulta em maior probabilidade de danos relevantes.

No que se refere aos meios empregados, verificou-se que a combinação de armas e explosivos resulta no pior desempenho, devido ao efeito conjunto de maior potencial destrutivo e maior dificuldade de neutralização. Por outro lado, cenários sem emprego de meios ofensivos apresentam melhor utilidade e demandam menor complexidade nas estratégias de proteção.

A análise por tipo de alvo evidenciou um comportamento de trade-off entre frequência e severidade dos eventos. Áreas mais críticas, como a área vital, apresentam maior probabilidade de neutralização, porém, quando atingidas, resultam em consequências significativamente mais severas, o que leva a piores valores de utilidade. Em contrapartida, áreas menos críticas podem apresentar maior frequência de eventos, mas com impactos reduzidos.

A análise de sensibilidade dos parâmetros de neutralização demonstrou que o modelo apresenta comportamento não linear em relação a esse fator, sendo mais

sensível a variações em determinadas faixas de valores. Para ameaças aéreas, verificou-se que a superioridade do sistema híbrido se mantém em cenários plausíveis, sendo necessária uma elevação significativa da probabilidade de neutralização do *jammer* para que este se torne competitivo, evidenciando a robustez da solução adotada.

A presença de ameaça interna mostrou-se um dos fatores mais críticos do modelo, impactando diretamente a utilidade e exigindo estratégias mais robustas e com maior nível de redundância. Observou-se ainda que esse impacto é mais acentuado no vetor aéreo, reforçando sua maior vulnerabilidade relativa. Adicionalmente, a análise de sensibilidade do impacto do *insider* indicou que a redução desse parâmetro diminui a necessidade de medidas adicionais de detecção, aproximando o comportamento do modelo daquele observado na ausência de ameaça interna.

Por fim, a análise de sensibilidade dos custos dos danos evidenciou que a estratégia ótima é mais sensível à redução dos valores atribuídos às consequências do que ao seu aumento. Enquanto a elevação dos custos reforça as estratégias já adotadas, a sua redução leva à adoção de soluções menos complexas, evidenciando que a decisão ótima depende do equilíbrio entre custo das medidas de proteção e severidade dos impactos considerados.

Os resultados apresentados neste capítulo evidenciam o comportamento do modelo frente a diferentes cenários operacionais e variações paramétricas, permitindo identificar os principais fatores que influenciam o desempenho das estratégias de proteção física. A partir dessas análises, torna-se possível compreender não apenas quais alternativas apresentam melhor desempenho, mas também as condições sob as quais essas escolhas se mantêm robustas ou se tornam sensíveis a alterações nos parâmetros do modelo. Nesse contexto, o capítulo seguinte apresenta as conclusões do trabalho, consolidando os principais achados, suas implicações para a tomada de decisão em segurança física e as limitações e possibilidades de aprimoramento do modelo proposto.

6 CONCLUSÃO E TRABALHOS FUTUROS

O presente trabalho teve como objetivo desenvolver e aplicar uma metodologia de apoio à decisão para a análise e otimização de estratégias de proteção física em instalações nucleares, utilizando Redes Bayesianas de Decisão estruturadas na forma de Diagramas de Influência com Memória Limitada (LIMID). A proposta buscou superar limitações de abordagens tradicionais, incorporando explicitamente o processo de tomada de decisão sob incerteza e permitindo a avaliação integrada entre desempenho operacional e custos associados.

A aplicação da metodologia a um estudo de caso representativo de uma instalação nuclear inserida em uma base naval hipotética permitiu avaliar diferentes combinações de medidas de detecção, atraso e resposta, considerando múltiplos cenários de ameaça e variáveis relevantes ao contexto da segurança física. Os resultados demonstraram que a eficácia das estratégias não depende exclusivamente do desempenho isolado de cada medida, mas principalmente da forma como essas medidas são combinadas, evidenciando a importância de abordagens integradas e multicamadas.

As análises realizadas indicaram que a probabilidade de neutralização exerce papel central no desempenho do sistema, influenciando diretamente os valores de utilidade esperada. Observou-se que melhorias nessa variável tendem a gerar ganhos significativos, especialmente em cenários com desempenho inicial reduzido, enquanto incrementos adicionais apresentam retornos marginais decrescentes à medida que o sistema se aproxima de níveis elevados de eficácia.

A avaliação dos diferentes vetores de acesso evidenciou que o vetor aéreo apresenta maior sensibilidade a variações nas condições de proteção, devido à menor redundância de medidas, o que reforça a necessidade de soluções específicas para esse tipo de ameaça. Nesse contexto, verificou-se que sistemas híbridos de neutralização apresentam desempenho superior em cenários plausíveis, mantendo-se como a alternativa mais robusta frente a variações paramétricas.

A presença de ameaça interna mostrou-se um fator crítico para o desempenho do modelo, impactando significativamente a utilidade esperada e exigindo a adoção de estratégias mais robustas e com maior nível de redundância. Os resultados indicaram que, na ausência de *insider*, determinadas medidas adicionais de detecção tornam-se

desnecessárias, enquanto sua presença demanda o fortalecimento das camadas de proteção, evidenciando a importância de considerar esse fator na modelagem de sistemas de segurança física.

Adicionalmente, a análise de sensibilidade dos parâmetros do modelo demonstrou sua consistência e robustez frente a variações em diferentes dimensões, incluindo a eficácia dos sistemas de neutralização, o impacto da ameaça interna e os valores atribuídos aos custos dos danos. Observou-se que a redução dos custos associados às consequências tende a influenciar a escolha das estratégias, favorecendo soluções menos complexas, enquanto o aumento desses custos reforça a adoção de estratégias mais robustas. Por outro lado, o custo associado à liberação de material nuclear apresentou influência limitada na decisão, em função da baixa probabilidade desse evento no modelo.

De forma geral, os resultados obtidos confirmam que a utilização de Redes Bayesianas de Decisão constitui uma ferramenta eficaz para o apoio à tomada de decisão em proteção física de instalações nucleares, permitindo a incorporação estruturada de incertezas, dependências entre variáveis e critérios de custo-benefício. A metodologia proposta mostrou-se capaz de fornecer subsídios quantitativos para a comparação entre estratégias, contribuindo para decisões mais fundamentadas e transparentes.

Como limitações do estudo, destaca-se a dependência de dados provenientes da literatura e de julgamentos de especialistas para a parametrização do modelo, o que pode introduzir incertezas adicionais. Além disso, o modelo considera um conjunto fixo de cenários de ameaça, não contemplando explicitamente a adaptação dinâmica do adversário frente às medidas de segurança adotadas.

Como proposta para trabalhos futuros, sugere-se a incorporação de modelos dinâmicos que considerem a adaptação do adversário ao longo do tempo, bem como a ampliação da base de dados empíricos utilizada na calibração das probabilidades da rede. Recomenda-se, ainda, a aplicação da metodologia desenvolvida a instalações reais ou a outros tipos de infraestruturas críticas, visando avaliar sua generalização e aplicabilidade em diferentes contextos operacionais.

Adicionalmente, propõe-se a integração da abordagem baseada em Redes Bayesianas e Diagramas de Influência de Informação Limitada (LIMID) com métodos clássicos de avaliação de Sistemas de Proteção Física, tais como o *Estimate of Adversary Sequence Interruption* (EASI) e o *Systematic Analysis of Physical Protection Effectiveness* (SAPE). Essa integração poderia auxiliar na definição da localização mais adequada para a implementação de medidas de proteção, considerando os caminhos de intrusão mais críticos e a maximização da efetividade do sistema.

Sugere-se, também, o refinamento do modelo por meio da inclusão de variáveis adicionais relacionadas às características físicas da instalação, tais como a extensão das áreas monitoradas, a cobertura e sobreposição dos sistemas de detecção e as restrições operacionais associadas ao emprego dos recursos de segurança. Por fim, recomenda-se a incorporação de métodos de Análise de Confiabilidade Humana (*Human Reliability Analysis* – HRA), permitindo avaliar a influência do desempenho humano sobre a capacidade de detecção, avaliação e resposta, contribuindo para uma representação mais abrangente e realista do Sistema de Proteção Física.

DECLARAÇÃO DE USO DE INTELIGÊNCIA ARTIFICIAL

Em conformidade com os princípios de transparência e integridade científica estabelecidos pela Portaria CNPq nº 2.664, de 6 de março de 2026, informa-se que o ChatGPT (OpenAI) foi utilizado durante a elaboração desta dissertação exclusivamente como apoio à revisão textual. A ferramenta não foi empregada para a geração autônoma de resultados científicos, definição da metodologia, construção do modelo, obtenção e análise dos dados ou formulação das conclusões do estudo. Todas as decisões metodológicas, verificações, interpretações e conclusões apresentadas neste trabalho são de responsabilidade exclusiva do autor.

REFERÊNCIAS

ALVAREZ, R. et al. .Reducing the hazards from stored spent power-reactor fuel in the United States. Science and Global Security, Abingdon, v. 11, n. 1, p. 1–51, 2003. DOI: 10.1080/08929880390214124.

ANDIWIJAYAKUSUMA, D. et al. . The development of EASI-based multi-path analysis code for nuclear security system with variability extension. Nuclear Engineering and Technology Volume 54, Issue 10, October 2022, Pages 3604-3613, 2022.

ARGENTI, F et al. Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network Reliab. Eng. Syst. Saf, 2018

ARGENTI, F et al. A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. Safety Science 94, 181-196, 2017.

ASSOCIATED PRESS. Fire destroys cooling tower at nuclear plant. 1986. Disponível em: https://web.archive.org/web/20180522041457/https://www.apnews.com/883b146491db3a85e86f02cc4d95387c. Acesso em: 28 mar. 2026.

BAYESFUSION. GeNIe Modeler User's Manual .Version 5.0.R2, 2024.

CHAARI, M. Z. Analysis of the power of drones and limitations of the anti-drone solutions on the Russian-Ukrainian battlefield. Security and Defence Quarterly, [s. l.], v. 51, n. 3, p. 38-73, 2025. DOI: 10.35467/sdq/208347.

CARLESS, T. , REDUS, K. , DRYDEN, R. Estimating nuclear proliferation and security risks in emerging markets using Bayesian Belief Networks. Energy Policy 159 (2021) 112549equação

CIS SHOW HARDWARE. **Commercial door installation price 2025**. 2025. Disponível em: https://cishowhardware.com/commercial-door-installation-price-2025/. Acesso em: 4 abr. 2026.

DEDRONE. DedroneTracker System Overview. Kassel, 2022.

DEGROOT, M; SCHERVISH, M. **Probability and statistics**. 4. ed. Boston: Addison-Wesley, 2012.

DIGITAL SECURITY GUARD. **Remote Video Monitoring Cost: Complete 2025 Pricing Guide**. 2025.

DRONESHIELD. DroneGun Tactical – Product Overview. Sydney, 2020.

FERGUSON, C., SETTLE, F. The Future of Nuclear Power in the United States. Federation of American Scientists, 2012

GARCIA, M. L. Design and Evaluation of Physical Protection Systems. 2a ed. Massachusetts, Elsevier Butterworth Heinemann, 2008.

GRACE, P. G.; RENJITH, V. Evolution of Safety and Security Risk Assessment methodologies towards the use of Bayesian Networks in Process Industries.Process Safety and Environmental Protection 149 (2021) 758–775

HAWILA, M. A.-M. M. "Combined Safety and Security Risk Evaluation Considering Safety and Security-Type Initiating Events", 2016. Disponível em: https://oaktrust.library.tamu.edu/items/f1cc2db9-e072-4874-945f-c801a292a621/full. Acesso em: 20 novembro de 2025.

HOU, B. et al.Optimal allocation of defensive resources in regional railway networks under intentional attacks. Reliability Engineering and System Safety, 257, 2025.

IAEA Nuclear power and the clean energy transition. IAEA Bulletin, v. 60, n. 2, Viena, 2019. Disponível em: https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull60-2/6020405.pdf. Acesso em: 06 abr. 2026.

IAEA. Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities. Viena, Áustria, International Atomic Energy Agency, 2021. Disponível em: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1875_web.pdf. Acesso em: 10 jan. 2025.

IAEA. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). Viena, Áustria, International Atomic Energy Agency, 2011.
Disponível em:https:https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf. Acesso em: 22 jan. 2025
IAEA Nuclear Safety and Security Glossary. Viena, Áustria, International Atomic Energy Agency. Disponível em: https://www-pub.iaea.org/MTCD/Publications/PDF/IAEA-NSS-GLOweb.pdf. Acesso em: 22 jan. 2025

IAEA. National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements. IAEA Nuclear Security Series No. 10-G (Rev. 1). Vienna: IAEA, 2021. Disponível em: https://www-pub.iaea.org/MTCD/Publications/PDF/P1926_web.pdf. Acesso em: 15 dde outubro de 2025.

IANINI, M. et al. A Bayesian-network approach for assessing the probability of success of physical security attacks to offshore oil&gas facilities, Ocean Eng, 2023

JENSEN, F. V.; NIELSEN, T. D. *Bayesian networks and decision graphs*. 2. ed. New York: Springer, 2007.

KANG, M ; KOH, M. Study on Bayesian Approach for Intrusion Detection in Physical Protection System of Nuclear Power Plants. Korean Nuclear Society Autumn Meeting Gyeongju, Korea, October 26-27, 2017

KIM, D.; KANG, J. Where nuclear safety and security meet. Bulletin of the Atomic Scientists, 68(1), 2012, 86-93. https://doi.org/10.1177/0096340211433021

Lanchester F.W., Mathematics in Warfare in The World of Mathematics, Vol. 4 (1956) Ed. Newman, J.R., Simon and Schuster, 2138–2157

MANNING, Christopher D.; RAGHAVAN, Prabhakar; SCHÜTZE, Hinrich. Introduction to Information Retrieval. Cambridge: Cambridge University Press, 2008.

MARRONI, G. et al. Securing Chemical Facilities Against Intentional Attacks: a Bayesian Network Approach for Asset Risk Assessment. CHEMICAL ENGINEERING TRANSACTIONS VOL. 111, 2024

MATTER, J.C. SAVI: "A PC-Based Vulnerability Assessment Program", SAND88-1279, 1988

MAUÁ, D. et al. Solving Limited Memory Influence Diagrams. Journal of Artificial Intelligence Research 44 (2012) 97-140, Itália, 2012.

MILLIAN, E., et al. Bayesian networks for student model engineering. Computers & Education, 55(4) (2010) :1663–1683.

MISURI, A. et al. A Bayesian network methodology for optimal security management of critical infrastructures, Rel. Eng. Syst. Saf., vol. 191, Nov. 2019

MOHSENDOKHT, M. et al. Enhancing maritime transportation security: A data-driven Bayesian network analysis of terrorist attack risks. Risk Analysis. 2025;45:283–306.

NATIONAL HOMELAND SECURITY KNOWLEDGEBASE. Underwater terrorism prevention plan informational bulletin. 2009. Disponível em: Acessar documento. Acesso em: 4 abr. 2026.

NEAPOLITAN, R. Learning Bayesian Networks. Northeastern-Illinois-University, Estados Unidos da América, 2003.Disponível em: https://analyticsconsultores.com.mx/wp-content /uploads/2019/04/Learning-Bayesian-Networks-R.E.-Neapolitan-NortheasternIllinoisUniversity.pdf . Acesso em: 10 jan. 2025

NORTH ATLANTIC TREATY ORGANIZATION (NATO). Undersea surveillance and sensor systems. Brussels, 2017.

PATÉ-CORNELL, E., GUIKEMA, S. Games and Risk Analysis, Three Examples of Single and Alternate Moves, in: Bier V. M., Azaiez M. N., 2009, Game Theoretic Risk Analysis of Security Threats, Springer.

PHILIPS, G. "New Vulnerability Assessment Technologies vs the Old VA Tools", New Meets Old, National Security Program Office. 2004.

POURRET, O. et al. Bayesian Networks: A Pratical Guide to Applications. ohn Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, 2008.

REUTERS. Japan nearly doubles Fukushima disaster-related cost to $188 billion. 2016. Disponível em: https://www.reuters.com/article/us-japan-fukushima-costs-idUSKBN13V0AB. Acesso em: 28 mar. 2026.

SANDLER, T., LAPAN H. E..The calculus of dissent: An analysis of terrorists’ choice of targets. Synthese, 76:245-261, 1988.

SANTOS, T. Análise de Risco de Um Sistema de Proteção Física de uma Base Naval Hipotética com Material Nuclear, Rio de Janeiro: UFRJ/COPPE, 2024.

SHACHTER, R. D.. Evaluating Influence Diagrams. Operations Research, 34:871-882, 1986

SINAPI. Sistema Nacional de Pesquisa de Custos e Índices da Construção Civil. Caixa Econômica Federal. 2024.

SVERIGES RADIO. Nuclear power plant incident cost estimated at 1 billion kronor. 2006. Disponível em: https://www.sverigesradio.se/artikel/937172. Acesso em: 28 mar. 2026.

TANG, Z. et al. Risk Analysis of Urban Dirty Bomb Attacking Based on Bayesian Network. Sustainabilit, 2019.

WALL, A., AGRAFIOTIS, I. A Bayesian approach to *insider* threat detection. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2021, 12(2), 48–84.

WANG, N. , WU, M. , YUEN, K. Assessment of port resilience using Bayesian network: A study of strategies to enhance readiness and response capacities. Reliability Engineering & System Safety Volume 237, September 2023

WANG, Qi-Ang; LU, Ao-Wen; NI, Yi-Qing; WANG, Jun-Fang; MA, Zhan-Guo. Bayesian Network in Structural Health Monitoring: Theoretical Background and Applications Review. 2025.

ZHU, R. et al. Modeling and Risk Analysis of Chemical Terrorist Attacks: A Bayesian Network Method. Int. J. Environ. Res. Public Health, 2020.

ZOU, B.; Yang, M.; Guo, J.; Wang, J.; Benjamin, E.-R.; Liu, H.; Li, W. *insider* threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation. Prog. Nucl. Energy , China, 2018

JANG, S.S, et al. 2009. Development of a vulnerability assessment code for a physical protection system: systematic analysis of physical protection effectiveness (SAPE). Nucl. Eng. Technol. 41 (5), 747–752.

SNELL, M. K. Report on Project Action Sheet PP05 Task 3 between the U.S. Department of Energy and the Republic of Korea Ministry of Education, Science, and Technology (MEST). Sandia National Laboratories, SAND2013-0039, 2013.

UNITED STATES. Nuclear Regulatory Commission (NRC). Technical study of spent fuel pool accident risk at decommissioning nuclear power plants. Washington, DC: U.S. Nuclear Regulatory Commission, 2001.

UNITED STATES. Department of Justice. Office of the Inspector General. Audit of the Department of Justice's Efforts to Protect Federal Facilities Against Threats Posed by Unmanned Aircraft Systems. Washington, DC, 2020

UNITED STATES NUCLEAR REGULATORY COMMISSION (NRC). Technical study of spent fuel pool accident risk at decommissioning nuclear power plants (NUREG-1738). Washington, DC: U.S. NRC, 2001. Disponível em: https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1738/. Acesso em: 06 abr. 2026.