UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIA E GEOCIÊNCIAS
PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL EM ENGENHARIA DE PRODUÇÃO

CARLOS EDUARDO PIRES DE ALBUQUERQUE

ANÁLISE DE RISCO TERRORISTA: revisão sistemática da literatura como suporte à decisão no planejamento de políticas de segurança pública

Recife
2019

CARLOS EDUARDO PIRES DE ALBUQUERQUE

ANÁLISE DE RISCO TERRORISTA: revisão sistemática da literatura como suporte à decisão no planejamento de políticas de segurança pública

Dissertação apresentada ao Programa de Pós-Graduação Profissional em Engenharia de Produção da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Engenharia de Produção.

Área de concentração: Pesquisa Operacional.

Orientador: Prof. Dr. Marcelo Hazin Alencar.

Recife

2019

Catalogação na fonte
Bibliotecário Gabriel Luz, CRB-4 / 2222

A345a Albuquerque, Carlos Eduardo Pires de.

Análise de risco terrorista: revisão sistemática da literatura como suporte à decisão no planejamento de políticas de segurança pública / Carlos Eduardo Pires de Albuquerque – Recife, 2019.

99 f.: fig., tabs.

Orientador: Prof. Dr. Marcelo Hazin Alencar.

Dissertação (Mestrado Profissional) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação Profissional em Engenharia de Produção, 2019.

Inclui referências.

1. Engenharia de produção. 2. Ameaças inteligentes. 3. Avaliação da ameaça. 4. Análise de risco terrorista. 5. Processo decisório. I. Alencar, Marcelo Hazin (Orientador). II. Título.

UFPE

658.5 CDD (22. ed.) BCTG / 2020-41

CARLOS EDUARDO PIRES DE ALBUQUERQUE

ANÁLISE DE RISCO TERRORISTA: revisão sistemática da literatura como suporte à decisão no planejamento de políticas de segurança pública

Dissertação de Mestrado Profissional apresentada ao Programa de Pós-Graduação Profissional em Engenharia de Produção, Centro de Tecnologia e Geociências da Universidade Federal de Pernambuco como parte dos requisitos parciais para a obtenção do título de Mestre em Engenharia de Produção.

Aprovada em: 02/12/2019.

BANCA EXAMINADORA

_____

Prof. Dr. Marcelo Hazin Alencar (Orientador)

Universidade Federal de Pernambuco

_____

Profa. Dra. Ana Paula Cabral Seixas Costa (Examinadora Interna)

Universidade Federal de Pernambuco

_____

Profa. Dra. Ana Paula H. Gusmão de Araújo Lima (Examinadora Externa)

Universidade Federal de Sergipe

“Respice post te, hominem te esse memento, memento mori - nam mors indecepta”

(Autor desconhecido)

RESUMO

A análise do risco terrorista deve se pautar em identificar e estudar os elementos constituintes para o desenvolvimento de uma avaliação da ameaça a fim de apoiar à decisão no planejamento de políticas de segurança públicas e em ações antiterroristas. O tema tem grande relevância no cenário internacional, porém os estudos no Brasil ainda são incipientes. O terrorismo é uma ameaça global que evolui constantemente com um impacto econômico global estimado em mais de 31 mil milhões de dólares segundo o Institute for Peace and Economics em 2018. Os estados devem atuar de forma integrada e cooperada para fazer frente a esse desafio em nível global, regional e nacional com base na defesa dos direitos humanos universais e o direito internacional, aliando um forte trabalho de inteligência ao desenvolvimento científico. O grande desafio da análise de risco terrorista é a pesquisa no comportamento humano devido a intencionalidade dos atos, os chamados adversários inteligentes, bem como dos resultados extremos da consecução do risco em face das suas características de baixa probabilidade e alto impacto cercada de incertezas. Este trabalho apresenta o cenário atual do estudo do risco terrorista com base em uma revisão sistemática e apresentação de uma análise da integração do ciclo da produção do conhecimento de inteligência com modelos de decisão com foco no antiterrorismo, suportando à construção da resiliência nacional. Objetiva contribuir para desenvolver o pensamento crítico no tema, bem como para fomentar novas pesquisas relacionadas a influência das ameaças inteligentes na consecução dos objetivos estratégicos nacionais, a fim de contribuir para a garantia da ordem pública e a incolumidade pública.

Palavras-chaves: Ameaças inteligentes. Avaliação da ameaça. Análise de risco terrorista. Processo decisório.

ABSTRACT

Terrorist risk analysis should be based on identifying and studying the constituent elements for the development of a threat assessment to support decision making in planning public security policies and antiterrorist actions. The theme has great relevance in the international scenario, however studies in Brazil are still incipient. Terrorism is a global threat that evolves constantly with an estimated global economic impact of over $ 31 billion according to the Institute for Peace and Economics in 2018. States must act in an integrated and cooperative way to meet this challenge at the global, regional and national based on the defense of universal human rights and international law, combining a strong work of intelligence to the scientific development. The major challenge of terrorist risk analysis is the research into human behavior due to the intentionality of the actions, the so-called intelligent adversaries, as well as the extreme results of risk taking in the face of their low probability characteristics and high impact surrounded by uncertainties. This paper presents a current scenario of terrorist risk study based on a systematic review and presentation of an integrated analysis of the intelligence knowledge production cycle with decision models focused on antiterrorism, supporting the organization of national resilience. It aims to contribute to the development of critical thinking on the subject, as well as to promote new research related to the influence of intelligent threats in the achievement of national strategic objectives, in order to contribute to the guarantee of public order and public safety.

Keywords: Intelligent threats. Threat assessment. Terrorist risk analysis. Decision Making.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O terrorismo é uma ameaça global que evolui constantemente com um impacto econômico global estimado em mais de 77 mil milhões de euros. Os Estados devem atuar de forma integrada e cooperada para fazer frente a esse desafio em nível global, regional e nacional, com base nos direitos humanos universais e o direito internacional (UNRIC, 2018).

No campo acadêmico, ilustres doutrinadores escreveram sobre o tema terrorismo focado nas mais diversas vertentes, sendo destacado apresentar a visão de Crenshaw (1983) *apud* Schmid e Jongman *et al.* (1988, p. 35) que destacada o uso da violência para fins políticos:

> [...] uma definição básica deve incluir os seguintes atributos: o uso sistemático da violência heterodoxo por pequenos grupos de conspiradores, com o objetivo de manipular as atitudes políticas em vez de derrotar um inimigo fisicamente. A intenção da violência terrorista é psicológica e simbólica, não material. O terrorismo é a violência premeditada e intencional, empregado em uma luta pelo poder político. Como Harold Lasswell definiu: 'Os terroristas são os participantes no processo político que se esforçam para obter resultados políticos, suscitando inquietações agudas'[1] (CRENSHAW, 1983 *apud* SCHMID; JONGMAN *et al.*, 1988, p. 35, tradução nossa).

Segundo Rapoport (2004), os acontecimentos na data de 11 de setembro de 2001 nos EUA, desencadeados por extremistas islâmicos, o tornaram o dia mais destrutivo na sangrenta história do terrorismo, um acontecimento sem precedentes, que iniciou uma segunda guerra ao terror[2] pelos norte-americanos. O evento gerou a explosão do medo na população e criou uma sensação de insegurança que não existia antes a não ser em áreas conflagradas, mudando toda a forma de pensamento e comportamento de uma época. A ameaça terrorista permanente ficou evidente e exigiu medidas de prevenção e segurança dos governos de todos o mundo.

Este evento extremo, que ceifou mais de 3.000 vidas e gerou um impacto econômico próximo de U$ 250 bilhões, levou o mundo a buscar um aprofundamento nos estudos dos modelos de gerenciamento do risco terrorista visando evitar a perda de vidas e os danos

[1] [...] a basic definition would include the following attributes: the systematic use of unorthodox violence by small conspiratorial groups with the purpose of manipulating political attitudes rather than physically defeating an enemy. The intent of terrorist violence is psychological and symbolic, not material. Terrorism is premeditated and purposeful violence, employed in a struggle for political power. As Harold Lasswell defined it: 'Terrorists are participants in the political process who strive for political results by arousing acute anxieties'.

[2] Após o assassinato do Presidente McKinley em 1901, Theodore Roosevelt, o vice-presidente norte-americano que assumiu, declarou que os anarquistas eram uma ameaça a toda raça humana e tentou lançar um esforço internacional para eliminar o terrorismo, que teria sido a primeira guerra ao terror contra a ameaça anarquista (RAPOPORT, 2004, p. 52).

econômicos, bem como o aprimoramento das estratégias nacionais de contrainteligência para sobreposição às ameaças na consecução dos objetivos estratégicos.

Ainda em 2001, os EUA foram palco de uma sequência de envio de esporos de antraz via postal para empresas de comunicação e lideranças políticas segundo Atlas (2002). Estes eventos culminaram com a publicação do *Homeland Security Act* 2002 (HSA), que criou o DHS, sendo a maior reorganização interna na estrutura governamental americana após a criação do Ministério da Defesa em 1947. O DHS tem como missão proteger os EUA do terrorismo, mantendo a nação a salvo da ameaça de ataques terroristas.

> O Departamento de Segurança Interna tem uma missão vital: proteger a nação das muitas ameaças que enfrentamos. Isso requer a dedicação de mais de 240.000 funcionários em trabalhos que vão da segurança da aviação e da fronteira à resposta a emergências, do analista de segurança cibernética ao inspetor de instalações químicas. Nossos deveres são amplos e nosso objetivo é claro - manter a América segura[3] (DHS, 2018).

O HSA 2002 determinou dentre outras medidas de integração a operação de programas de pesquisas de alta qualidade e desenvolvimento de forma mais ampla possível, no meio acadêmico e privado, por meio de financiamento estatal, com a criação dos Centros Universitários, ou de Segurança Interna, visando o estabelecimento de um sistema coordenado de melhoria da segurança interna norte-americana (HSA, 2002).

Estes centros atuam como parte da estratégia nacional de contrainteligência no desenvolvimento de soluções de ciência e tecnologia multidisciplinares voltados para a Segurança Interna, e na formação, especialização e aperfeiçoamento dos especialistas em Segurança Interna com ênfase no gerenciamento do risco. As avaliações de risco terroristas devem ser parte permanente do pensamento crítico sobre as necessidades estratégicas nacionais.

Considerando o impacto mundial do tema que envolve atores transnacionais, a elaboração desta pesquisa pretende identificar e estudar os elementos constituintes para o desenvolvimento de uma avaliação da ameaça no contexto da análise do risco terrorista que servirá de apoio à Decisão no planejamento de Políticas de Segurança Públicas e em ações antiterroristas. O tema tem grande relevância no cenário internacional, porém, na pesquisa conduzida, não se observou no Brasil estudos que exploraram o estudo do risco e a consequente necessidade de antecipação

[3] The Department of Homeland Security has a vital mission: to secure the nation from the many threats we face. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector. Our duties are wide-ranging, and our goal is clear - keeping America safe.

de cenários com foco nos objetivos nacionais, preservação de vidas e mitigação de impactos econômicos.

1.1 ESTRUTURA DA DISSERTAÇÃO

A dissertação está estruturada da seguinte forma:

O capítulo 1 apresenta a introdução do trabalho, onde é realizado um breve panorama sobre o tema no cenário mundial e nacional destacando a sua contemporaneidade. Apresenta sua relevância e o potencial de contribuir para garantia da consecução dos objetivos estratégicos nacionais e a estabilidade interna e externa no tocante a ordem e incolumidade pública.

O capítulo 2 apresenta o contexto e a descrição do problema abordando a atuação da Polícia Federal no tocante à inteligência e antiterrorismo como forma de prover o assessoramento estratégico de inteligência e a persecução criminal, contribuindo para a salvaguarda do Estado Democrático de Direito.

O capítulo 3 reúne a base conceitual e a revisão da literatura, apresentando a metodologia empregada, o planejamento da revisão sistemática e a estruturação da formulação das questões de pesquisas baseadas em busca primária com termos chaves e análise primária do tema no Web of Science® – Coleção Principal (*Thomson Reuters Scientific*), detalhando as fases a serem percorridas para atingir o objetivo da pesquisa.

O capítulo 4 contém a fundamentação teórica e a revisão da literatura agregando conhecimentos atuais e com base no estado da arte. Os conceitos de risco e incerteza são integrados a sua análise e gestão, bem como a exploração dos tópicos terrorismo, avaliação de ameaças, modelos de análise do risco terrorista como forma de lastrear a análise dos resultados da revisão sistemática de literatura.

O capítulo 5 traz a apresentação e a discussão dos resultados visando representar o atual estado de desenvolvimento do tema e suas tendências, por meio de uma análise de dados bibliométricos com a ferramenta VOSviewer 1.6.11, que foi desenvolvida para análise, mapeamento e visualização de dados bibliométricos pela *Leiden University*.

Por fim, o capítulo 6 apresenta as conclusões resultantes da pesquisa e análises realizadas, e as oportunidades de trabalhos futuros na área pesquisada.

1.2 JUSTIFICATIVA E RELEVÂNCIA

Em relação à relevância acadêmica, esta pesquisa tem uma importância teórica e prática, visto que os riscos de Segurança Pública e Defesa, duas atividades constitucionais do Estado Brasileiro, envolvem eventos de alto impacto e baixa probabilidade, de grande incerteza, mas que caso se concretizem podem impactar em perdas de muitas vidas e danos irreparáveis.

São parcos os estudos no campo nacional que abordem a relevância do tema e os modelos praticados no cenário internacional atinentes ao assunto avaliação da ameaça no contexto da análise de risco terrorista de forma acadêmica, tão pouco institucionalmente.

O cenário nacional carece de referências acadêmicas desenvolvidas a partir do "estado da arte" para contribuir definitivamente com a consolidação do tema como fundamental na área da SP&D, de forma a servir de referência e fornecer subsídios aos futuros pesquisadores para o desenvolvimento de novas pesquisas possibilitando o desenvolvimento de doutrina nacional no campo da análise do risco terrorista.

A Polícia Federal passa por um momento de transição interna em virtude da recente tipificação do crime de terrorismo, onde necessita manter o foco no trabalho de inteligência que visa a antecipação de cenários e a negação de ameaças ao Estado Democrático de Direito, e consolidar a persecução criminal na temática. A experiência no antiterrorismo é ponto fundamental que vai sustentar o desenvolvimento da necessária consolidação no cenário nacional por meio da atividade de polícia judiciária nos crimes de terrorismo.

A pesquisa explora o cenário mundial, as tendências e os principais estudos oferecendo, dessa forma, mais referências doutrinárias e acadêmicas neste novo momento. Busca robustecer os processos atuais por meio da apresentação da integração do ciclo da produção de conhecimento com um modelo de processo holísticos para decisões antiterroristas, onde são destacados os atores, as técnicas, incertezas e oportunidades que podem contribuir para o desenvolvimento de um framework futuro para tão sensível tema. Comparativamente é apresentado a relação das decisões com o Ciclo de Boyd e o ciclo de um ataque terrorista, de forma a enquadrar temporalmente as ações e decisões.

A relevância social é destacada porque os resultados desta pesquisa permitirão que seja aprofundado o conhecimento sobre a ameaça terrorista, fenômeno que vem assolando todo o mundo, onde por conta da globalização, vem sendo potencializadas por meio de interações com redes criminosas transnacionais. A participação do tema na agenda política mundial amplia seu status como assunto sensível e prioritário, gerando importantes discussões quanto à sua

prevenção e repressão, sendo mister, o aprofundamento dos estudos nacionais com urgência por meio da pesquisa científica visando apoiar o desenvolvimento nacional e fortalecer o setor público e a incolumidade pública com base na resiliência nacional.

No campo pessoal, é destacada a possibilidade de consolidar estudos pretéritos sobre os temas abordados, ampliar os conhecimentos no desenvolvimento do projeto de pesquisa, e contribuir ao meio acadêmico e com o meio governamental para subsidiar e assessorar a implementação de procedimentos e normas legais que influenciem diretamente na prevenção e repressão ao crime organizado transnacional e ao terrorismo, garantindo a execução dos objetivos nacionais estratégicos.

1.3 OBJETIVOS DO TRABALHO

A presente pesquisa tem por finalidade oferecer aos pesquisadores, analistas e decisores um panorama atualizado sobre o estudo da análise de risco terrorista e suas características que a distinguem dos estudos do risco nos eventos naturais e mecânicos, enfatizando a relevância do maior entendimento do adversário inteligente, a fim de oferecer condições de redução de incerteza no processo decisório, elaboração de programas e políticas públicas.

1.3.1 Objetivo geral

Apresentar um estudo sobre avaliação das ameaças e modelos de análise do risco terrorista baseado a fim de servir como referência para o desenvolvimento de Doutrina Nacional.

1.3.2 Objetivos específicos

a) Elencar breves conceitos e definições sobre terrorismo e outras ameaças ao Estado Democrático de Direito;
b) Realizar uma revisão sistemática sobre análise de risco do terrorismo;
c) Apresentar um panorama sobre Análise de Risco do Terrorismo no contexto estratégico da Segurança Pública e Defesa;

d) Analisar a integração do ciclo da produção do conhecimento com um modelo de processo decisório para decisões antiterroristas com impactos nos níveis tático, operacional e estratégico.

2 CONTEXTO E DESCRIÇÃO DO PROBLEMA

Com vistas a permitir a maior assimilação da pesquisa e o entendimento das etapas seguidas, é relevante esclarecer que a Polícia Federal é a polícia judiciária da União, possuindo como atribuição constitucional a apuração de infrações penais contra a ordem política e social, bem como daquelas que tenham repercussão interestadual ou internacional e exija repressão uniforme, dentre outras de menor relação com o tema da pesquisa.

Antes da Lei Antiterrorismo a Divisão Antiterrorismo da Polícia Federal produzia conhecimentos de Inteligência, e os crimes vinculados ao terrorismo eram apurados pelas especializadas, atualmente ela também já atua em investigações. A atividade de Inteligência é dividida em dois grandes ramos: a produção do conhecimento (inteligência propriamente dita) e a proteção ao conhecimento (contrainteligência), negação das ameaças. Ambos os ramos devem ser olhados como interdependentes, partes de um todo, sem limites precisos, mas fundamentalmente integrados.

No contexto do assessoramento estratégico, a Polícia Federal representa o Ministério da Justiça no Sistema Brasileiro de Inteligência (Sisbin), que tem por objetivo promover a integração das ações de inteligência no Brasil, reunindo 39 órgãos federais para intercâmbio de informações e cooperações multilaterais.

Dentro dessa perspectiva, destaca-se que ela se torna o ator prioritário no contexto de subsidiar as ações do Ministério da Justiça, com atuação destacada para a Diretoria de Inteligência Policial que promove o assessoramento estratégico ao Diretor-Geral, e consequentemente ao Ministro da Justiça, por meio da produção de conhecimentos, para subsidiar a tomada de decisões em diferentes níveis.

Este trabalho contribuirá para fortalecer a atuação da Polícia Federal de forma a desenvolver novas capacidades de contribuição no Sisbin, e na Comunidad de Policías de América (Ameripol), estando inclusive mais preparada para eventuais participações caso ocorra a reativa do Grupo 3+1 sobre a segurança na Tríplice Fronteira[4].

O antiterrorismo é uma atividade típica de contrainteligência, ramo da inteligência e visa antecipar, evitando as consequências dos atos terroristas. Ele se desenvolve por meio de um trabalho integrado e estruturado pelos órgãos de inteligência, com o objetivo de delinear as

[4] O "Grupo 3 + 1 sobre Segurança da Área Tríplice Fronteira" reuniu os governos da Argentina, Brasil, Paraguai e Estados Unidos em 2002 com o objetivo de fortalecer a segurança na região. Após um hiato, há relatos de discussões entre as nações da TBA e os Estados Unidos sobre seu relançamento (NIELSEN, 2019).

atividades terroristas servindo como instrumento de assessoramento para o planejamento de políticas públicas de segurança e para operações repressivas, provendo a devida antecipação de cenários ao Estado.

Atividade prioritária é a análise de ameaças que consiste em um processo contínuo de compilação e análise de todas as informações disponíveis sobre atividades terroristas em potencial por grupos terroristas que podem perpetrar ações contra o Estado, tem função primordial na garantia da consecução dos objetivos estratégicos nacionais. A avaliação de ameaças integra a análise de ameaças com o ambiente de segurança dentro do qual nossas capacidades de defesa atuam visando determinar o nível da ameaça nacional (GORTNEY, 2010).

Os dias atuais carregam em si a incerteza resultante da quantidade de informações disponíveis para amparar decisões nos mais diversos níveis organizacionais. Nesse contexto, a pesquisa busca por meio da revisão sistemática de literatura fornecer subsídios para o reforço da atuação da instituição no assessoramento estratégico, codificando um fluxo de integrado de ações com conhecimentos e atores envolvidos.

A análise da integração entre o ciclo de produção do conhecimento de inteligência e o processo decisório no campo do antiterrorismo visa proporcionar ganhos que vão desde a integração dos atores para modelagem das ameaças e o estabelecimento do contexto, até a tomada da decisão. O produto gerado será uma análise de risco mais robusta que vai se integrar ao processo decisório com foco no antiterrorismo visando garantir a capacidade de se promover a eficiência das ações e reduzir as incertezas em tomadas de decisão com riscos envolvidos de baixa probabilidade, porém de alto impacto. Tais riscos envolvem inclusive a perda de vidas e perdas financeiras, podendo afetar diretamente a estabilidade interna do país, bem como a economia nacional e internacional.

Através da análise de uma representação integrada de tão complexa interação, é necessário que seja realizada a análise de cenários com potenciais ameaças e oportunidades, buscando a capacidade de agir preventivamente através do planejamento de suas ações no sentido de mitigar perdas ou aproveitar cenários favoráveis.

O próximo capítulo apresentará a fundamentação teórica e a revisão de literatura de forma a contribuir para a formação do pensamento crítico nas bases conceituais necessárias a estruturação do trabalho sobre o tema a partir do estado da arte.

3 FUNDAMENTAÇÃO TEÓRICA E REVISÃO DA LITERATURA

O capítulo tem como foco primário o objetivo de agregar valor na avaliação da ameaça e sua aplicação na análise do risco terrorista, procurou-se nesta revisão da literatura preliminar agregar conhecimentos demonstrando o panorama atual com base no "estado da arte".

A fundamentação teórica e a revisão da literatura que abordam os seguintes tópicos que congregam as bases conceituais sobre as quais se constrói este trabalho: terrorismo, análise de riscos, avaliação das ameaças, análise do risco terrorista e seus principais modelos. Busca-se apresentar um lastro para apoiar a análise dos resultados da revisão sistemática de literatura.

3.1 FUNDAMENTAÇÃO TEÓRICA

Risco é o efeito da incerteza nos objetivos (ABNT, 2009, p. 1), podendo resultar em incidente ou acidente, ou até mesmo oportunidade. A cultura do risco permite trabalhar a gestão dos recursos e atividades mitigadoras contribuindo para a estabilidade interna. Faz se imperioso o efetivo planejamento de alocação de recursos visando atingir a eficiência e mitigar ao menor custo os eventuais resultados danosos de consecução de evento crítico.

De acordo com Garrick e Kaplan (1981) quando analisamos um risco, estamos tentando imaginar como será o futuro, construir um cenário, resultante de alguma ação ou inação. Cenário é um conjunto de realizações a partir de um conjunto de eventos incertos. Fundamentalmente a análise de risco busca responder três perguntas: (i) O que pode acontecer? (isto é, o que pode dar errado?); (ii) Qual a probabilidade de isso acontecer? e (iii) Se isso acontecer, quais são as consequências?

As perguntas guiam o analista para a identificação, medição, quantificação e avaliação dos riscos e consequências. O gerenciamento do risco baseia-se em um segundo triplo de perguntas: o que pode ser feito e quais opções estão disponíveis? Quais são os trade-offs em termos de custos, benefícios e riscos? e quais são os impactos das decisões políticas atuais sobre opções futuras? (HAIMES, 1991, p.169).

O processo de avaliação de riscos e gestão de riscos é efetivamente baseado em responder aos dois triplos de pergunta apresentados, onde as respostas as perguntas de cada triplo vão reforçar a necessidade de uma modelagem multiperspectiva, interdisciplinar, de forma a abarcar a totalidade das possíveis fontes de risco e ações decorrentes para gerenciar o risco.

A análise da ameaça no contexto do antiterrorismo consiste em um processo contínuo de identificação e monitoramento de atividades terroristas com potencial execução de ação contra o Estado. O enfoque é dado nos fatores da existência, capacidade, intenção ou motivação, histórico e divisões do grupo terrorista, bem como do ambiente estabelecido no contexto (PUB, 1994, p.243).

A avaliação da ameaça é requisito fundamental e atividade crítica por meio da qual os ativos e vulnerabilidades são analisados e confrontados com as capacidades e intenções do adversário para identificação dos riscos associados e aprimoramento do assessoramento no processo decisório, visando subsidiar o planejamento e adoção das medidas mitigadoras no campo da Segurança Pública e Defesa. Deve ser um esforço sistemático contínuo que depende de informações de inteligência para reduzir as incertezas e propiciar uma avaliação mais precisa, reduzindo a incerteza para não gerar avaliações que sejam meras informações sobre os riscos potenciais.

Atualmente no estudo do risco do terrorismo, onde são estudados eventos de baixa probabilidade e consequências catastróficas, um dos pontos chaves de discussão é a questão da conceituação como uma função de probabilidade e consequência, sendo crescente a abordagem para uma função de interações entre atores adaptativos ou inteligentes.

Diferente dos eventos não desejados causados por ameaças naturais ou sistêmicas (desastres naturais ou falhas mecânicas), os riscos do terrorismo envolvem a ação de adversários inteligentes, capazes de tomar decisões sucessivas conforme as ações mitigadoras, resultando na impossibilidade de serem regidas pelo acaso, mas sim pela intencionalidade e capacidade de adaptação (PARNELL *et al*., 2010, p. 33).

Os adversários inteligentes crescem em importância e criticidade no tema em virtude da sua capacidade adaptativa por meio da observação e percepção racional em face de futuras ações a serem executadas pelas forças de segurança e defesa. A condição adaptativa deve ser considerada com ênfase no desenvolvimento de modelos que forneçam estimativas precisas de risco, reduzindo as incertezas, de modo a apoiar adequadamente a tomada de decisão de gerenciamento de risco (GUIKEMA, 2012, p. 1117).

3.1.1 Terrorismo

Diversas definições de terrorismo podem ser encontradas nas mais diversas áreas de conhecimentos, podendo ser citadas suas ocorrências nos campos da antropologia, sociologia,

psicologia, história, ciências políticas, relações internacionais e criminologia, dentre outros. A evolução e variação histórica de suas ocorrências, os interesses políticos, e o fato de ser objeto de estudo de uma ampla gama de carreiras podem ser elementos geradores da dificuldade de definição do termo, bem como do estabelecimento de uma tipificação penal, não só a nível nacional, mas também internacionalmente.

No campo acadêmico, ilustres doutrinadores escreveram sobre o tema focado nas mais diversas vertentes, sendo destacado apresentar a visão de Crenshaw (1983) *apud* SCHMID e JONGMAN *et al*. (1988, p. 35).

> [...] uma definição básica deve incluir os seguintes atributos: o uso sistemático da violência heterodoxo por pequenos grupos de conspiradores, com o objetivo de manipular as atitudes políticas em vez de derrotar um inimigo fisicamente. A intenção da violência terrorista é psicológica e simbólica, não material. O terrorismo é a violência premeditada e intencional, empregado em uma luta pelo poder político. Como Harold Lasswell definiu: 'Os terroristas são os participantes no processo político que se esforçam para obter resultados políticos, suscitando inquietações agudas'[5] (CRENSHAW, 1983 *apud* SCHMID e JONGMAN *et al*., 1988, p. 35, tradução nossa)

O caráter político também é abordado por Hoffman (2006) que enfatiza o uso do poder conquistado para promoção de mudança política por meio de um sistema de intimidação coercitiva:

> O terrorismo, no mais amplamente aceito uso contemporâneo do termo, é fundamentalmente e inerentemente político. E está vinculado de forma inextricável ao poder: a busca, a conquista e o uso do poder para conseguir mudança política. O terrorismo é, assim, violência – ou igualmente importante, ameaça de violência-, usada e direcionada na perseguição de objetivo político ou a seu serviço[6] (HOFFMAN, 2006).

Trabalhando nos tipos de motivação terrorista, baseados em suas categorias – racional, psicológica e cultural –, Whittaker (2005) *apud* CRENSHAW (1995, p. 40-41) explicita o tocante a forma como se molda, sendo extremamente importante destacar a diferenciação

[5] [...] a basic definition would include the following attributes: the systematic use of unorthodox violence by small conspiratorial groups with the purpose of manipulating political attitudes rather than physically defeating an enemy. The intent of terrorist violence is psychological and symbolic, not material. Terrorism is premeditated and purposeful violence, employed in a struggle for political power. As Harold Lasswell defined it: 'Terrorists are participants in the political process who strive for political results by arousing acute anxieties'.

[6] Terrorism, in the most widely accepted contemporary usage of the term, is fundamentally and inherently political. It is also ineluctably about power: the pursuit of power, the acquisition of power, and the use of power to achieve political change. Terrorism is thus violence - or, equally important, the threat of violence—used and directed in pursuit of, or in service of, a political aim.

primária com a violência criminosa. Fica posteriormente ressaltado o engajamento político de organizações criminosas para através da indução do medo forçar mudanças de comportamento político:

> Os objetivos do terrorismo o distinguem de outros atos violentos destinados ao benefício pessoal, como a violência criminosa. Não obstante, a definição permite a inclusão da violência pelo crime organizado quando ele procura influenciar política de governo. Alguns cartéis de drogas e outras organizações criminosas internacionais se engajam na ação política com a intenção de induzir o medo em outras pessoas, que não suas vítimas, para fazer com que o governo e outros públicos-alvo mudem seus comportamentos políticos (WHITTAKER, 2005 *apud* CRENSHAW, 1995, p. 40-41).

Com base nas definições destaca-se o uso da violência e da força planejados contra população civil, motivações políticas, atos imprevisíveis, cruéis e destrutivos. Sendo importante destacar que a violência serve somente como meio para através da exploração da publicidade atingir seu objetivo final. Fica claro também as ameaças do uso de táticas e técnicas terroristas por organizações criminosas no interesse econômico e não de mudança política.

No contexto sulamericano, fora os inúmeros atentados perpetrados pelos grupos operantes na onda nova esquerda conforme Rapoport (2004), que classifica a ocorrência do terrorismo em ondas, que são ciclos de atividades em dado período de tempo, caracterizado por expansões e contrações, com caráter transnacional e atividades similares ocorrendo em vários países, impulsionada por energia predominante comum que caracteriza os grupos participantes e as relações mútuas.

A onda Anarquista iniciou-se nos idos de 1880, sendo também conhecida por "era de ouro dos assassinatos", onde Theodore Roosevelt lançou o primeiro esforço para eliminar o terrorismo. A onda Anticolonial aconteceu na década de 20 estendendo-se por cerca de 40 anos, sendo caracterizada pelas lutas de independência travadas pelos "guerreiros da liberdade". Em 1960 tem início a onda Nova Esquerda, resultante da bipolarização do mundo e da expansão dos grupos de esquerda com ações de sequestros, sendo que essa ainda possui resquícios na atualidade, como por exemplo, o Sendero Luminoso (Peru) e as Forças Armadas Revolucionárias da Colômbia (Farc). A onda Religiosa surge em 1979, caracterizada pelo extremismo e pela martirização dos terroristas suicidas, ocorrendo como ameaça mais intensa nos dias de hoje conforme Rapoport (2004).

Na Argentina a onda esquerda promoveu atentados em grande escala, sendo caracterizada por violência sangrenta, tanto da parte dos terroristas quanto dos repressores. Um dos grupos, os Montoneros, iniciaram sua campanha assassinando o ex-presidente Aramburu em 1970, vitimaram

inicialmente estrangeiros, e depois foram se voltando contra o Exército, a Polícia, os políticos e os líderes sindicais moderados, causando a morte de muitos inocentes que ocasionalmente estavam nos locais dos atentados de acordo com Whitakker (2005).

Outro ponto relevante que novamente traz a Argentina ao cenário do terrorismo sul-americano, e também mundial, foram os atentados perpetrados contra organizações judaicas na Argentina[7], em 1992 e 1994. Tais eventos aliados ao primeiro atentado contra o World Trade Center em 1993[8], destacam no contexto sul-americano a importância estratégica assumida pela região da Tríplice Fronteira Brasil, e geraram uma securitização na região e nas Américas, onde autoridades americanas identificaram indicativos de uma forma emergente de terrorismo internacional que ameaçava todo o continente, nos moldes do praticado no Oriente Médio.

Além da ocorrência da onda nova esquerda presente no continente sulamericano, ocorreram estes atentados na Argentina vinculados à onda religiosa, que continua como uma das principais ameaças terroristas no cenário mundial atual.

Hoje identificamos como ameaça transnacional contemporânea a convergência entre o terrorismo e o crime organizado, onde os dois atores se associam no interesse de seus objetivos, existindo inclusive a probabilidade da integração de suas ações com um híbrido, gerando grandes preocupações aos Estados.

3.1.2 A convergência entre o crime e o terrorismo

Atualmente as organizações criminosas são capazes de explorar os mais amplos movimentos das pessoas, dos produtos e do dinheiro, graças à evolução tecnológica, através da utilização de modernos sistemas de telecomunicação e da internet. A identificação de tal fato motivou as autoridades europeias, a promover uma reunião em Berlim dos Ministros de Justiça da UE, visando à implantação de cooperação com a finalidade de se estabelecer uma força mais unida e poderosa contra o crime organizado (MONTOYA, 2007, p. 67).

---

[7] Na Argentina, no ano de 1992, a embaixada de Israel foi atacada com artefatos explosivos que vitimaram 29 pessoas e resultou em outras 240 feridas. Dois anos depois, em 1994, ocorreu o maior atentado terrorista registrado no continente, quando a Sede da Associação Mutual Israelita Argentina – AMIA foi palco de uma ação terrorista suicida com a utilização de um carro-bomba, matando 96 pessoas e ferindo outras 300 de diversas nacionalidades. Nesses episódios, que guardam características similares, o grupo libanês Hezbollah[7] foi apontado como autor dos atentados, e levantamentos realizados na época apontaram indícios de que a ação fora planejada na região da Tríplice Fronteira (Paraguai – Brasil – Argentina) (WOLOSZYN, 2010, p. 27).

[8] Atentado com carro-bomba na garagem subterrânea do prédio perpetrado por terroristas islâmicos causando seis mortes e deixando mais de 1000 feridos, e que tinha por objetivo derrubar uma torre pelo comprometimento das fundações para cair sobre a outra. (AMARAL, 2008, p. 155)

Os grupos terroristas estão se associando ao crime organizado, dois fenômenos tradicionalmente separados começaram a revelar semelhanças operacionais e organizacionais, ambos os atores se aproveitam das estruturas individuais e passam a atuar conjuntamente, buscando países onde a estrutura político-social encontra-se instável, conseguindo dessa maneira se infiltrarem nesses estados e por meio de uma simbiose se fortalecer.

> Antes da queda da União Soviética, o terrorismo e o crime organizado transnacional (TOC) foram relegados a "baixa política" e, muitas vezes isolado à esfera doméstica. A emergência posterior de uma elevada transição no ambiente de segurança internacional, muitas vezes colocadas dentro do contexto da globalização e a ascensão de rede não-estatais, desafiou essa percepção. Terrorismo e o TOC, conforme sua evolução desde 1989, podem ser definidos como atores não-estatais capazes de competir pelo controle de funções do Estado e território. A proeminência de violentos atores não-estatais no ambiente de segurança contemporânea, portanto, questiona os pontos de vista tradicionais dominantes em matéria de segurança [ ] que elevam o estado acima de todos os outros atores. Não é possível diretamente explicar e entender as ameaças representadas pelo crime organizado, o terrorismo, ou a sua convergência, uma "nova" estrutura para conceptualização as ameaças à segurança no século XXI tornou-se uma necessidade[9] (MAKARENKO, 2005, p. 385, tradução nossa).

Como exemplo regional podemos citar as Farc, em processo de desmobilização, que ganharam destaque no cenário mundial através da integração intercontinental entre grupos terroristas para treinamento e troca de experiências, financiando a promoção desses intercâmbios através do lucro da droga.

Notadamente, este tipo de ameaça complexa, de natureza racional, diferente dos desastres naturais e falhas mecânicas, demanda um aperfeiçoamento e investimentos no seu estudo de forma a ser contraposta de forma eficiente, para evitar perdas de vidas e danos econômicos.

---

[9] Prior to the fall of the Soviet Union, terrorism and transnational organised crime (TOC) were relegated to 'low politics' and often isolated to the domestic realm. The subsequent emergence of a highly transitional international security environment, often placed within the context of globalisation and the rise of networked non-state actors, has challenged this perception. Terrorism and TOC, as they have evolved since 1989, can be defined as non-state actors capable of competing for control over state functions and territory. The prominence of violent non-state actors in the contemporary security environment thus questions the dominant traditional views on security (i. e. realism) that elevate the state above all other actors. Unable to directly explain and understand the threats posed by organised crime, terrorism, or their convergence, a 'new' framework for conceptualising security threats in the twentyfirst century has become a necessity.

> Ligações entre o IRA e os narco-terroristas do grupo Forças Armadas Revolucionárias da Colômbia [...] foram suspeitas por algum tempo. No entanto, um elemento importante dessa conexão foi estabelecido em agosto de 2001, quando autoridades colombianas prenderam três peritos de explosivos do IRA em circunstâncias suspeitas, em Bogotá. Relatórios de inteligência britânicos estimam que nos últimos anos as FARC pagaram a 'agentes' do IRA 2 milhões de dólares americanos para treinamento de armas, explosivos e técnicas de guerrilha urbana, o uso de contas bancárias 'offshore'; desde 1998, entre cinco e quinze desses peritos ficaram indo e vindo entre a Colômbia e a Europa. Em abril de 2002, o General Tapas Fernando, chefe do Estado-Maior Conjunto Colombiano, testemunhou para o Comitê de Relações Internacionais da Câmara, que na Colômbia sete membros do IRA tinham treinado colombianos, cubanos, iranianos, e talvez combatentes Basco no uso de armas e de inteligência para o propósito terrorista. O IRA e as Farc também pode ter colaborado no fornecimento de armas aos rebeldes na Nicarágua, em 2000[10] (KARAKAN; CURTIS; 2002, p. 6, tradução nossa).

3.1.3 Fontes de ameaça

Ameaça é uma indicação de dano potencial à vida, informação, operações, o ambiente e / ou propriedade, podendo ser uma ocorrência natural ou criada pelo homem. Quando humana inclui capacidades, intenções e métodos de ataques de adversários, usados para explorar circunstâncias ou ocorrências com a intenção de causar dano. Pode referir-se a um indivíduo, organização, ação ou evento e para fins de cálculo de risco, a ameaça de um risco intencional é geralmente estimada como a probabilidade de um ataque ser tentado por um adversário, que engloba tanto a intenção quanto a capacidade adversária. Não existindo a intencionalidade, a ameaça é normalmente estimada como a probabilidade de um perigo se manifestar (DHS, 2017).

Risco pode ser definido como potencial para um resultado indesejado fruto de um incidente, evento ou ocorrência, conforme estimado por sua probabilidade e consequência associadas. Em um aprimoramento, pode ser definido como potencial para um resultado adverso avaliado em função de ameaças, vulnerabilidades e consequências associadas a um incidente, evento ou ocorrência. Seu estudo é focado para comparação de diferentes situações futuras, podendo ser abordado nos níveis estratégico, operacional e tático. No contexto do risco

[10] Links between the IRA and the terrorist narcotics group Revolutionary Armed Forces of Colombia (Spanish initialism FARC) have been suspected for some time. However, a major element of that connection was established in August 2001, when Colombian authorities arrested three IRA explosives experts under suspicious circumstances in Bogota. British intelligence reports have estimated that in recent years the FARC has paid IRA operatives about US$2 million for training in arms, explosives, and techniques of urban warfare, using offshore bank accounts; since 1998, between five and fifteen such experts are believed to have moved back and forth between Colombia and Europe. In April 2002, General Fernando Tapas, chief of the Colombian Joint Chiefs of Staff, testified to the House International Relations Committee that in Colombia seven IRA members had trained Colombian, Cuban, Iranian, and perhaps Basque fighters in the use of arms and intelligence for terrorist purposes. The IRA and FARC also may have cooperated in supplying arms to insurgents in Nicaragua in 2000.

terrorista, a probabilidade de um evento não desejado pode ser analisada com base nas ameaças e vulnerabilidades (DHS, 2010).

Após os ataques do 11 de setembro, diversos organismos internacionais se mobilizaram no reforço das proteções contra ameaças terroristas. No contexto da segurança marítima foi estabelecido o ISPS CODE[11] na conferência de dezembro de 2002 da Organização Marítima Internacional (IMO) como uma emenda à Convenção Internacional para a Salvaguarda da Vida Humana no Mar (SOLAS). O Código determina um conjunto de requisitos para fortalecer as práticas de segurança de embarcações e portos contra o terrorismo, descreve os procedimentos mínimos de segurança que todos os navios e portos devem cumprir para melhorar a segurança marítima em geral. As embarcações que não atendem a esses requisitos de gerenciamento do risco terrorista, ou que saiam de um porto não qualificado no tocante a segurança, podem ter a atracação negada no seu porto de destino (GREENBERG, 2006, p.63-65).

No contexto da aviação civil, o transporte aéreo de passageiros e de carga, sofreu diversas adaptações no tocante a segurança das operações após os eventos ocorridos em 11 de setembro de 2001 nos Estados Unidos da América em face das ameaças crescentes. Neste contexto, um dos impactos no Brasil foi o PNAVSEC[12] que define ameaça como uma intenção declarada de causar prejuízo, dano ou outra ação hostil a alguém, não se restringindo apenas a um evento isolado, podendo ser compreendida como circunstância ou tendência (BRASIL, 2010).

A segurança da aviação civil é ameaçada por atos de interferência ilícita contra a aviação civil, notadamente atos de terrorismo, que a legislação define como ato ou atentado que coloca em risco a segurança da aviação civil e o transporte aéreo, a saber: a) apoderamento ilícito de aeronave em voo; b) apoderamento ilícito de aeronave no solo; c) manutenção de refém a bordo de aeronaves ou nos aeródromos; d) invasão de aeronave, de aeroporto ou das dependências de instalação aeronáutica; e) introdução de arma, artefato ou material perigoso, com intenções criminosas, a bordo de aeronave ou em um aeroporto; f) comunicação de informação falsa que coloque em risco a segurança de aeronave em voo ou no solo, dos passageiros, tripulação, pessoal de terra ou público em geral, no aeroporto ou nas dependências de instalação de navegação aérea; e g) ataque a aeronaves utilizando Sistema Antiaéreo Portátil (BRASIL, 2010).

[11] Código Internacional de Proteção de Navios e Port Facility
[12] Programa Nacional de Segurança da Aviação Civil Contra Atos de Interferência Ilícita (PNAVSEC).

A Abin elenca em seu Método Arena de Análise de Riscos que as “fontes de ameaça” consistem em entidades, grupos de pessoas, fenômeno da natureza ou agente biológico que apresentam potencial de provocar situações de ameaça ao objeto da avaliação de risco (BRASIL, 2015).

O DHS define a avaliação das ameaças da como um esforço sistemático para identificar e avaliar as ameaças terroristas existentes ou potenciais a uma jurisdição e seus ativos. Com base na dificuldade de avaliação precisa das capacidades, intenções e táticas terroristas, essas avaliações podem gerar apenas informações gerais sobre os riscos potenciais, considerando todo o espectro de ameaças, atividades terroristas e criminosas, incluindo também os desastres naturais e acidentes graves (LESON, 2005, p.6).

A partir do estudo das ameaças e vulnerabilidades, probabilidades e impactos, dentre outros critérios, foram desenvolvidos os modelos de análise de risco terrorista de forma a contribuir para a redução da incerteza nas tomadas de decisões e para a governança.

3.1.4 Modelos de análise do risco terrorista

Após os ataques do 11 de setembro nos EUA o terrorismo passou a ser ameaça global, nos anos seguintes ocorreram os grandes atentados na Espanha e Inglaterra, França, Bélgica, Turquia, Rússia, Indonésia, Índia e Paquistão, e diversos outros no continente africano e outros nos EUA, como na Maratona de Boston, São Bernardino e Miami. Notícias diárias reforçam a condição de ameaça transnacional no campo da segurança e defesa, estabilidade e a paz. Estes eventos consolidam o tema como imperativo de ações preventivas com base em estudos de risco e planejamento estratégico para antecipar as ameaças.

As consequências do terrorismo se refletem na sociedade no tocante a sensação de insegurança e do medo da população, no campo político, econômico e militar, sendo motivo de criação na Organização das Nações Unidas de um escritório para ajudar os Estados-membros a implementar a estratégia global da ONU de combate ao terrorismo (ONU, 2018).

A análise do risco terrorista concentra-se em permitir o desenvolvimento de estratégias que mitiguem os riscos por meio da prevenção e proteção física em uma notória combinação de modelos qualitativos e quantitativos em face da natureza multifacetada e complexa do terrorismo. O grande desafio da análise de risco terrorista é a pesquisa no comportamento humano devido a intencionalidade dos atos, os chamados adversários inteligentes, bem como dos resultados extremos da consecução do risco.

As principais abordagens utilizadas pelo DHS para avaliar os riscos do terrorismo com base na avaliação da ameaça incluem análise probabilística de risco (PRA), teoria dos jogos, teoria das possibilidades e métodos “soft scoring risk”. Recentemente a PRA emergiu como abordagem predominante, referindo-se a um grupo de técnicas que modela os possíveis resultados de um evento inicial utilizando árvores de eventos, segundo Winterfeldt (2016).

Atualmente a Análise de Risco Adversário cresce de relevância no meio acadêmico pela abordagem antagônica das ameaças com base em riscos adaptativos como o terrorismo e a sabotagem, podendo ser modelado por meio da otimização ou teoria dos jogos, diferente da análise de risco tradicional onde o risco é estocástico, oriundo de causas naturais ou falhas técnicas (IRGC, 2015, p.6).

Uma abordagem qualitativa atual é o Método Deliberativo para Classificação de Risco de abordagem qualitativa foi desenvolvido para avaliar decisões e prioridades em desastres naturais, eventos terroristas e acidentes graves vem sendo empregado para auxiliar no planejamento estratégico de segurança pelo DHS. O método prioriza as ameaças e perigos físicos decorrentes do terrorismo e outras ameaças intencionais e não intencionais por meio de especialistas de risco conforme Lundberg e Willis (2015).

No contexto da análise de inteligência, o DHS por meio da Federal Management Emergency Agency (FEMA) utilizou um modelo privado desenvolvido pela indústria do seguro, o Modelo de Terrorismo Probabilístico estimando os riscos do macroterrorismo baseados em cenários de ataques específicos para comparar e avaliar os riscos em diferentes áreas urbanas no intuito de direcionar análises no contexto da proteção das infraestruturas e decisões de alocação de recursos dentro do programa Iniciativa de Segurança de Área Urbana(UASI) (WILLIS, 2007, p. 13-14).

A análise de risco surge como ferramenta fundamental para dar suporte ao desenvolvimento de ações, programas e políticas públicas no campo do antiterrorismo oferecendo conhecimento de alto valor agregado aos decisores como forma de assessoramento estratégico.

3.1.5 O emprego da análise de risco na inteligência estratégica

Os dias atuais carregam em si a incerteza resultante da quantidade de informações disponíveis para amparar decisões nos mais diversos níveis organizacionais. A integração dessas informações e a produção de um conhecimento mais confiável são fatos necessários para

permitir que sejam tomadas decisões embasadas, garantindo segurança aos tomadores de decisão e às organizações no seu desenvolvimento futuro.

Segundo o *Department of Homeland Security* (DHS[13]), o gerenciamento de riscos é o processo de identificação, análise, avaliação e comunicação dos riscos, através da sua aceitação, evitação, transferência ou controle a um nível aceitável, considerando os custos associados e benefícios de quaisquer ações tomadas (DHS, 2011, p. 7). A gestão de riscos surgiu de maneira mais eficiente agregando valor no assessoramento ao processo decisório quando elaborada com base no Ciclo da Produção do Conhecimento de Inteligência e suas técnicas acessórias.

A análise de risco (AR) é a técnica capaz de antecipar ameaças e oportunidades, proporcionando às organizações a capacidade de agir preventivamente evitando perdas ou maximizando o sucesso. Através da compreensão da natureza do risco e da determinação de seu nível, baseado em critérios de probabilidade e da estimativa dos impactos resultantes do acontecimento de um evento, é possível apresentar ações que mitiguem os riscos inerentes e auxiliem na condução de resultados positivos, de forma a subsidiar a tomada de decisão em nível estratégico conforme Albuquerque e Andrade (2014) "A tecnologia e a inovação devem ser elementos constituintes dos processos modelados para robustecer a tomada de decisão".

3.1.6 Sistemas de informações e novas tecnologias

Dentro do contexto de sociedade da informação entramos em uma nova era, a do *big data*. Segundo Choi e Lambert (2017), uma quantidade massiva de dados está disponível e o avanço das tecnologias de informação permitem que sejam desenvolvidas soluções analíticas para atender ao processo decisório e subsidiar a tomada de decisões. Sua utilização inteligente pode atuar de forma a reduzir a incerteza como o uso de algoritmos, *machine learning* e inteligência artificial gerando análises preditivas.

Um sistema integrado de apoio à decisão possibilita um assessoramento estratégico às políticas públicas de governo, trabalhando de forma sistemática e integrada as informações e eventos, de modo a subsidiar a tomada de decisão, buscando antecipar cenários e tendências que possam gerar eventos não desejados.

[13] Responsável pelo Gerenciamento de Riscos de Infraestruturas Críticas, Autoridade e de Eventos Nacionais nos Estados Unidos, efetivando inclusive convênios com Universidades para criação do National Center for Risk and Economic Analysis of Terrorism Events – CREATE.

Eventos terroristas são altamente imprevisíveis, e tem o impacto potencializado pela surpresa empregada. O desenvolvimento de novas tecnologias torna-se imperativo, especificamente de sistemas de decisão capazes de reduzir as incertezas e prover a adequada análise de risco integrando a análise de dados em massa. Segundo Toure e Gangopadhyay (2016), prover novas soluções tecnológicas capazes de atender a velocidade das decisões pode ser o diferencial para reduzir a distância entre os atores envolvidos, garantindo maior capacidade de se tomar a melhor decisão.

A utilização do *big data* pode permitir que seja obtidas estimativas quantitativas de probabilidade, frutos da análise de grande massa de dados, gerando resultados mais robustos do que as qualitativas baseadas nos dados, se tornado um diferencial e permitindo a combinação de técnicas para as melhores projeções de cenários e análises consolidadas. O homem mantém seu papel primordial no desenvolvimento da inteligência das análises e empregando as máquinas para ampliação da capacidade analítica.

3.2 REVISÃO DA LITERATURA

Como resultados dos ataques do 11 de setembro de 2001 no contexto norte-americano, o país se tornou o responsável pela mudança no pensamento e abordagem do risco terrorista em nível mundial, por meio de estudos e aplicações nas políticas públicas e na consecução de seus objetivos estratégicos nacionais por meio do DHS. O departamento tem por tarefa identificar e priorizar os riscos - compreender a ameaça, a vulnerabilidade e as consequências, para então aplicar os recursos de maneira econômica[14]. A filosofia de gestão de risco do DHS e outras atividades para desenvolver abordagens, modelos e ferramentas de avaliação e gerenciamento de riscos apropriados fazem parte da estratégia de gerenciamento de risco do Departamento por meio do Escritório de Análise e Gerenciamento de Risco, cuja finalidade é garantir que informações e análises de risco sejam fornecidas para informar uma ampla gama de decisões sobre segurança interna[15] (KEENEY, WINTERFELDT, 2011, p.1470-1471).

A estrutura de avaliação e gerenciamento de riscos, conforme inclui a estimativa dos riscos que são enfrentados com o terrorismo e os necessários investimentos para mitigação, que pautam as ações de prevenção e combate ao terrorismo. Sua estimativa baseia-se no estudo: da

[14] Michael Chertoff então secretário do Departamento de Segurança Interna dos EUA (DHS) em 2007.

[15] Janet Napolitano, secretária do DHS seguinte.

ameaça, pela probabilidade dos tipos e alvos de ataques, e a adoção de contramedidas preventivas e dissuasivas para redução da ameaça; da vulnerabilidade, com base na probabilidade de sucesso do ataque ou tentativa e a redução com contramedidas; das consequências dos ataques e tentativas, onde se inclui a perda de vidas e os impactos econômicos diretos e indiretos, em caso de sucesso do atacante e administração das consequências para redução dos impactos; e alocação de recursos orçamentários para políticas e ações de combate ao terrorismo (ibid).

A ameaça e a vulnerabilidade podem ser tratadas com ferramentas como a análise de risco probabilística, suportadas por desenvolvimentos de pesquisas no campo, e o tratamento das consequências e os custos devem se pautar como reflexo dos valores e preocupações da nação, por meio dos objetivos estratégicos e da estratégia nacional de contrainteligência. Estes objetivos devem refletir os valores da população e sua concordância, mesmo que tenham que limitar liberdades civis em prol da redução do risco e capacidade de administrar as consequências, servindo de meio de unificação da nação e do DHS estabelecendo uma estrutura de valores comuns (KEENEY, WINTERFELDT, 2011).

A compreensão do conceito do risco terrorista é parte primordial no estudo de uma avaliação de risco profissional, baseada em um conjunto de critérios que permitam o desenvolvimento conforme a perspectiva da abordagem. As abordagens baseadas na probabilidade e consequência devem ser empregadas com cautela por não refletirem de forma completa as ameaças e ataques, consequências e as incertezas em um contexto de adaptação pelos adversários, ou seja, as interações entre indivíduos e organizações. Estes três componentes devem constituir os principais pilares do conceito do risco de terrorismo, para ser possível o desenvolvimento de métodos para avaliar o risco, identificando um conjunto de ameaças, ataques e medidas de consequências associados aos possíveis cenários de resultados, juntamente com uma descrição das incertezas e interações entre os adversários conforme Aven e Guikema (2015).

Abordando o modelo do DHS pós 9-11, Leson (2005, p.6-9) elenca que o processo de inteligência é a base da avaliação de ameaças. A exploração sistemática da informação relacionada com o crime pode conduzir e apoiar a avaliação e análise do terrorismo e grupos terroristas de forma confiável. O esforço da inteligência deve permitir o monitoramento continuo das ameaças enfrentadas pela instituição governamental e as evoluções de cenários. Como dados essenciais para compor a análise da ameaça do adversário cita os tipos, categorias,

objetivo, efetivos, meta, ações de planejamento, momentos críticos, técnicas e táticas, e a capacidade.

As ações para busca destas informações devem ser fruto de um esforço conjunto, independente de efetivo, com base no comprometimento, ações internas e externas, inclusive por operações de inteligência, bem como a capacitação do efetivo para análise, identificação de alvos, modelagem e tarefas acessórias. O cálculo dos níveis da ameaça será baseado nas combinações dos fatores presentes: existência, capacidade, intenção, história, direcionamento, e ambiente de segurança (ibid).

Cornell e Guikema (2002, p.2) abordando modelagem probabilística de ameaças terroristas apresentam um modelo global simples do espectro das ameaças terroristas baseado na análise e probabilidade de sistemas, que visa trabalhar as informações disponíveis e projetar as ligações nos diferentes, permitindo a classificação das ameaças em várias dimensões de consequências de ataques sofridos e a avaliação das medidas mitigadoras.

Destaca que em condições onde dados históricos são limitados, como na modelagem da ameaça terrorista, a ênfase deve ser direcionada para a estrutura do modelo analisado e para o raciocínio, e não nos valores numéricos, visando identificar os parâmetros mais críticos de maior valor para informações adicionais. Desta forma, as principais variáveis de um modelo global são: os diferentes grupos ou indivíduos que podem ser potenciais perpetradores (por exemplo, grupos fundamentalistas islâmicos), os objetivos desses grupos (e o peso dos diferentes atributos dos objetivos em suas preferências e trade-offs), os meios à sua disposição (material, habilidades, dinheiro e meios de comunicação), a natureza das ameaças potenciais (nucleares, biológicas, convencionais, etc.), as diferentes classes de alvos (por exemplo, edifícios, redes, indivíduos ou grupos de indivíduos), e os meios de entrega (por exemplo, navios ou aviões) (CORNELL, GUIKEMA, 2002, p. 5-7).

Além das variáveis referenciadas que descrevem os potenciais grupos terroristas, seus meios e suas intenções, o modelo inclui: as informações de inteligência coletadas pelos EUA e seus aliados; as contramedidas subsequentes; e o nível resultante de dano causado um ataque total ou parcialmente bem-sucedido. Desta maneira as variáveis chaves do modelo global são os grupos mais propensos a planejar um ataque, a estratégica destes grupos e os tipos de ataques praticados e possíveis (ibid).

A análise de risco probabilística (PRA) é usada a mais de 30 anos de forma relevante na avaliação de riscos e para pautar decisões no governo e na indústria no tocante ao gerenciamento de riscos em diversas áreas: ambiental, médica e segurança industrial. A aplicação no campo

do risco terrorista é recente por meio da abordagem com diversas ferramentas como árvores de eventos, árvores de falhas e árvores de decisão (EZELL *et al*., 2010; PATÉ-CORNELL, 2007). A grande pauta da discussão e o desafio é a sua modelagem para aplicação com adversários inteligentes que podem se adaptar face as ações defensivas planejadas, diferentes das ameaças naturais ou oriundas de falhas de sistemas tecnológicos.

Na análise de risco probabilístico (PRA), os perigos incertos foram modelados usando distribuições de probabilidade para ameaças, vulnerabilidades e consequências. Os dados foram obtidos a partir de análises estatísticas de eventos passados, testes, modelos, simulações e avaliações de especialistas no assunto (SME). Os analistas de risco têm usado técnicas de PRA, incluindo árvores de eventos, árvores de falhas, árvores de ataque, dinâmica de sistemas e modelos de Markov, para avaliar, comunicar e gerenciar o risco de perigos incertos (EZELL *et al*., 2010; PATÉ-CORNELL, 2007).

Parnell *et al.* (2010, p.33-35) em um modelo de gerenciamento do risco do bioterrorismo baseado no risco adversário, destaca que estudando adversários inteligentes a intenção do adversário deve ser considerada porque suas ações futuras com base em nossos preparativos serão derivadas dos seus objetivos e de suas capacidades os atingir, vindo a ser reveladas em um cenário dinâmico. Nesse contexto defende que modelar os objetivos proporcionará uma visão mais ampla das possíveis ações do adversário a fim de considerar a intente do adversário. Modelar os objetivos do adversário fornecerá uma visão mais ampla das possíveis ações dos oponentes, em vez de trabalhar exaustivamente nas probabilidades das possíveis ações. Enfatiza que a intenção adversária (probabilidade de decisões) deve ser uma saída e não entrada para modelos de análise de risco.

O desenvolvimento de ferramentas práticas e de teorias para analisar o cálculo estratégico de adversários inteligentes atuando em cenários com resultados aleatórios cresceu em interesse com a aplicação do tema no contraterrorismo, segurança cibernética e decisões complexas. No contexto do contraterrorismo são abordados alguns modelos: simultâneos de ataque e defesa, sequenciais de defesa, ataque e defesa e sequenciais de ataque a defesa com informações privadas. O termo análise de risco adversário é usado para descrever abordagens cuja solução é obtida por meio de um modelo bayesiano como função das capacidades, probabilidades e utilidades usadas pelo oponente em sua análise (INSUA *et al.*, 2016, p. 742; RIOS; INSUA, 2012, p.1)

INSUA *et al.* (2016) descreve que na ARA, a finalidade é dar suporte a parte que empregará uma abordagem analítica de decisão para solucionar seu problema de tomada de

decisão. Com base nisto, é necessário prever a ação das outras partes, e com base na sua própria estratégia, os resultados derivados para si e para os adversários. Não se trata de um novo método de solução, podendo ser definido como uma abordagem bayesiana da teoria dos jogos, tendo sido proposto, não-construtivamente, por Kadane e Larkey[16] e Raiffa[17].

O Método Deliberativo para Classificação de Riscos, ou Método de Classificação de Riscos Carnegie Mellon, foi desenvolvido para tratar de questões incertas na política ambiental na década de 70, quando se concluiu que os riscos ambientais eram analisados com base em percepções, de forma não sistemática, ao invés de se considerar o risco real. Com base nisto, Morgan *et al.* (1996) propuseram uma estrutura para um método de classificação de risco com atuação de representantes das partes interessadas por meio de um processo sistemático com múltiplas estimativas quantitativas e qualitativas de consequência (LUNDBERG, WILLIS, 2016, p.5-6).

O Método Deliberativo para Classificação de Riscos caracteriza-se por cinco etapas: 1) identificação dos riscos a serem classificados; 2) identificação dos atributos necessários para descrição dos riscos; 3) descrição de cada um dos riscos selecionados em termos dos atributos; 4) seleção dos participantes e realização da classificação de risco e; 5) análise dos resultados identificando as questões destacadas nos rankings resultantes (ibid).

Lundberg e Willis (2015) apresentam uma avaliação comparativa dos riscos de segurança interna, com base nas recomendações do painel da Academia Nacional de Ciências (NAS)[18] que orientou que o DHS empregasse métodos de avaliação comparativa de riscos qualitativos como parte de sua abordagem ao planejamento estratégico. No estudo foram comparados dez perigos, incluindo desastres naturais, terrorismo e acidentes graves, com base em um conjunto estabelecido de atributos com ênfase nos riscos de saúde, econômicos, sociais, ambientais e governamentais. Destaca que há uma variedade de técnicas que podem ser úteis para a comparação de todos os riscos, incluindo o Analytic Hierarchy Process, técnica de análise de risco multicritério e outras.

[16] Kadane J, Larkey B. Subjective probability and the theory of games. Management Science, 1982; 28:113–120.
[17] Raiffa H. The Art and Science of Negotiation. Harvard University Press, Cambridge, MA, 1982; Raiffa H, Richardson J, Metcalfe D. Negotiation Analysis: The Science and Art of Collaborative Decision. Cambridge, MA: Harvard University Press, 2002.
[18] A Academia Nacional de Ciências (NAS) é uma sociedade privada, sem fins lucrativos, de acadêmicos ilustres. Estabelecido por um Ato do Congresso, assinado pelo Presidente Abraham Lincoln em 1863, a NAS é encarregada de fornecer conselhos objetivos e independentes à nação norte-americana em assuntos relacionados à ciência e tecnologia.

A construção de modelos baseados em eventos são fruto de uma análise detalhada das consequências de cenários de ataque específicos, incluindo a análise de sensibilidade dos parâmetros que afetam as consequências. Vários componentes podem ser incluídos para modelagem dos eventos e dos alvos, considerando especialistas para julgamentos de probabilidade e consequência. O ponto forte do modelo são os detalhes e o fraco são as muitas estimativas para atingir o detalhamento na análise (WILLIS, 2006, p.25).

O RMS (Terrorism Risk Model) é um exemplo de modelo baseado em evento que foi desenvolvido como uma ferramenta para as indústrias de seguros e resseguros avaliarem os riscos do macroterrorismo[19]. O risco é abordado como uma função de cenários de ameaças específicas e vulnerabilidades, cálculo das consequências anuais esperadas (humana e econômica) de diversas ameaças terroristas e avaliações da probabilidade relativa de diferentes tipos de ataques a diferentes alvos, por meio do julgamento de especialistas incluindo a abordagem à capacidade da ameaça e propensão à múltiplos ataques coordenados (ibid).

3.2.1 Análise crítica e a contribuição para a pesquisa acadêmica nacional

Como resultados dos ataques do 11 de setembro de 2001, os EUA conduziram a mudança no pensamento e abordagens ao risco terrorista em nível mundial, desenvolvendo estudos e programas que contribuem para a formulação de estratégias e políticas públicas na prevenção e repressão ao terrorismo de forma a contribuir para a não ocorrência deste tipos de eventos que resultam em grandes perdas político-econômicas e de civis inocentes (KEENEY, WINTERFELDT, 2011, p.1470-1471).

O emprego da gestão de risco por meio de modelos apropriados, frutos de investimentos em pesquisa científica nas universidades americanas, por meio de centros de excelência do DHS, fazem parte de uma estratégia que tem por finalidade fortalecer a tomadas de decisões no campo da segurança interna e preparar gerações futuras para este enfrentamento.

Os principais pilares do conceito do risco de terrorismo devem ser constituídos de três componentes a fim de tornar possível o desenvolvimento de métodos para avaliar o risco, identificando um conjunto de ameaças, ataques e medidas de consequências associados aos possíveis cenários de resultados, juntamente com uma descrição das incertezas e interações entre os adversários conforme Aven e Guikema (2015).

[19] O RMS define macroterrorismo como ataques capazes de causar (1) perdas econômicas superiores a US $ 1 bilhão, ou (2) mais de 100 fatalidades ou 500 feridos, ou (3) danos maciçamente simbólicos.

Abordando o modelo do DHS pós 9-11, Leson (2005, p.6-9) elenca que o processo de inteligência é a base da avaliação de ameaças. A exploração sistemática da informação relacionada com o crime pode conduzir e apoiar a avaliação e análise do terrorismo e grupos terroristas de forma confiável. O esforço da inteligência deve permitir o monitoramento continuo das ameaças enfrentadas pela instituição governamental e as evoluções de cenários.

Cornell e Guikema (2002, p.2) abordando modelagem probabilística de ameaças terroristas apresentam um modelo global simples do espectro das ameaças terroristas baseado na análise e probabilidade de sistemas. As variáveis são os grupos mais propensos a planejar um ataque, a estratégica destes grupos e os tipos de ataques praticados e possíveis, de forma a classificar as ameaças em várias dimensões de consequências de ataques sofridos e a avaliação das medidas mitigadoras.

A análise de risco probabilística (PRA) é usada a mais de 30 anos de forma relevante na avaliação de riscos e para pautar decisões no governo e na indústria no tocante ao gerenciamento de riscos em diversas áreas: ambiental, médica e segurança industrial, sendo recente sua aplicação no campo do risco terrorista por meio da abordagem com diversas ferramentas como árvores de eventos, árvores de falhas e árvores de decisão (EZELL *et al*., 2010; PATÉ-CORNELL, 2007).

Parnell *et al.* (2010, p.33-35) em um modelo de gerenciamento do risco do bioterrorismo baseado no risco adversário, destaca que estudando adversários inteligentes a intenção do adversário deve ser considerada porque suas ações futuras com base em nossos preparativos serão derivadas dos seus objetivos e de suas capacidades os atingir, vindo a ser reveladas em um cenário dinâmico. A modelagem dos objetivos oferece uma melhor visão da intente do adversário, enfatizando que a intenção adversária (probabilidade de decisões) deve ser uma saída e não entrada para modelos de análise de risco.

Lundberg e Willis (2015) apresentam uma avaliação comparativa dos riscos de segurança interna qualitativa como parte de sua abordagem ao planejamento estratégico. A construção de modelos baseados em eventos são fruto de uma análise detalhada das consequências de cenários de ataque específicos, incluindo a análise de sensibilidade dos parâmetros que afetam as consequências (WILLIS, 2006, p.25).

Nesse contexto, os modelos apresentados visam mitigar os possíveis impactos de um ataque aprimorando defesas e desenvolvendo a resiliência. A capacidade de administrar as consequências é fortalecida por meio de reações ativas e respostas às emergências, baseadas em planos de contingência e exercícios, treinamento e outras preparações para eventos não

desejados. A superação do evento e a conseguinte recuperação devem ser suportadas pelas ações necessárias para que empresas e governo retomem suas operações de forma eficiente baseados em programas previamente planejados derivados das análises de risco terrorista.

A grande pauta da discussão dos modelos probabilísticos e o desafio a ser enfrentado é a sua modelagem para aplicação com adversários inteligentes que podem se adaptar face as ações defensivas planejadas, diferentes das ameaças naturais ou oriundas de falhas de sistemas tecnológicos.

A análise de risco adversário é uma abordagem cuja solução é obtida por meio de um modelo bayesiano como função das capacidades, probabilidades e utilidades usadas pelo oponente em sua análise.

A construção de modelos qualitativos baseados em eventos pode incluir vários componentes na modelagem dos eventos e dos alvos, considerando especialistas para julgamentos de probabilidade e consequência. O ponto forte do modelo são os detalhes e o fraco são as muitas estimativas para atingir o detalhamento na análise. O RMS é um exemplo de modelo baseado em evento que foi desenvolvido como uma ferramenta para as indústrias de seguros e resseguros avaliarem os riscos do macroterrorismo.

Conforme apresentado, existem subsídios que podem fomentar um embrião de pesquisa em assunto tão relevante no cenário mundial: o risco terrorista. O cenário atual com as interações entre o crime organizado e o terrorismo na América do Sul, permite que a academia brasileira explore tais eventos e cenários de risco, que tem potencial de impactar tanto em território nacional como em outros continentes. Os principais modelos apresentam condições de serem aplicados em estudos no Brasil, bem como contribuir para antecipação de cenários e produção de conhecimento estratégico.

4 METODOLOGIA

Neste capítulo é apresentada a metodologia abordada no presente trabalho expondo sua posição segundo seu objetivo, classificação, natureza e dados, além de descrever detalhadamente os processos da revisão da literatura.

A pesquisa é classificada em relação ao objetivo como exploratória. Segundo Turrioni e Mello (2012), a pesquisa exploratória visa proporcionar maior entendimento do problema, com vistas a torná-lo compreensível ou a construir hipóteses, por meio de levantamentos bibliográficos, e análise de exemplos que fomentem a compreensão.

Quanto a forma de abordagem a pesquisa é classificada como quantitativa. De acordo com Turrioni e Mello (2012), a abordagem quantitativa considera que tudo pode ser quantificável, o que significa traduzir em números opiniões e informações para classificá-las e analisá-las. Empresa recursos e técnicas capazes de permitir a mensurabilidade, causalidade, generalização e replicação. Distingue-se da qualitativa pela ênfase da estruturação da pesquisa, em oposição ao foco na perspectiva do indivíduo.

Em relação aos dados é definida como uma pesquisa bibliográfica, onde uma Revisão Sistemática da Literatura (*Systematic Literature Review* – SLR) sobre o tema análise de risco terrorista foi estruturada, contemplando artigos publicados em periódicos e revistas indexados nas bases *Web of Science*®– Coleção Principal (*Thomson Reuters Scientific*) da plataforma Capes. O detalhamento da SLR é apresentado no subitem 4.1 a seguir.

4.1 CONCEITUAÇÃO DA REVISÃO SISTEMÁTICA DA LITERATURA

Uma revisão sistemática da literatura é um meio de identificar, avaliar e interpretar toda a pesquisa disponível relevante para determinada questão de pesquisa, área ou fenômeno selecionado. Uma revisão sistemática é uma forma de estudo secundário, fruto da contribuição de outros estudos de comprovada relevância, os estudos primários (KITCHENHAM, 2004, p.1).

As principais motivações para as revisões sistemáticas segundo Kitchenham (2004) são: resumir as evidências empíricas dos benefícios e limitações de um método ágil específico; identificar lacunas em pesquisas atuais a fim de apresentar áreas para desenvolvimento adicional; subsidiar e fornecer uma base, contexto ou referências para início de novas

pesquisas; analisar a relação de sustentação entre evidências empíricas e hipóteses teóricas ou gerar novas hipóteses.

Realizar uma revisão sistemática envolve várias atividades distintas, que podem ser agrupadas em três fases principais: planejamento; realizar a revisão; e relatar a revisão. Destaca-se as principais etapas na literatura que conduziram esta revisão conforme as três fases respectivamente: elaborar as perguntas de pesquisa, criar o protocolo de revisão e validar o protocolo; identificar as pesquisas relevantes, selecionar os estudos primários, avaliar as qualidades dos estudos, extrair os dados necessários, e sintetizar os dados; escrever um relatório da revisão sistemática e validar o relatório (BRETON *et al.*, 2007).

4.2 FORMULAÇÃO DAS QUESTÕES DE PESQUISA

A atividade mais importante durante o planejamento do protocolo de planejamento é formular a questão de pesquisa segundo Kitchenham (2004). Sua modelagem permitirá que sejam atingidos os objetivos estabelecidos de forma que os resultados encontrados contribuam para o refinamento das análises, gerando conexão e aderência ao tema.

As questões de pesquisa buscam definir o interesse do pesquisador por meio da delimitação da pesquisa, abrangência na base existente, e identificação de tendências para trabalhos futuros (KITCHENHAM, 2004, p.1).

Esta revisão sistemática busca responder questões no interesse da pesquisa, ou seja, identificar as atividades de pesquisa desenvolvidas por meio de uma análise histórica e conjugá-la com as tendências de pesquisas atuais olhando para o futuro, de forma a identificar bases de pesquisas e encaixar o tema no atual espaço temporal de produção de conhecimento (KITCHENHAM, 2004, p.6).

Esses elementos vão permitir que seja compreendido a evolução do desenvolvimento da temática, inclusive com comparações a linhas temporais de eventos não desejados ocorridos e decisões subsequentes, que contribuem para a construção desse lastro utilizado na formação do convencimento para a tomada de decisão e no desenvolvimento de políticas públicas.

As perguntas tem como objeto: a identificação da evolução da quantidade de publicações e suas citações; as áreas de pesquisa que refletem as pesquisas no tema ameaças inteligentes no tocante a citações e organizações; a influência de autores e periódicos; a análise das principais palavras-chaves por meio da análise bibliométrica; a influência dos critérios nas análises de riscos; os principais modelos de abordagem ao risco terrorista para adversários inteligentes; as

tendências para a pesquisa que podem contribuir no interesse nacional; e os modelos de abordagem estratégica ao risco terrorista que podem contribuir com o desenvolvimento das atribuições constitucionais da Polícia Federal.

As questões de pesquisa são apresentadas no tópico abaixo e serão aprofundadas no capítulo seguinte.

4.2.1 Questões de pesquisa

Seguem questões de pesquisa que serão detalhadas no capítulo 5:

- Como a análise do risco terrorista evoluiu em termos do número de trabalhos publicados e aumento de citações?
- Em que áreas de pesquisa e aplicações de campo a abordagem a ameaças inteligentes no contexto do risco terrorista é predominante para citações e organizações?
- Quais autores e periódicos mais influenciaram o desenvolvimento do tema de pesquisa?
- Quais as principais palavras-chaves encontradas por meio da análise bibliométrica?
- Qual a influência dos critérios selecionados no resultado de uma análise de risco de terrorismo?
- Quais os modelos principais de abordagem ao risco terrorista para os adversários inteligentes?
- Quais são as tendências da pesquisa para as ameaças inteligentes mais relevantes no cenário atual que podem impactar no cenário nacional causando perdas e danos?
- Quais os modelos de abordagem estratégica do risco terrorista que podem ser aplicados no contexto nacional de forma a fortalecer as estratégias nacionais de consecução dos objetivos estratégicos com ênfase nas atribuições da PF como Polícia Judiciária, Marítima, Aeroportuária e de Fronteiras?

4.3 PLANEJAMENTO DA REVISÃO

O desenvolvimento das palavras-chaves relacionadas ao assunto e objetivo desta revisão foi dado pelos termos primários “terrorismo” e “análise de risco”. Com base nos termos apresentados na Tabela 1, foi realizada uma pesquisa inicial nos idioma português e inglês no

campo “todos os campos”[20] e por meio de termos exatos, buscando a intensidade das publicações em cada idioma, onde foi atingido um resultado que demonstra a fraca exploração do tema no contexto nacional e inviabiliza a pesquisa em português, determinando a imperativa necessidade da busca no idioma inglês em virtude da análise das ocorrências nos resultados de pesquisas.

Tabela 1 - Resultados da pesquisa inicial

Termos	**Ocorrências**
“terrorismo”	24
“terrorism”	20.517
"análise de risco*"	2
“risk analysis”	23.307
“risco terrorista”	0
“terrorism risk”	152
“terrorismo” *AND* “análise de risco”	0
“terrorism” AND “risk analysis”	313

Fonte: o Autor (2019).

A partir desta primeira abordagem foram determinados dois grupos de palavras chaves, onde o primeiro se relaciona ao contexto do terrorismo (T) e o segundo a abordagem ao risco (R) Inicialmente, dois grupos de palavras-chave foram formados, com 34 e 27 ocorrências. As palavras foram resultado de cruzamento entre brainstorms, material das disciplinas do curso, pesquisas em publicações, dicionários técnicos, e outras fontes abertas. Das palavras selecionadas inicialmente, foram excluídas *“security’, “hazard” e “attack”.*

Os dois grupos de palavras com protocolo validado são apresentados na Tabela 2, sendo que para a pesquisa no *Web of Science* foram formados expressões resultantes da interação entre os dois grupos por meio de operadores de lógica booleana *“AND”*, resultantes da equação lógica, onde um termo do primeiro grupo foi combinado com o termo do segundo grupo,

20 Nota explicativa no WoS: Informe os termos de tópicos para pesquisar os seguintes campos em um registro: Tópico (Título, Resumo, Palavras-chave, Keywords Plus); Autor, Editor, Autoria compartilhada, Autor grupo; Identificador de autor; Nome da publicação; DOI; Ano da publicação; Endereço; Organização-aprimorada; Conferência; Idioma; Tipo de documento; ISSN; Agência financiadora; Texto sobre financiamento; Número do subsídio; e Número de acesso.

gerando uma total de 918 expressões contendo os grupos de palavras chaves, como por exemplo: *(“risk analy*”) AND (“homeland security”))*.

Tabela 2 - Protocolo validado (grupos de palavras chaves)

Conjunto de palavras chaves relacionadas ao Terrorismo	Conjunto de palavras chaves relacionadas à abordagem ao risco
“homeland security”, “terroris”, “bioterroris*”, “counterterroris*”, “islami* terroris*”, “cyberterroris*”, “lone wolf terroris*”, “narcoterroris*”, “single-issue terroris*”, “homegrow* terroris*”, “grass-roots terroris*”, “grassroots terroris*”, “radicalizat*”, “sectarism”, “extremis*”, “suicid* attack*”, “terroris* attack”, “terroris* research*”, “terroris* risk”, “terroris* threat*”, “terroris* value*”, “organiz* crim*”, “criminal organization*”, “crime-terror”, “crime-terror continuum”, “cartel”, “mafia”*	*“risk analy*”, “threat analy*”, “terroris* analysis”, “risk assessment*”, “threat assessment*”, “risk evaluat*”, “threat evaluat*”, “estimat* risk”, “risk management*”, “risk perception*”, “risk mitigat*”, “risk model*”, “risk research*”, “risk value*”, “risk* identif*”, “risk-based”, “probabilistic risk”, “quantitative risk assessment*”, “quantiativ* method*”, “qualitative* risk assessment*”, “qualitativ* method*”, “security evaluatio*”, “security assessment*”, “securit* analy*”, “severit* index*”, “decision analysis”, “decision theory”, “operational research”, “multicriteria”, “multi-criteria”, “VFT”, “value-focused thinking”, “risk value”, “uncertaint*”*

Fonte: O Autor (2019).

4.4 CONDUÇÃO DA REVISÃO

As simulações de pesquisas vieram sendo realizadas no final do segundo semestre de 2018 e os dados foram coletados em fevereiro de 2019. A escolha do período teve como referencial os acontecimentos do 9-11 nos Estados Unidos da América onde quase 3.000 pessoas morreram vítimas de atentados terroristas e que gerou um prejuízo global na casa dos 250 bilhões de dólares.

Foram coletados apenas artigos em inglês da coleção principal do Web of Science, uma plataforma de pesquisa para acesso a bases de dados bibliográficas com um serviço de indexação de citações por meio de assinaturas online gerido pela *Thomson Reuters*, anteriormente conhecida como *ISI Web of Knowlegde.*

O escopo da pesquisa abrange a porcentagem por tópicos com base nas palavras chaves identificando a intensidade de ocorrência na área de pesquisa “Categorias do *Web of Science*”. A equação lógica final foi aplicada na coleção principal do *Web of Science*, para o “período

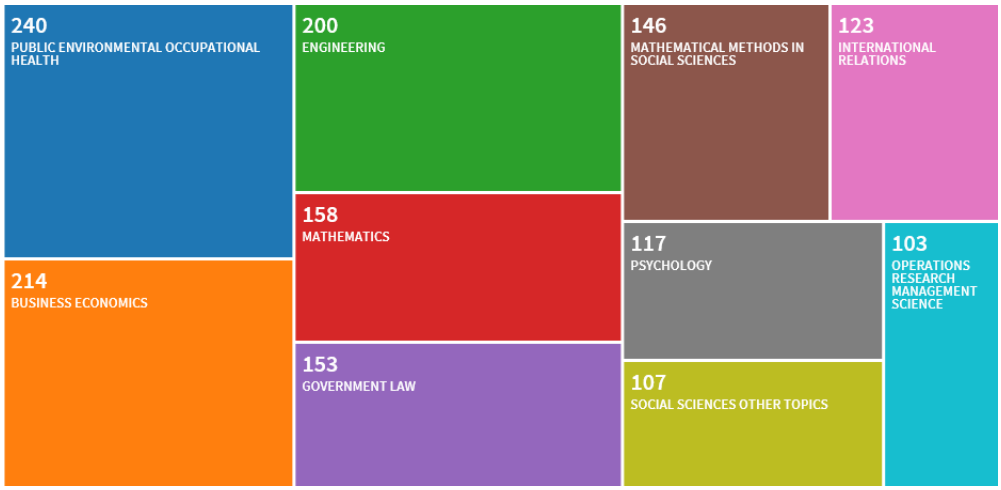
personalizado" de 2001 a 2018, refinada pela busca somente de artigos científicos em inglês, excluindo-se os demais "tipos de documentos" e idiomas, tendo sido encontrados 1.480 artigos de 745 periódicos com o conjunto de palavras chaves com base no filtro *Topic* (TS) conforme apresentado na Figura 1.

Figura 1 - Publicação por ano (2001-2018)

Fonte: O Autor (2019).

Nesta análise da produção no contexto da mesma busca sobre o tema em relação as áreas, encontramos periódicos publicados em 106 áreas distintas, destacados graficamente na Figura 2. Os artigos quando classificados pela plataforma são enquadrados em mais de uma área e categoria do *WoS*.

Figura 2 – Concentração de artigos nas áreas de pesquisa



Fonte: O Autor (2019).

Nesta análise da produção em relação aos periódicos, encontramos as publicações em 745 periódicos com o conjunto de palavras chaves com base no filtro *Topic* (TS) conforme apresentado na Figura 3. Destaca-se o periódico *Risk Analysis*, publicada em nome da *Society for Risk Analysis*, que aborda pesquisas empíricas e serve de ponto focal para o tema, ranqueada entre as 10 principais revistas do *ISI Journal Citation Reports*, nas categorias ciências sociais e métodos matemáticos.

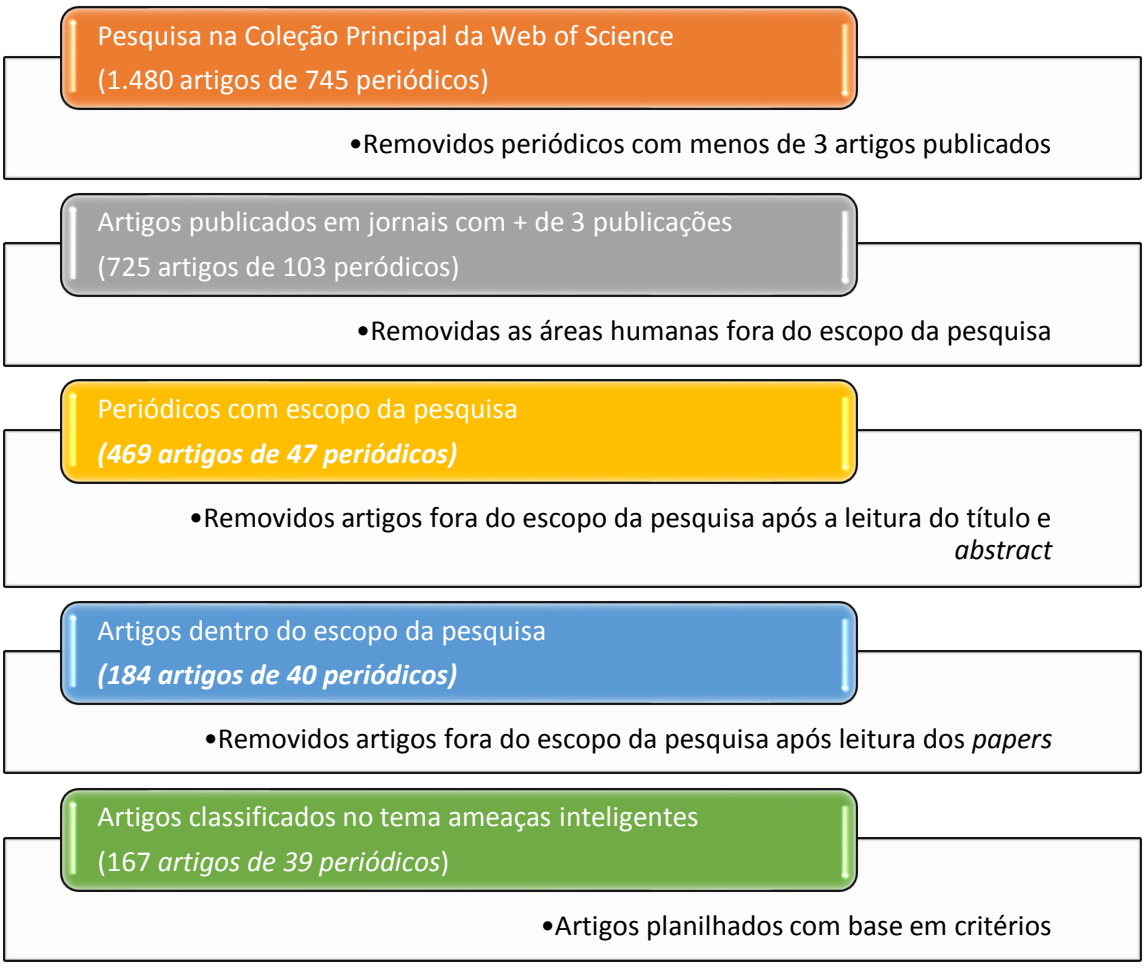
Figura 3 – Periódicos com artigos publicados no tema

Fonte: O Autor (2019).

4.4.1 Encerramento da revisão sistemática

A primeira análise bruta demonstra a heterogeneidade e a transversalidade do tema. Com a finalidade de refinar a pesquisa foram usados filtros, com o objetivo de realmente determinar os artigos com foco na área de interesse da pesquisa, foram excluindo alguns periódicos com menor impacto no tema, dada a grande ocorrência de publicações. Os filtros realizados foram os seguintes: periódicos que tenham mais de 3 artigos publicados; periódicos de áreas vinculadas ao campo da pesquisa, excluindo as da área de humanas e outras abordagens humanísticas com análises subjetivas; leitura de títulos e abstracts excluindo periódicos fora do escopo da pesquisa; e leitura completa dos artigos visando efetivamente eliminar os divergentes do escopo da pesquisa. O fluxograma e síntese das ações estão representados na Figura 5.

Figura 4 – Síntese das ações



Fonte: O Autor (2019).

Os artigos classificados no tema ameaças inteligentes foram planilhados conforme os seguintes critérios, distribuídos em 29 colunas: (1) informação de citação; (2) autores; (3) título; (4) título da fonte; (5) ano da publicação; (6) DOI; (7) total de citações; (8) média de citações por ano; (9) a (26) citação por ano de 2001 a 2018; (27) foco do artigo; (28) métodos; (29) campo de aplicação; (30) área de pesquisa; e (31) informações de financiamento.

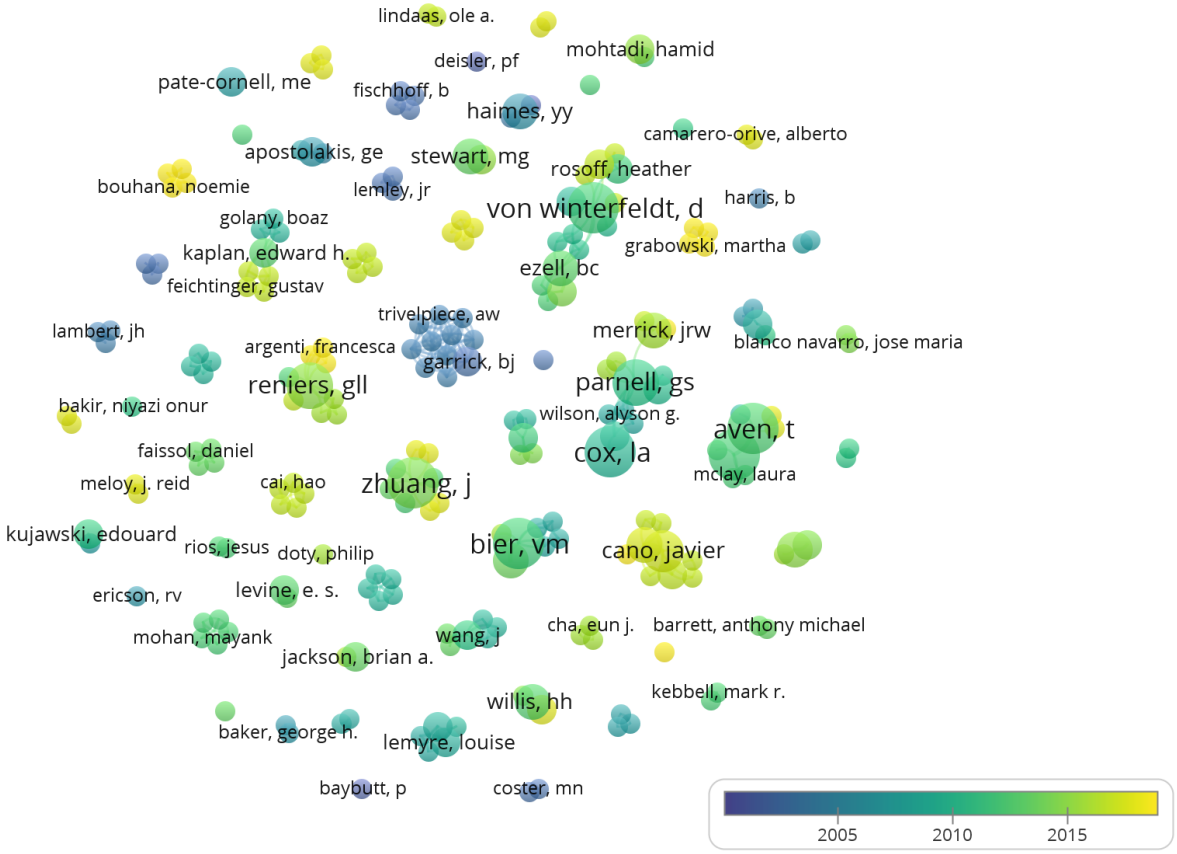
Após a aplicação dos filtros e processo de remoção dos artigos fora do escopo da pesquisa, foram extraídos os dados completos dos registros da pesquisa final sob forma de "texto sem formatação" e realizada a análise de dados bibliométricos na ferramenta *VOSviewer* 1.6.11, que foi desenvolvida para análise, mapeamento e visualização de dados bibliométricos pela *Leiden University*. Os artigos foram analisados conforme o ano de publicação, categorias do WoS, autores, citações, países e organização orientados pelas questões de pesquisa.

5 APRESENTAÇÃO DOS RESULTADOS E DISCUSSÃO DA REVISÃO SISTEMÁTICA DE LITERATURA

A revisão sistemática analisou periódicos publicados no período entre 2001 e 2018, resultando em uma coleção final de 167 artigos, escritos por 359 autores. A pesquisa tem por objetivo representar o atual estado do desenvolvimento do tema, as aplicabilidades no cenário nacional, as tendências das ameaças no contexto internacional por meio das respostas às questões de pesquisa formuladas e desenvolvidas, e como suporte à decisão no planejamento de políticas de segurança pública

A análise bibliométrica da produção dos autores por ano dentro da pesquisa selecionada está representada na Figura 5, onde as cores indicam a temporalidade da produção, quanto maior o círculo, maior é a produção do autor.

Figura 5 - Autores por ano

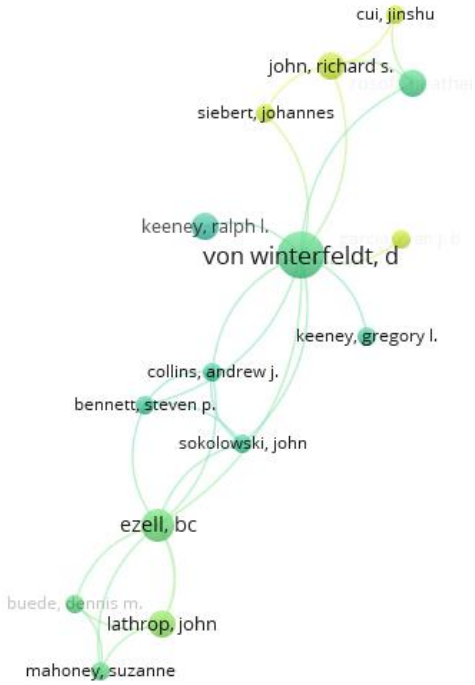


Fonte: O Autor (2019).

Foram formados 66 (sessenta e seis clusters), onde podemos verificar que os clusters com tons mais azuis são os mais antigos, indo do ano de 2001 até 2005, onde as esferas começam a se tornarem esverdeadas, e na sequência após 2010 vão assumindo um tom crescente de amarelo, até atingir 2018.

Os principais clusters permitem analisar a integração entre os autores. O principal cluster apresenta autores que iniciaram pesquisa que são referências no tema após o 9-11 e continuam até hoje contribuindo com o tema principalmente com a modelagem de valores e o impacto econômico.

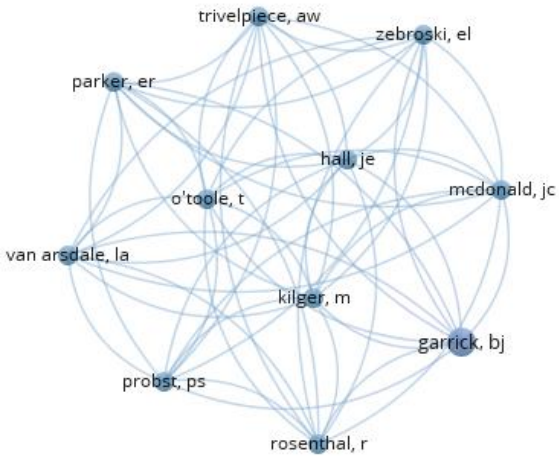
Figura 6 - Análise de *clusters* - 11/9



Fonte: O Autor (2019).

Este cluster apresenta os autores com as produções mais antigas relacionadas ao tema, todo o cluster com tons de azul e que são as referências mais antigas nas citações da pesquisa acadêmica.

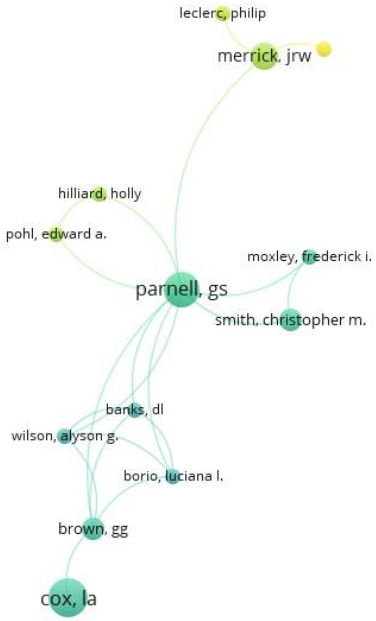
Figura 7 - Autores com produções mais antigas



Fonte: O Autor (2019).

O segundo maior cluster apresenta autores centrais do pós 9-11 e que mantém suas pesquisas de forma contínua dentre outros temas nas ameaças biológicas e a relação com adversários inteligentes.

Figura 8 – Autores na área de ameaças biológicas

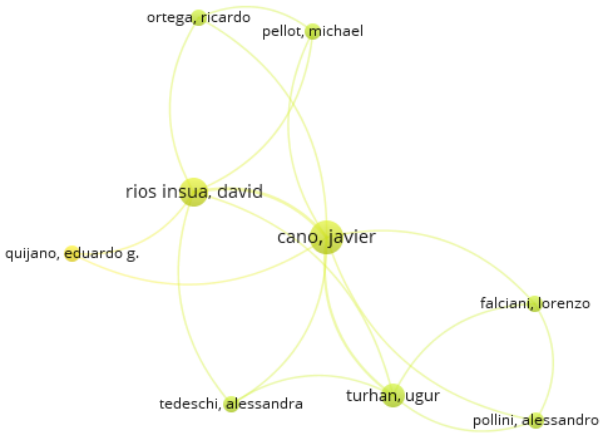


Fonte: O Autor (2019).

Este cluster se destaca por agrupar os autores com pesquisas mais atuais, destacando-se o estudo da análise do risco adversário, modelo que busca reduzir as incertezas por meio da

integração de técnicas e que busca refinar a aplicação da teoria dos jogos e a análise de risco probabilística.

Figura 9 - Autores com abordagens atuais como risco adversário



Fonte: O Autor (2019).

No contexto das abordagens atuais como risco adversário destacam-se os seguintes autores com quantidade de artigos indicados: Cano, Javier (4); Rios Insua David (8); e Turhan, Ugur (2). Com um artigo os demais: Quijano, Eduardo G.; Tedeschi, Alessandra; Falciani, Lorenzo; Pollini, Alessandro; Pellot, Michael, e Ortega, Ricardo.

A análise macro dos primeiros resultados permite identificar o potencial do assunto e a força da pesquisa científica, claramente demonstrado por uma série temporal onde a evolução dos estudos fica comprovada. O 9-11 surge como evento potencializador que definitivamente coloca a análise de risco do terrorismo como tema de Estado com forte impacto econômico e social, catapultado a impulsionador de políticas públicas para garantia do desenvolvimento e do equilíbrio da economia.

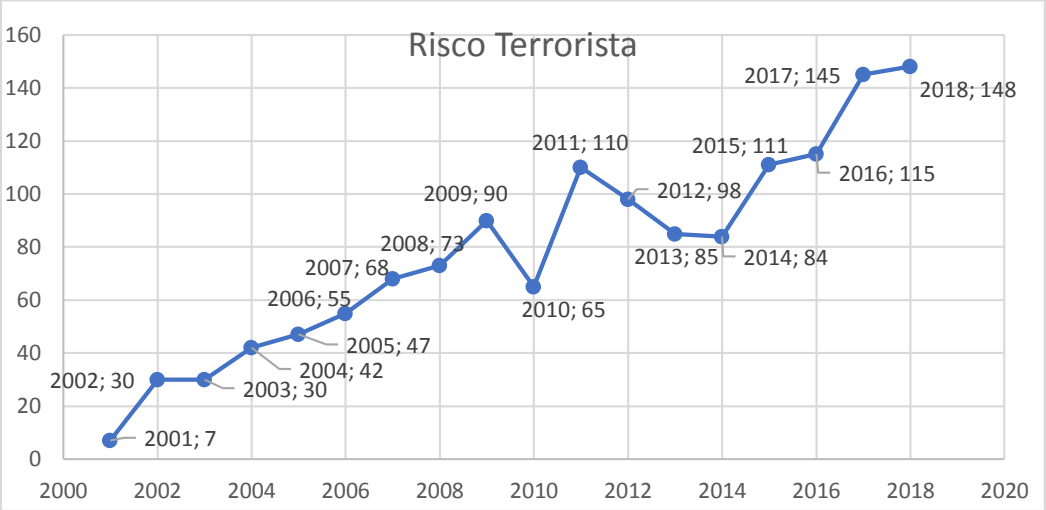
As questões seguintes irão aprofundar a análise e permitir conclusões mais profundas e sólidas sobre o atual status das pesquisas sobre o tema e suas tendências na academia, de forma a contribuir com o desenvolvimento de políticas públicas e a consecução dos objetivos estratégicos dos Estado, protegendo vidas e reduzindo as perdas político-econômicas.

5.1 EVOLUÇÃO DAS PUBLICAÇÕES

- *Como a análise do risco terrorista evoluiu em termos do número de trabalhos publicados e aumento de citações?*

Como pode ser visto na Figura 10, a produção acadêmica evoluiu de forma crescente a partir de 2001, com pequenos momentos de retração, e retomada posterior em virtude de eventos que atentam para necessidade de vigilância e estudos permanentes, como no caso de Estocolmo, cuja tipologia foi resultante de radicalização e apoio ao Estado Islâmico, onde foram utilizados homens-bomba e explosivos, sendo o primeiro ataque do terrorismo islâmico nos países nórdicos. Em 2011 ocorreu um ataque de extrema-direita na Noruega, onde foi usado um carro bomba e assassinato seletivo com armas automáticas.

Figura 10 - Evolução da produção acadêmica na visão macro



Fonte: O Autor (2019).

Esta primeira análise foi realizada com base no resultado da primeira pesquisa, analisando os dados de forma bruta, em todo o escopo de ocorrência resultante da pesquisa com os dois grupos de palavras chaves relacionados ao terrorismo (T) e abordagens ao risco (R), oferecendo a visão macro da abordagem ao tema. Os resultados após aplicação das técnicas de refinamento são apresentados na sequência.

Em vista de contextualizar os dados analisado, foi extraído do Global Terrorism Database (GTD) os principais eventos terroristas ocorridos no período da pesquisa e complementado com os principais eventos do ano de 2018, de forma a oferecer condições de realização de uma análise mais profunda das variações na produção. O GTD é um banco de dados de código aberto que inclui informações sobre eventos terroristas em todo o mundo de 1970 a 2017, com atualizações anuais adicionais planejadas para o futuro. Ao contrário de muitos outros bancos de dados de eventos, o GTD inclui dados sistemáticos sobre incidentes terroristas domésticos e

transnacionais e internacionais que ocorreram durante esse período e agora incluem mais de 180.000 casos (START, 2005).

O Global Terrorism Database - ou GTD - começou em 2001, quando pesquisadores da Universidade de Maryland obtiveram um grande banco de dados originalmente coletado pelo Pinkerton Global Intelligence Services (PGIS). O GTD faz parte do *National Consortium for the Study of Terrorism and Responses to Terrorism* (START, 2019), um centro de educação e pesquisa, voltado para a ciência e a tecnologia de segurança interna, que foi lançado em 2005 como um dos Centros de Excelência apoiados pelo Departamento de Segurança Interna dos Estados Unidos, fruto do HSA 2002.

Tabela 3 - Principais ataques terroristas 2001-2011

Ano	Ação - alvo	Cidade	País
2001	Ataque com Aviões - World Trade Center (Complexo de Edifícios)	New York	EUA
2004	Explosivos - Sistema de Trens Suburbanos	Madrid	Espanha
	Sequestro - Escola Número Um	Beslan	Rússia
2005	Explosivos - Sistema de Transporte Público (metrô e ônibus)	London	Inglaterra
2010	Homem-bomba – Centro da Cidade	Stockholm	Suécia
2011	Explosivos e assassinatos – Prédios do Governo e reunião política trabalhista	Oslo	Noruega

Fonte: O Autor (2019).

Podemos identificar que após 2013, de acordo com o GTD, com um recrudescimento dos ataques, principalmente nos alvos ocidentais, contra países que atuavam nas coalizões contra o Estado Islâmico, ocorre um novo pico de crescimento da produção, fomentado pelas perdas de vidas e outros danos causados pelos atentados conforme a Tabela 4.

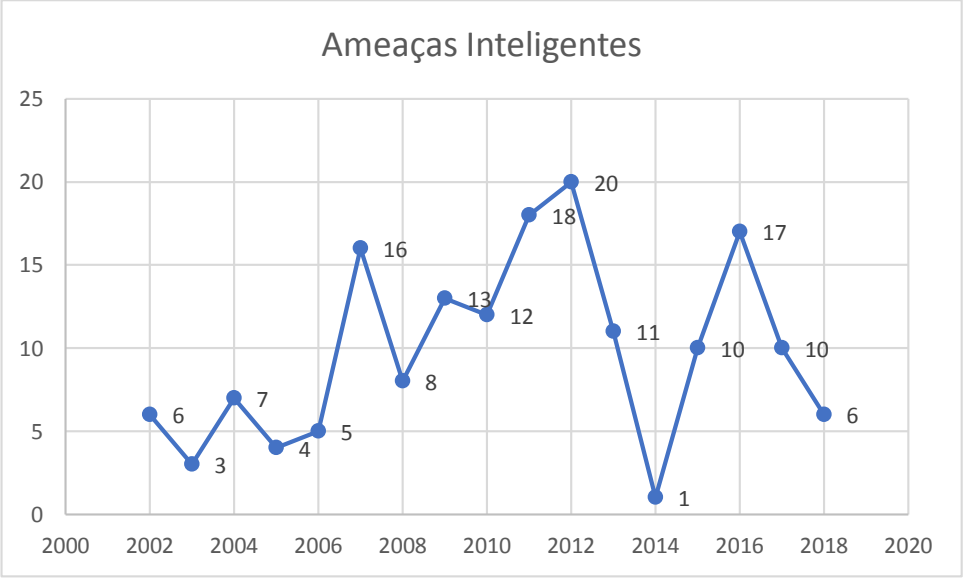
Com relação ao tema específico, análise de risco com foco nas ameaças inteligentes, observamos de forma análoga o crescimento dos estudos, cujo foco se baseia na consideração da intenção do adversário, capaz de tomar decisões futuras dinâmicas com base em nossos preparativos, seus objetivos e sua capacidade de atingi-los de acordo com a Figura 11.

Tabela 4 - Principais ataques terroristas 2013-2018

Ano	Ação - Alvo	Cidade	País
2013	Explosivo improvisado - Maratona de Boston	Boston	EUA
	Envio de ricina – Presidente e senador americanos	Washington	EUA
	Mulher Bomba- Sistema de Transportes	Volvogrado	Rússia
	Tomada de reféns e assassinatos - Shopping Center	Nairóbi	Quênia
2015	Assassinatos - Charles Ebdo	Paris	França
	Explosivos e assassinatos - Bataclan e outros locais	Paris	França
	Homens-bomba – Estação de Trem	Ankara	Turquia
	Assassinatos – Sinagoga	Copenhague	Dinamarca
2016	Assassinato – Embaixador Russo na Turquia	Ankara	Turquia
	Assassinatos – Boate Pulse (LGBT)	Miami	EUA
	Homens-bomba – Aeroporto e Metrô	Bruxelas	Bélgica
	Atropelamentos – Dia da Bastilha e Mercado de Natal	Nice e Berlim	França, Alemanha
2017	Homem-bomba – Show de Ariana Grande	Manchester	Inglaterra
	Atropelamentos – Centro da cidade	Estocolmo, Nova York, Barcelona e Londres	Suécia, EUA, Espanha e UK.
2018	Assassinatos - Festival de Inverno de Strassburg	Strassburg	França

Fonte: O Autor (2019).

Figura 11 - Evolução da produção acadêmica para ameaças inteligentes



Fonte: O Autor (2019).

Ocorre uma maior ocorrência de eventos dinâmicos, onde são exploradas não só as vulnerabilidades, mas exploradas a alocação dos recursos contraterrorismo e ações com múltiplos ataques, utilizando meios alternativos combinados aos tradicionais explosivos, onde se almeja ampliar os danos, como no uso de armas automáticas e veículos para atropelamentos.

A nova forma de atuação leva as forças de segurança a reverem seus métodos e proporciona para academia a chance de produzir estudos que venham antecipar as ameaças e tendências, contribuindo para o aprimoramento da defesa e proteção da sociedade por meio da integração com as autoridades governamentais.

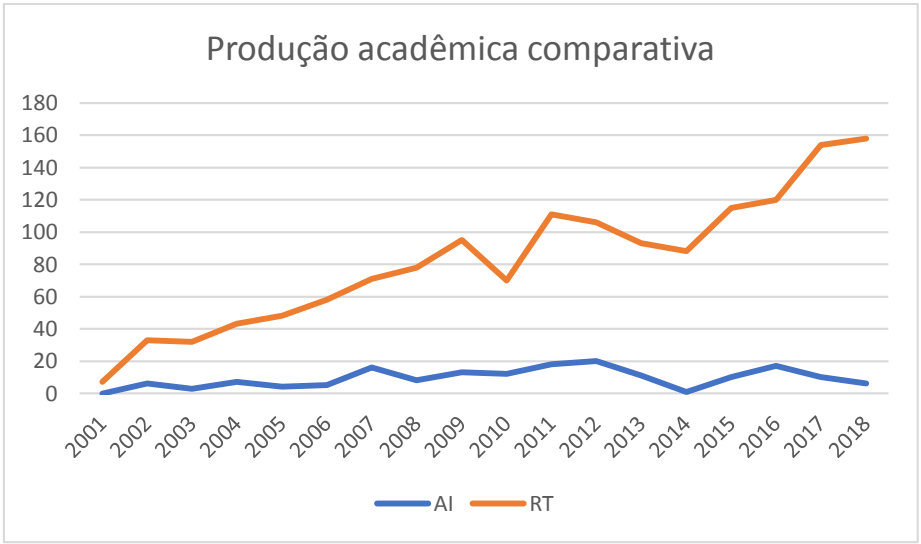
Tabela 5 - Dados numéricos da produção acadêmica

AP	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
RT	7	33	32	43	48	58	71	78	95	70	111	106	93	88	115	120	154	158
AI	0	6	3	7	4	5	16	8	13	12	18	20	11	1	10	17	10	6

Fonte: O Autor (2019).

Na Tabela 5 e Figura 12 é demonstrada a comparação durante os anos da produção acadêmica (AP) do tema risco terrorista com foco nas ameaças inteligentes (AI) e o total do tema risco terrorista (RT), demonstrando que o tema mantém o acompanhamento da trajetória da área com menos intensidade, mas representa uma área a ser explorada com possiblidade de estudos significativos. O total de estudos representa 11,3% da produção acadêmica no período em referência.

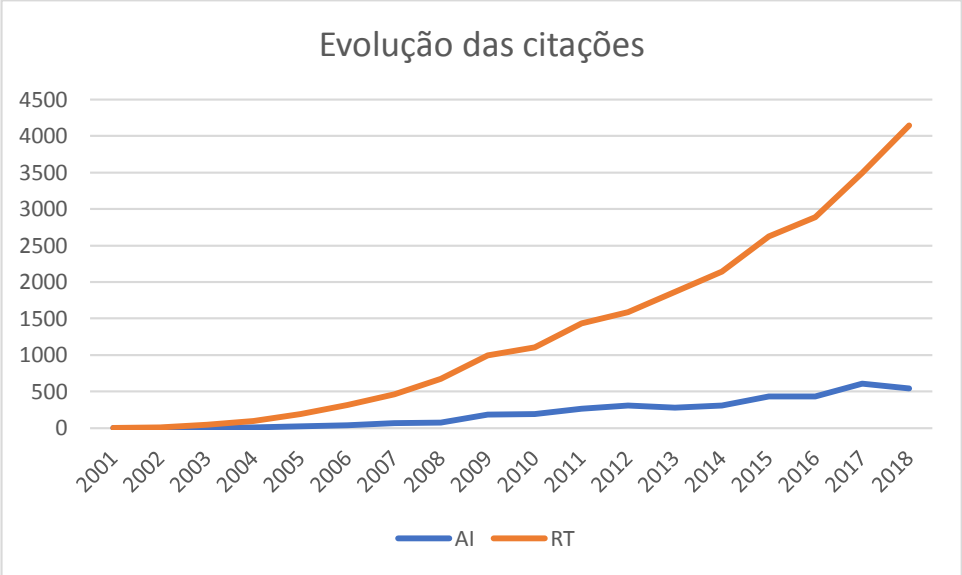
Figura 12 - Comparativo de produção acadêmica



Fonte: O Autor (2019).

Em relação às citações, a Figura 13 indica o crescente aumento de forma exponencial, afirmando a importância e relevância do tema. Após 2012, o crescimento apresentado é maior podendo ser fruto da nova forma de ataques perpetrados contra os países que atuavam na coalizão da Guerra da Síria, gerando em um número elevado de perdas de vidas e prejuízos financeiros, que impactam diretamente na estabilidade internas dos Estados. Esses ataques geraram a perda de cidadãos de diversas nações devido a estarem presentes nos locais à trabalho, estudando, turismo ou mesmo residindo.

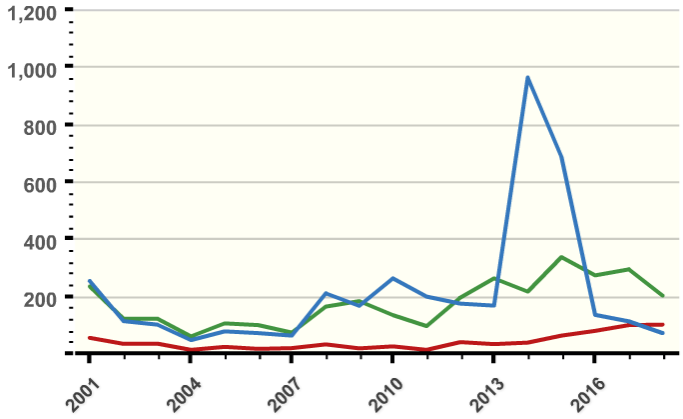
Figura 13 - Evolução das citações



Fonte: O Autor (2019).

Em relação às citações, observa-se graficamente a demonstração da evolução comparativamente entre o estudo das ameaças inteligentes e o risco terrorista e o número de atentados nos principais países alvos de acordo com sua região. A Figura 14 demonstra o total de ataques terroristas nas principais regiões de interesse da pesquisa: em vermelho a América do Norte, em verde o oeste da Europa e em Azul o leste da Europa. Fica claramente identificável o grande pico de atentados entre 2013 e 2016, resultantes de atentados na Turquia base de repressão ao Estado Islâmico, que se alinha com um maior aprofundamento dos estudos. A análise de citações por autores e artigos será abordada em outra questão de pesquisa.

Figura 14 - Número de ataques terroristas por região



Fonte: GTD (2019)

5.2 ÁREAS DE PESQUISA E APLICAÇÕES DE CAMPO

- Em que áreas de pesquisa e aplicações de campo a abordagem a ameaças inteligentes no contexto do risco terrorista é predominante para citações e organizações?

As principais áreas de pesquisa do WoS[21] consideradas para o estudo são apresentadas na Figura 15, onde podemos observar a multidisciplinariedade do tema, destacando as cinco principais categorias do *Web of Science: Public Environmental Occupational Health* (71) que representa 42,52%, *Mathematics* (67) e *Mathematical Methods in Social Sciences* (67) que cada uma representa 40,12%, *Operations Research Management Science* (34) com 20,36%, e *Engineering* (33) com 19,76%, e *Business Economic* com 13,77%.

[21] As áreas de pesquisa formam um esquema de categorização de assunto compartilhado por todas as bases de dados de produtos do Web of Science. Como resultado, é possível identificar, recuperar e analisar os documentos a partir de diversas bases de dados relacionadas ao mesmo assunto. Periódicos e livros cobertos pela *Principal Coleção do Web of Science* são atribuídos a pelo menos uma categoria do Web of Science. Todas as categorias do Web of Science são associadas a uma área de pesquisa.

Figura 15 - Artigos por áreas de pesquisa do WoS

Fonte: O Autor (2019).

As principais categorias do WoS encontradas no estudo das ameaças inteligentes são apresentadas na Figura 16 no total dos 167 artigos selecionados, onde podemos observar a multidisciplinariedade do tema, destacando as cinco principais categorias do *Web of Science*: *Public Environmental Occupational Health* (71) com 42,52%, *Mathematics Interdisciplinary Applications* (67) e *Social Sciences Mathematical Methods* (67) com 40,12%, *Operations Research Management Science* (34) com 20,36%, e *Management* (21) com 12,58%.

Figura 16 - Artigos por categorias WoS

Fonte: O Autor (2019).

Utilizando a ferramenta VOS viewer, por meio da análise baseada na coautoria das redes bibliométricas, utilizando os critérios de mínimo de 4 artigos e 20 citações, foi realizada a análise dos países. De acordo com Eck e Waltman (2014) é possível identificar a interação entre pesquisadores, instituições de pesquisa ou países com base no número de publicações que eles criaram em conjunto.

A força do link representada na Tabela 6 é usada para normalizar a intensidade das ligações entre os países, a qual será maior conforme sua frequência de integração na produção com outros países.

Tabela 6 - Artigos e citações por países no VOS viewer

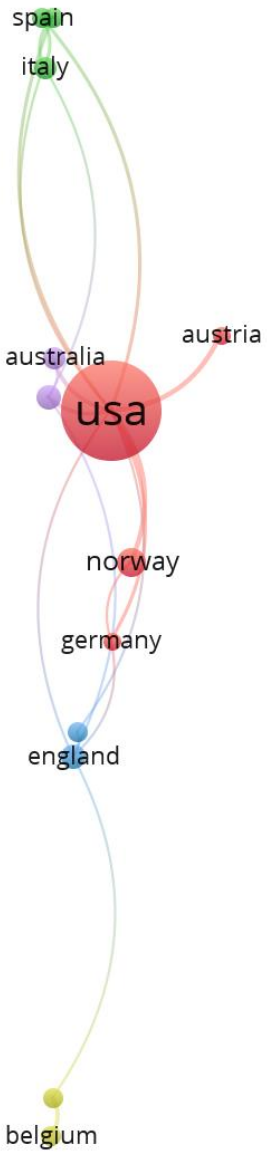
País	Artigos	Citações	Força do Link
USA	120	3128	17
Turkey	5	24	6
Spain	5	33	6
Italy	6	74	6
Peoples R China	8	225	6
Netherlands	5	64	4
England	8	105	4
Australia	6	151	4
Norway	10	257	4
Belgium	5	35	3
Canada	5	112	2

Fonte: O Autor (2019).

A análise dos resultados por meio do VOS viewer demonstra que os cinco países que mais produzem são os seguintes conforme a Tabela 6: USA (120), Noruega (10), Inglaterra (8), China (8), Austrália e Itália (6). Em relação as citações encontramos os cinco mais citados: USA (3128), Noruega (257), China (225), Áustria (174), Austrália (151). Dentre eles se destacam os países vítimas de atentados e participantes históricos de coalizões militares no combate ao terrorismo.

Quanto maior a importância de um país na rede, maior o rótulo e o círculo apresentados na Figura 17, onde a quantidade de linhas indica a maior interação com outros países, e a largura indica a força de interação entre os colaboradores. Os Estados Unidos aparecem nessa rede como o mais atuante.

Figura 17 - Análise de rede de coautoria por país

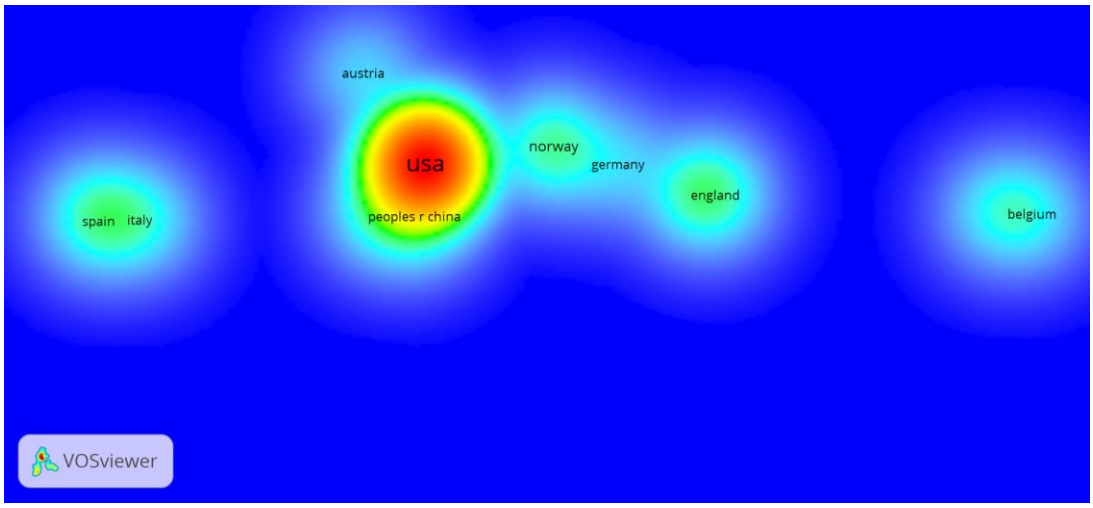


Fonte: O Autor (2019).

Com base na análise de visualização de densidade do item, cada ponto é representado em uma cor, por padrão entre azul e vermelho, conforme a densidade na sua área periférica. Quanto maior a quantidade de itens vizinhos com maior peso, a cor tenderá ao vermelho. Existindo itens vizinhos de menor força, a cor tenderá ao azul.

Analisando os clusters, grupos que se formam por afinidade ou proximidade, encontramos: Áustria, Alemanha, Noruega e Estados Unidos; Itália, Espanha e Turquia; Canadá e Inglaterra; Bélgica e Holanda; Austrália e China; destaca-se a força de Estados Unidos e China no estudo do tema.

Figura 18 - Visualização de densidade da produção e citações por países



Fonte: O Autor (2019).

Em relação às organizações, atuando por meio da análise baseada na coautoria das redes bibliométricas, utilizando os critérios mínimos de 2 artigos e 20 citações, resultou em classificar 38 organizações. Na Tabela 7, indo da esquerda para a direita, encontram-se as organizações classificadas com base na força do link (FL), pela quantidade de artigos publicados (A) e pela quantidade de citações (C). As abreviaturas seguem os padrões apresentados no WoS.

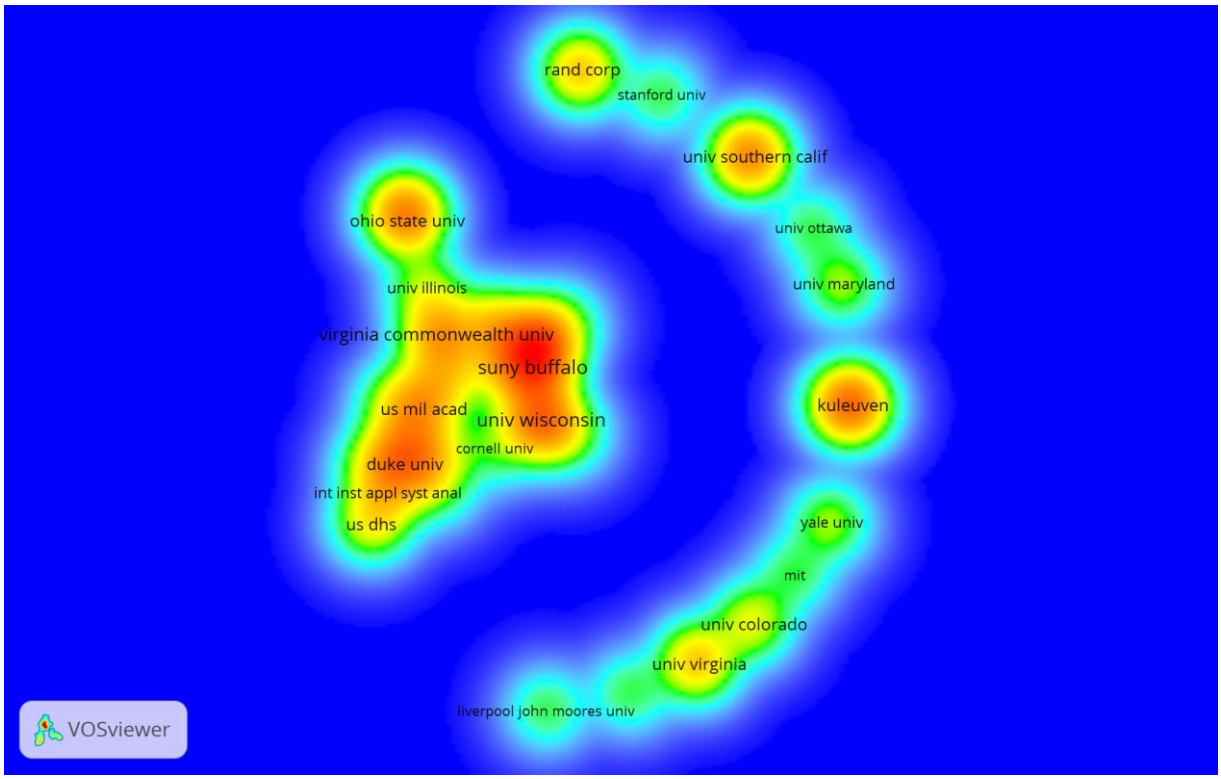
Tabela 7 - Organizações classificadas por força do link, artigos e citações

	Organizações	FL	Organizações	A	Organizações	C
1	Kuleuven	7	Suny Buffalo	10	Cox Associates	367
2	Univ Antwerp	7	Univ Stavanger	10	Suny Buffalo	274
3	Us Mil Acad	7	Univ Wisconsin	10	Univ Stavanger	257
4	Delft Univ Technol	6	Virginia Commonwealth Univ	7	MIT	256
5	Ohio State Univ	6	Univ Southern Calif	6	Univ Wisconsin	252
6	Duke Univ	5	Rand Corp	6	Univ Colorado	215
7	Univ Newcastle	5	Univ Virginia	6	Univ Virginia	196
8	Univ Pittsburgh	5	Us Mil Acad	5	Int Inst Appl Syst Anal	167
9	Virginia Commonwealth Univ	5	Johns Hopkins Univ	5	Virginia Commonwealth Univ	147
10	Cato Inst	4	Kuleuven	4	Rand Corp	135
11	Innovat Decis Inc	4	Univ Antwerp	4	Univ Southern Calif	132
12	Suny Buffalo	4	Ohio State Univ	4	Innovat Decis Inc	127
13	Univ Stavanger	4	Duke Univ	4	Us Mil Acad	122
14	USN	4	Univ Newcastle	4	Oak Ridge Natl Lab	122
15	Int Inst Appl Syst Anal	3	Innovat Decis Inc	4	US DHS	118

Fonte: O Autor (2019).

Realizando a análise de visualização de densidade das organizações com base nas organizações encontramos 8 clusters contendo 28 organizações, e 10 organizações, de acordo com a Figura 19.

Figura 19 - Visualização por densidade das organizações por artigos e citações



Fonte: O Autor (2019).

Dentre as organizações encontramos alguns dos Centros de Excelência de C & T do DHS[22] e o próprio DHS, que são financiadas por força do HSA 2002, desenvolvendo soluções de ciência e tecnologia multidisciplinares, orientadas para o cliente com foco nas ciências de segurança interna e soluções tecnológicas, ajudando a treinar a próxima geração de especialistas em segurança interna conforme a Tabela 8.

Dentre as 10 organizações que não possuem força de link, apesar de produção e citações consideráveis representados, são demonstradas na Tabela 9 conforme destaque: a Universidade de Maryland que lidera o Consórcio Nacional para o Estudo do Terrorismo e Respostas ao Terrorismo (START), oferecendo aos formuladores de políticas e profissionais descobertas

[22] https://www.dhs.gov/science-and-technology/centers-excellence

empíricas sobre os elementos humanos da ameaça terrorista e informa decisões sobre como desarticular os terroristas. e grupos terroristas; e a Universidade do Sul da Califórnia que lidera o Centro Nacional de Análise de Risco e Análise Econômica de Eventos Terroristas (CREATE), desenvolvendo ferramentas avançadas para avaliar os riscos, custos e consequências do terrorismo; e a Universidade de Illinois que lidera o Instituto de Resiliência à Infraestrutura Crítica (CIRI) realizando pesquisas e educação para melhorar a resiliência da infraestrutura dos EUA e de seus proprietários e operadores.

Tabela 8 - Cluster e organizações sem força de link

Cluster	Organizações	Cluster	Organizações
1	Georgetown Univ	2	Cornell Univ
	Innovat Decis Inc		Nyu
	Johns Hopkins Univ		Oak Ridge Natl Lab
	Suny Buffalo		Univ Pittsburgh
	Univ Illinois		Univ Wisconsin
	Univ Michigan	4	Duke Univ
	Univ Stavanger		Int Inst Appl Syst Anal
	Virginia Commonwealth Univ		US DHS
3	Cato Inst	6	Cox Associates
	Ohio State Univ		USN
	Univ Newcastle	7	Univ Texas Austin
5	Delft Univ Technol		US Mil Acad
	Kuleuven	8	Univ Southern Calif
	Univ Antwerp		Vanderbilt Univ

Fonte: O Autor (2019).

Tabela 9 - Entidades sem força de link

Organizações	Artigos	Citações	Força
MIT	2	256	0
univ colorado	4	215	0
univ virginia	6	196	0
rand corp	6	135	0
yale univ	3	98	0
univ maryland	3	88	0
liverpool john moores univ	2	76	0
univ ottawa	2	33	0
stanford univ	2	23	0
oregon dept environm qual	2	20	0

Fonte: O Autor (2019).

5.3 AUTORES

- *Quais autores e periódicos mais influenciaram o desenvolvimento do tema de pesquisa?*

De acordo com o protocolo inicial validado e em termos de produção macro no tema risco terrorista, encontra-se na Tabela 10 o resultado gráfico dos principais autores representados por seus nomes conforme o WoS, quantidade de artigos publicados, porcentagem em relação aos 1480 da pesquisa macro e as referências dos autores conforme os artigos publicados na base WoS com destaque para os seguintes: Zhuang J (16), Stewart MG (14), Haimes YY(11), Bier VM (9), Lambert JH (9), Lemyre L (9), Reniers G (9), Aven T (8), Cox LA (8), e Von Winterfeldt D (8).

Tabela 10 - 10 principais autores

Autores	A	%	Referências do autor
Zhuang J	16	1.081	[Zhuang, Jun] SUNY Buffalo, Dept Ind & Syst Engn, Buffalo, NY 14260 USA.
Stewart MG	14	0.946	[Stewart, Mark G.] Univ Newcastle, Ctr Infrastruct Performance & Reliabil, Newcastle, NSW, Australia.
Haimes YY	11	0.743	[Haimes, YY], Univ Virginia, Ctr Risk Management & Engn Syst, 112 Olsson Hall, Charlottesville, VA 22903 USA.
Bier VM	9	0.608	[Bier, Vicki M.] Univ Wisconsin, Dept Ind & Syst Engn, Madison, WI USA.
Lambert JH	9	0.608	Lambert, JH] Univ Virginia, Dept Syst & Informat Engn, Ctr Risk Management Engn Syst, Charlottesville, VA USA.
Lemyre L	9	0.608	[Lemyre, Louise] Univ Ottawa, Sch Psychol, Ottawa, ON K1N 6N5, Canada.
Reniers G	9	0.608	[Reniers, Genserik] Delft Univ Technol, Safety Sci Grp, Jaffalaan 5, Delft, Netherlands; Univ Antwerp, Engn Management Dept, Res Grp ARGoSS, Prinsstr 13, B-2000 Antwerp, Belgium; KULeuven, CEDON, Campus Brussels, B-1000 Brussels, Belgium.
Aven T	8	0.541	[Aven, Terje] Univ Stavanger, Risk Management, Stavanger, Norway.
Cox LA	8	0.541	[Cox, LA] Univ Colorado, 503 Franklin St, Denver, CO 80218 USA; [Cox, Louis Anthony (Tony), Jr.] Cox Associates, Denver, CO 80218 USA.
Von Winterfeldt D	8	0.541	[von Winterfeldt, Detlof] Int Inst Appl Syst Anal, A-2361 Laxenburg, Austria; [von Winterfeldt, Detlof] Univ Southern Calif, Daniel Epstein Dept Ind & Syst Engn, 3715 McClintock Ave, GER 240, Los Angeles, CA 90089 USA.

Fonte: O Autor (2019)

Analisando os periódicos, seguindo o mesmo modelo da análise dos autores, encontra-se na Tabela 11 aqueles que tiveram o maior número de publicações e citações normalizados pela força do link. O periódico *Risk Analysis* (Wiley, 111 River St, Hoboken 07030-5774, NJ USA) se destaca sobremaneira, com fator de impacto 2,564 (2018) e 3,161 (5 anos), sendo Q1 em

Mathematics, Interdsiciplinary Aplications; Public, Environmental & Occupational Health (edição SSCI); *e Social Sciences, Mathematical Methods na Jornal Citation Report Category.*

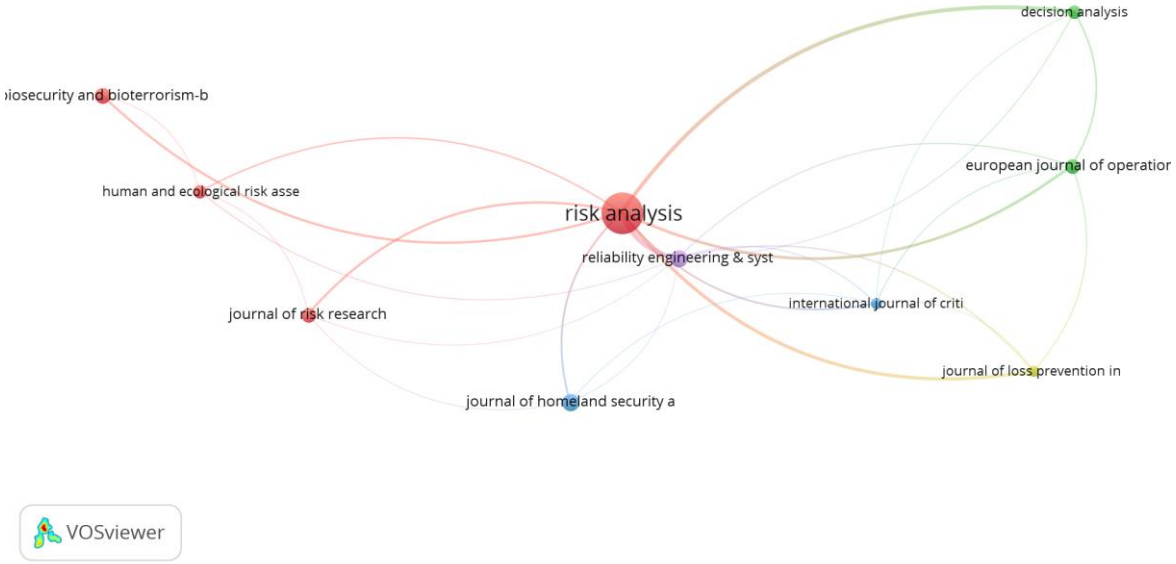
Tabela 11 - Principais periódicos

Periódico	A	%	C	FL
Risk Analysis	136	9.189	3443	240
Reliability Engineering & System Safety	24	1.622	511	87
Decision Analysis	14	0.946	160	56
Journal of Loss Prevention In the Process Industries	10	0.676	103	46
European Journal of Operational Research	18	1.216	250	40
Journal of Risk Research	18	1.216	113	20
Biosecurity and Bioterrorism-Biodefense Strategy Practice and Science	21	1.419	314	18
International Journal of Critical Infrastructure Protection	10	0.676	110	17
Journal of Homeland Security and Emergency Management	24	1.622	86	15
Human and Ecological Risk Assessment	14	0.946	61	11

Fonte: O Autor (2019).

A análise bibliométrica na Figura 20 demonstra a centralização e o tamanho da tag e da esfera do periódico Risk Analysis, colocando o periódico em posição de destaque com força de link (240) ligado a todos os demais periódicos relacionados.

Figura 20 - Visualização de redes dos principais periódicos

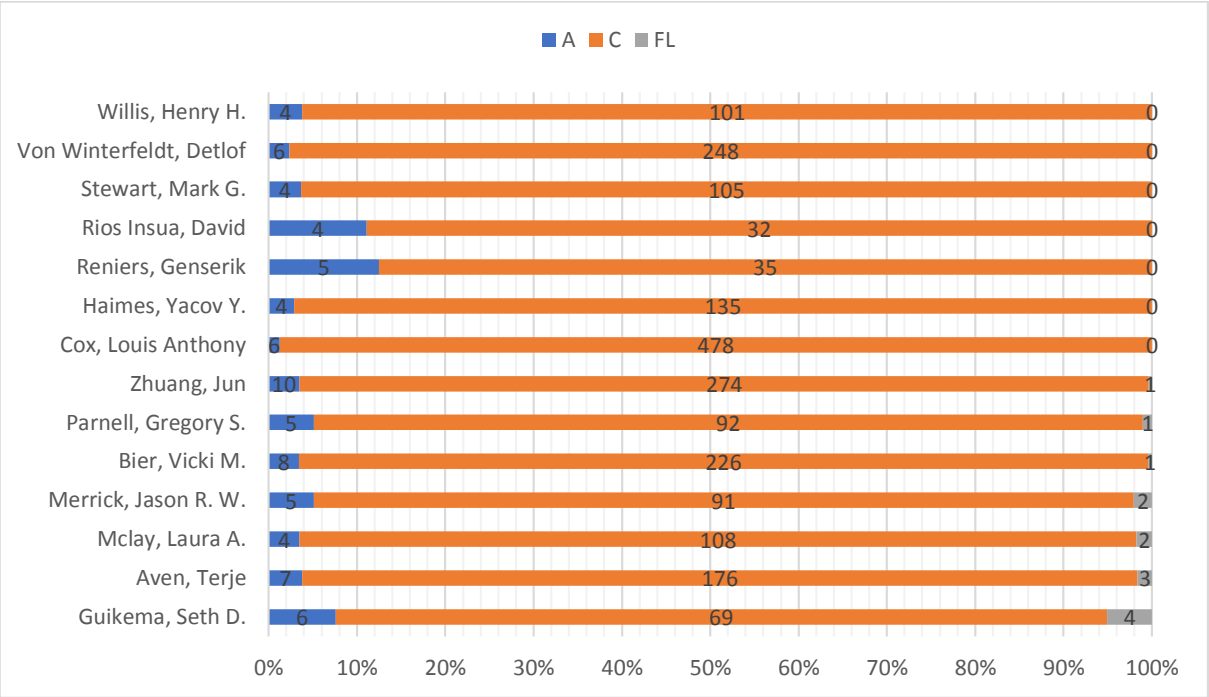


Fonte: O Autor (2019).

A *Reliability Engineering & System Safety* (Elsevier Sci Ltd, The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, Oxon, England) aparece em segundo lugar por força de link (87) e muito próxima da *Risk Analysis*, demonstrando alinhamentos nas linhas e cooperação, com fator de impacto 4,039 (2018) e 4,302 (5 anos), sendo Q1 em Engineering, Industrial; Operations Research & Management Science na Jornal Citation Report Category.

Realizando uma análise de coautoria dos autores com ênfases em ameaças inteligentes no contexto do risco terrorista, tendo como parâmetros pelo menos 4 (quatro) artigos (A) e 30 citações (C), encontra-se como resultado na Figura 21 normalizada pela força do link (FL) de cada autor, encontrando-se a predominância dos seguintes autores de artigos: Zhuang, Jun (10); Bier Vicki M. (8); Terje Aven (7); Seth D. Guikema, Louis Anthony Cox e Detlof Von Winterfeldt (6); Jason R. W Merrick, Gregory S. Parnell, e Genserik Reniers (5); Laura A. Mclay, Yacov Y. Haimes, David Rios Insua, Mark G. Stewart e Henry H. Willis (4). Em relação as citações se destacam os seguintes autores: Louis Anthony Cox (478); Jun Zhuang (274), Detlof Von Winterfeldt (248), Vicki M. Bier (226); Terje Aven (176), Yacov Y. Haimes (135).

Figura 21 - Principais autores



Fonte: O Autor (2019).

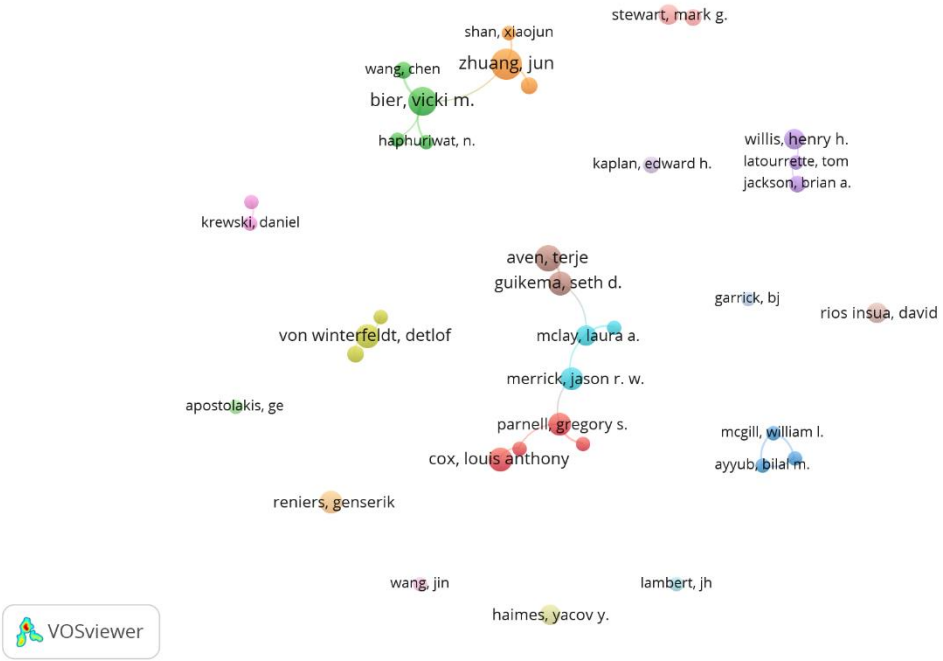
A Figura 22 apresenta os cinco clusters formados, abrangendo os grupos de pesquisa, que se dedicam ao estudo das ameaças inteligentes no contexto do risco terrorista, com destaque para as cores que indicam a temporalidade do estudo, onde o amarelo representa os estudos mais recentes e os azuis escuros os estudos mais antigos. Encontramos Yacov, Cox e Bier com cores mais azulados indicando mais tempo de publicações, e Rios Insua, Reniers e Zhuang com publicações mais recentes.

Figura 22 - *Clusters* de pesquisa

Fonte: O Autor (2019).

Efetuando variações nos critérios de análise para 2 artigos (A) e 30 citações (c) surgem as relações de intensidade de coautoria com outros autores com menor produtividade no tema, mas extremamente relevantes no contexto acadêmico. Destacam-se por importância os seguintes clusters, destacando que o tamanho do círculo com o nome do autor tem tamanho proporcional a sua relevância. *Cluster* 1: (Brown, Gerald G), (Cox, Louis Anthony), (Parnell, Gregory S.), e (Smith, Cristopher M.); *cluster* 2: (Bier, Vicki M.), (Haphuriwat, Naraphorn), (Wang, Chen), e (Zimmerman, Rae); *cluster* 3: (Ayyub, Bilal M.), (Kaminskiy, Mark), e (McGill, William L.); *cluster* 4: (Von Winterfeldt, Detlof), (Keeney, Ralph L.), e (Ezell, Barry Charles); *cluster* 5: (Jackson, Brian A.), (Latourette, Tom), e (Willis, Henry H.); *cluster 6*: (Jacobson, Sheldon H.), Mclay, Laura A.), e (Merrick, Jason RW); *cluster* 7: (Hausken, K), (Shan, Xiaojun), e (Zhuang, Jun); *cluster* 8: (Aven, Terje), e (Guikema, Seth D.); *cluster* 9: (Krewski, Daniel) e (Lemyre, L); *cluster* 10: (Mueller, John) e (Stewart, Mark G.). Os demais oito autores não formam cluster com esses critérios de análise conforme apresentado na Figura 23.

Figura 23 - Análise de coautoria

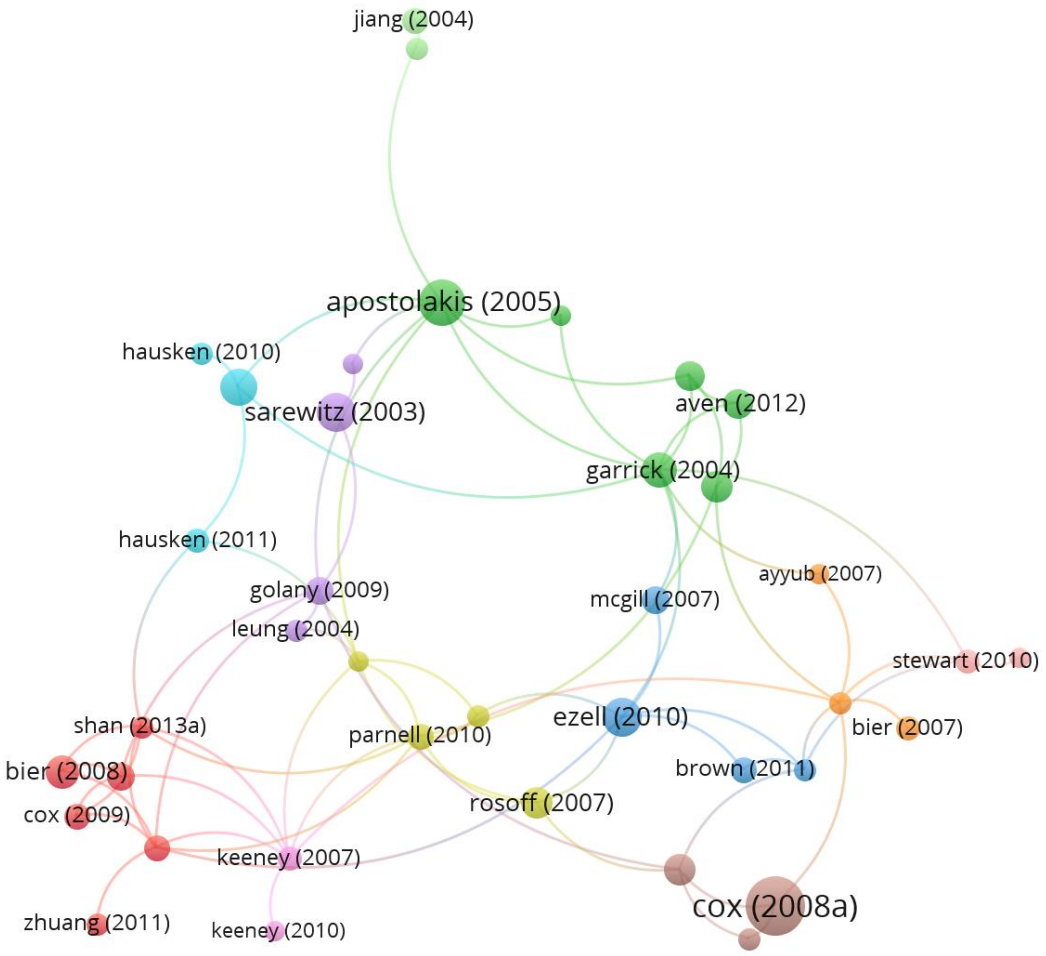


Fonte: O Autor (2019).

A análise de citações de artigos, usando como critério (C) o mínimo de 30 citações, encontra como resultado 52 artigos classificados, ordenados pela quantidade de *links* (L) que apresentam com outros artigos, sendo apresentados na Figura 24 e na Tabela 12.

O mapa apresentado exclui por indicação do VOS viewer os artigos que não possuem links. Na Figura 24, é apresentado um mapa dos trabalhos mais relevantes sobre ameaças inteligentes no contexto do tema risco terrorista. Os trabalhos mais relevantes apresentam maior circunferência, destacando-se: Nikoofal (2012), Rios (2012), Shan (2013), Merrick (2011), Parnell (2010), Ezell (2010), Cox (2009), e Rios Insua (2009).

Figura 24 - Análise de citações por artigos



Fonte: O Autor (2019).

A Tabela 12 contém as principais informações sobre os artigos com o número de citações (C), quantidade de links (L), informações de citação e DOI. Foram registrados os 10 mais relevantes classificados pela força do link como normatização.

Tabela 12 - Principais artigos com informações de citação

Artigo	C	L	Informações de citação	DOI
garrick (2004)	93	9	GARRICK, B. John *et al*. Confronting the risks of terrorism: making the right decisions. **Reliability Engineering & System Safety**, v. 86, n. 2, p. 129-176, 2004.	https://doi.org/10.1016/j.ress.2004.04.003
apostolakis (2005)	155	8	APOSTOLAKIS, George E.; LEMON, Douglas M. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. **Risk Analysis: An International Journal**, v. 25, n. 2, p. 361-376, 2005.	https://doi.org/10.1111/j.1539-6924.2005.00595.x

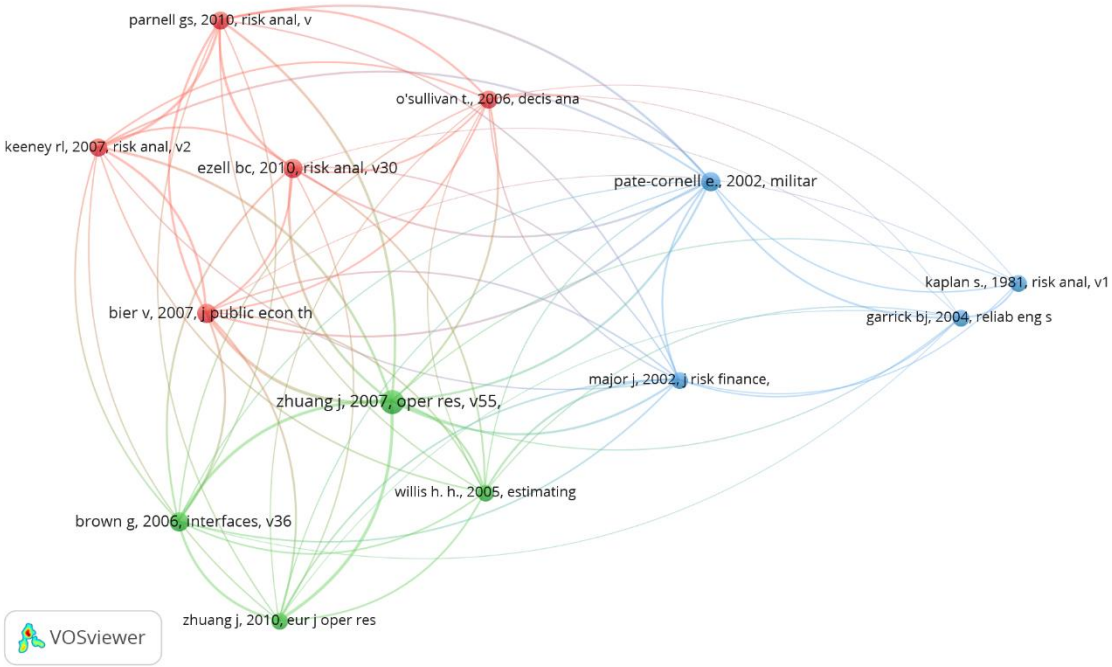
Tabela 12 - Principais artigos com informações de citação (continuação)

Artigo	C	L	Informações de citação	DOI
nikoofal (2012)	47	8	NIKOOFAL, Mohammad E.; ZHUANG, Jun. Robust allocation of a defensive budget considering an attacker's private information. **Risk Analysis: an International Journal**, v. 32, n. 5, p. 930-943, 2012.	https://doi.org/10.1111/j.1539-6924.2011.01702.x
merrick (2010)	33	7	MERRICK, Jason RW; MCLAY, Laura A. Is screening cargo containers for smuggled nuclear threats worthwhile? **Decision Analysis**, v. 7, n. 2, p. 155-171, 2010.	https://doi.org/10.1287/deca.1100.0171
ezell (2010)	111	7	EZELL, Barry Charles *et al*. Probabilistic risk analysis and terrorism risk. **Risk Analysis: an International Journal**, v. 30, n. 4, p. 575-589, 2010.	https://doi.org/10.1111/j.1539-6924.2010.01401.x
parnell (2010)	47	7	PARNELL, Gregory S.; SMITH, Christopher M.; MOXLEY, Frederick I. Intelligent adversary risk analysis: A bioterrorism risk management model. **Risk Analysis: an International Journal**, v. 30, n. 1, p. 32-48, 2010.	https://doi.org/10.1111/j.1539-6924.2009.01319.x
dillon (2009)	38	7	DILLON, Robin L.; LIEBE, Robert M.; BESTAFKA, Thomas. Risk- based decision making for terrorism applications. **Risk Analysis: an International Journal**, v. 29, n. 3, p. 321-335, 2009.	https://doi.org/10.1111/j.1539-6924.2008.01196.x
keeney (2007)	40	7	KEENEY, Ralph L. Modeling values for anti-terrorism analysis. **Risk Analysis: an International Journal**, v. 27, n. 3, p. 585-596, 2007.	https://doi.org/10.1111/j.1539-6924.2007.00910.x
shan (2013a)	38	6	SHAN, Xiaojun; ZHUANG, Jun. Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender–attacker game. **European Journal of Operational Research**, v. 228, n. 1, p. 262-272, 2013.	https://doi.org/10.1016/j.ejor.2013.01.029
golany (2009)	55	6	GOLANY, Boaz *et al*. Nature plays with dice–terrorists do not: Allocating resources to counter strategic versus probabilistic risks. **European Journal of Operational Research**, v. 192, n. 1, p. 198-208, 2009.	https://doi.org/10.1016/j.ejor.2007.09.001

Fonte: O Autor (2019).

Analisando a co-citação entre os artigos, ferramenta que consegue mensurar os links entre dois artigos, mais antigos, que são citados simultaneamente por um terceiro artigo, mais recente (VAN ECK, WALTMAN, 2016, p.6). Quanto mais intensa forem as citações, mas relevantes os artigos são como forma de contribuição com novos trabalhos. Foi utilizado como critério o mínimo de 15 co-citações para gerar o mapa ilustrado na Figura 25.

Figura 25 - Mapa de co-citações de artigos



Fonte: O Autor (2019).

Na visualização em redes, o tamanho de cada nó representa a quantidade de citações (C) que o artigo recebeu na análise de co-citação. Os nós que possuem mais proximidade possuem uma relação mais forte de co-citação, ou seja, maior a quantidade de atores mais recentes que os citaram. Esta análise pode indicar pelos clusters formados a base teórica de determinadas linhas de pesquisa. Os artigos estão classificados pela força do link (FL). A rede de cocitação apresenta três clusters (CL), numerados na coluna da esquerda da Tabela 13.

Tabela 13 - Principais referências co-citadas

CL	Referências citadas	Artigo	C	FL
2	zhuang j, 2007, oper res, v55, p976, doi 10.1287/opre.1070.0434	Balancing Terrorism and Natural Disasters—Defensive Strategy with Endogenous Attacker Effort	31	100
1	bier v, 2007, j public econ theory, v9, p563, doi 10.1111/j.1467-9779.2007.00320.x	Choosing what to protect: strategic defensive allocation against an unknown attacker	20	71

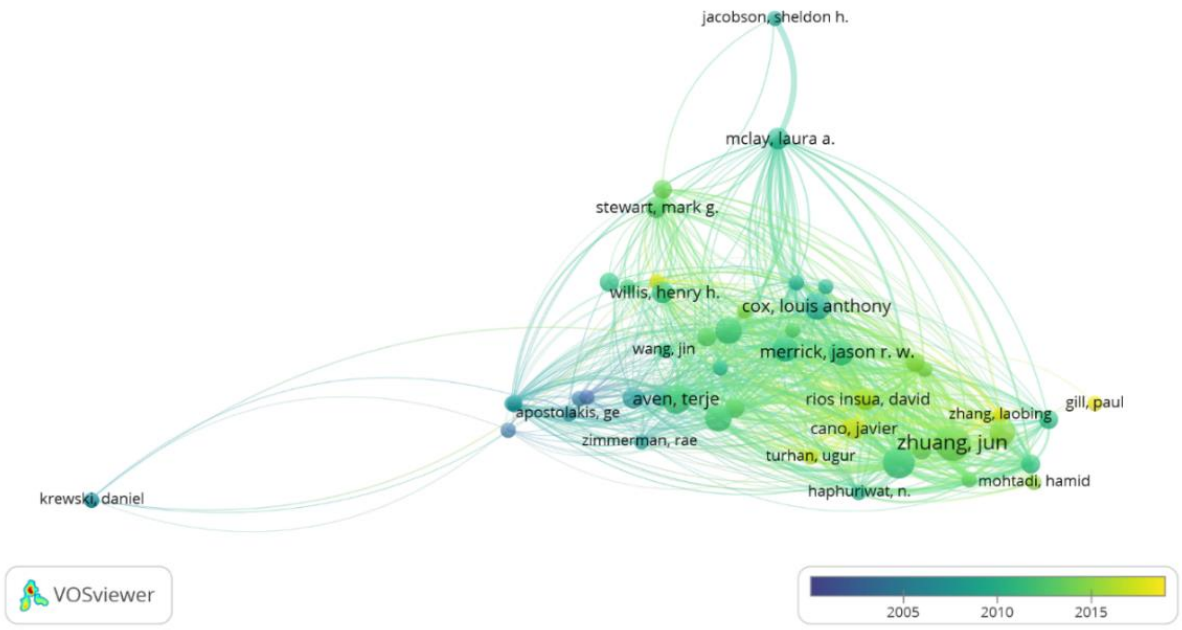
Tabela 1314 - Principais referências co-citadas (continuação)

CL	Referências citadas	Artigo	C	FL
1	parnell gs, 2010, risk anal, v30, p32, doi 10.1111/j.1539-6924.2009.01319.x	Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management Model	17	66
1	ezell bc, 2010, risk anal, v30, p575, doi 10.1111/j.1539-6924.2010.01401.x	Probabilistic Risk Analysis and Terrorism Risk	19	60
1	keeney rl, 2007, risk anal, v27, p585, doi 10.1111/j.1539-6924.2007.00910.x	Modeling Values for Anti-Terrorism Analysis	18	60
3	pate-cornell e., 2002, military operations, v7, p5	Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures.	19	57
2	brown g, 2006, interfaces, v36, p530, doi 10.1287/inte.1060.0252	Defending Critical Infrastructure	19	56
2	zhuang j, 2010, eur j oper res, v203, p409, doi 10.1016/j.ejor.2009.07.028	Modeling secrecy and deception in a multiple-period attacker–defender signaling game	15	52
3	major j, 2002, j risk finance, v4, p15, doi 10.1108/eb022950	Advanced Techniques for Modeling Terrorism Risk	15	48
1	o'sullivan t., 2006, decis anal, v3, p63	A decision analysis to evaluate the cost-effectiveness of MANPADS countermeasures	17	45
2	willis h. h., 2005, estimating terrorism	Estimating terrorism risk	15	44
3	garrick bj, 2004, reliab eng syst safe, v86, p129, doi 10.1016/j.ress.2004.04.003	Confronting the risks of terrorism: making the right decisions	15	21
3	kaplan s., 1981, risk anal, v1, p11, doi 10.1111/j.1539-6924.1981.tb01350.x	On The Quantitative Definition of Risk	15	14

Fonte: O Autor (2019).

Diferente da co-citação, a análise de link de acoplamento bibliográfico, constante na Figura 26 representa o link entre dois autores que citam o mesmo autor, indicando que os artigos que apresentam mais artigos citados comumente possuem maior nível de acoplamento bibliográfico. O acoplamento pode indicar pesquisas com temas ou bases próximas, núcleos referenciais de desenvolvimento científico, e até mesmo servir de referências de análise para futuros estudos. Foi estabelecido como critério o mínimo de 3 artigos publicados para análise, no contexto do *VOS viewer* impactam os artigos produzidos (A), as citações (C) e a normalização pela força do link (FL) na ordenação final.

Figura 26 - Visualização de sobreposição de acoplamento bibliográfico por autores



Fonte: O Autor (2019).

Com base na análise de visualização de sobreposição podem identificar que os nós conseguem indicar a temporalidade dos autores, bem como a intensidade e proximidade dos atores indicando que existe um núcleo forte de pesquisas relacionadas à ameaças inteligentes visando antecipar cenários e assessorar o processo decisório. Os clusters do acoplamento bibliográfico ficam demonstrados na Tabela 14, explicitando os integrantes por linha.

Tabela 1415 - Cluster do acoplamento bibliográfico

1. abkowitz, mark d.	haimes, yacov y.	mcgill, william l.	garrick, bj
apostolakis, ge	hope, bk	zimmerman, rae	lambert, jh
aven, terje	kaminskiy, mark	guikema, seth d.	wang, jin
ayyub, bilal m.	kujawski, edouard		
2. brown, gerald g.	keeney, ralph l.	parnell, gregory s.	levine, e. s.
cox, louis Anthony	merrick, jason r. w.	smith, christopher m.	lathrop, john
ezell, barry charles		von winterfeldt, detlof	
3. bier, vicki m.	mohtadi, hamid	wang, chen	zhuang, jun
haphuriwat, n.	reniers, genserik	zhang, laobing	shan, xiaojun
hausken, k.			
4. jackson, brian a.	lundberg, russell	stewart, mark g.	
latourrette, tom	mueller, john	willis, henry h.	
5. bhashyam, sumitra sri	kaplan, edward h	montibeller, gilberto	gill, paul
6. cano, javier	rios insua, david	turhan, ugur	
7. jacobson, sheldon h.	mclay, laura a.		
8. krewski, Daniel	lemyre, l		

Fonte: O Autor (2019).

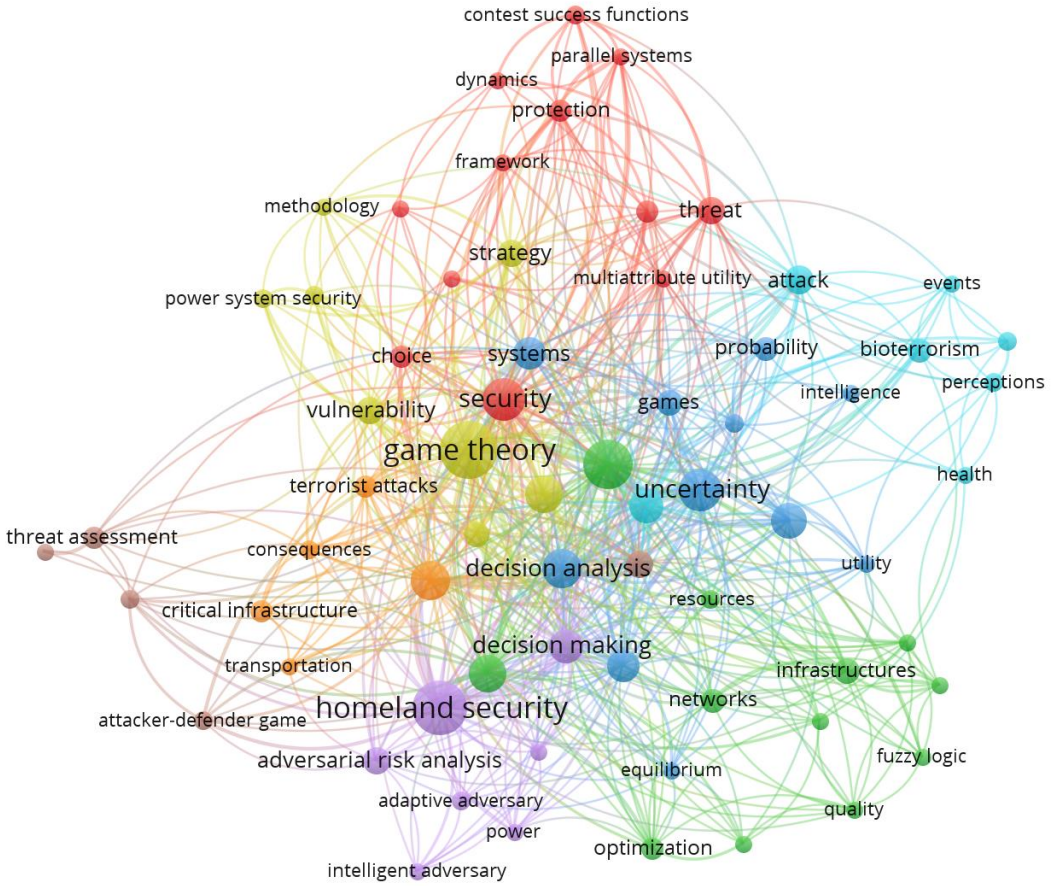
5.4 PALAVRAS-CHAVE

- Quais as principais palavras-chaves encontradas por meio da análise bibliométrica?

A análise de palavras chaves também é um excelente referencial de pesquisa. Em alguns casos, especialmente na literatura antiga, estas palavras são restritas a palavras individuais, nos artigos mais modernos podem resultar em termos. A análise das relações de co-ocorrência entre palavras chaves é determinada pelo número de artigos da base de pesquisa em que as duas palavras aparecem simultaneamente, no título, resumo ou nas listas de palavras-chave (VAN ECK; WALTMAN, 2014, p.287).

Analisando os links entre as palavras chaves, e as redes formadas, é possível identificar as evoluções na pesquisa conforme agregação de termos com base nas temáticas indicadas pelos links entre as palavras chaves. O tamanho dos nós indicam a frequência de ocorrência de uma palavra-chave, e sua relação é mais próxima conforme sua proximidade. A Figura 27 apresenta as redes de co-ocorrências das palavras chaves ligadas a pesquisa principal.

Figura 27 - Mapa de co-ocorrência de palavras chaves em redes



Fonte: O Autor (2019).

O critério para seleção das palavras foi de pelo menos três ocorrências, nos 167 artigos selecionados, resultando em 69 palavras chaves e oito clusters, conforme a Tabela 15. Foram excluídas as seguintes palavras chaves por serem o próprio tema macro da pesquisa: *risk*, *terrorism*, *terrorism risk*, *terrorism risk analysis*, e *risk analysis.*

Tabela 15 - *Clusters* formados na análise de co-citação de palavras chaves

Cl	Palavras Chaves
1	*Choice, Contest Success Functions, Defense, Dynamics, Emergency Response, Framework, Multiattribute Utility, Parallel Systems, Protection, Security, Simulation, Threat*
2	*Fuzzy Logic, Infrastructures, Natural Disasters, Networks, Optimization, Programs, Quality, Resource Allocation, Resources, Risk Assessments, Safety, Vulnerability Analysis*
3	*Aviation Security, Counterterrorism, Decision Analysis, Equilibrium, Games, Intelligence, Probabilistic Risk, Probability, Systems, Uncertainty*
4	*Attacker, Game Theory, Methodology, Power System Security, Risk Management, Strategy, Terrorist Threats, Vulnerability*
5	*Adaptive Adversary, Adversarial Risk Analysis, Decision Making, Homeland Security, Intelligent Adversary, Power, Terrorism Applications*

Tabela 1615 - Clusters formados na análise de co-citação de palavras chaves (continuação)

Cl	Palavras Chaves
6	*Attack, Bioterrorism, Events, Health, Management, Perceptions, Risk Communication*
7	*Consequences, Critical Infrastructure, Models, Terrorist Attacks, Transportation,*
8	*Attacker-Defender Game, Decision, Forensic Science, Terrorist, Threat Assessment*

Fonte: O Autor (2019).

5.5 CRITÉRIOS DA ANÁLISE DE RISCO

- Qual a influência dos critérios selecionados no resultado de uma análise de risco de terrorismo?

A definição e compreensão do risco de terrorismo depende de critérios, alguns importados das definições tradicionais de análise de risco e outros particulares da temática terrorismo. A abordagem tradicional ensina que o risco é função da probabilidade e consequência, definição relevante para fenômenos naturais e mecânicos, mas que carece de aprimoramento em virtude das interações entre indivíduos e organizações motivadas (chamados na literatura de adversários inteligentes, racionais ou adaptativos).

A capacidade de adaptação do adversário aumenta o grau da incerteza, com reflexos diretos no estudo da ameaça, interações, probabilidades e consequências. Aumenta o número de variáveis necessárias para a análise do risco e construção do cenário com critérios robustos de forma a proporcionar conhecimento suficiente para assessorar a tomada de decisão.

Após o 9-11, o mundo passou a olhar a gerenciamento de risco com outro foco, passando a usar ferramentas analíticas disponíveis para entender as ameaças envolvidas, valorar as vulnerabilidades por meio de um processo analítico visando avaliar o risco e mitigar a ameaça. Os estudos dos eventos de baixa probabilidade e alta consequência dotados da incerteza passaram a ser norteadores da pesquisa nas abordagens para o desenvolvimento de uma base para a tomada de decisão como no método de avaliação quantitativa de riscos (QRA), cujo cerne é a teoria dos cenários estruturantes (GARRICK *et al.*, 2004, p. 130).

> Como os cenários, consequências e probabilidades são agregados é uma questão de preferência, mas as distribuições de probabilidade observadas anteriormente são escolhas populares, pois revelam não apenas as consequências, mas também as incertezas envolvidas. No decorrer da aplicação do QRA a atos evidentes, como sabotagem e terrorismo, a teoria foi modificada pelos profissionais para acomodar de

> forma mais eficiente as diferenças entre a análise de acidentes e a análise terrorista[23] (GARRICK *et al.*, 2004, p. 130).

No modelo americano, vários métodos relevantes no estabelecimento de prioridades para proteção de infraestruturas críticas baseiam-se na fórmula: Risco = Consequência x Vulnerabilidade x Ameaça, como no exemplo de alocações de recursos na Análise e Gerenciamento de Risco para Proteção de Dados Críticos (RAMCAPTM) usada pelo Departamento of Homeland Security sendo um modelo de Avaliação Probabilística do Risco (PRA) (COX, 2008, p. 1749-1750). As definições constantes no RAMCAPTM estão apresentadas na Tabela 16.

Tabela 1176- Definições do RAMCAP

Definições do RAMCAP
Risco: O potencial de perda ou dano devido à probabilidade de um evento indesejado e suas consequências adversas, sendo medido pela combinação da probabilidade e consequências de um evento adverso, ou seja, consecução de uma ameaça, com considerações sobre a incerteza. Basicamente calculado como fruto de três fatores: ameaça, vulnerabilidade e consequência.
Risco condicional: Abordagem desconsiderando a intenção do adversário, com foco nas consequências, vulnerabilidades e os recursos do atacante, sendo utilizada para decisões de gerenciamento de risco de longo prazo. A capacidade adversária, as contramedidas e as vulnerabilidades residuais geralmente são integradas na forma de probabilidade do sucesso adversário.
Consequência: O resultado de uma ocorrência de evento, incluindo perdas e efeitos imediatos, de curto e longo prazo, diretos e indiretos, podendo incluir vidas, lesões, perdas financeiras e econômicas, danos ambientais, bem como outros efeitos mais difusos como desdobramentos políticos, perda de moral, incapacidades operacionais e outros danos colaterais.
Ameaça: qualquer indicação, circunstância ou evento com potencial para causar a perdas ou danos a um ativo ou população, sendo baseada na análise da intenção (motivação) e capacidade de um adversário realizar ações que causem dano a um ativo ou população. É descrito como produto da ameaça (probabilidade de ocorrência de um evento intencional não desejado), vulnerabilidade (probabilidade de sucesso no ataque) e consequências (perdas resultantes do impacto de um ataque bem-sucedido)

Fonte: Adaptado de Cox (2008).

[23] How the scenarios, consequences, and likelihoods are aggregated is a matter of preference, but the probability distributions noted earlier are popular choices as they reveal not only the consequences, but the uncertainties involved. In the course of applying QRA to overt acts such as sabotage and terrorism, the theory has been modified by practitioners to more efficiently accommodate the differences between accident analysis and terrorista analysis.

Cresce a importância da análise da incerteza, principalmente nos adversários inteligentes, fruto de um processo dinâmico resultante de interações entre atacante e defesa. A representação da incerteza se relaciona ao processo decisório do adversário e no seu comportamento adverso previsto, a indefinição do tempo, forma e modo, bem como a sua capacidade de se adaptar aos movimentos de defesa, sendo mais ampla que a probabilidade (GUIKEMA, 2012, p.1119).

5.6 MODELOS DE RISCO

- *Quais os modelos principais de abordagem ao risco terrorista para os adversários inteligentes?*

Os atentados terroristas de 11 de setembro de 2001 nos Estados Unidos estimularam os EUA a fortalecer suas defesas domésticas e a perseguir os responsáveis pelos atos terroristas, liderando um esforço global contra o terrorismo em diversas áreas. Após o evento os presidentes das Academias Nacionais de Pesquisa (Ciências, Engenharia, Medicina e Conselho Nacional) ofereceram os seus conselhos e afirmaram que a nova guerra exigiria um enfoque na complexa interação entre questões tecnológicas, sociológicas e políticas (NRC, 2002, p. 9).

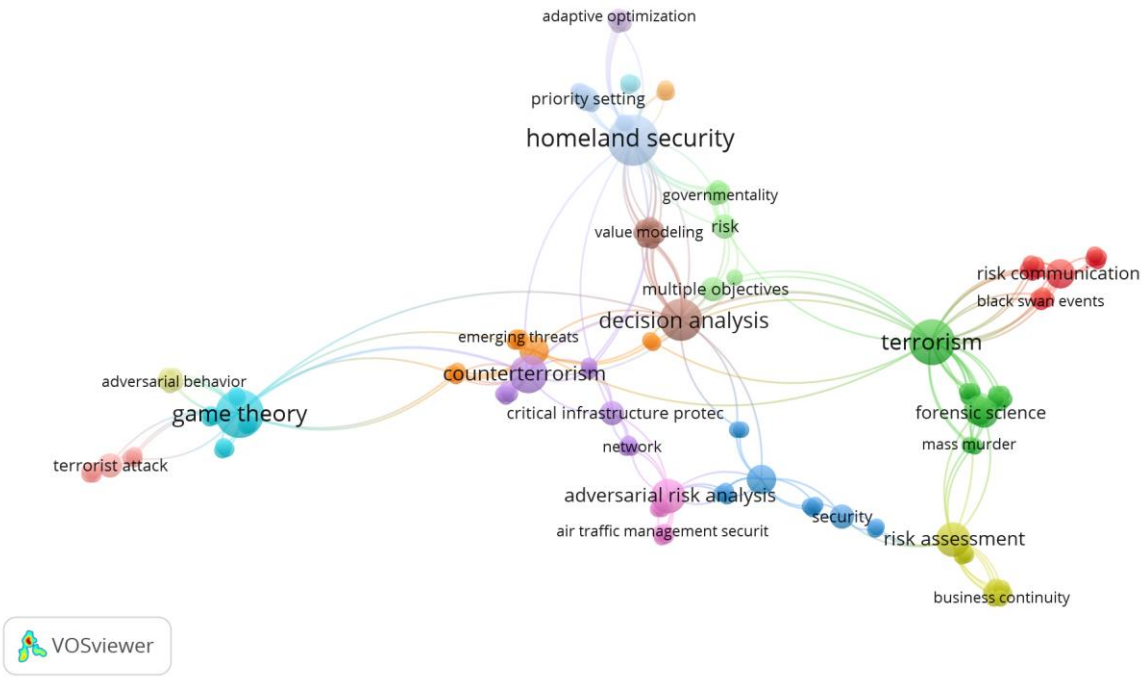
Apesar da análise de risco de terrorismo ser necessária formalmente como disciplina para todo o governo, academia e setor privado, existiam limitações para utilizar métodos quantitativos. Baseado nisso foi realizado uma distinção entre os métodos qualitativos e quantitativos de avaliação de risco, com pleno convencimento de que era fundamental utilizar métodos sistemáticos e rigorosos para quantificar as incertezas em virtude do potencial de consequências catastróficas. Métodos qualitativos podem ser utilizados para análise dos riscos de ataques terroristas, mas primordial é quantificar o risco de ameaças com potencial de consequências catastróficas (GARRICK, 2004, p.132-133).

Proteger infraestruturas complexas contra terroristas, que são considerados adversários inteligentes, é fundamentalmente diferente de proteger contra acidentes aleatórios ou atos da natureza. As avaliações do risco de segurança têm utilizado metodologias híbridas que associam uma análise qualitativa a uma análise quantitativa na identificação e caracterização do perfil de agressores ou terroristas. Técnicas quantitativas que envolvem análises probabilísticas condicionais de eventos e consequências têm sido desenvolvidas com base na opinião de especialistas, determinando probabilidades subjetivas de ocorrência dos eventos e avaliação conceitual da criticidade dos alvos potenciais, bem como das consequências dos ataques destas ameaças (WILLIS, 2007).

Os adversários inteligentes são um componente fundamental da análise de risco do terrorismo. Ao contrário dos riscos naturais e de engenharia, os adversários inteligentes adaptam seu comportamento às ações do defensor. Eles se adaptam a ações futuras prováveis observadas, percebidas e imputadas por aqueles que defendem o sistema que estão tentando influenciar. Os modelos de avaliação de risco precisam considerar esses comportamentos adaptativos em potencial para fornecer estimativas precisas de risco futuro de adversários inteligentes e apoiar adequadamente a tomada de decisões de gerenciamento de risco.

Considerando os artigos publicados nos últimos cinco anos, identificamos na Figura 28 os principais clusters formados na análise das palavras chaves dos autores. A análise de decisão e a análise de risco adversário, os métodos de aplicação mais recente e mais discutidos atualmente com o objetivo de reduzir as incertezas, detém posição central no gráfico, com múltiplos links, ligados principalmente a infraestruturas críticas, gerenciamento do tráfico aéreo, multi-objetivos, ameaças emergentes, e contraterrorismo. A teoria de jogos aparece com proximidade ao comportamento adversário e ataque terrorista, demonstrando pela imagem duas características do seu emprego.

Figura 28 - Palavras chaves de autores dos últimos 5 anos



Fonte: O Autor (2019).

Conforme Guikema (2012), são quatro os principais tipos de modelos utilizados para adversários inteligentes. A análise de risco probabilística (árvore baseada em eventos) onde através da elicitação de especialistas são estimadas as probabilidades das ações adversas como variáveis aleatórias (GARRICK *et al.*, 2004, p.129-176). Com base na probabilidade as decisões são orientadas.

Métodos de análise de decisão onde o comportamento do adversário é analisado como decisões tomadas maximizadas pela utilidade, a partir das preferências e convencimentos do adversário, avaliadas pela defesa, sobre o cenário geral e suas próprias ações (PARNELL *et al.*, 2010, p.32-48).

Métodos teóricos de jogos que utilizam o conceito analítico das prováveis decisões, abordando a adaptação adversária como decisões estratégicas modeladas nas prováveis ações da defesa, e tratam a adaptação adversária como decisões tomadas com base em uma avaliação estratégica e modelagem das ações prováveis do defensor, avaliadas pela defesa, sobre o cenário geral e suas próprias ações, onde ninguém fica com o resultado desejado, mas com o menos ruim, não considerando também a incerteza (DIGNE *et al.*, 2009, p.31-43; PATE-CORNELL, GUIKEMA, 2002, p-5-23).

Métodos estatísticos e machine-learning (ML) também são empregados e desenvolvem modelos de comportamento adversário, como padrões de futuros ataques, baseados em históricos de eventos e outros cruzamentos de padrões (La FREE *et al.*, 2009, p.445-473).

Os quatro métodos apresentados apresentam formas distintas de modelagem dos adversários inteligentes, uns maximizando a utilidade na modelagem (PRA, análise de decisão e teoria dos jogos), enquanto o ML foca no comportamento histórico. A teoria dos jogos, as árvores de eventos e os métodos estatísticos se baseiam na natureza estratégica da ameaça, com víes distintos, a primeira por modelagem, e os demais conforma a elicitação de dados. Não existe ainda um padrão reconhecido, e o tema encontra-se em pesquisas das propriedades desejáveis para um modelo definido conforme Guikema (2012).

Insua *et al*. (2009) aborda o confronto entre dois adversários inteligentes que tomam decisões dinâmicas ou sequenciais, sem resultado previsível e expectativa de equilíbrio podem ser estudados pela análise de risco adversária, somando conceitos de teoria dos jogos e PRA. A análise do risco adversário utiliza a modelagem da estrutura de decisão da parte atacante (adversário) para gerar um modelo probabilístico de representação do ataque. As informações são utilizadas para solução dos problemas de decisão da defesa, considerando a assimetria das

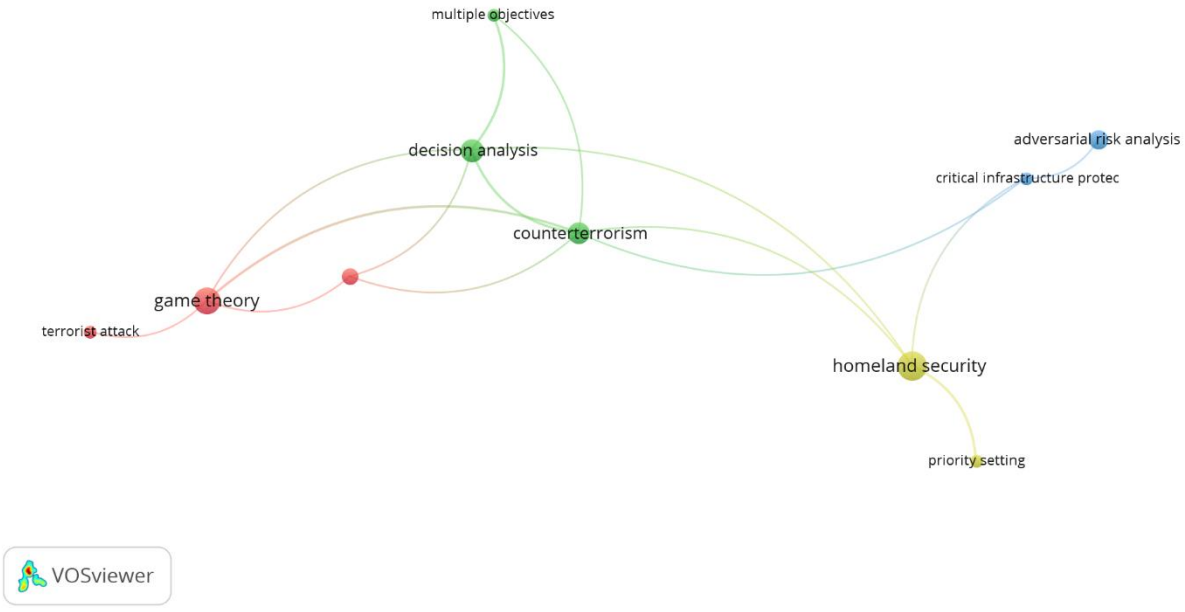
informações, as incertezas e espelhamento das ações do adversário baseado em um espelhamento continuo de decisões (INSUA *et al*., 2009).

5.7 TENDÊNCIAS

- Quais são as tendências da pesquisa para as ameaças inteligentes mais relevantes no cenário atual que podem impactar no cenário nacional causando perdas e danos?

Com base na análise dos cinco últimos anos de publicação, a Figura 29 demonstra por meio da análise das palavras chaves dos autores com o critério de pelo menos duas ocorrências, a formação da seguinte rede contendo dez nós, formando quatro clusters: game theory, probabilistic risk analysis e terrorist attack; counterterrorrism, decision analysis e multiple objective; adversarial risk analysis e critical infrastructure protection; homeland security e pirority setting.

Figura 29 - Rede de palavras-chaves de autores nas tendências atuais



Fonte: O Autor (2019).

Para refinamento da análise, apresentada na Tabela 17 como palavras-chaves (PC), ocorrências (O) e força do link (FL) foram excluídas as seguintes palavras: terrorism, risk, risk

analysis e security por serem genéricas ao tema. Conforme sugestão do programa, dois *clusters* foram suprimidos por não possuírem links com o principal: *forensic science*, *threat assessment*, e *risk assessment;* e *risk communication.*

Tabela 1718 - Palavras chaves de autores 2014-2018

Cluster	PC	O	FL
2	*decision analysis*	6	11
2	*counterterrorism*	5	8
	~~*forensic science*~~	~~3~~	~~7~~
	~~*threat assessment*~~	~~3~~	~~7~~
4	*homeland security*	9	6
1	*game theory*	8	5
2	*multiple objectives*	2	5
1	*probabilistic risk analysis*	3	4
	~~*risk assessment*~~	4	4
3	*critical infrastructure protection*	2	3
3	*adversarial risk analysis*	4	2
4	*priority setting*	2	2
	~~*risk communication*~~	3	2
1	*terrorist attack*	2	1

Fonte: O Autor (2019).

A formação dos clusters indica as tendências de pesquisa na atualidade, onde aos temas indicados como *Adversarial Risk Analysis* e *Decision Analysis* apresentam como características a melhoria no processo decisório por meio da redução da incerteza, uma fragilidade dos modelos apenas probabilísticos, bem como a preocupação com adversários inteligentes, capazes de ir além do acaso do evento e interagir com múltiplas ações. As demais palavras-chaves indicam a preocupação permanente com a segurança interna e as infraestruturas críticas que dão sustentação a toda a sociedade.

Nesse contexto, entende-se como ações que possam fazer oposição as ameaças inteligentes que possam causar perdas ao Estado:

- O desenvolvimento de uma análise da ameaça em nível nacional de maneira que possa ser monitorada continuamente, servindo de base para edição de relatório anual de ameaças e para elaboração de políticas públicas e programas no campo da segurança econômica, interna e nacional.

- Elaboração de estudo para implantação de um centro estratégico nacional de avaliação de ameaças por meio da cooperação entre órgão de segurança e defesa.

- Desenvolvimento de programa acadêmico de cunho nacional criando centros de excelências nas principais universidades para o desenvolvimento de pesquisas direcionadas ao impacto das ameaças em cada área governamental.

- A aplicação de modelo multicritérios de decisão para priorização de abordagem a ameaças inteligentes.

- O desenvolvimento de modelo de gestão de riscos com ênfase na expansão do crime organizado transnacional ameaça que estreita ações com o terrorismo.

- O estudo da integração entre as fontes de inteligência e sua integração com as bases de dados visando o desenvolvimento de sistema de apoio a decisão que faça o processamento de uma grande massa de dados.

5.8 MODELOS DE RISCO PARA O CONTEXTO NACIONAL

- Quais os modelos de abordagem estratégica do risco terrorista que podem ser aplicados no contexto nacional de forma a fortalecer as estratégias nacionais de consecução dos objetivos estratégicos com ênfase nas atribuições da PF como polícia judiciária, marítima, aeroportuária e de fronteiras?

A grande oportunidade para reforçar a segurança interna do país por meio da atuação da Polícia Federal (PF) exercendo as suas atribuições constitucionais de Polícia Marítima, Aeroportuária e de Fronteiras (PMAF) é a integração dos métodos e modelos apresentados no trabalho na produção de conhecimento de inteligência, e nas atividades de Polícia Judiciária da União. A segurança interna atua em área concorrente com a Segurança Nacional, e a capacidade de inteligência, antiterror e investigativa, focadas no monitoramento de ameaças, construções de cenários e capacidade de ações a Polícia Federal, atuando por meio da inteligência e do antiterrorismo na construção de cenários.

Segundo Haimes (1998, 2001) "todo o processo de avaliação e gestão de risco é essencialmente uma síntese e amalgamação do empírico e do normativo, do quantitativo e do qualitativo, e da evidência objetiva e subjetiva"[24]. A sua construção é multidisciplinar, fruto de trabalho de analistas e especialistas, somando as contribuições de pesquisadores da área de exatas com os modelos numéricos e estatísticos, com os de humanas, área de ciências e

[24] is essentially a synthesis and amalgamation of the empirical and the normative, the quantitative and the qualitative, and of objective and subjective evidence.

comportamentais-organizacionais, que contribuíram com a compreensão e dimensionamento das interações e percepções.

A análise das ameaças terroristas é uma tarefa extremamente complexa, com impacto direto na segurança interna do país, visto que os riscos resultantes são de baixa probabilidade, alto impacto e um nível elevado de incerteza. Dada sua relevância, a integração dos dados disponíveis nas diversas fontes deve ser utilizada como matéria prima pelos analistas de inteligência com a finalidade de oferecer capacidade de redução da incerteza e ordenação dos riscos a fim de propiciar o estabelecimento das prioridades das ações de contrainteligência para negar as ameaças e permitir a consecução dos objetivos estratégicos nacionais (NRC, 2002, p.294).

Cabe destacar o prefácio da Estratégia Nacional de Contrainteligência dos Estados Unidos que explicita que "os objetivos estratégicos essenciais não devem mudar a cada ano; no entanto o processo de gestão de riscos exige que a Comunidade de Contrainteligência atue continuamente a avaliar vulnerabilidades, oportunidades e desafios" (EUA, 2007, p. 6)

O processo holístico de decisões antiterroristas apresentado na Figura 30 visa abordar o problema da definição da integração entre atores, fluxo de informações, incertezas, processos e riscos existentes no atual modelo decisório na Polícia Federal. A divisão temporal em passado, presente e futuro permite explicitar a execução das ações de forma cronológica, criando uma lógica e sincronismo para eficiência do processo.

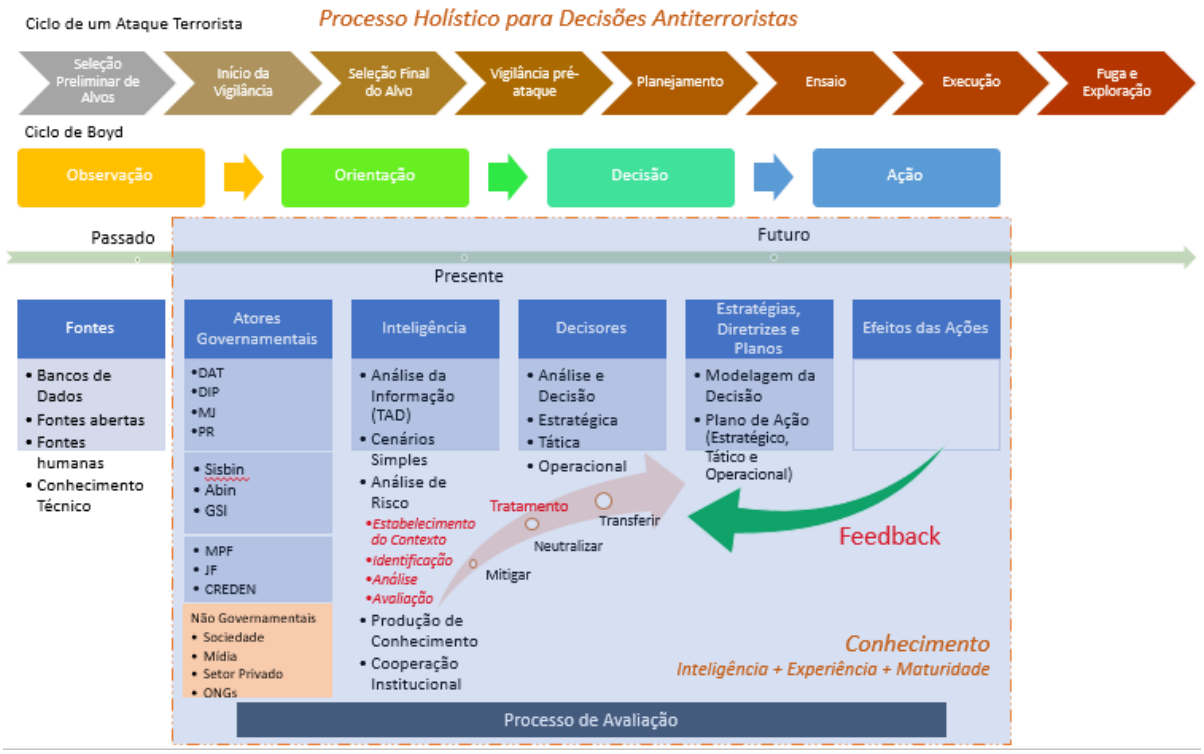
A integração da análise de risco com o processo decisório na fase de inteligência (presente), lastreada pela base teórica pretérita (passado) e o monitoramento dos atores de forma dinâmica, oferece as condições necessárias para uma tomada de decisão segura, com subsídios para a elaboração de estratégicas, políticas e diretrizes visando negar as ameaças e garantir a consecução dos objetivos estratégicos.

Ao compararmos as fases de um ataque terrorista, que segue a mesma lógica de uma ação de operações de inteligência, onde existe uma seleção preliminar de alvos, o início da vigilância, a seleção final do alvo, a vigilância pré-ataque, o planejamento da ação em si, o ensaio da execução do atentado, a execução em si, e a fuga e exploração da publicidade. A fuga ocorre em casos não suicidas, mas ambas as situações são seguidas pela fase do objetivo maior do terrorismo: atingir o oxigênio da publicidade.

O processo de tomada de decisão é apresentado por vários modelos, onde por meio de reações a estímulos formam-se as hipóteses como resultado. Para cada hipótese são desenvolvidas as opções, e a partir daí existe a decisão. O Coronel John Boyd (1987)

desenvolveu e introduziu um modelo definitivo de tomada de decisão: o ciclo OODA. Como parte de sua teoria de conflito “transiente, assimétrico e rápido” ele introduziu o ciclo composto dos seguintes estágios: observar, orientar, decidir e agir (OODA). Tem como premissa que a tomada de decisão é fruto de um comportamento racional com descrição nos quatro estágios (LUESSEN, 2003, p.69).

Figura 30 - Processo holístico de decisão antiterrorista



Fonte: Adaptado de Cohen and Blanco (2014).

As quatro principais classes de risco para a segurança interna são: riscos para as vidas humanas e para a propriedade individual, liberdade e liberdade; riscos para as infraestruturas organizacionais e para a continuidade das operações do governo, incluindo as infraestruturas militares, e de concentração de dados e informações; riscos para infraestruturas críticas cibernéticas e físicas; e riscos para os setores socioeconômicos. É imperativo a identificação detalhada dessas fontes de risco e a capacidade de profundidade no conhecimento, a fim de assessorar uma tomada de decisão sólida, possível somente com a integração entre integração do conhecimento produzido das fontes e integrado com os demais atores (HAYMES, 2002, p.37).

As decisões derivadas do ciclo devem ser capazes de atender aos três níveis de decisão: estratégico, onde o foco são as políticas e planos nacionais do órgão ou ações que possuam aderência extra instituição, demandando que as decisões sejam pautadas em conhecimento que possam subsidiar a elaboração de políticas e programas e que miram os objetivos estratégicos.

As de cunho tático, que envolvem os desdobramentos dos planos nacionais nas unidades especializadas e resultam em ações que contribuem para o somatório de resultados a fim negar as ameaças antecipadas e evitar a concretização dos riscos, servindo de ferramentas para construção do futuro desejado.

A análise de ameaças deve ser a referência para formulação de estratégias nacionais de defesa e outros planos de contingência contra infraestruturas críticas e alvos sensíveis, assessorados nesse processo decisório complexo pela Polícia Federal com conhecimentos que abordem as ameaças e vulnerabilidades de forma dinâmica, antecipando cenários e apresentando ações possíveis para identificação de novos problemas e oportunidades a fim de fortalecer a segurança interna e permitir a priorização de ações com foco na defesa da nação (NRC, 2002, p.343).

O desenvolvimento de políticas públicas necessita de monitoramento constante de cenários a fim de permitir a continuidade do planejamento de longo prazo para orientar as ações estatais indo além de governos, mas sim no interesse da nação e de acordo com os objetivos estratégicos suportados pelo trabalho de inteligência no assessoramento estratégico, sendo checado e refinado por meio da comunicação permanente.

A fim de se atingir o sucesso e se negar as ameaças terroristas, é fundamental que o processo decisório se conclua antes da consecução do objetivo criminoso, por meio do trabalho de inteligência e análise de dados que permitam a negação da ameaça por meio da ação representada pelo Ciclo de Boyd e antes da execução do atentado.

O ciclo se enquadra perfeitamente no processo decisório antiterrorista apresentado, onde a vantagem tática é obtida pela redução da incerteza fruto do trabalho intelectual de produção do conhecimento de inteligência, suportado pela integração de bases disponíveis e demais atores, visando garantir as condições de tomada de decisão antes do adversário inteligente completar o seu próprio ciclo. O constante feedback oferece condições de atualização de cenários e a maior possibilidade de sucesso frente as adaptações do adversário, minando suas capacidades e negando a ameaça.

6 CONCLUSÕES E SUGESTÕES PARA TRABALHOS FUTUROS

Seguem as conclusões e algumas sugestões para novos estudos relacionados a temática abordada neste trabalho.

6.1 CONCLUSÕES

Com base na análise e estudo dos conceitos e definições, integrando o contexto e as ameaças atuais ao Estado Democrático de Direito, identificamos que a produção acadêmica no tema análise de risco terrorista evoluiu de forma crescente a partir de 2001, com pequenos momentos de retração, e retomada posterior em virtude de eventos de baixa probabilidade e alto impacto, que demonstraram a necessidade de ampliação de vigilância e demandas crescentes de alocação de recursos contraterrorismos que resultam em investimentos.

O panorama estratégico do emprego da análise de risco terrorista no contexto da SP&D apresenta o crescimento prioritário das pesquisas continuadas em virtude do advento de novas técnicas e táticas empregadas, bem como da ocorrência de ataques múltiplos com ausência de lógica. Após 2013, ocorre um recrudescimento dos ataques, principalmente nos alvos ocidentais, contra países que atuavam nas coalizões contra o Estado Islâmico, ocorre um novo pico de crescimento da produção, fomentado pelas perdas de vidas e outros danos causados pelos atentados.

A capacidade de adaptação do adversário aumenta o grau da incerteza, com reflexos diretos no estudo da ameaça, interações, probabilidades e consequências. Aumenta o número de variáveis necessárias para a análise do risco e construção do cenário com critérios robustos de forma a proporcionar conhecimento suficiente para assessorar a tomada de decisão.

As abordagens as ameaças inteligentes se torna prioritária em função da necessidade de antecipação de cenários para tomadas de decisão buscando mitigar riscos dos altos impactos, negando a ameaça por meio da construção do conhecimento sobre a interpretação das intenções dos adversários, a fim de quebrar seu ciclo de decisão e reduzir as incertezas face a multiplicidade de possíveis alvos.

Os modelos de avaliação de risco precisam considerar esses comportamentos adaptativos em potencial para fornecer estimativas precisas de risco futuro de adversários inteligentes e apoiar adequadamente a tomada de decisões de gerenciamento de risco. A nova forma de atuação leva as forças de segurança a reverem seus métodos e proporciona para academia a

chance de produzir estudos que venham antecipar as ameaças e tendências, contribuindo para o aprimoramento da defesa e proteção da sociedade por meio da integração com as autoridades governamentais.

Ainda não existe um padrão reconhecido uniformemente para a análise do risco terrorista, e o tema encontra-se em pesquisas das propriedades desejáveis para que seja definido um modelo mais eficiente de abordagem ao problema. Os principais métodos apresentam formas distintas de modelagem dos adversários inteligentes, uns maximizando a utilidade na modelagem (PRA, análise de decisão e teoria dos jogos), enquanto o machine learning foca no comportamento histórico. A teoria dos jogos, as árvores de eventos e os métodos estatísticos se baseiam na natureza estratégica da ameaça, com viés distintos, a primeira por modelagem, e os demais conforma a elicitação de dados.

O tema mais recente, análise de risco adversário, aborda o confronto entre dois adversários inteligentes utiliza a modelagem da estrutura de decisão gerando informações que são utilizadas para solução dos problemas de decisão da defesa, considerando a assimetria das informações, as incertezas e espelhamento das ações do adversário baseado em um espelhamento continuo de decisões.

As tendências de pesquisa na atualidade indicam para temas como Risco Adversário e Análise da Decisão onde se busca a melhoria no processo decisório por meio da redução da incerteza, bem como a preocupação com adversários inteligentes, capazes de ir além do acaso do evento e interagir com múltiplas ações.

A grande oportunidade para reforçar a segurança interna do país por meio da atuação da Polícia Federal (PF) exercendo as suas atribuições constitucionais de Polícia Marítima, Aeroportuária e de Fronteiras (PMAF) é a integração dos métodos e modelos de análise de risco apresentados no trabalho com a produção de conhecimento de inteligência, e nas atividades de Polícia Judiciária da União. A segurança interna atua em área concorrente com a Segurança Nacional, e a capacidade de inteligência, antiterror e investigativa, focadas no monitoramento de ameaças, construções de cenários e capacidade de ações a Polícia Federal. As atuações por meio da inteligência e do antiterrorismo na construção de cenários podem ser robustecidas pelas aplicações nos níveis estratégico, operacional e tático, como fruto da utilização e aperfeiçoamento de um modelo de decisão antiterrorista apresentado, com maior lastro para melhores decisões, inclusive no fator tempo.

No contexto do processo decisório, a análise do risco deve ser parte fundamental na fase de inteligência, devendo ser elaborada com forte análise de base pretérita de conhecimentos e

informações, a fim de permitir a identificação e o monitoramento dos atores de forma dinâmica, oferecendo as condições necessárias para uma tomada de decisão segura, com subsídios para a elaboração de estratégicas, políticas e diretrizes visando negar as ameaças e garantir a consecução dos objetivos estratégicos.

A análise de ameaças deve ser a referência para formulação de estratégias nacionais de defesa e outros planos de contingência contra infraestruturas críticas e alvos sensíveis, assessorados nesse processo decisório complexo pela Polícia Federal com conhecimentos que abordem as ameaças e vulnerabilidades de forma dinâmica, antecipando cenários e apresentando ações possíveis para identificação de novos problemas e oportunidades a fim de fortalecer a segurança interna e permitir a priorização de ações com foco na defesa da nação.

6.2 SUGESTÕES PARA TRABALHOS FUTUROS

Como trabalhos futuros a esta dissertação, sugere-se:

- Desenvolvimento de modelo de análise de contexto apoiada por ferramentas e técnicas da Ciências de Dados;

- Análise comparativa das ameaças inteligentes nas diversas formas de ocorrência do terrorismo;

- Estudo dos impactos econômicos resultantes de ações das ameaças inteligentes nos custos de defesa e segurança nacional; e

- Desenvolvimento de um Sistema de Apoio a Decisão capaz de processar análises de riscos terroristas.

O estudo do risco é ação estratégica fundamental para ar suporte ao desenvolvimento dos Estados, contribuindo de forma indelével para a formulação de políticas públicas e os seus planejamentos estratégicos. A integração entre a área acadêmica e as áreas governamentais que atuam com assuntos estratégicos pode permitir um ganho relevante com investimentos em pesquisas sobre o risco e seus impactos no desenvolvimento econômico. A Polícia Federal identificou esse potencial e avança como pioneira e referência na temática, servindo de modelo para a administração pública federal.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO 31000- 2009:** gestão de riscos - princípios e diretrizes. Rio de Janeiro: ABNT, 2009.

AMARAL, Arthur Bernardes do. **A Guerra ao terror e a tríplice fronteira na agenda de segurança dos estados unidos**. 2008. Dissertação (Mestrado em Relações Internacionais) - Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2008.

ASKELAND, Tore; FLAGE, Roger; AVEN, Terje. Moving beyond probabilities–strength of knowledge characterisations applied to security. **Reliability Engineering & System Safety**, v. 159, p. 196-205, 2017.

ATLAS, Ronald M. Bioterrorism: from threat to reality. **Annual Reviews in Microbiology**, v. 56, n. 1, p. 167-185, 2002.

AVEN, Terje; GUIKEMA, Seth. On the concept and definition of terrorism risk. **Risk analysis**, v. 35, n. 12, p. 2162-2171, 2015.

BAKIR, Niyazi Onur. A Stackelberg game model for resource allocation in cargo container security. **Annals of Operations Research**, v. 187, n. 1, p. 5-22, 2011.

BAYKAL-GUERSOY, Melike *et al*. Infrastructure security games. **European Journal of Operational Research**, v. 239, n. 2, p. 469-478, 2014.

BIER, Vicki M. Choosing what to protect. **Risk Analysis: An International Journal**, v. 27, n. 3, p. 607-620, 2007.

BIER, Vicki M.; HAPHURIWAT, Naraphorn. Analytical method to identify the number of containers to inspect at US ports to deter terrorist attacks. **Annals of Operations Research**, v. 187, n. 1, p. 137-158, 2011.

BIER, Vicki M.; KOSANOGLU, Fuat. Target-oriented utility theory for modeling the deterrent effects of counterterrorism. **Reliability Engineering & System Safety**, v. 136, p. 35-46, 2015.

BOMPARD, Ettore *et al*. Risk assessment of malicious attacks against power systems. **IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans**, v. 39, n. 5, p. 1074-1085, 2009.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.** Brasília: Presidência da República, [1988]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Constituicao.htm. Acesso em: 15 mai. 2018.

_____. **Avaliações de Riscos.** Agência Brasileira de Inteligência. Brasília, [2016]. Disponível em: http://www.abin.gov.br/atuacao/produtos/avaliacoes-de-riscos/. Acessado em: 14 ago. 2018.

_____. **Decreto Nº 7.168, de 5 maio 2010.** Brasília: Presidência da República, [1980]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/decreto/d7168.htm. Acesso em: 15 ago. 2018.

_____. **Lei nº 13.260, de 16 de março de 2016.** Brasília: Presidência da República, [1980]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 01 ago. 2018.

BRERETON, Pearl *et al*. Lessons from applying the systematic literature review process within the software engineering domain. **Journal of systems and software**, v. 80, n. 4, p.571-583, 2007.

BUEDE, Dennis M. *et al*. Using plural modeling for predicting decisions made by adaptive adversaries. **Reliability Engineering & System Safety**, v. 108, p. 77-89, 2012.

BULLOCK, Richard K.; DECKRO, Richard F.; WEIR, Jeffery D. Methodology for competitive strategy development. **Computers & operations research**, v. 35, n. 6, p. 1865-1873, 2008.

BUSBY, Jeremy Simon; GREEN, Benjamin; HUTCHISON, David. Analysis of affordance, time, and adaptation in the assessment of industrial control system cybersecurity risk. **Risk Analysis**, v. 37, n. 7, p. 1298-1314, 2017.

CANO, Javier *et al*. Modeling current and emerging threats in the airport domain through adversarial risk analysis. **Journal of Risk Research**, v. 19, n. 7, p. 894-912, 2016.

CANO, Javier *et al*. Security economics: an adversarial risk analysis approach to airport protection. **Annals of Operations Research**, v. 245, n. 1-2, p. 359-378, 2016.

CHEN, Guo *et al*. Exploring reliable strategies for defending power systems against targeted attacks. **IEEE Transactions on Power Systems**, v. 26, n. 3, p. 1000-1009, 2011.

CHOI, Tsan- Ming; LAMBERT, James H. Advances in risk analysis with big data. **Risk analysis**, v. 37, n. 8, p. 1435-1442, 2017.

COLES, John; ZHUANG, Jun. Decisions in disaster recovery operations: a game theoretic perspective on organization cooperation. **Journal of Homeland Security and Emergency Management**, v. 8, n. 1, 2011.

COX, JR, Louis Anthony. Game theory and risk analysis. **Risk Analysis: An International Journal**, v. 29, n. 8, p. 1062-1068, 2009.

COX, JR, Louis Anthony. Some limitations of "Risk= Threat× Vulnerability× Consequence" for risk analysis of terrorist attacks. **Risk Analysis: An International Journal**, v. 28, n. 6, p. 1749-1761, 2008.

CRENSHAW, M. (ed.). **Terrorism in context.** Pennsylvania State: Pennsylvania State University Press, 1995.

_____. (ed.). **Terrorism, Legitimacy, and Power**: the consequences of political violence. Middletown, CO: Wesleyan University Press, 1983.

CURTIS, Glenn E.; KARACAN, Tara. **The nexus among terrorists, narcotics traffickers, weapons proliferators, and organized crime networks in Western Europe**. Washington, DC: Federal Research Division, 2002. Disponível em: http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf. Acesso em 21 jul. 2018.

DE ALBUQUERQUE, Carlos Eduardo Pires; DE ANDRADE, Felipe Scarpelli. O Emprego da Análise de Risco como Ferramenta de Inteligência Estratégica. **Revista Brasileira de Ciências Policiais**, v. 4, n. 2, p. 107-121, 2014.

DHS, U. S. **National Strategy for Homeland Security**. 2007. Disponível em: https://www.dhs.gov/national-strategy-homeland-security-october-2007#. Acesso em: 15 ago. 2018.

_____. **Lexicon, Terms and Definitions**. 2010. Disponível em: <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>. Acesso em: 15 ago. 2018.

_____. **Lexicon, Terms and Definitions**. 2017. Disponível em: <https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf>. Acesso em: 15 ago. 2018.

_____. **Risk management fundamentals**. 2011. Disponível em: https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf. Acesso em: 15 ago. 2018.

EUA. ESTADOS UNIDOS DA AMÉRICA. **The National Counterintelligence Strategy of the United States of America**. Washington DC: NCIX, 2007. Disponível em: https://fas.org/irp/ops/ci/cistrategy2007.pdf . Acesso em 10 dez. 2019.

EZELL, Barry C.; BEHR, Joshua; COLLINS, Andrew. Identifying factors that influence terrorist decisions and target selection. **Journal of Homeland Security and Emergency Management**, v. 9, n. 1, 2012.

EZELL, Barry Charles *et al*. Probabilistic risk analysis and terrorism risk. **Risk Analysis:** an International Journal, v. 30, n. 4, p. 575-589, 2010.

EZELL, Barry Charles *et al*. Probabilistic risk analysis and terrorism risk. **Risk Analysis:** an International Journal, v. 30, n. 4, p. 575-589, 2010.

EZELL, Barry; COLLINS, Andrew. Response to Parnell, Smith, and Moxley, Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management Model. **Risk Analysis:** an International Journal, v. 30, n. 1, 2010.

FENG, Qilin *et al*. Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. **Journal of Loss Prevention in the Process Industries**, v. 43, p. 614-628, 2016.

GARCIA, Ryan JB; VON WINTERFELDT, Detlof. Defender–attacker decision tree analysis to combat terrorism. **Risk Analysis:** an International Journal, v. 36, n. 12, p. 2258-2271, 2016.

GOLANY, Boaz *et al*. Nature plays with dice–terrorists do not: Allocating resources to counter strategic versus probabilistic risks. **European Journal of Operational Research**, v. 192, n. 1, p. 198-208, 2009.

GORTNEY, W. E. **Antiterrorism.** Joint publication 3-07.2. Department of Defense, 2010.

GREENBERG, Michael D. *et al*. **Maritime terrorism:** Risk and liability. Santa Monica: Rand Corporation, 2006.

GREENBERG, Michael R. *et al*. Risk- based decision support tools: Protecting rail-centered transit corridors from cascading effects. **Risk Analysis**: An International Journal, v. 31, n. 12, p. 1849-1858, 2011.

GUIKEMA, Seth D.; AVEN, Terje. Assessing risk from intelligent attacks: A perspective on approaches. **Reliability Engineering & System Safety**, v. 95, n. 5, p. 478-483, 2010.

GUIKEMA, Seth D.; AVEN, Terje. Is ALARP applicable to the management of terrorist risks? **Reliability Engineering & System Safety**, v. 95, n. 8, p. 823-827, 2010.

GUIKEMA, Seth. Modeling intelligent adversaries for terrorism risk assessment: Some necessary conditions for adversary models. **Risk Analysis: a**n International Journal, v. 32, n. 7, p. 1117-1121, 2012.

GUPTA, Sushil *et al*. Disaster management from a POM perspective: Mapping a new domain. **Production and Operations Management**, v. 25, n. 10, p. 1611-1637, 2016.

HAIMES, Yacov Y. Roadmap for modeling risks of terrorism to the homeland. **Journal of Infrastructure Systems**, v. 8, n. 2, p. 35-41, 2002.

HAIMES, Yacov Y. Total risk management. **Risk analysis:** an International Journal, v. 11, n. 2, p. 169-171, 1991.

HAPHURIWAT, Naraphorn; BIER, Vicki M. Trade-offs between target hardening and overarching protection. **European Journal of Operational Research**, v. 213, n. 1, p. 320-328, 2011.

HAPHURIWAT, Naraphorn; BIER, Vicki M.; WILLIS, Henry H. Deterring the smuggling of nuclear weapons in container freight through detection and retaliation. **Decision Analysis**, v. 8, n. 2, p. 88-102, 2011.

HARRIS, Bernard. Mathematical methods in combatting terrorism. **Risk Analysis:** an International Journal, v. 24, n. 4, p. 985-988, 2004.

HAUSKEN, Kjell. Defense and attack of complex and dependent systems. **Reliability Engineering & System Safety**, v. 95, n. 1, p. 29-42, 2010.

HAUSKEN, Kjell. Protecting complex infrastructures against multiple strategic attackers. **International Journal of Systems Science**, v. 42, n. 1, p. 11-29, 2011.

HAUSKEN, Kjell. Strategic defense and attack for series and parallel reliability systems. **European Journal of Operational Research**, v. 186, n. 2, p. 856-881, 2008.

HAUSKEN, Kjell; HE, Fei. On the effectiveness of security countermeasures for critical infrastructures. **Risk Analysis:** an International Journal,, v. 36, n. 4, p. 711-726, 2016.

HE, Fei; ZHUANG, Jun. Modelling 'contracts' between a terrorist group and a government in a sequential game. **Journal of the Operational Research Society**, v. 63, n. 6, p. 790-809, 2012.

HILLIARD, Holly; PARNELL, Gregory S.; POHL, Edward A. Evaluating the effectiveness of the global nuclear detection architecture using multiobjective decision analysis. **Systems Engineering**, v. 18, n. 5, p. 441-452, 2015.

HOFFMANN, Bruce. **Inside Terrorism**. New York: Columbia University Press, 2006.

INSUA, David Rios; BANKS, David; RIOS, Jesus. Modeling opponents in adversarial risk analysis. **Risk Analysis:** an International Journal, v. 36, n. 4, p. 742-755, 2016.

INSUA, David Rios; RIOS, Jesus; BANKS, David. Adversarial risk analysis. **Journal of the American Statistical Association**, v. 104, n. 486, p. 841-854, 2009.

INSUA, David Ríos *et al*. Multithreat multisite protection: A security case study. **European Journal of Operational Research**, v. 252, n. 3, p. 888-899, 2016.

IRGC. **Comparing methods for terrorism risk assessment with methods in cyber security.** Workshop report. International Risk Governance Council. Switzerland: Lausanne, 2016. Disponível em: https://www.irgc.org/wp-content/uploads/2016/01/Terrorism-Cyber-Security-28-29-May-2015-Workshop-Report.pdf. Acesso em 08 ago. 2018.

JACKSON, Brian A.; LATOURRETTE, Tom. Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries. **Journal of Air Transport Management**, v. 48, p. 26-33, 2015.

JENELIUS, Erik; WESTIN, Jonas; HOLMGREN, Åke J. Critical infrastructure protection under imperfect attacker perception. **International Journal of Critical Infrastructure Protection**, v. 3, n. 1, p. 16-26, 2010.

JONGMAN, Albert J. **Political terrorism:** a new guide to actors, authors, concepts, data bases, theories, and literature. New York: Routledge, 2017.

KEENEY, Ralph L.; VON WINTERFELDT, Detlof. A value model for evaluating homeland security decisions. **Risk Analysis: An International Journal**, v. 31, n. 9, p. 1470-1487, 2011.

KELLER, L. Robin; KOPHAZI, Kelly M. From the Editors—Deterrence, Multiattribute Utility, and Probability and Bayes' Updating. **Decision analysis**, v. 8, n. 2, 2011.

KIM, Kyo-Nam; YIM, Man-Sung; SCHNEIDER, Erich. A study of insider threat in nuclear security analysis using game theoretic modeling. **Annals of Nuclear Energy**, v. 108, p. 301-309, 2017.

KITCHENHAM, Barbara. Procedures for performing systematic reviews. **Keele, UK, Keele University**, v. 33, n. 2004, p. 1-26, 2004.

KROSHL, William M.; SARKANI, Shahram; MAZZUCHI, Thomas A. Efficient allocation of resources for defense of spatially distributed networks using agent- based simulation. **Risk Analysis: a**n International Journal, v. 35, n. 9, p. 1690-1705, 2015.

KUJAWSKI, Edouard. A Probabilistic Game- Theoretic Method to Assess Deterrence and Defense Benefits of Security Systems. **Systems Engineering**, v. 19, n. 6, p. 549-566, 2016.

KUJAWSKI, Edouard. Accounting for terrorist behavior in allocating defensive counterterrorism resources. **Systems Engineering**, v. 18, n. 4, p. 365-376, 2015.

LATHROP, John; EZELL, Barry. Validating Terrorism Risk Assessment Models–Lessons Learned from 11 Models. **Improving Homeland Security Decisions**, p. 54, 2017.

LESON, Joel. **Assessing and managing the terrorism threat**. Washington: Bureau of justice assistance, 2005.

LUESSEN, Lawrence H. A Self- Consistent Context for Unit- and Force- Level Tactical Decision- Making. **Naval engineers journal**, v. 115, n. 1, p. 67-78, 2003.

LUNDBERG, Russell. **Comparing homeland security risks using a deliberative risk ranking methodology**. The Pardee RAND Graduate School, 2013.

_____. Deliberative Risk Ranking to Inform Homeland Security Strategic Planning. **Journal of Homeland Security and Emergency Management**, v. 13, n. 1, p. 3-33, 2016.

LUNDBERG, Russell; WILLIS, Henry. Assessing Homeland Security Risks: A Comparative Risk Assessment of 10 Hazards. **Homeland security affairs**, v. 11, n. 10, 2015.

MAKARENKO, Tamara. **The Crime-Terror Continuum**: modelling 21st Century Security Dynamics. 2005. (Ph.D.'s thesis in International Politics). University of Wales, Wales, 2005. Disponível em: http://cadair.aber.ac.uk/dspace/bitstream/handle/2160/1958/Tamara%20Makarenko%20PhD.pdf. Acesso em: 08 jul. 2018.

MATHEWS, Timothy; LOWENBERG, Anton D. The interdependence between homeland security efforts of a state and a terrorist's choice of attack. **Conflict Management and Peace Science**, v. 29, n. 2, p. 195-218, 2012.

MERRICK, Jason RW; LECLERC, Philip. Modeling adversaries in counterterrorism decisions using prospect theory. **Risk Analysis:** an International Journal, v. 36, n. 4, p. 681-693, 2016.

MERRICK, Jason; PARNELL, Gregory S. A comparative analysis of PRA and intelligent adversary methods for counterterrorism risk management. **Risk Analysis:** an International Journal, v. 31, n. 9, p. 1488-1510, 2011.

MOHTADI, Hamid. Risk- Mitigating Policies and Adversarial Behavior: Case of Backlash. **Risk Analysis:** an International Journal, v. 37, n. 3, p. 459-470, 2017.

MONTOYA, Mario Daniel. **Máfia e crime organizado:** aspectos legais. Autoria mediata. Responsabilidade penal das estruturas organizadas de poder. Atividades criminosas. Rio de Janeiro: Lumen Juris, 2007.

NATIONAL RESEARCH COUNCIL *et al*. **Making the nation safer:** the role of science and technology in countering terrorism. Washington: National Academies Press, 2002.

NAVARRO, José María Blanco; VILLAVERDE, Jéssica Cohen. The future of counter-terrorism in Europe. The need to be lost in the correct direction. **European journal of futures research**, v. 2, n. 1, p. 50, 2014.

NIELSEN, Sarah. **Fighting Terror in the Tri-Border Area**. Woodrow Wilson International Center for Scholars. 2019. Disponível em: https://www.wilsoncenter.org/article/fighting-terror-the-tri-border-area. Acesso em: 04 dez. 2019.

NIKOOFAL, Mohammad E.; ZHUANG, Jun. On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness. **European Journal of Operational Research**, v. 246, n. 1, p. 320-330, 2015.

NIKOOFAL, Mohammad E.; ZHUANG, Jun. On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness. **European Journal of Operational Research**, v. 246, n. 1, p. 320-330, 2015.

NIKOOFAL, Mohammad E.; ZHUANG, Jun. Robust allocation of a defensive budget considering an attacker's private information. **Risk Analysis:** an International Journal, v. 32, n. 5, p. 930-943, 2012.

PALA, Ali; ZHUANG, Jun. Security screening queues with impatient applicants: A new model with a case study. **European Journal of Operational Research**, v. 265, n. 3, p. 919-930, 2018.

PARNELL, Gregory S. *et al.* Scientists urge DHS to improve bioterrorism risk assessment. **Biosecurity and Bioterrorism**, v. 6, n. 4, p. 353-356, 2008.

PARNELL, Gregory S.; SMITH, Christopher M.; MOXLEY, Frederick I. Intelligent adversary risk analysis: A bioterrorism risk management model. **Risk Analysis:** an International Journal, v. 30, n. 1, p. 32-48, 2010.

PARNELL, Gregory S.; SMITH, Christopher M.; MOXLEY, Frederick I. Intelligent adversary risk analysis: A bioterrorism risk management model. **Risk Analysis:** an International Journal, v. 30, n. 1, p. 32-48, 2010.

PATÉ-CORNELL, Elisabeth. Probabilistic risk analysis versus decision analysis: similarities, differences and illustrations. In: Abdellaoui M., Luce R.D., Machina M.J., Munier B. (ed.) **Uncertainty and Risk.** Berlin: Springer, 2007, p. 223-242.

POLÍCIA FEDERAL. **Relatório de Gestão do Exercício de 2015**. 2016.

POURAKBAR, Morteza; ZUIDWIJK, Rob A. The role of customs in securing containerized global supply chains. **European Journal of Operational Research**, v. 271, n. 1, p. 331-340, 2018.

PUB, Joint. **Department of Defense Dictionary of Military and Associated Terms**. Pub 1-02, v. 23, 1994. Disponível em: https://fas.org/irp/doddir/dod/jp1_02.pdf. Acessado em: 01 ago. 2018.

QUIJANO, Eduardo G.; INSUA, David Ríos; CANO, Javier. Critical networked infrastructure protection from adversaries. **Reliability Engineering & System Safety**, v. 179, p. 27-36, 2018.

RAPOPORT, David C. **Attacking Terrorism:** Elements of a Grand Strategy. The Four Waves of Modern Terrorism. Washington, DC: Georgetown University Press, 2004, p. 46-73. Disponível em: http://www.international.ucla.edu/media/files/Rapoport-Four-Waves-of-Modern-Terrorism.pdf. Acesso em: 01 mai. 2018.

RIOS, Jesus; INSUA, David Rios. Adversarial risk analysis for counterterrorism modeling. **Risk Analysis:** an International Journal, v. 32, n. 5, p. 894-915, 2012.

ROTHSCHILD, Casey; MCLAY, Laura; GUIKEMA, Seth. Adversarial risk analysis with incomplete information: A level- k approach. **Risk Analysis**: an International Journal, v. 32, n.7, p. 1219-1231, 2012.

SAMUEL, Andrew; GUIKEMA, Seth D. Resource allocation for homeland defense: Dealing with the team effect. **Decision Analysis**, v. 9, n. 3, p. 238-252, 2012.

SHAN, Xiaojun; ZHUANG, Jun. Cost of equity in homeland security resource allocation in the face of a strategic attacker. **Risk Analysis:** an International Journal, v. 33, n. 6, p. 1083-1099, 2013.

SHAN, Xiaojun; ZHUANG, Jun. Modeling credible retaliation threats in deterring the smuggling of nuclear weapons using partial inspection - A three-stage game. **Decision Analysis**, v. 11, n. 1, p. 43-62, 2014.

SINHA, Ankur *et al*. Solving bilevel multicriterion optimization problems with lower level decision uncertainty. **IEEE Transactions on Evolutionary Computation**, v. 20, n. 2, p. 199-217, 2015.

START. **National Consortium for the Study Of Terrorism and Responses to Terrorism**. Global Terrorism Database (GTD). 2019. Disponível em: http://www.start-dev.umd.edu/gtd/. Acesso em: 12 nov 2019.

TALARICO, Luca *et al*. MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries. **Reliability Engineering & System Safety**, v. 138, p. 105-114, 2015.

TORRES, Jacob M.; BRUMBELOW, Kelly; GUIKEMA, Seth D. Risk classification and uncertainty propagation for virtual water distribution systems. **Reliability Engineering & System Safety**, v. 94, n. 8, p. 1259-1273, 2009.

TOURE, Ibrahim; GANGOPADHYAY, Aryya. Real time big data analytics for predicting terrorist incidents. In: 2016 IEEE Symposium on Technologies for Homeland Security (HST). **Proceedings […].** IEEE, 2016.

UNITED STATES. **Homeland Security Act of 2002**. Congress. House. Select committee on Homeland Security. 2002. Disponível em: https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf. Acesso em: 05 ago. 2018.

UNRIC. **Conferência Inédita de Alto-Nível sobre Contraterrorismo.** Centro Regional de Informações das Nações Unidas. 2017. Disponível em: https://www.unric.org/pt/actualidade/32458-conferencia-inedita-de-alto-nivel-sobre-contraterrorismo. Acesso em: 12 ago. 2018.

VAN ECK, Nees Jan; WALTMAN, Ludo. Visualizing Bibliometric Networks. In: Ding Y., Rousseau R., Wolfram D. (eds) **Measuring Scholarly Impact.** Cham: Springer, 2014. p. 285-320.

VAN ECK, Nees Jan; WALTMAN, Ludo. **VosViewer manual:** manual for VosViewer version 1.6. 5. Leiden: CWTS, 2016.

VON WINTERFELDT, Detlof. **How Should We Measure Terrorism Risk?** The Regulatory Review. Washington, Philadelphia, PA: Penn Program on Regulation - University of Pennsylvania - Law School. 2016. Disponível em: https://www.theregreview.org/2016/08/25/xu-how-should-we-measure-terrorism-risk/ 2/4. Acesso em: 10 ago. 2018.

WANG, Chen; BIER, Vicki M. Expert elicitation of adversary preferences using ordinal judgments. **Operations Research**, v. 61, n. 2, p. 372-385, 2013.

WANG, Chen; BIER, Vicki M. Target-hardening decisions based on uncertain multiattribute terrorist utility. **Decision Analysis**, v. 8, n. 4, p. 286-302, 2011.

WANG, Shouqiang; BANKS, David. Network routing for insurgency: An adversarial risk analysis framework. **Naval Research Logistics (NRL)**, v. 58, n. 6, p. 595-607, 2011.

WANG, Xiaofang; ZHUANG, Jun. Balancing congestion and security in the presence of strategic applicants with private information. **European Journal of Operational Research**, v. 212, n. 1, p. 100-111, 2011.

WEIN, Lawrence M.; BAVEJA, Manas. Using fingerprint image quality to improve the identification performance of the US Visitor and Immigrant Status Indicator Technology Program. Proceedings of the National Academy of Sciences, v. 102, n. 21, p. 7772-7775, 2005.

WHITE, Richard; BOULT, Terrance; CHOW, Edward. A computational asset vulnerability model for the strategic protection of the critical infrastructure. **International Journal of Critical Infrastructure Protection**, v. 7, n. 3, p. 167-177, 2014.

WHITTAKER, David J. (Org). **Terrorismo:** um retrato. Rio de Janeiro: Biblioteca do Exército, 2005.

WILLIS, Henry H. *et al.*. **Estimating terrorism risk**. Santa Monica: Rand Corporation, 2006.

WILLIS, Henry H. *et al.* **Terrorism risk modeling for intelligence analysis and infrastructure protection**. Santa Monica: Rand Corporation, 2007.

WOLOSZYN, André Luís. **Terrorismo Global**. Rio de Janeiro: Biblioteca do Exército, 2010.

XU, Jie; ZHUANG, Jun. Modeling costly learning and counter-learning in a defender-attacker game with private defender information. **Annals of Operations Research**, v. 236, n. 1, p. 271-289, 2016.

XU, Jie; ZHUANG, Jun; LIU, Zigeng. Modeling and mitigating the effects of supply chain disruption in a defender–attacker game. **Annals of Operations Research**, v. 236, n. 1, p. 255-270, 2016.

YAGHLANE, Asma Ben; AZAIEZ, M. Naceur. Systems under attack-survivability rather than reliability: Concept, results, and applications. **European Journal of Operational Research**, v. 258, n. 3, p. 1156-1164, 2017.

ZHANG, Laobing; RENIERS, Genserik. A game- theoretical model to improve process plant protection from terrorist attacks. **Risk Analysis:** An International Journal, v. 36, n. 12, p. 2285-2297, 2016.

ZHANG, Laobing; RENIERS, Genserik. Applying a Bayesian Stackelberg game for securing a chemical plant. **Journal of loss prevention in the process industries.-Stoneham**, v. 51, p. 72-83, 2018.

ZILINSKAS, Raymond A.; HOPE, Bruce; NORTH, D. Warner. A discussion of findings and their possible implications from a workshop on bioterrorism threat assessment and risk management. **Risk Analysis:** An International Journal, v. 24, n. 4, p. 901-908, 2004.