# MODELO PARA MAPEAMENTO DE AMEAÇAS CIBERNÉTICAS
# *CYBER THREAT MODELING FRAMEWORK*

Renato Carvalho Raposo de Melo; Robson de Oliveira Albuquerque; Fábio Lúcio Lopes de Mendonça
Professional Post-Graduation Program in Electrical Engineering - PPEE - Electrical Engineering Department,
Faculty of Technology, University of Brasília (UnB), Brasília, Brazil, Zip Code 70910-900
E-mail: renato.melo@aluno.unb.br; robson@redes.unb.br; fabio.mendonca@redes.unb.br;

***Abstract*—O espaço cibernético redimensionou os limites dos campos de disputa entre grandes organizações e governos. Doutrinas e estratégias de segurança vêm sendo adaptadas ao mundo de ameaças cibernéticas cada vez mais complexas. Parte do sucesso na adaptação e sobrevivência a esse cenário recai sobre a capacidade de se entender ameaças às quais os sistemas a serem protegidos estão sujeitos. Neste artigo, apresentamos um método para mapeamento de ameaças cibernéticas de alta complexidade com o objetivo de auxiliar técnicos e gestores a gerar e analisar conhecimento útil sobre ameaças cibernéticas, tanto em ambiente governamental quanto corporativo.**

***Palavras-Chave - Segurança Cibernética; Ameaças Cibernéticas; Mapeamento de Ameaças; Inteligência de Ameaças; Avalição de Riscos; Advanced Persistent Threats.***

***Abstract*—The Cyberspace has reshaped the boundaries of the dispute fields used by organizations and governments. Organizational security doctrines and strategies have been adapted to face the ever-growing complexity of cyber threats. Part of the success in surviving in that environment depends on the ability one has to understand the nature of the threats aiming the systems to be protected. In this work, we propose a framework to map high complex cyber threats to help technical and management personnel with the task of generating useful knowledge, both in corporate and government cyber security sectors.**

***Keywords— Cyber Security; Cyber Threats; Threat Assessment; Cyber Threat Intelligence; Risk Assessment; Advanced Persistent Threats.***

## I. INTRODUÇÃO

Atores ofensivos classificados como *Advanced Persistent Threats* (APTs) são especializados no emprego de técnicas complexas para, anônima e persistentemente, atacar alvos de alto valor, incluídos sistemas de grandes organizações e governos [1].

No mercado de *Cyber Threat Intelligence* (CTI), são publicados relatórios sobre atores ofensivos baseados em diferentes parametrizações e metodologias [2]. Tais publicações, em geral, investigam origens e vetores de ataques cibernéticos com foco em implementação de medidas de segurança e contenção de danos. Análises mais amplas versando sobre motivações estratégicas e objetivos mediatos dos adversários, todavia, são menos comuns [3].

Este trabalho propõe um método para mapeamento de ameaças cibernéticas de alta complexidade direcionadas a organizações e governos. Com foco em patrocinadores, conjuntura internacional e agentes ofensivos, o método proposto é dedicado a cenários complexos, majoritariamente determinados por disputas internacionais e conflitos geopolíticos.

Baseado na estruturação dos processos de reunião e análise de dados, o método apreende conceitos de Gestão de Risco, de *Cyber Threat Intelligence* e de modelos de Atribuição Cibernética. Esta pesquisa, contudo, não discute aspectos eminentemente técnicos de ações cibernéticas ofensivas ou mecanismos de engenharia reversa e análise de artefatos.

A principal contribuição deste trabalho, portanto, é a consolidação de um método para mapeamento de ameaças cujo resultado extrapole o arcabouço puramente técnico e se mostre útil também à esfera da alta gestão de segurança cibernética organizacional.

O artigo foi dividido em quatro seções, além desta Introdução. Na Seção II, Trabalhos Relacionados, discorremos sobre publicações relevantes e conceitos basilares do método. Na Seção seguinte III, Método para Mapeamento de Ameaças, detalhamos os componentes e as fases de aplicação do método. A Seção IV, Apresentação de Resultado, discute a aplicação do método proposto por meio de um estudo de caso. Por fim, na Seção V, Conclusão, sintetizamos os aspectos principais do artigo e linhas de pesquisa para trabalhos futuros.

## II. TRABALHOS RELACIONADOS

Esta seção apresenta trabalhos relevantes e conceitos fundamentais à compreensão do método proposto.

### *A. Advanced Persistent Threats*

Alshamrani *et al.* [4] destaca que APTs são grupos bem estruturados, financiados por organizações ou governos e dedicados a atingir objetivos específicos sobre alvos selecionados. Valeros *et al.* [5] detalha APT específico, cuja atuação cibernética aponta para espionagem direcionada aos setores diplomático, militar e político na América Latina, abarcando, portanto, recorte geográfico diferente daquele formado pelos principais atores globais.

A *Cybersecurity and Infrastructure Security Agency* (CISA), no Alert (AA21-048A) de 2021 [6], atestou que atores APTs ligados à Coréia do Norte atacaram, com objetivos financeiros, organizações em pelo menos trinta países. Alertas CISA são importantes modelos para o método apresentado neste artigo por trazerem em seu bojo o contexto geopolítico.

*2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*
*22 – 25 June 2022, Madrid, Spain*
ISBN: 978-989-33-3436-2

### B. Atribuição Cibernética

Romanosky *et al.* [7] define a Atribuição Cibernética como o processo de coleta, análise e associação de evidências de ações maliciosas a um perpetrador. Aborda dois tipos de Atribuição Cibernética: a Atribuição puramente técnica e a Atribuição Política, que exige a compreensão da conjuntura geopolítica, associações e motivações dos atores ofensivos.

Cook *et al.* [8] ressalta que a análise dos objetivos de uma campanha pode indicar quais atores se beneficiariam dos resultados alcançados, fundamentando um processo de Atribuição centrado em patrocinadores.

Skopik *et al.* [9], a partir da criação de método *Cyber Attribution Model* (CAM), aborda o problema das false *flags* na Atribuição Cibernética. O contexto sociopolítico é considerado, junto aos aspectos técnicos, na análise dos ataques e na busca por false *flags*.

### C. Cyber Threat Intelligence

Gong *et al.* [10] propõe um framework para análise de ameaças direcionadas a Infraestruturas Críticas (IC) e conceitua CTI como um sistema de segurança de resposta a ataques cibernéticos baseado na produção de conhecimento sobre ameaças a partir de dados diversos.

Melo e Silva *et al.* [11] traz uma metodologia de avaliação de plataformas de CTI e protocolos de Inteligência de Ameaças. O artigo descreve o fluxo do processo de produção de Inteligência de Ameaças e estruturou o método geral "5W3H" (*what, who, why, when, where, how, how much and how long*) para desdobramento de tópicos objeto de análise.

Amaro *et al.* [12] propõe um framework metodológico e uma ferramenta para processamento de dados e indicadores sobre ameaças cibernéticas, buscando entender e reagir com eficiência a incidentes cibernéticos, considerando o grande volume de dados disponíveis em fontes abertas.

### D. Gestão de Risco e Avaliação de Ameaças

O guia NIST 800-30R1 [13] assevera que o propósito da Avaliação de Risco é identificar ameaças às organizações ou ao país; vulnerabilidades internas e externas às organizações; impactos causados pela exploração das vulnerabilidades organizacionais; e a probabilidade de ocorrência do dano. O guia propõe uma Avaliação de Risco em quatros passos: Preparação; Execução (que abarca a identificação de fontes de ameaças); Comunicação de Resultados; e Avaliação continuada.

A publicação NIST 800-39 [14] oferece um guia para Gestão de Risco para a Segurança da Informação. O documento destaca que, para entender a "Ameaça", é preciso conhecer, entre outros quesitos, capacidades, objetivos e parâmetros para seleção de alvos dos adversários.

Bodeau *et al.* [15] compara frameworks de Mapeamento de Ameaças e reitera que uma das abordagens possíveis da Avaliação de Risco aloca a "Ameaça" como elemento central do processo de análise, princípio que serviu como linha mestra para a construção deste artigo.

O framework ODNI [16] e a sua extensão técnica elaborada pela NSA/CSS [17] apresentam um ciclo de vida da ação adversária, dividindo a ação ofensiva em seis estágios. O modelo se propõe a trazer eficiência à Análise de Ameaças Cibernéticas e ao compartilhamento de informações, buscando utilidade tanto para as esferas gerencial e decisória quanto técnica.

O modelo TARA [18] foi desenvolvido para Avaliação de Risco associada a agentes de ameaças cibernéticas. A metodologia tem como um de seus componentes uma biblioteca composta por 22 arquétipos de agentes de ameaças. Ao prever impactos decorrentes das ações ofensivas, o modelo TARA elenca efeitos de cunho organizacional, que extrapolam os efeitos puramente cibernéticos.

O framework Cyber Prep 2.0 [19] serve igualmente ao mapeamento de APTs e de ameaças cibernéticas convencionais. O modelo estipula cinco classes de adversários, diferentes entre si em termos de objetivos; escopo; persistência; e preocupação com detecção. Acerca dos impactos potencialmente causados pela ação adversa, o modelo considera tanto efeitos cibernéticos quanto efeitos não-cibernéticos.

O IDDL/ATC [20], por sua vez, constitui-se numa abordagem da Segurança Cibernética baseada no Mapeamento de Ameaças. A ameaça, segundo esse modelo, é o elemento mais crítico da gestão de riscos.

A Tabela I registra a compatibilidade dos modelos citados nos quatro parágrafos anteriores com três elementos centrais do método proposto neste artigo: distinção clara entre as figuras de "Adversário" e "Agente"; atenção à "Conjuntura" geopolítica como fator de constituição da Ameaça; e a consideração de "Impactos" não-cibernéticos de alcance organizacional no rol de efeitos potenciais decorrentes de uma ação ofensiva.

TABELA I: COMPARAÇÃO ENTRE MODELOS DE AVALIAÇÃO DE AMEAÇAS CIBERNÉTICAS

| Modelo | Adversário/Agente[1] | Conjuntura[2] | Impactos[3] |
|---|---|---|---|
| ODNI [16] [17] | Não | Não | Não |
| TARA [18] | Não | Não | Sim |
| Cyber Prep [19] | Não | Não | Sim |
| IDDL/ATC [20] | Não | Não | Não |

1. Distinção clara entre "Adversário" e "Agente".
2. Atenção à "Conjuntura" geopolítica como fator de constituição da Ameaça.
3. Consideração de "Impactos" não-cibernéticos de alcance organizacional no rol de efeitos potenciais decorrentes de uma ação ofensiva.

## III. MÉTODO PARA MAPEAMENTO DE AMEAÇAS CIBERNÉTICAS

O mapeamento de Ameaças Cibernéticas pelo método proposto é realizado em duas fases distintas. A primeira fase estabelece os parâmetros para reunião dos dados que caracterizam a Ameaça. A segunda fase consiste na conclusão do processo com apresentação de impactos prováveis e avaliação analítica.

Ameaça foi definida como o conjunto dos vários elementos que moldam o cenário e estabelecem a probabilidade de o Adversário agir contra o sistema sob proteção. Esse conjunto de elementos é formado pelas características da organização alvo; pelas

*2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*
*22 – 25 June 2022, Madrid, Spain*
ISBN: 978-989-33-3436-2

características do Adversário e do Agente; pela dinâmica das relações entre organização alvo e Adversário; e por eventos externos capazes de influenciar o comportamento dos atores envolvidos. A Fig. 1 apresenta a ideia geral do método. As duas fases serão detalhadas nas subseções seguintes.

Ao tratarmos de reunião de dados, é inescapável considerarmos as diferentes iniciativas de normatização que buscam proteger dados pessoais na internet, a exemplo da GDPR [21]. Ainda que não seja objeto de discussão específica neste artigo, é preciso considerar que as categorias de dados que fundamentam o método de mapeamento proposto podem se enquadrar em hipóteses previstas no campo normativo e, portanto, devem ser adequadas aos moldes da legislação vigente.

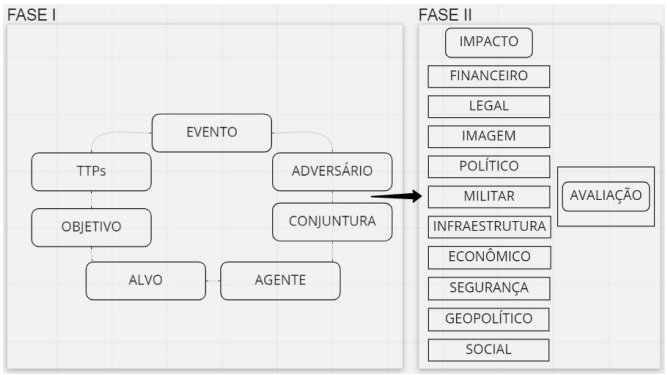


Figura 1: Representação gráfica do Método.

### *A. Fase I - Circular*

Nesta fase, os dados essenciais à caracterização da Ameaça são reunidos em sete categorias (estabelecidas a partir do detalhamento dos supracitados elementos que constituem a Ameaça): Evento; Adversário; Conjuntura; Agente; Objetivo; Táticas, Técnicas e Procedimentos (TTPs); e Alvo. Dados das mais diversas fontes alimentarão cada uma das sete categorias, fomentando um processo de detalhamento da Ameaça como subsídio para análise e conclusão do mapeamento em si.

Em face da complexidade das Ameaças às quais o método se direciona, a disponibilidade e a confiabilidade de dados são variáveis. Por esse motivo, não há ordenação rígida de fluxo nos processos de reunião e análise. Em outros termos, o processo pode ser iniciado por quaisquer das sete categorias elencadas. Daí em diante, os esforços de reunião e análise passam a ser orientados tanto pelo surgimento de novos dados quanto por desdobramentos analíticos alcançados.

Dessa flexibilidade decorre a característica circular da Fase I do método e a possibilidade de emprego do método como ferramenta preventiva. O emprego preventivo, por exemplo, permite que o processo se inicie a partir da percepção de mudanças na relação entre a organização alvo e um Adversário, antes mesmo da ocorrência de evento ofensivo contra o sistema sob proteção.

As sete categorias de dados que compõem a Fase I serão detalhadas a seguir.

*1) Evento:* Reúne os dados de descrição e identificação de evento cibernético ofensivo relacionado à Ameaça sob análise. Deve conter, pelo menos, os dados dispostos na Tabela II.

TABELA II: EVENTO

| | |
|---|---|
| Denominação | Denominações do evento empregadas pelas principais fontes consultadas; |
| Resumo | Características gerais do evento sob análise; |
| Natureza | Ação isolada ou campanha cibernética duradoura ou contra alvos diversos; |
| Recorte temporal | Data de ocorrência do evento, tempo de duração da campanha ou data de conhecimento do fato; |
| Alcance geográfico | Local, nacional, regional ou global. |

*2) Adversário:* Adversário deve ser entendido como o patrocinador e principal beneficiário dos resultados de evento cibernético. No contexto do método proposto, Adversários são, primordialmente, Estados Nacionais. Todavia, também podem figurar como Adversários atores não-estatais capazes de executar ações ofensivas de alta complexidade, a exemplo de grandes grupos empresariais ou políticos, organizações criminosas ou grupos terroristas.

*3) Conjuntura:* A Conjuntura é essencialmente formada pela dinâmica das relações entre a organização alvo e o Adversário e por eventos externos capazes de influenciar o comportamento dos atores envolvidos.

Diante de Adversários estatais, a Conjuntura oscilará majoritariamente em função de interações geopolíticas. Excetuam-se Ameaças formadas por Adversários estatais cuja atuação extrapola o contexto da disputa geopolítica com o país alvo. A exemplo de campanhas conduzidas por Adversários estatais com objetivos majoritariamente financeiros, cujo rol de alvos não se limita a países com os quais há embates geopolíticos diretos.

Adversários não-estatais também são influenciados por oscilações de Conjuntura. Acordos de cooperação internacional para combate a crimes cibernéticos; irrupção de conflitos internacionais; realinhamentos geopolíticos; e graves alterações econômicas, por exemplo, podem gerar mudanças capazes de afetar o comportamento de Adversários não-estatais.

Ademais, tanto atores estatais quanto não-estatais são suscetíveis a mudanças abruptas capazes de impulsionar o surgimento de novas Ameaças. Eventos dessa natureza, potencialmente imprevisíveis, intencionais ou não, são classificados como "Crises" no método proposto.

Por conseguinte, o desenho da Conjuntura deve englobar:

a. Status das relações diplomáticas;
b. Disputas econômicas, políticas, ideológicas e territoriais;
c. Conflitos militares; e
d. Crises.

*4) Agente:* Trata-se do indivíduo ou grupo executor direto das ações ofensivas. De modo geral, os Agentes correspondem aos grupos APT que conduzem as ações ofensivas de alta complexidade.

Em eventos conduzidos por entes não-estatais, os papéis de Adversário e Agente são, muitas vezes, ocupados pela mesma organização. Tome-se como exemplo desse cenário a ação de


ISBN: 978-989-33-3436-2

grupos APT dedicados a perpetrar ataques de *Ransomware* contra sistemas de Infraestruturas Críticas (IC) por motivação puramente financeira.

Grupos hacker foram classificados como Agentes específicos, diferentes de organizações criminosas, por dois motivos: a) sua atuação puramente cibernética os diferencia legalmente de grupos criminosos tradicionais; b) grupos hacker internacionais estão sujeitos a diferentes ordenamentos jurídicos nacionais, o que pode lhes render diferentes classificações.

Nesse esteio, dentre outros elementos considerados úteis à descrição dos Agentes, elencamos:

a. Denominações: identificar o Agente por meio de denominações empregadas pelas principais fontes consultadas;
b. Natureza: parte orgânica da estrutura governamental do país Adversário ou terceiro país; unidade ou integrante de organizações criminosas ou terroristas; empresa legalmente constituída; e indivíduo ou grupo hacker independente ou atuando sob contrato ou coação;
c. Motivação: ideológica; financeira; por coação; satisfação pessoal; ganho organizacional; entre outros;
d. Data de início das atividades;
e. Recorte geográfico de atuação;
f. Histórico de atuação;
g. Assinaturas técnicas;
h. Grupos ou indivíduos relacionados;

*5) Alvo:* Aponta o sistema atacado em determinado Evento ou sistemas visados no contexto da Ameaça sob análise. Entre os sistemas com maior probabilidade de sofrerem ataques de alta complexidade aparecem os diversos segmentos de IC, a exemplo de transporte; abastecimento hídrico e energético; comunicações e informação; e sistema de saúde [22].

Esta categoria também inclui como alvo sistemas que reúnem dados pessoais, independentemente de serem bases mantidas por entes governamentais ou privados. Tal inclusão se fundamenta no histórico de ataques cibernéticos, conduzidos por Adversários estatais, dedicados a acessar dados pessoais mantidos em bases diversas, provavelmente com objetivo de Espionagem [23].

Elencam-se, pois, como alvos mais prováveis:

a. IC;
b. Sistemas administrativos governamentais;
c. Setor de Defesa;
d. Sistema Financeiro;
e. Setor produtivo;
f. Centros de pesquisa científica;
g. Entidades políticas;
h. Empresas de comunicação e mídia;
i. Bases de dados pessoais.

*6) Objetivo:* Trata-se dos objetivos não-cibernéticos e imediatos do Adversário. São "não-cibernéticos" na medida em que não se confundem com os objetivos cibernéticos buscados pelo Agente na execução do ataque. O acesso a informações sobre a topologia de rede do alvo, por exemplo, é um objetivo cibernético, um meio para atingimento do Objetivo não-cibernético.

São, ademais, "imediatos" por sua natureza tática, o que os diferencia dos objetivos mediatos, que podem ser descritos, genericamente, como o ganho de vantagem estratégica.

No método proposto foram elencados cinco Objetivos:

a. Espionagem;
b. Interferência Externa;
c. Ganho financeiro;
d. Disrupção; e
e. Terrorismo.

*7) Táticas, Técnicas e Procedimentos:* Esta categoria elenca TTPs empregados pelo Agente para consecução dos Objetivos. Não se trata do detalhamento de artefatos, códigos ou processos executados nas ações ofensivas, mas da determinação do meio utilizado para atingimento do Objetivo.

A expressão "TTPs" foi empregada em conotação ampla, reunindo elementos de categorias mais segmentadas, normalmente vistas em plataformas de CTI [24]. Dessa forma, foi mantido o grau desejado de tecnicidade do método, que se pretende útil tanto às instancias técnicas quanto gerenciais.

Foram elencados os seguintes TTPs:

a. *Ransomware*;
b. Extração ou Exposição de dados;
c. Alteração ou Destruição de dados;
d. Negação de Serviço;
e. *Defacement*;
f. Transferência de Fundos;
g. Destruição de Hardware ou Software.

### *B. Fase II - Saída do Método*

Na segunda fase de aplicação do método, são apresentados prováveis danos decorrentes de ações ofensivas derivadas das Ameaças, além de uma conclusão com anotações ou desdobramentos analíticos úteis ao processo decisório organizacional.

Para tanto, a Fase II se subdivide em dois segmentos: Impactos e Avaliação.

*1) Impactos:* são os danos que extrapolam os efeitos cibernéticos imediatos aos sistemas comprometidos e se materializam nos diversos estratos de atuação organizacional. São, portanto, consequências a serem endereçadas na esfera gerencial e decisória.

O Método elenca onze tipos de impactos prováveis, dispostos na Tabela III [15] [25] [26].

TABELA III: IMPACTO

| | |
|---|---|
| Financeiro | Perda financeira direta; Custos judiciais; Custos por responsabilização judicial; Custos de recuperação e readaptação de sistemas de Infraestruturas Críticas. |
| Legal | Alterações de legislação; Responsabilização por danos a terceiros; Responsabilização por quebra contratual |
| Imagem | Dano à imagem no âmbito interno; Dano à imagem no âmbito internacional. |


ISBN: 978-989-33-3436-2

| | |
|---|---|
| Político | Comprometimento do processo decisório; Instabilidade política interna. |
| Militar | Não atingimento de objetivo militar; Perda de vantagem militar; Perda de capacidade militar. |
| Infraestrutura | Dano físico; Dano a cadeia logística; Comprometimento de serviço crítico. |
| Econômico | Inviabilização de acordo econômico; Perda de vantagem competitiva; Enfraquecimento de setor econômico. |
| Segurança | Não atingimento de objetivo de segurança; Perda de capacidade de prover segurança. |
| Geopolítico | Crise diplomática; Perda de alinhamento diplomático; Enfraquecimento de posição política internacional. |
| Social | Instabilidade social; Perda de vidas humanas. |

*2) Avaliação:* A Avalição, por fim, deve conter conclusões ou anotações pertinentes para o caso em tela. Podem se referir a desdobramentos prováveis do caso; recomendações técnicas; e discussões diversas.

## IV. APRESENTAÇÃO DE RESULTADO

Esta seção apresenta o resumo de estudo de caso que ilustra a aplicação do método proposto. Os dados reunidos são oriundos de Fontes Abertas.

Trata-se de Ameaça cibernética de natureza estatal, mapeada a partir do Evento denominado *Operation Exchange Marauder* [27], que ganhou visibilidade no começo de 2021.

Baseando-se na vitimologia e TTPs, a Operação foi atribuída, "com elevada confiabilidade", ao Agente denominado Hafnium, provável grupo de espionagem patrocinado pela China [27] [28] [29]. Hafnium teria natureza de parte orgânica da estrutura governamental do país Adversário ou grupo hacker atuando sob contrato ou coação [30] [31] [32].

A China, portanto, ocupa a posição de Adversário, o que insere a Ameaça numa Conjuntura ampla de conflito geopolítico entre os atores de projeção global EUA e China. Considerando os Alvos identificados, a TTP de "Extração de Dados" e a Conjuntura, o Objetivo da campanha foi classificado como "Espionagem".

A consolidação do mapeamento é apresentada na Tabela IV, junto com o apontamento dos Impactos e uma breve Avaliação.

TABELA IV: APLICAÇÃO DO MÉTODO EM UM ESTUDO DE CASO.

| | |
|---|---|
| Evento | *Operation Exchange Marauder;*<br>Exploração de vulnerabilidades *zero-day* da aplicação de serviço de correio eletrônico Microsoft Exchange para acesso indevido a caixas de correio eletrônico e comprometimento de redes;<br>Jan. - Mar. 2021;<br>Campanha nacional direcionada aos EUA.<br>Desdobramentos ganharam alcance global com a exploração, por outros atores, das vulnerabilidades reveladas. |
| Adversário | China – Atividades maliciosas atribuídas ao governo chinês têm afetado diversos setores dos EUA, a exemplo de sistema de saúde; sistema financeiro; setor de Defesa; IC; sistemas administrativos governamentais; e setor produtivo. A China representa um prolífico e efetivo ator engajado em Espionagem cibernética, com capacidades ofensivas substanciais. Tem conduzido campanhas globais para roubo de dados de propriedade intelectual. Operações cibernéticas ofensivas chinesas têm explorado empresas de telecomunicações e softwares largamente utilizados no mundo. Avalia-se que China pode lançar ataques capazes de gerar, no mínimo localmente e temporariamente, disrupção de sistemas de IC dos EUA. [33] |
| Conjuntura | Em 2018, houve o recrudescimento das disputas geopolíticas entre EUA e China. Com gênese majoritariamente econômica, esse cenário de disputa global atualmente se manifesta em diversas esferas, entre outras: tecnologia; segurança cibernética; militar; diplomacia; mídia; alta educação e pesquisas científicas; Direitos Humanos; e ideologia e valores. A crise gerada pela pandemia de COVID-19 agravou o quadro de disputa entre os atores [34]. |
| Agente | Denominações: Hafnium (MITRE);<br>Provável parte orgânica da estrutura governamental do país Adversário; ou grupo hacker atuando sob contrato ou coação.<br>Ativo desde jan. 2021;<br>Ataca primordialmente alvos ligados aos EUA: Setor de Defesa; Centros de Pesquisa (Pesquisas sobre doenças infecciosas); Entidades políticas; Setor produtivo.<br>Opera geralmente a partir de Servidores Virtuais Privados nos EUA. |
| Alvo | Bases de dados pessoais; Sistemas administrativos governamentais; Setor produtivo; IC. |
| Objetivo | Espionagem. |
| TTPs | Extração de dados. |
| Resultado | **Impacto**: Financeiro; Legal; Imagem; Econômico; Militar; Segurança; Infraestrutura.<br>**Avaliação**: Trata-se de Ameaça inserida em Conjuntura específica de conflito entre EUA e China. O Agente concentrar-se-ia em Alvos de valor estratégico definidos pelo Adversário. Todavia, após a divulgação das vulnerabilidades exploradas, outros atores as aproveitaram em contextos diversos e contra países estranhos à campanha original. |

## V. CONCLUSÃO

Este trabalho apresentou um método para mapeamento de ameaças cibernéticas de alta complexidade voltado à produção de conhecimento útil ao processo decisório organizacional no campo da Segurança Cibernética.


ISBN: 978-989-33-3436-2

Baseado em conceitos de Gestão de Risco, CTI e Atribuição Cibernética, o método orienta o processo de produção de conhecimento por meio da estruturação das atividades de reunião e análise de dados. A apresentação de breve estudo de caso ilustrou a aplicação do método preconizado.

Há variadas linhas para desdobramento de trabalhos futuros. Uma delas é a especificação de uma fase de planejamento anterior às fases de aplicação do método apresentadas neste trabalho. Além disso, a automação do processo de reunião de dados em conformidade com o método traria ganhos significativos. Noutra senda, a construção de um modelo para produção de alertas em casos de alterações nas Ameaças já mapeadas é igualmente útil.

## AGRADECIMENTOS

Os autores agradecem o suporte da ABIN TED 09/2018. *R.d.O.A. gratefully acknowledges the General Attorney of the Union - AGU grant 697.935/2019; the General Attorney's Office for the National Treasure PGFN grant 23106.148934/2019-67; the support from EC Horizon 2020 HEROES project grant 101021801.*

## REFERÊNCIAS BIBLIOGRÁFICAS

[1] N. Mohamed and B. Belaton, "Sbi model for the detection of advanced persistent threat based on strange behavior of using credential dumping technique," *IEEE Access*, vol. 9, pp. 42919– 42932, 2021, doi:10.1109/ACCESS.2021.3066289.

[2] K. Oosthoek and C. Doerr, "Cyber threat intelligence: A product without a process?" International Journal of Intelligence and CounterIntelligence, vol. 34, no. 2, pp. 300–315, 2021, doi:10.1080/08850607.2020.1780062.

[3] M. Connell and S. Vogler, "Russia's approach to cyber warfare (1rev)," Center for Naval Analyses Arlington United States, Tech. Rep., 2017, acessado em: 7/02/2022. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1032208.pdf

[4] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1851–1877, 2019, doi:10.1109/COMST.2019.2891891.

[5] V. Valeros, M. Rigaki, and S. Garcia, "Machete: Dissecting the operations of a cyber espionage group in latin america," in 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Stockholm: IEEE, 2019, pp. 464–473, doi:10.1109/EuroSPW.2019.00058.

[6] CISA, "Applejeus: Analysis of north korea's cryptocurrency malware," Cybersecurity and Infrastructure Security Agency (CISA), Tech. Rep., 2021, acessado em: 7/02/2022. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa21-048a

[7] S. Romanosky and B. Boudreaux, "Private-sector attribution of cyber incidents: benefits and risks to the us government," International Journal of Intelligence and CounterIntelligence, vol. 34, no. 3, pp. 463–493, 2021, doi: 10.1080/08850607.2020.1783877.

[8] A. Cook, A. Nicholson, H. Janicke, L. Maglaras, and R. Smith, "Attribution of cyber attacks on industrial control systems," EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, vol. 3, no. 7, 2016, doi:10.4108/eai.21-4-2016.151158.

[9] F. Skopik and T. Pahi, "Under false flag: using technical artifacts for cyber attack attribution," Cybersecurity, vol. 3, no. 1, pp. 1–20, 2020, doi:10.1186/s42400-020-00048-4.

[10] S. Gong and C. Lee, "Cyber threat intelligence framework for incident response in an energy cloud platform," Electronics, vol. 10, no. 3, p. 239, 2021, doi:10.3390/electronics10030239.

[11] A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque, and L. J. García Villalba, "A methodology to evaluate standards and platforms within cyber threat intelligence," Future Internet, vol. 12, no. 6, p. 108, 2020, doi:10.3390/fi12060108.

[12] L. J. Borges Amaro, B. W. Percilio Azevedo, F. L. Lopes de Mendonca, W. F. Giozza, R. d. O. Albuquerque, and L. J. García Villalba, "Methodological framework to collect, process, analyze and visualize cyber threat intelligence data," Applied Sciences, vol. 12, no. 3, 2022, doi:10.3390/app12031205.

[13] NIST, Guide for Conducting Risk Assessments, NIST Special Publication 800-30 (Revision 1), 2012, doi:10.6028/NIST.SP.800-30r1. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/ nistspecialpublication800-30r1.pdf

[14] ——, Managing information security risk: Organization, mission, and information system view, 2011, doi:10.6028/NIST.SP.800-39. [Online]. Available: https:// csrc.nist.gov/publications/detail/sp/800-39/final

[15] D. Bodeau, C. McCollum, and D. Fox, "Cyber threat modeling: Survey, assessment, and representative framework," The Homeland Security Systems Engineering and Development Institute, Operated by The MITRE Corporation, Tech. Rep., 2018, acessado em: 8/02/2022. [Online]. Available: https: //apps.dtic.mil/sti/pdfs/ AD1108051.pdf

[16] ODNI. (2018) Cyber threat framework. Disponível em: https:// www.dni.gov/index.php/cyber-threat-framework. Acessado em: 8/02/2022.

[17] NSA. (2018) Nsa/css technical cyber threat framework v2. Disponível em: https://www.nsa.gov/Press-Room/Cybersecurity-AdvisoriesGuidance/smdsearch11747/2018/. Acessado em: 6/02/2022.

[18] INTEL, Prioritazing Information Security Risks with Threat Agent Risk Assessment, acessado em: 25/03/2022. [Online]. Available: http://media10.connectedsocialmedia.com/intel/10/5725/ Intel_IT_Business_Value_Prioritizing_Info_Security_Risks_with_TARA.pdf

[19] D. Bodeau and R. Graubart, "Cyber prep. 2.0: Motivating organizational cyber strategies in terms of threat preparedness," MITRE Corporation, Tech. Rep., 2016, acessado em: 28/02/2022. [Online]. Available: https://www.mitre.org/sites/default/files/publications/15-0797cyber-prep-2-motivating-organizational-cyber-strategies.pdf

[20] M. Muckin, "A threat-driven approach to cyber security methodologies , practices and tools to enable a functionally integrated cyber security organization," Lockheed Martin Corporation, Tech. Rep., 2015, acessado em: 19/02/2022. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper Threat-Driven-Approach.pdf

[21] F. Pereira, P. Crocker, and V. R. Leithardt, "Padres: Tool for privacy, data regulation and security," SoftwareX, vol. 17, p. 100895, 2022, doi: doi.org/10.1016/j.softx.2021.100895.

[22] USA. (2018) National cyber strategy. Disponível em: https://trumpwhitehouse.archives.gov/wpcontent/uploads/2018/09/National-Cyber-Strategy.pdf. Acessado em: 6/02/2022.

[23] M. Chen, "China's data collection on us citizens: implications, risks, and solutions," Journal of Science Policy e Governance, vol. 15, 2019. [Online]. Available: http://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/chen_jspg_v15.pdf

[24] MITRE, MITRE ATT&CK Matrix for Enterprise, acessado em: 8/02/2022. [Online]. Available: https://attack.mitre.org/tactics/ enterprise/

[25] R. Thornton and M. Miron, "Towards the 'third revolution in military affairs'," The RUSI Journal, vol. 165, no. 3, pp. 12–21, 2020, doi:10.1080/03071847.2020.1765514.

[26] R. Bejtlich, M. Cantos et al., "Cyber war in perspective: Russian aggression against ukraine," NATO Cooperative Cyber Defence Centre of Excellence, Tech. Rep., 2015, acessado em: 8/02/2022. [Online]. Available: https://ccdcoe.org/uploads/ 2018/10/CyberWarinPerspective_full_book.pdf

[27] Microsoft. (2021) Hafnium targeting exchange servers with 0-day exploits. Disponível em: https://www.microsoft.com/ security/blog/2021/03/02/hafnium-targeting-exchangeservers/. Acessado em: 5/02/2022.

[28] MANDIANT. (2021) Detection and response to exploitation of microsoft exchange zero-day vulnerabilities. Disponível em: https://www.mandiant.com/resources/detection-response-toexploitation-of-microsoft-exchange-zero-day-vulnerabilities. Acessado em: 16-02-2022.



ISBN: 978-989-33-3436-2

[29] J. Slowik. (2021) Examining exchange exploitation and its lessons for defenders. Disponível em: https://www.domaintools.com/resources/ blog/examining-exchangeexploitation-and-its-lessons-for-defenders. Acessado em: 1702-2022.
[30] MITRE, MITRE ATT&CK Groups HAFNIUM, acessado em: 15/02/2022. [Online]. Available: https://attack.mitre.org/ groups/G0125/
[31] CISA, "Mitigate microsoft exchange server vulnerabilities," Cybersecurity and Infrastructure Security Agency (CISA),
[32] Tech. Rep., 2021, acessado em: 16/02/2022. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa21-062a
[33] UK. (2021) Uk and allies hold chinese state responsible for a pervasive pattern of hacking. Disponível em: https://www.gov.uk/government/news/uk-and-allies-holdchinese-state-responsible-for-a-pervasive-pattern-of-hacking. Acessado em: 17-02-2022.
[34] CISA, "China cyber threat overview and advisories," Cybersecurity and Infrastructure Security Agency (CISA), Tech. Rep., 2022, acessado em: 6/04/2022. [Online]. Available: https://www.cisa.gov/uscert/china?msclkid=416a7ed3b5aa11ec805da4c19849c68e
[35] N. C. Bing, "Great Power Diplomacy With Chinese Characteristics and US-China Trade-War", in title: The Political Logic of the US–China Trade Wars, Shiping Huan, London/UK, Lexington Books, 2022, pp. 95 – 113, ISBN: 1793624992, 9781793624994.


ISBN: 978-989-33-3436-2