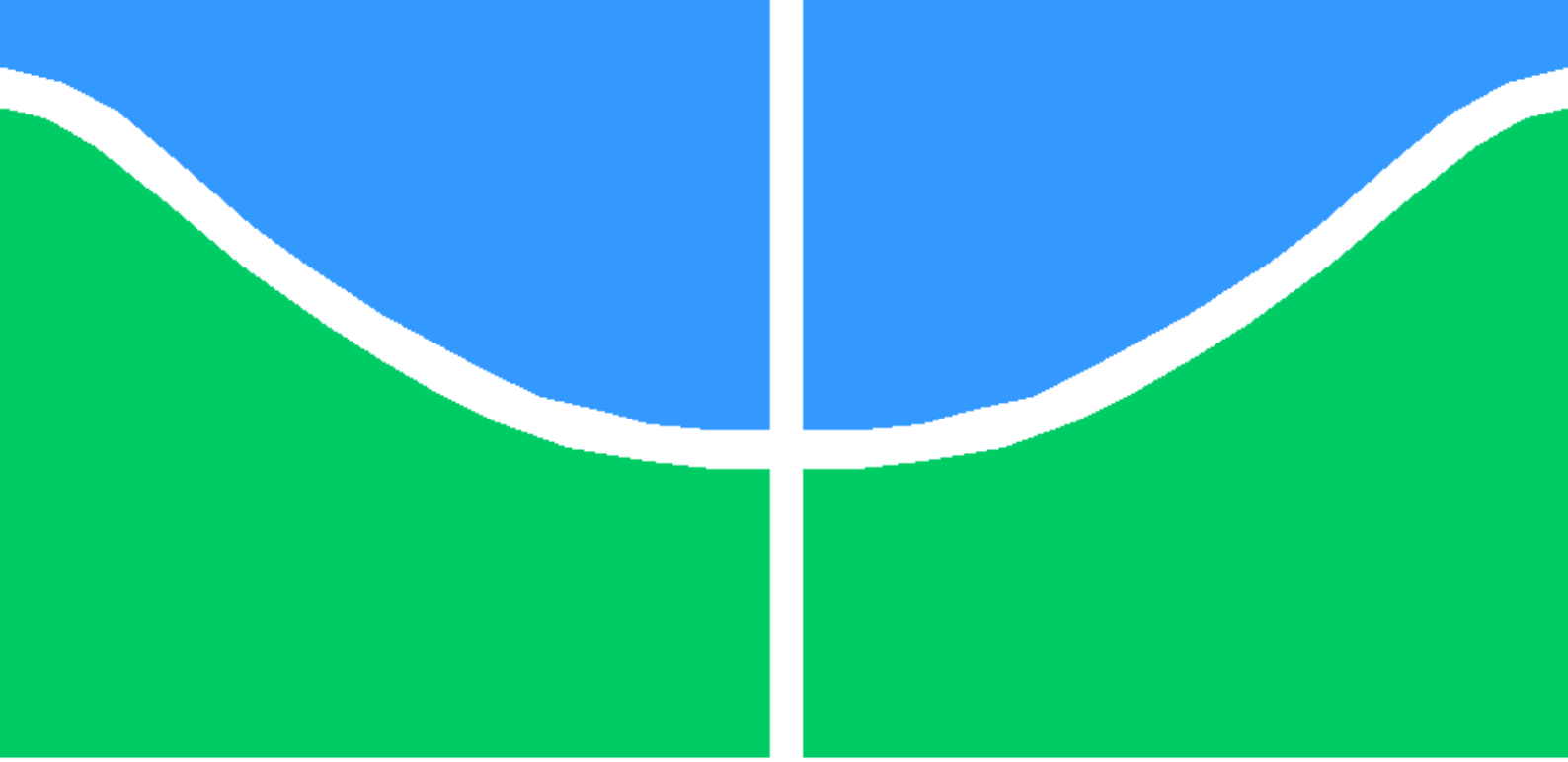

MODELO PARA MAPEAMENTO DE AMEAÇAS CIBERNÉTICAS

RENATO CARVALHO RAPOSO DE MELO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MODELO PARA MAPEAMENTO DE AMEAÇAS CIBERNÉTICAS

RENATO CARVALHO RAPOSO DE MELO

Orientador: PROF. DR. FÁBIO LÚCIO LOPES DE MENDONÇA, ENE/UNB

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO - PPEE.MP.040

BRASÍLIA-DF, 26 DE MAIO DE 2023.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MODELO PARA MAPEAMENTO DE AMEAÇAS CIBERNÉTICAS

RENATO CARVALHO RAPOSO DE MELO

DISSERTAÇÃO DE MESTRADO ACADÊMICO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM ENGENHARIA ELÉTRICA.

APROVADA POR:

Prof. Dr. Fábio Lúcio Lopes de Mendonça, ENE/UnB
Orientador - Presidente

Prof. Dr. Robson de Oliveira Albuquerque, ENE/UnB
Coorientador

Prof. Dr. Rafael Rabelo Nunes, ENE/UnB
Examinador Interno

Prof. Dr. Raimundo Vasconcelos, IFB/DF
Examinador Externo

BRASÍLIA, 26 DE MAIO DE 2023.

FICHA CATALOGRÁFICA
RENATO CARVALHO RAPOSO DE MELO
MODELO PARA MAPEAMENTO DE AMEAÇAS CIBERNÉTICAS
2023xv, 75p., 201x297 mm
(ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023)
Dissertação de Mestrado - Universidade de Brasília
Faculdade de Tecnologia - Departamento de Engenharia Elétrica

REFERÊNCIA BIBLIOGRÁFICA

RENATO CARVALHO RAPOSO DE MELO (2023) MODELO PARA MAPEAMENTO DE AMEAÇAS CIBERNÉTICAS. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPEE.MP.040, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 75p.

CESSÃO DE DIREITOS

AUTOR: RENATO CARVALHO RAPOSO DE MELO
TÍTULO: MODELO PARA MAPEAMENTO DE AMEAÇAS CIBERNÉTICAS.
GRAU: Mestre ANO: 2023

_____

RENATO CARVALHO RAPOSO DE MELO
Depto. de Engenharia Elétrica (ENE) - FT Universidade de Brasília (UnB) Campus Darcy Ribeiro CEP 70919-970 - Brasília - DF - Brasil

Agradecimentos

Agradeço a Deus pela vida, por todas as bençãos e oportunidades concedidas. A meus pais pelo amor e exemplo. A minha esposa pelo apoio sereno e leveza de todos os dias.

Aos Professores do PPEE pela dedicação ao ofício, em especial aos orientadores Fábio Mendonça e Robson Albuquerque. Ao Professor Fábio, agradeço pela cordialidade e tranquilidade encorajadoras. Ao Professor Robson, por toda paciência e atenção prestadas em benefício deste trabalho desde os primeiros dias.

Ao colega e amigo Marcelo Garcia, obrigado pelo incentivo e ensinamentos em tantos assuntos.

MODELO PARA MAPEAMENTO DE AMEAÇAS CIBERNÉTICAS.

Autor: Renato Carvalho Raposo de Melo
Orientador: Fábio Lúcio Lopes de Mendonça
Coorientador: Robson Albuquerque
Programa de Pós-graduação Profissional em Engenharia Elétrica - PPEE
Brasília, 26 de maio de 2023

Os conflitos travados entre grandes corporações e governos, iniciados nos tradicionais universos de disputas comerciais, políticas e ideológicas, foram carreados para o Campo de Batalha Cibernético. As organizações se veem impelidas a buscar eficiência por meio dos diversos recursos de Tecnologia da Informação disponíveis, ao mesmo tempo que buscam se proteger de ameaças cibernéticas cada vez mais complexas. Nesta dissertação, propomos um Modelo para Mapeamento de Ameaças Cibernéticas de alta complexidade voltado às esferas decisórias de grandes corporações e governos. O Modelo orienta os processos de reunião e análise de dados que caracterizam fundamentalmente ameaças cibernéticas adversariais, permitindo que as organizações percebam de maneira melhor estruturada o cenário de riscos nos quais estão inseridas.

Palavras-chave: **Segurança Cibernética – Ameaças Cibernéticas – Inteligência de Ameaças - *Advanced Persistent Threats – Cyber Threat Intelligence* - Guerra Cibernética - Crime Cibernético - Terrorismo Cibernético - Espionagem, Interferência Externa e Disrupção**.

CYBER THREAT MODELING FRAMEWORK.

Author: Renato Carvalho Raposo de Melo
Supervisor: Fábio Lúcio Lopes de Mendonça
Pot-graduate Program Professional on Electrical Engineeering - PPEE
Brasilia, 26 de maio 2023

The conflicts involving governments and multinational corporations traditionally carried out on the fields of economics, politics and ideology have been transferred to Cyber Space as a new battlefield. Both public and private organizations are driven to achieve efficiency through digitalization while also having to defend themselves from ever evolving risks presented by different cyber threats. This work proposes a Cyber Threat Assessment Framework focused on highly complex adversarial threats and is dedicated to support the decision-making process of governments and high value corporations. The proposed Framework organizes the efforts of collecting and analyzing data concerning adversarial cyber threats in order to provide useful intelligence on risks that affect the system to be defended.

Keywords: **Cyber Security; Cyber Threats; Threat Assessment; Cyber Threat Intelligence; Risk Assessment; Advanced Persistent Threats; Cyberwarfare; Cybercrime; Cyberterrorism; Espionage, Foreign Interference and Disruption**.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE TERMOS E SIGLAS

APT	Advanced Persistent Threats
CAM	Cyber Attribution Model
CISA	Cybersecurity and Infrastructure Security Agency
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CSS	Central Security Service
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DoS	Denial of Service
EUA	Estados Unidos da América
FSB	Federal Security Service
GRU	Organization of the Main Intelligence Administration
IC	Infraestrutura Crítica
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ONU	Organização das Nações Unidas
RaaS	Ransomware as a Service
SCADA	Supervisory Control And Data Acquisition
SQL	Structured Query Language
SRV	Foreign Intelligence Service
TTP	Tactics, Techniques, and Procedures
USDT	U.S. Department of the Treasury

Capítulo 1

Introdução

Nos idos de 1993, Arquilla (1993) [3] já explanava que a "revolução informacional", por meio do avanço das tecnologias computacionais e de comunicação, alteraria significativamente a maneira como as organizações se estruturariam diante da necessidade de adaptação ao universo da Informação como um recurso estratégico. Essa mudança trouxe também maior difusão e redistribuição de poder, favorecendo atores tradicionalmente mais fracos, em detrimento das organizações hegemônicas. Por meio de formas mais eficientes de coleta, armazenamento, processamento, difusão e utilização, a Informação passou a figurar no rol dos recursos determinantes para projeção de poder no ambiente das disputas geopolíticas.

Com o passar dos anos, o espaço cibernético redimensionou os limites territoriais nacionais e ações cibernéticas ofensivas passaram, inequivocamente, a ser percebidas como potenciais ameaças à soberania nacional [4]. Doutrinas de Defesa, Segurança e Inteligência dos principais atores geopolíticos, consequentemente, passaram a experimentar processos de adequação à irrefreável necessidade de inserção no mundo cibernético [5].

A ocorrência de ataques cibernéticos cada vez mais profundos e complexos aumenta à medida que evoluem os estágios de integração de redes de computadores [6] e o uso de novas tecnologias e serviços distribuídos. Grupos e organizações dedicados a perpetrar ataques contra alvos de alto valor, aí incluídos diversos sistemas governamentais, figuram como relevantes agentes de ameaça no espaço cibernético [7].

Atores ofensivos classificados como *Advanced Persistent Threats* (APTs) são especializados no emprego de técnicas complexas para, de forma anônima, lenta e persistente, invadir sistemas de alvos selecionados com o objetivo de acessar dados protegidos ou interromper processos organizacionais [8]. Apesar das técnicas de anonimização usadas por APTs, toda operação cibernética deixa vestígios [9] e a atribuição de ataques cibernéticos, por mais complexa que seja a tarefa, é medida imprescindível aos esforços de reação a tais ameaças [10].

Relatórios de *Cyber Threat Intelligence* (CTI) de organizações privadas e agências governamentais, versando sobre atores ofensivos diversos, estão disponíveis em fontes abertas. A complexidade dos eventos cibernéticos avaliados nesses relatórios varia largamente, abarcando desde

ações de hacktivismo, executadas por meio de técnicas relativamente simples [11], até operações profundas executadas por APTs com patrocínio estatal.

Essas publicações de CTI, em geral, abarcam as origens e vetores de ataques cibernéticos com foco em implementação de medidas de segurança e contenção de danos. Análises mais amplas, especialmente valiosas em casos de ataques patrocinados por Estados, que englobem motivações estratégicas, objetivos imediatos ou de longo prazo, reações prováveis e medidas de dissuasão, todavia, são menos acessíveis [12]. Além disso, os relatórios são construídos sob diferentes parametrizações e metodologias [13], além de, não-raramente, responderem a interesses comerciais ou políticos obscuros.

O Brasil foi alvo preferencial e principal fonte de ataques on-line na América Latina em 2017 [14] e continua sendo apontado com um dos principais ambientes de proliferação de crimes cibernéticos do mundo [15] [16] [17]. Singularidades linguísticas e culturais levam criminosos cibernéticos brasileiros a se especializarem em ações contra alvos nacionais [18]. Grupos hackers brasileiros, por exemplo, têm se provado séria ameaça a instituições financeiras e forçado essas organizações à constante adaptação [19].

Apesar da preferência por desenvolver malwares especificamente para uso no país, uma característica também encontrada no universo criminoso cibernético de China e Rússia, cibercriminosos brasileiros, conhecidos por sua criatividade, têm expandido sua atuação para outras partes do mundo. [20]

A importância econômica e geopolítica do Brasil, ademais, coloca o país como alvo potencial de ataques perpetrados por agentes externos, cujas ações ameaçam a segurança de dados sensíveis e Infraestruturas Críticas (ICs) nacionais. Ações cibernéticas de Espionagem e Sabotagem de sistemas críticos, vale ressaltar, vêm sendo inequivocamente identificadas ao redor do mundo desde 2003 [21].

Diante, portanto, das dificuldades inerentes à preparação e reação a um cenário cada vez mais preocupante de riscos cibernéticos, este trabalho propõe um modelo para mapeamento de ameaças cibernéticas de alta complexidade voltado a grandes organizações e governos. Com foco em patrocinadores, conjuntura internacional e agentes ofensivos, o Modelo proposto é direcionado a ameaças decorrentes de cenários intrincados, majoritariamente determinados por disputas internacionais e conflitos geopolíticos.

1.1 Objetivos Geral e Específicos

O intuito desta pesquisa é construir um modelo que permita aos gestores governamentais e corporativos compreender de maneira mais eficiente as ameaças cibernéticas de alta complexidade a que suas organizações estão sujeitas. Cumpre observar, todavia, que este trabalho não se propõe a discutir aspectos eminentemente técnicos de ações cibernéticas ofensivas. Não há, portanto, discussão detalhada sobre mecanismos de engenharia reversa, análise de artefatos, contra-

medidas ou melhores práticas de segurança, entre outros assuntos correlatos, haja vista o público ao qual o modelo se destina.

Para construção deste Modelo, portanto, é preciso identificar os componentes que formam a ameaça cibernética, aí incluídos agentes e patrocinadores, táticas, técnicas e procedimentos, elementos condicionantes estrurais e conjunturais, além dos impactos e consequências advindos da materialização da ameaça.

Uma vez identificados os componentes da ameaça, formando a base teórica do Modelo proposto, o próximo objetivo intermediário é estruturar os processos de reunião de dados que especifiquem cada um desses componentes. Em seguida, para conclusão do trabalho, tomando-se por base o rol de dados reunidos acerca de cada um dos componentes citados, tem-se como último objetivo apresentar impactos decorrentes, resultados analíticos e avaliações.

O Modelo para Mapeamento de Ameaças objeto dessa dissertação, por fim, apreende fundamentalmente conceitos das áreas de Gestão de Risco, *Cyber Threat Intelligence* e modelos de Atribuição Cibernética.

1.2 Motivação e Justificativa

O desenvolvimento deste Modelo para Mapeamento de Ameaças Cibernéticas foi motivado pela clara percepção de que o tratamento dos riscos decorrentes do massivo emprego de redes de computadores por organizações públicas e privadas deve ser elevado ao status de prioridade em Segurança. Tanto no escopo das disputas geopolíticas diretas entre nações, quanto do risco aos sistemas corporativos de valor estratégico, as ameaças adversariais devem ser endereçadas com máxima eficiência.

Nesse esteio, agências de Inteligência governamentais têm desenvolvido capacidades cibernéticas ofensivas e defensivas que passaram a permear praticamente todas as áreas de sua atuação. A construção dessa capacidade, todavia, depende da competência dessas organizações em analisar adequadamente o cenário das disputas no Espaço Cibernético, conhecendo os riscos a ele inerentes e o poderio e objetivos de seus adversários.

No universo corporativo, grandes empresas expostas aos conflitos geopolíticos estão aumentando consideravelmente seus investimentos em Segurança Cibernética. Gestores corporativos classificam os riscos geopolíticos e cibernéticos entre os mais preocupantes. Empresas multinacioais e globais, mesmo que não sofram ataques diretos, podem ser colateralmente afetadas por eventos cibernéticos ofensivos. Parece consolidado o entendimento que as capacidades cibernéticas se tornaram parte do arsenal nas disputas geopolíticas, com ataques cada vez mais sofisticados [22].

Apesar da importância do tema, modelos de mapeamento de ameaças cibernéticas, notadamente numa abordagem adversarial, estão menos disponíveis publicamente. Modelos desta natureza, como parte da disciplina de CTI em expansão, têm também como finalidade sensibilizar

gestores e técnicos que o inimigo não é um robô, mas sim um agente ou adversário dotados de variadas motivações [23].

1.3 Contribuições

A principal contribuição deste trabalho é a consolidação de um modelo para mapeamento de ameaças cibernéticas de alta complexidade, cujos resultados extrapolem o arcabouço puramente técnico e se mostrem úteis também à esfera da alta gestão organizacional, tanto no segmento governamental quanto corporativo.

O Modelo proposto disponibiliza à alta gestão um roteiro para melhor compreensão dos riscos e ameaças cibernéticas. O Modelo, nesse esteio, traz subsídios para tomada de decisão no nível estratégico, mitigando o estranhamento que os pormenores eminentimente técnicos da área de Tecnologia da Informação, tradicionalmente, geram nos círculos da alta direção organizacional e governamental.

Como parte da contribuição advinda desta pesquisa, deu-se a publicação do artigo intitulado *Cyber Threat Modeling Framework* na "17th Iberian Conference on Information Systems and Technologies (CISTI)", em 2022 [24]. O artigo expõe de forma resumida as bases teóricas e prática do Modelo para Mapeamento de Ameaças Cibernéticas objeto desta dissertação, agora apresentado em versão expandida e melhorada em abrangência e detalhamento.

1.4 Organização do Trabalho

Este trabalho foi organizado em cinco capítulos. o Capítulo 1, Introdução, versa sobre premissas básicas do tema, objetivos, contribuições da pesquisa e organização do texto. O Capítulo 2, Trabalhos Relacionados e Estado da Arte, discorre sobre publicações relevantes e conceitos fundamentais ao desenvolvimento e entendimento do Modelo proposto.

No Capítulo 3, o Modelo é apresentado em detalhes, havendo uma subseção para cada uma das fases que compõem o processo de mapeamento objeto da pesquisa. A penúltima seção, Capítulo 4, Apresentação de Resultados, consiste na exposição dos resultados alcançados por meio de sete estudos de caso que ilustram a aplicação do método desenvolvido. Ao final, chegamos à Seção 5, Conclusão e Trabalhos Futuros, onde estão sintetizados os aspectos principais da dissertação e são apresentadas linhas de pesquisa pertinentes para trabalhos futuros.

Capítulo 2

Trabalhos Relacionados e Estado da Arte

Nesta seção, conceitos fundamentais e referências teóricas são discutidos tomando-se por base trabalhos relevantes para o tema da pesquisa. Elementos considerados basilares à compreensão do Modelo proposto serão explicitados nas seções seguintes. Alguns campos de pesquisa foram especialmente importantes para o desenvolvimento deste trabalho e, a cada um deles, foi dedicada uma seção ou subseção própria.

2.1 Advanced Persistent Threats

A expressão e o conceito de *Advanced Persistent Threats* foram cunhados pela Força Aérea dos EUA ao tratar do cenário específico de espionagem cibernética conduzida por agentes ofensivos de alta capacidade patrocinados por Estados Nacionais. Com o passar dos anos, o fenômeno evoluiu e esses agentes classificados como APTs passaram também a buscar outros objetivos de naturezas econômica, política e estratégica, sempre pautados pelo esforço de manterem-se indetectáveis em acessos clandestinos a estruturas e informações críticas. [25]. Apesar da gênese do conceito de APT advir, portanto, das disputas entre Estados Nacionais, não demorou para que tais atores ofensivos se voltassem também contra corporações detentoras de volumosos recursos financeiros ou dados sensíveis de elevado valor estratégico ou comercial. [26]

APTs diferenciam-se de agentes ofensivos cibernéticos ordinários na medida em que se constituem de grupos bem estruturados, muitas vezes financiados por grandes organizações ou governos nacionais, e dedicados a atingir objetivos específicos sobre alvos selecionados. Esses atores ofensivos apresentam três características fundamentais: a) persistência temporal na busca dos objetivos pré-definidos; b) adaptabilidade às contramedidas desdobradas pelos defensores do sistema alvo; c) e alta capacidade de se manterem ativos e ofensivos durante um evento ou campanha. [26].

Na mesma linha, Rosencrance (2021) [27] destaca a complexidade das ações ofensivas conduzidas por grupos APTs, marcadas pela avançada exploração de vulnerabilidades *zero-day*; constante evolução e adaptação a mudanças nos sistemas alvo; e premente necessidade por mecanis-

mos eficientes de administração e coordenação das campanhas. Vejamos:

> *To gain access, APT groups often use advanced attack methods, including advanced exploits of zero-day vulnerabilities, as well as highly-targeted spear phishing and other social engineering techniques. To maintain access to the targeted network without being discovered, threat actors will continuously rewrite malicious code to avoid detection and other sophisticated evasion techniques. Some APTs are so complex that they require full-time administrators to maintain the compromised systems and software in the targeted network.* (Rosencrance, 2021) [27]

Vários são os modelos, comumentes denominados de "ciclos de vida de APTs", que buscam apresentar uma descrição macro do fluxo de ação desses agentes ofensivos quando em campanha. De modo geral, é seguro tomar como arcabouço básico do ciclo de vida de APTs a divisão em sete estágios proposta pelo largamente conhecido framework *The Cyber Kill Chain* [28], uma adptação cibernética de conceitos doutrinários militares que descrevem a estrutura de um ataque armado clássico. As sete fases propostas pelo *The Cyber Kill Chain* são:

a. *Reconnaissance* - Reunião de dados sobre o alvo, como endereços de e-mail e dados pessoais;

b. *Weaponization* - Construção de código malicioso específico para o evento ou adaptação de malware para o alvo selecionado;

c. *Delivery* - Entrega do pacote malicioso pelo canal de comunicação estabelecido;

d. *Exploitation* - Exploração de vulnerabilidade mapeada para execução de código malicioso no sistema alvo;

e. *Installation* - Instalação do pacote malicioso no sistema alvo;

f. *Command and Control (C2)* - Estabelecimento do canal para controle remoto do sistema ou parte do sistema alvo;

g. *Actions on objectives* - Com a estrutura montada, consecução do objetivo da ação ofensiva.

O framework NSA/CSS [29], por sua vez, se propõe a discutir o ciclo de vida da ação adversária. A publicação apresenta seis estágios da ação ofensiva, que abarcam as seguintes atividades e objetivos:

a. Administração - Planjamento; Desenvolvimento de recursos necessários à ação; e Reunião de informações sobre o alvo e sobre o estágio da própria operação.

b. Engajamento - Entrega do código malicioso pelos diversos canais de comunicação com o sistema alvo; Eploração de vulnerabilidades;

c. Presença - Execução do código malicioso; Reconhecimento do sistema alvo; Escalonamento de privilégios; Construção de acesso por meio de roubo de credenciais; Movimentação lateral; e Persistência e consolidação do acesso por meio de modificações no sistema.

d. Efeito - Atingimento dos efeitos almejados: Monitoramento; Exfiltração; Modificação; Negação; e Destruição.

e. Processos continuados - Análise, Avaliação e *Feedback*; Estabelecimento de mecanismos de Comando e Controle; Evasão e aplicação de medidas de antidetecção e anonimização.

Por meio de fluxos de ação semelhantes aos exemplificados acima, guardadas as peculiaridades dos diferentes casos concretos, APTs de variadas matrizes e dedicados a objetivos diversos utilizam malwares sofisticados para explorar vulnerabilidades dos sistemas alvo. Tais agentes ofensivos, então, instalam mecanismos externos de comando e controle para monitorar continuamente o sistema invadido e extrair grandes volumes de dados de interesse por um extenso período de tempo. [30]

Em novembro de 2022, a Kaspersky publicou mais uma edição do seu *"APT trends report"* [31], destacando as tendências de atuação de APTs observadas no mais recente recorte temporal. O relatório ressaltou que: a) as campanhas APT têm se espalhado geograficamente, com expansão de ataques à Europa, EUA, Coreia do Sul, Brasil e Oriente Médio; b) os alvos selecionados são diversos, incluídos governos e corpos diplomáticos, setor de Defesa, sistema financeiro, setor de tecnologia e segmentos de apostas; c) geopolítica permanece como um motivador central da atuação de APTs e espionagem segue como um objetivo primordial de muitas campanhas, apesar dos relevantes casos de ofensivas de ransomware dedicadas a ganhos financeiros.

A associação de APTs com Estados Nacionais, reiteramos, é reconhecida desde as primeiras discussões sobre o tema. Lemay (2018) [32], ainda mais categórico, chegou a classificar a expressão *Advanced Persistent Threat* como um eufemismo para nominar grupos de espionagem cibernética patrocinados por Estados. Na mesma pesquisa, o autor ressaltou que, apesar das dificuldades de atribuição, a China é apontada como o país que mais abriga grupos APT diretamente relacionados às operações patrocinadas pelo próprio governo. Também merecem destaque, assevera o autor, a Rússia; as potências ocidentais, aqui incluídos os membros da aliança de Inteligência *Five Eyes* - Austrália, Canadá, Nova Zelândia, Reino Unido e EUA - somados à França e Israel; além de países que vêm evoluindo em capacidades cibernéticas nos últimos anos, como Índia e Paquistão.

A capacidade cibernética ofensiva do Estado chinês foi novamente reconhecida pela comunidade de Inteligência do governo dos EUA em 2022. Por meio do *Annual Threat Assessment of the U.S. Intelligence Community* (2022) [33], destacou-se que o potencial de conflitos entre Estados Nacionais perdura como uma ameaça crítica à Segurança Nacional dos EUA e, cada vez mais, a China se aproxima de uma posição de paridade com os EUA nas disputas econômica, militar e tecnológica, senão vejamos:

We assess that China presents the broadest, most active, and persistent cyber espio-

> *nage threat to U.S. Government and private sector networks. China's cyber pursuits and export of related technologies increase the threats of attacks against the U.S. homeland, suppression of U.S. web content that Beijing views as threatening to its control, and the expansion of technology-driven authoritarianism globally.* (Annual Threat Assessment, 2022) [33]

O aparato cibernético de Inteligência, Defesa e Segurança chinês é complexo e nele estão incluídos tanto partes orgânicas da estrutura governamental, quanto agentes não-governamentais atuanto sob contrato. Apesar das dificuldades em se atingir grau de certeza no mapeamento dessa estrutura, há, alem dos já citados agentes contratados, pelo menos cinco grandes divisões governamentais que desenvolvem ações ofensivas passiveis de classificação com APTs, quais sejam: Forças Armadas; Ministério da Segurança Estatal; Ministério da Segurança Pública; agência de "administração"do ciberespaço; e o departamento de "propaganda"e da Frente Única de Trabalho. Todo esse aparato atua basicamente, com considerável sobreposição de áreas de responsabilidade, em ações de Guerra Cibernética, Espionagem, controle de dissidentes, regulação de conteúdo e de transferêcia de dados internacionais ("Grande Firewall da China"), operações de influência e propaganda interna e externa, alteraçoes legislativas e campanhas de ransomware para ganho financeiro [34].

Valeros (2019) [35], por sua vez, abarcando recorte geográfico diferente daquele formado pelos principais atores globais, o que torna seu trabalho especialmente interessante para o escopo desta dissertação, registra que, apesar de ter havido crescimento do número de operações de espionagem cibernética na última década em todo o mundo, eventos e campanhas direcionados à América Latina são fortemente subdimensionados. Em contraponto a essa realidade, o autor traz como objeto central de sua pesquisa exemplo de APT com atuação primordial na América Latina.

O APT analisado por Valeros na pesquisa supracitada, denominado de "Machete", atua de maneira altamente bem coordenada em campanhas de espionagem cibernética direcionada aos setores diplomático, militar e político na América Latina. As características do código malicioso empregado e os tipos de dados buscados nas campanhas revelam que não se trata de uma estrutura desenhada para ser desdobrada contra alvos indiscriminados em busca de ganhos financeiros. Ao contrário, as TTPs empregadas e os dados extraídos nas ofensivas seriam utéis apenas para atores interessados em influenciar e ganhar vantagens estratégicas nos estratos governamental e político. Ademais, após seis anos de acompanhamento desse APT específico, o pesquisador assevera a alta probabilidade de se tratar de um único grupo operando sob patrocínio estatal.

Ainda em Valeros (2019) [35], Machete é descrito como um APT cujos alvos prioritários são aqueles de lingua espanhola, consequência esperada diante do fato da quase totalidade dos países da América Latina adotarem o espanhol como idioma oficial. Há, todavia, campanhas que empregaram documentos escritos em português para servirem como iscas em ações de *spear-phishing*. Tal evidência, registre-se, denota que o Brasil foi também alvo do APT Machete no período avaliado pelo pesquisador. Mais detalhes sobre a atuação do APT Machete serão apresentados na Seção 4.

Afastando-nos do conceito clássico de *Advanced Persistent Threats* como ferramentas de espionagem, cumpre destacar que têm ganhado volume e importância os casos de APTs dedicados a campanhas com objetivo de ganhos financeiros. Tais eventos, por conseguinte, diferem daqueles tradicionalmente relacionados aos conflitos geopolíticos entre Estados Nacionais, marcados por ações de Espionagem, Disrupção e Interferência Externa. Tome-se como registro desse fenômeno o Alert (AA21-048A) de 2021 [36], da Cybersecurity and Infrastructure Security Agency (CISA), do governo dos Estados Unidos da América, que atesta que atores APTs ligados à República Popular da Coréia do Norte atacaram organizações, em pelo menos trinta países, com o objetivo de roubar criptomoedas.

Em julho de 2022, nova publicação da CISA (Alert AA22-187A) [37] versou sobre campanha de ransomware mais uma vez atribuída à Coreia do Norte. O malware batizado de "Maui", segundo o Alert citado, vem sendo utilizado por atores cibernéticos patrocinados pela Coreia do Norte, desde maio de 2021, contra organizações de sistemas de saúde pública. Sistemas de saúde teriam sido escolhidos como alvos diante da avaliação, pelos atores ofensivos norte-coreanos, de se tratar de serviço crítico para a vida humana, aumentando as chances de rápido pagamento do resgate demandado.

No mesmo esteio, o serviço de Inteligência da Coreia do Sul afirmou que Coreia do Norte percebe a Guerra Cibernética como um instrumento voltado a diferentes propósitos, capaz de elevar enormemente a capacidade ofensiva de seu exército nacional. Ataques cibernéticos vêm sendo empregados pela Coreia do Norte com objetivos que vão desde ganhos financeiros, por meio de campanhas de ransomware, a espionagem e destruição de sistemas de computadores adversários [38]. O caso norte-corenao será também retomado na Seção 4.

2.2 Atribuição Cibernética

O "Anonimato"é um pilar do conceito original da Internet, que pressupõe a criação de um ambiente livre capaz de preservar a identidade do cidadão, protegendo-o da vigilância e punição de Estados autoritários. Os cada vez mais avançados recursos tecnológicos de privacidade na Internet, todavia, permitem também que agentes ofensivos, estatais e não-estatatais, se beneficiem do manto do anonimato para práticas que vão desde crimes de pequena monta até grandes operações de Interferência Externa ou Disrupção [39].

Os arcabouços políticos e legais, tanto no âmbito dos ordenamentos jurídicos e sistemas políticos nacionais, quanto na esfera do Direito e Relações Internacionais, dificilmente conseguem acompanhar o ritmo da evolução tecnológica que altera os diversos segmentos das atividades humanas. Essa constatação é especialmente aplicável à dinâmica das Ameaças Cibernéticas - marcada pela forte característica transfronteiriça e robustecida pelos abundantes recursos de anonimização - o que nos leva a abordar o largamente discutido "problema da atribuição cibernética" [30].

Na expressão de Rid (2015) [40], a atribuição é a "arte"de apontar quem cometeu determinado

crime, uma questão tão antiga quanto o crime em si. Uma correta atribuição, destaca o autor, é o principal insumo de todas as formas de dissuasão e coerção. Por outro lado, uma atribuição equivocada levará à perda de credibilidade e, consequentemente, de segurança. Por meio do modelo denominado *"Q"model*, Rid organiza o processo de atribuição em três camadas de análise: técnica e tática; operacional; e estratégica, vide Figura 2.1. A primeira pressupõe o esclarecimento dos aspectos técnicos do incidente e se resume ao "como"; a segunda camada ocupa-se da arquitetura de alto nível do ataque e do perfil do atacante, encerrando-se no "o que"; enquanto a última camada, estratégica, tem como objetivo desvendar quem é responsável pelo ataque, avaliando as motivações, impactos e respostas apropriadas, resumindo-se no "quem e porquê".

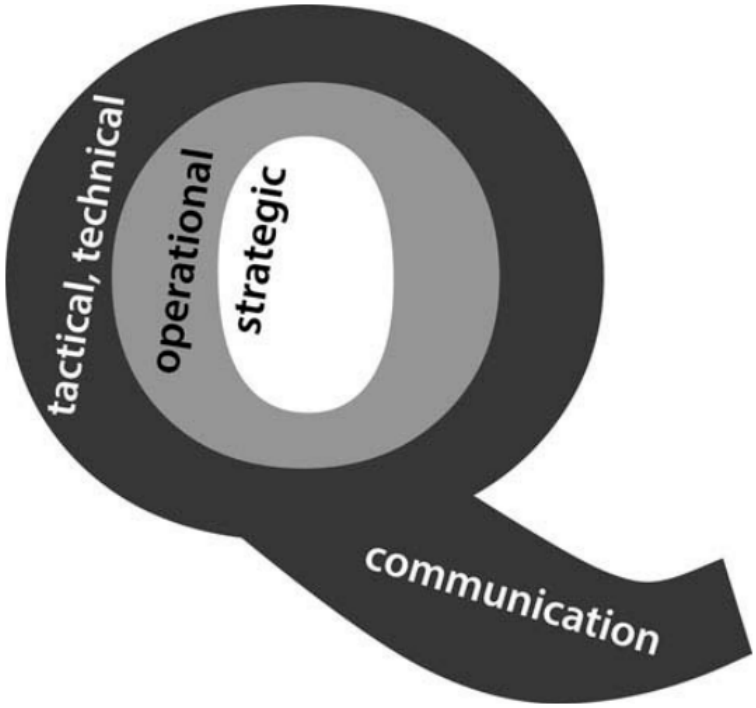

Figura 2.1: Modelo de Atribuição Cibernética - Q Model
Fonte: Rid, 2015 [40]

Romanosky (2021) [41] ensina que Atribuição Cibernética pode ser entendida como o processo de coleta, análise e associação de atividades maliciosas a um ente perpetrador identificável. O autor trata de dois tipos principais de Atribuição Cibernética, conforme explicitado abaixo e também representado na Figura 2.2:

a. Atribuição puramente técnica, que consiste na associação de artefatos cibernéticos a uma campanha ou evento ofensivo. O núcleo desse processo se baseia na reunião de artefatos que denunciem modificações em hardware ou software do sistema alvo para determinação de origem do ataque. Além das ferramentas forenses, fontes de Inteligência, a exemplo de Fontes Humanas, Inteligência de Sinais e Fontes Abertas, são também empregadas na reunião de provas e indícios, aportando maior confiabilidade aos resultados de atribuição. Tais recursos, tradicionalmente disponíveis aos serviços de Inteligência dos Estados Nacionais, têm sido empregados por organizações privadas de segurança cibernética de forma cada vez mais eficiente;

b. Atribuição política é considerada pelo autor como o tipo mais desafiador de atribuição, pois exige a compreensão, entre outros aspectos, da conjuntura geopolítica e das associações e motivações dos atores ofensivos. A análise desses dados visa a associar determinado evento ou campanha cibernética ao agente perpetrador - não raramente classificado como APT - e, eventualmente, aos patrocinadores estatais. Em alguns casos, a análise de um único evento não resulta em respostas satifatórias, sendo necessário a reunião de dados oriundos de eventos diversos para identificação de TTPs e assinaturas técnicas atribuíveis a determinado agente. Ademais, os objetivos politicos dos Estados Nacionais nem sempre são abertamente declarados. Essa obscuridade, somada ao o uso de *proxys* para condução das campanhas, emprego de *false flags* e operações de desinformação, pode levar a conclusões equivocadas.

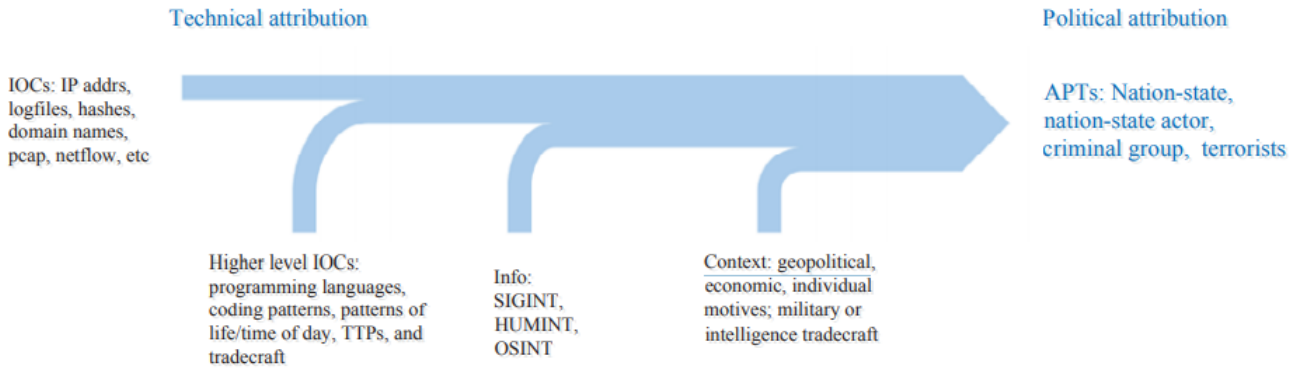

Figura 2.2: Atribuição Técnica x Atribuição Política
Fonte: Romanosky, 2021 [41]

Egloff (2012) [1] destaca que o processo de atribuição de um evento ofensivo a Estados Nacionais é ainda mais complexo diante dos diferentes graus possíveis de envolvimento da estrutura governamental na campanha sob análise. O autor apresenta dez níveis de maior ou menor participação de orgãos ou agentes governamentais em determinado evento ou campanha ofensiva. Em um extremo da gradação proposta teremos o Estado Nacional genuinamente dedicado ao esforço de proibir a operação de um agente ofensivo que atua sob sua jurisdição. Na outra ponta, teremos os casos em que a agressão é conduzida diretamente por agentes da estrutura orgânica do próprio Estado ou por atores terceirizados integrados ao aparato governamental. Naturalmente, quanto menos imiscuído estiver o governo nas fases de planejamento e de coordenação e controle da operação, maior será a margem de *plausible deniability*. Consequentemente, maior será a difilculdade do processo de atribuição.

Os dez níveis de envolvimento propostos por Egloff e suas respectivas descrições estão explicitados na Tabela 2.1

Cook (2016) [42], ao tratar de atribuição de ataques a sistemas de controle industrial, se aproxima do conceito de Atribuição Política ao defender que a análise dos objetivos de uma campanha ofensiva pode indicar quais atores estatais se beneficiariam dos resultados alcançados, contribuindo para o desenvolvimento de um processo de atribuição centrado na figura do

Tabela 2.1: Graus de envolvimento governamental com agentes cibernéticos ofensivos [1] (tradução nossa).

Grau de envolvimento	Descrição
Integração	O governo nacional conduz operações usando agentes orgânicos ou agentes subcontratados integrados à estrutura estatal.
Execução	O governo nacional conduz operações usando agentes sob controle estatal direto.
Descontrole	Agentes integrantes da estrutura estatal atuam sem consentimento governamental.
Ordenação	O governo nacional dirige agentes subcontratados para executar operações em seu benefício.
Coordenação	O governo nacional coordena operações de terceiros agentes por meio de "sugestões".
Suporte	Operação controlada e conduzida por terceiros agentes, mas com suporte estatal.
Encorajamento	Operação controlada e conduzida por terceiros agentes, mas encorajada pelo governo nacional por meio de políticas de Estado.
Ignorada	O governo nacional sabe da atuação de agentes ofensivos, mas opta por não intervir.
Proibição inadequada	O governo nacional intenciona, mas é incapaz de neutralizar os agentes ofensivos.
Proibição	O governo nacional atuará para neutralizar os agentes ofensivos.

patrocinador. Agências de CTI, vale ressaltar, empregam o conceito de Atribuição Política em seus processos ao ressaltarem a importância dos ataques complexos serem analisados não como um fim em si mesmos, mas como um meio para atingimento de objetivos financeiros, políticos, militares e econômicos.

Goel (2021) [39], por sua vez, subdivide a Atribuição Cibernética em *"what-attribution"*, referindo-se ao esforço forense para identificação do tipo de ataque sob análise; e *"who-attribution"*, que consiste no exame das Táticas, Técnicas e Procedimentos para indicação do perpetrador das ações ofensivas. O autor reforça o entendimento que o problema da atribuição perpassa, além do primordial campo das discussões técnicas, os ambientes de debate político, estratégico e jurídico.

Ainda que na maioria dos casos seja possível reunir dados relevantes sobre os perpetadores das ações ofensivas, há considerável risco dos esforços de atribuição resultarem em erros ou em insolubilidade. Os atores ofensivos mais sofisticados implementam todos os esforços para manterem-se indetectáveis no interior dos sistemas-alvo encobrindo os sinais de intrusão, notadamente através da exploração de programas executáveis nativos, uso de ferramentas legítimas de *pentest* e ataques *fileless*, além de lançar distrações, conhecidas como *false flags*, e outras técnicas anti-forenses. Não por acaso, eventos e campanhas ofensivas podem passar anos sem uma correta

atribuição [43].

Pahi 2019 [44] e Skopik (2020) [45], a partir da criação de método denominado *Cyber Attribution Model (CAM)*, abordam o problema das *false flags* no processo de Atribuição Cibernética. Ambas as publicações reforçam que as *false flags*, apesar de há muito empregadas nos campos de batalha tradicionais, adotam caracterísiticas específicas e são mais facilmente executáveis no Espaço Cibernético.

De forma mais eficiente, se comparados a agressões militares ou terroristas, ataques cibernéticos podem ser encobertos por meio de alteração, fasificação ou destruição de registros digitais. Ademais, identidades podem ser forjadas e ataques podem ser disfarçados de acidentes ou incompetência, entre outros mecanismos. Ainda que disfarçar ou encobrir completamente um ataque seja extremamente difícil, também é um enorme desafio garantir a origem e integridade dos indícios que levaram à atribuição [40]. A correta atribuição de ataques cibernéticos, por outro lado, é positiva na construção de confiança e redução do risco de escalonamento de conflitos internacionais [46].

Nos idos de 2012, Reich (2012) [47] já afirmava que o problema mais crítico da Internet estava atrelado ao anonimato, à rastreabilidade e à atribuição. O autor asseverou que ações ofensivas cibernéticas, tanto com objetivo de ganhos financeiros quanto para acessar dados confindenciais ou causar disrupção, vêm sendo empregadas, cada vez mais, por uma gama de diferentes atores estatatais e não-estatatais. Esses agentes ofensivos, em diferentes níveis de complexidade, exploram recursos tecnologicos na busca por anonimização, o que gera, consenquentemente, dificuldades no processo de atribuição cibernética. Sem a correta atribuição, as medidas repressivas de natureza jurídica, miltares ou políticas restam prejudicadas. Afinal, atingir conclusões analíticas capazes de associar patrocinadores e agentes ofensivos a determinada campanha não é tarefa especialmente desafiadora. Reunir, todavia, elementos probatórios técnicos que sustentem tais conclusões nos tribunais ou nos processos decisórios militares, por exemplo, é tarefa bem mais difícil [47].

A Atribuição Cibernética, por conseguinte, não se traduz em um corpo parametrizado de provas capaz de convencer qualquer interlocutor. Ao contrário disso, melhor se expressa como um conjunto de argumentos em vários níveis de fundamentação, cuja suficiência para levar ao convencimento as diferentes audiências é relativa.

A partir dessa premissa, Junior (2016) [48] defende que há três principais audiências a serem consideradas quando se trata de ameaças cibernéticas contra Estados Nacionais, quais sejam: os próprios decisores governamentais, que demandarão determinado grau de probabilidade de seus aparatos de Segurança, Defesa e Inteligência; o patrocinador ou agente agressor, que mesmo se aferrando à negativa de envolvimento no caso não poderá ter certeza da capacidade forense e da consequente robustez alcançada na atribuição conduzida pelo alvo ou por terceiros; e os públicos doméstico e internacional, cujo convencimento pode ser politicamente relevante para se alcançar legitimidade em eventual retaliação ou medida judicial.

Vencidas as fases de produção do conhecimento sobre o responsável pela agressão e de con-

vencimento dos interlocutores desejados, há ainda que se tomar a decisão acerca de como empregar os resultados de atribuição alcançados. Chega-se, neste ponto, a uma escolha de natureza estratégica, especialmente sensível diante da hipótese de se atribuir publicamente um ataque cibernético. Inicialmente, o alvo da ação ofensiva deve considerar se pretende reagir ou simplemnte tolerar a agressão, e, em um segundo estágio, se tal escolha será ou não publicizada. Essa decisão, dentre outros aspectos, passa pela avaliação da robustez do corpo probatório da atribuição; da existência de retaliações viáveis; do risco de escalonamento do conflito; do risco de exposição das próprias capacidades técnicas; além dos riscos e consequências políticas, econômicas e comerciais para si e para outrem [49].

Em sua proposta de framework dedicado à estruturação do processo de atribuição pública de ataques cibernéticos por Estados, Egloff (2021) [1] destaca que a publicização da atribuição é um meio para determinados fins. Ao decidir por atribuir publicamente uma agressão cibernética, a vítima, ou mesmo terceira parte interessada, deve ter clareza de quais objetivos almeja alcançar com essa exposição. O modelo proposto pelo autor preconiza quatro elementos a serem considerados no processo de tomada de decisão sobre publicizar ou não os resultados da atribuição. Resumidamente, os fatores elencados são:

a. Inteligência - perpassa a capacidade técnica de se alcançar suficiente probabilidade na atribuição; avaliação do risco de expor fontes, metódos e capacidades de seu aparato de Inteligência; avaliar a oportunidade de se antecipar a exposição dos fatos, antes que outros atores o façam; e considerar o dano que a exposição das TTPs empregadas no ataque podem causar ao agente agressor.

b. Severidade do incidente - compreende a legitimidade da ação ofensiva; a motivação por trás do ataque; e os efeitos causados pelo evento. Tais elementos resaltam a necessidade de se considerar o quão contundente será o protesto da vítima quando da publicização do ataque. Diferentes tipos de ataques, motivações e mesmo diferentes perpetradores serão mais firmemente condenados no cenário internacional que outros. Portanto, a vítima deve considerar se a gravidade da reprimenda passível de ser aplicada ao agressor suplanta os riscos da atribuição pública.

c. Geopolítica - tanto o histórico quanto o momento específico que atrevessam as relações entre os Estados contendores devem ser considerados. Mesmo nações aliadas praticam intrusões entre si, notadamente com objetivo de espionagem. O custo de gerar ruídos ou mesmo escalonamento das disputas bilaterais com a atribuição pública deve ser sopesado em relação ao ganho almejado.

d. Ações subsequentes - capacidade do Estado atacado de conduzir adequadamente medidas subsequentes à atribuição pública. Ainda que a atribuição pública por si só seja capaz de gerar consequências positivas para a vítima, convém avaliar as próprias capacidades de explorar os ganhos derivados de ações subsequentes.

O caso de hackeamento da Sony Pictures Entertainment, em 2014, serve de ilustração do processo de Atribuição Cibernética e publicização dos resultados. A ofensiva da Coreia do Norte contra referida companhia levou os EUA a retaliar economicamente o adversário, após atribuição pública do ataque. O governo norte-americano foi forçado a navegar por uma série de condicionantes antes de implementar tais medidas. Além de adotarem abertamente a defesa de uma empresa privada, numa postura que contrariou sua conhecida relutância em assumir a política de proteção de suas redes empresariais, os EUA não teriam encontrado um alvo proporcional a ser retaliado na Coreia do Norte. Como resultado, optaram por reagir na seara dos embargos econômicos, manobrando em um domínio diferente daquele do Espaço Cibernético [49].

O problema da atribuição, especialmente no contexto dos conflitos internacionais, dificulta consideravelmente a aplicação das medidas tradicionais de dissuasão militar ao campo de batalha cibernético. A crescente dependência de sistemas informatizados e integrados para o adequado funcionamento das sociedades contemporâneas criou uma nova dimensão de risco no cenário internacional. As práticas defensivas empregadas por entes governamentais e não-governamentais diante de tais riscos não poderiam deixar de aproveitar os conhecimentos já consolidados sobre Dissuasão no mundo dos conflitos cinéticos [48].

Em linhas gerais, dissuadir significa demonstrar que a agressão planejada pelo ator ofensivo não se justifica em termos de custo-benefício. Tradicionalmente, a dissuasão é alcançada por meio de quatro mecanismos: ameaça crível de punição ao agente agressor; impedimento de alcance dos objetivos do agressor; temor que as consequências nocivas do ataque impactem o próprio agressor; e termor de extrapolar limites normativos e morais que tragam prejuízos de natureza política. No espaço cibernético, contudo, a ameaça de punição é dificultada pelo fato de, antes de se punir o agente perpetrador da agressão, é preciso identificá-lo, o que nos remete ao problema da atribuição. Ademais, não há consenso na comunidade internacional se as medidas de resposta a ataques e intrusões cibernéticas devem se limitar igualmente ao Espaço Cibernético ou se ações cinéticas seriam também aceitáveis [48].

Para contornar as dificuldades de punição de agentes agressores, portanto, os esforços de dissuasão cibernética envidados pela maioria dos governos e organizações acaba se limitando a medidas de defesa passiva, direcionadas a negar ao agressor o atingimento dos objetivos propostos. Para além dessas medidas, a maior parte dos atores conta apenas com a expectativa genérica de que o temor de sofrer consequências inadvertidamente ou de ver-se envolto em celeumas políticas ou morais arrefeça o animo agressivo de seus adversários [48]

Tran [50], por sua vez, aborda a questão da Atribuição de outra perspectiva e propõe que o problema seja endereçado no campo jurídico. O autor ressalta que os avanços técnicos já alcançados são, em potencial, suficientes para solucionar o problema da Atribuição desde que o arcabouço jurídico internacional passe pelas necessárias adequações. Traçando um paralelo com o Direito Penal, a tese se fundamenta no fato dos julgamentos e condenações raramente se sustentarem em um tipo único, e por si só incontestável, de prova. Em verdade, os casos são solucionados por um corpo bem mais heterogêneo de indícios, que, acumulados, mostram-se bastantes para levar o julgador ao livre convencimento.

Lancelot [51], também pelo enfoque jurídico, ressaltou a posição central que o problema da Atribuição Cibernética ocupa entre as causas da lacuna normativa internacional sobre Guerra Cibernética. Em conflitos militares recentes, permeados por ações de Guerra Cibernética, a culpa por associação ou baseada em evidências circunstanciais foi suficiente, segundo o autor, para se alcançar a Atribuição Política, mesmo diante da incapacidade de se atingir atribuição taxativa pela vertente puramente técnica.

A questão central da atribuição pelo enfoque jurídico, portanto, é como criar um sistema legal suficientemente regulamentado para permitir e legitimar julgamentos de Atribuição Cibernética internacional. Apesar das discussões sobre Atribuição habiterem, majoritariamente, a zona de intersecção entre tecnologia e política, há também a faceta jurídica a ser endereçada. A criação dessa instância jurídica, em tese, criaria um ambiente dotado de maior imparcialidade, distante da onipresente desconfiança que assola os debates entre adversários políticos. Como resultado, a atribuição processada pelo referido sistema legal seria dotada de maior legitimidade, criando condições mais favorávéis à adequada responsabilização dos agressores nos termos da legislação internacional, aqui incluídas ações militares sob a égide do Art. 51 da Carta das Nações Unidas. Por outro lado, a incapacidade do acusador de provar a responsabilidade do acusado resultaria no encerramento da contenda, retirando a possibilidade de aplicação legítima, sob a ótica do Direito Internacional, de qualquer retaliação [50] [52].

2.3 Avaliação de Risco e *Cyber Threat Intelligence*

O Modelo para Mapeamento de Ameaças Cibernéticas apresentado nesta pesquisa foi estruturado sobre marcos teóricos que balizam as atividades de Avalição de Risco e, mais delimitadamente, de *Cyber Threat Intelligence.* Algumas publicações de ambos os segmentos tiveram especial importância na construção do modelo ora proposto.

Sistemas de Informação estão sujeitos a uma série de "ameaças", que incluem ataques deliberados, erros e eventos naturais. Tais ocorrências têm o potencail de gerar danos à infraestrutura, operação e ativos de companhias e governos, além de impactos sobre a população civil. É imperativo, portanto, que decisores organizacionais detenham informações suficientes para a adequada gestão do risco inerente aos sistemas sobre os quais são responsáveis. Para tanto, a Gestão de Risco é alicerçada em quatro subprocessos: delimitação do risco ou definição de um contexto de risco; avaliação do risco; resposta ou tratamento do risco; e monitoramento do risco [53]

A Avaliação de Risco, enquanto um dos componente da Gestão de Risco, consiste no processo de identificação de 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 [54].Para efeito de nossa pesquisa, cumpre destacar, dois desses componetes formam a linha mestra seguida para estruturação do Modelo proposto, quais sejam: identificação de ameaças à organização e identificação dos impactos causados pela ocorrência de evento danoso.

Diferentes concepções do que é a "Ameaça"são defendidas pelos vários modelos de Gestão de Risco. O *Federal Financial Institutions Examination Council (FFIEC) Information Security (IS) Handbook on Risk Assessment* [55] aborda a "Ameaça"como qualquer evento capaz de causar dano ao sistema sob proteção e atesta que "Ameaças"advém de "Agentes"internos ou externos, cujas variadas capacidades e motivações exigem o emprego de diferentes formas de mitigação e controle de risco.

O *National Institute of Standards and Technology (NIST)*, na *Special Publication* 800-30R1 [54], por sua vez, propõe uma Avaliação de Risco em quatros passos: Preparação; Execução; Comunicação de Resultados; e Avaliação continuada. Na fase de Execução, o guia NIST inclui o estágio de identificação de fontes de ameaças e define a "Ameaça"como:

> "Qualquer circunstância ou evento com potencial para afetar negativamente o funcionamento de uma organização - incluindo a missão, função, imagem e reputações institucionais - seus ativos, indivíduos, outras organizações ou a Nação por meio de acesso não autorizado, destruição, exposição ou modificação de informação ou negação de serviço de sistema informatizado."(NIST 2011, tradução nossa) [54].

A partir desse conceito de Ameaça, decorrem duas outras definições basilares: "Fontes de Ameaças"e "Agentes de Ameaças" [54]. As Fontes de Ameaça são divididas em: adversariais, acidentais, estruturais e ambientais. Dentre essas, em congruência com ao escopo de aplicação do nosso Modelo, nos interessam, unicamente, as Fontes de Ameaças adversariais, que correspondem às Ameaças opostas por *"Threat Actors"* ou, em vernáculo, por Agentes de Ameaças. Ameaças de fontes acidentais, estruturais e ambientais, consequentemente, fogem ao escopo deste trabalho.

As Ameaças Adversariais podem ser assim definidas:

> "Indivíduos, grupos, organizações ou Estados que buscam explorar a depedendência de outras organizações por recursos cibernéticos, a exemplo de informação digitalizada; tecnologia da informação e de comunicações; e capacidades de processamento tecnológico de informação e comunicações. "(NIST 2011, tradução nossa) [54].

Outro ponto conceitual a ser esclarecido, antes de adentrarmos no detalhamento do Modelo, diz respeito à conotação dada às figuras do "Adversário"e do "Agente de Ameaças". Nosso método considera que Adversários e Agentes são atores distintos, que ocupam papéis diferentes na formação da Ameaça. Enquanto o Adversário ocupa a posição de patrocinador da campanha ou evento ofensivo, o Agente é o executor do ataque propriamente dito, a instância técnica responsável pela operação de intrusão ou de influência.

O conceito de Adversários foi adotado na acepção de "competidores", emprestada do campo das Relações Internacionais. Trata-se, portanto, de atores posicionados no mesmo "nível", cujos interesses podem conflitar em diferentes situações. A posição oposta à de Adversários é ocupada por "aliados", assim entendidos como atores em posição de cooperação e não de disputa. Cumpre

ressaltar, todavia, que o status de Adversário ou Aliado não é definido por características dos atores em si, mas pelo cenário conjuntural que os envolve. Os Atores podem mudar de status ao longo do tempo ou a depender do recorte temático no qual estão inseridos, passando de Aliados a Adversários, e vice-versa. O exemplo clássico dessa relação competitiva entre Adversários e Aliados é a dinâmica entre Estados Nacionais no ambiente geopolítico [56] [57].

É preciso considerar, todavia, que atores não-estatais capazes de patrocinar ações ofensivas de alta complexidade, a exemplo de grandes grupos empresariais ou politícos e organizações terroristas ou paramilitares, também podem figurar como Adversários para efeito do Modelo proposto em pelo menos duas hipóteses. A primeira ocorre quando entidades não-estatais demonstram capacidade para se igualar a Estados Nacionais e com eles disputar recursos ou ameaçar suas posições geopolíticas, apesar de serem atores dotados de natureza constitutiva diferente.

A segunda hipótese aventa a possibilidade da disputa se dar unicamente entre entes não-estatais, sem participação governamental. Nesse caso, o sistema a ser protegido pertenceria a uma estrutura não-governamental, assim como o ente patrocinador da ação ofensiva, caso em que se trataria de atores de mesmo nível, portanto, numa relação de disputa entre Adversários.

Digna de nota é a posição ocupada por organizações criminosas em nosso Modelo. Em consonância com as linhas de discussão apresentadas na Subseção 2.4.1.1, entendemos que grupos criminosos podem figurar como Adversários caso sua atuação tenha objetivos que extrapolem o puro ganho financeiro. Grandes organizações criminosas atuais são capazes de ameaçar a Segurança Nacional de países. Essas organizações, muitas vezes, atuam na zona cinzenta que divide os teóricos sobre classificá-las ou não como grupos terroristas. Nesses casos, é possível que as ações ofensivas por eles executadas tenham objetivos políticos, e não meramente financeiros, colocando-os no rol de possíveis Adversários não-estatais [58] [59].

Esta pesquisa, por conseguinte, esta direcionada aos cenários de Ameaças advindas dos conflitos geopolíticos entre Estados Nacionais e grandes organizações de diferentes segmentos, além das Ameaças integradas por grupos terroristas e agentes criminosos de elevada capacidade técnica e cujas ações ofensivas são capazes de vulnerabilizar sistemas de Infraestruturas Críticas e setores estratégicos.

É possível conduzir a identificação de Ameaças a partir de, pelo menos, três focos, cada uma delas centrada em um componente. A primeira direção, centrada no Adversário ou Agente de Ameaça, parte do mapeamento das capacidades e características do atacante, seguido da sua inserção no ambiente de interesse; a segunda, centrada no Sistema, consiste na especificação do sistema a ser protegido, seguido da identificação das prováveis ameaças direcionadas a esse sistema; a terceira direção, centrada nos Ativos, começa pelo mapeamento dos ativos e culmina na identificação das ameaças com significativa probabilidade de materializarem alguma ação danosa a tais ativos. As três abordagens estão resumidas na Figura 2.3 [60].

Modelos de mapeamento centrados no Adversário ou no Agente de Ameaça, portanto, baseiam-se na identificação das características do atacante como medida inicial. Essa caracterização do Agente ou Adversário deve incluir, pelo menos, as TTPs utilizadas, ferramentas,

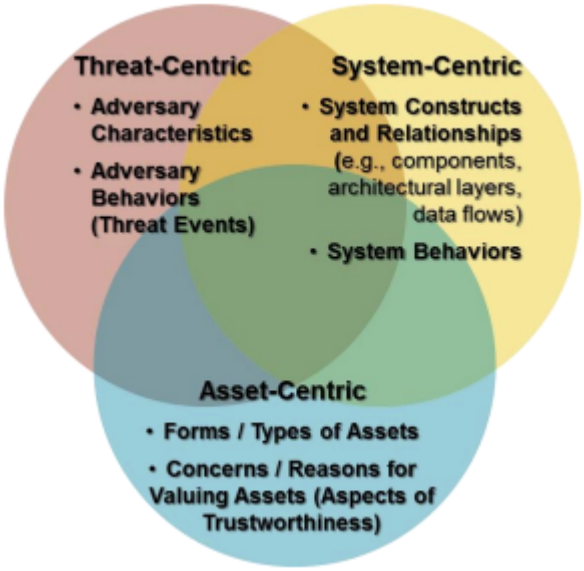

Figura 2.3: Abordagens para identificação de ameaças.
Fonte: Bodeau, 2018 [60]

motivações, intenções, recursos, capacidades e comportamento [61]. Em posicionamento doutrinário semelhante, o NIST [53] atesta que, para entender o componente "Ameaça", é preciso conhecer, entre outros quesitos, capacidades, objetivos e parâmetros para seleção de alvos dos “Adversários” elencados.

A atividade de *Cyber Threat Intelligence* (CTI), por sua vez, consiste na identificação, reunião, processamento e análise de dados sobre eventos ofensivos cibernéticos [61]. Trata-se da implementação do ciclo de Produção do Conhecimento de Inteligência em um campo técnico específico, voltado para o universo das ameaças cibernéticas e detém, por conseguinte, pontos de contato com a fase de identificação da ameaça contida na Análise de Risco.

O processo de Produção de Conhecimento, genericamente entendido como produção de Inteligência, pode ser aplicado a contextos diversos, com o objetivo basilar de transformar tópicos completamente desconhecidos em completamente conhecidos. Para tanto, a produção de Inteligência é guiada por um protocolo básico de reunião e processamento de dados, seguido de análise dos resultados alcançados, culminando na produção de Inteligência [2].

Para efeito deste Modelo de Mapeamento de Ameaças, passível também de classificação como método de CTI, a Inteligência produzida deve ser útil e oportuna, na medida em que se destina, em última instância, a neutralizar a Ameaça objeto de análise. Nesse esteio, chega-se ao conceito de Inteligência acionável, que adiciona as fases de *Deployment* e *Dissemination* ao fluxo ordinário de produção de Inteligência. A junção de todas essas fases, por fim, constitue o fluxo de produção de Inteligência de Ameaças [2], resumido na Figura 2.4.

Gong (2021) [62] conceitua CTI como um sistema de segurança de resposta a ataques cibernéticos baseado na produção de conhecimento sobre ameaças a partir de dados diversos. Os dados são gerados nas várias interfaces dos Sistemas Informatizados capazes de produzir registros sobre eventos relevantes para a segurança. O autor ressalta a importância do aproveitamento dessas

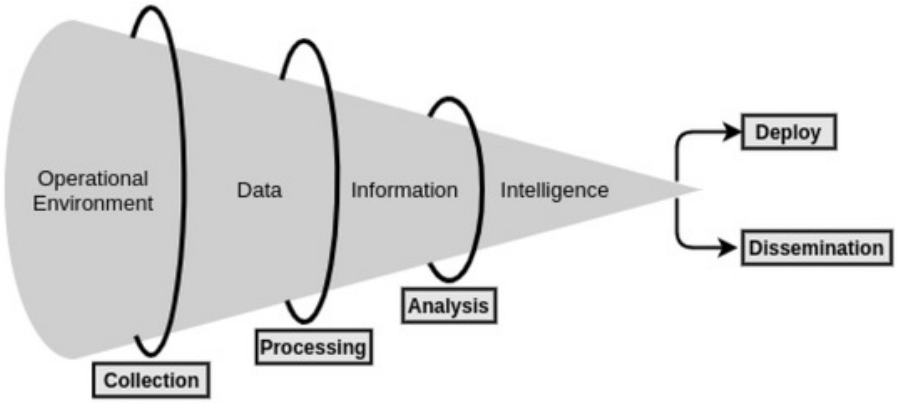

Figura 2.4: Fluxo do processo de produção de Inteligência de Ameaças.
Fonte: Silva, 2020 [2]

pistas deixadas em *cyberatacks* para identificação dos elementos caracterizadores das ameaças, trazendo proatividade aos esforços de resposta e aumentando as chances de sucesso na Atribuição.

Parte substancial do desafio de se produzir de CTI, ressalta Amaro (2022) [63], consiste em vencer o problema que envolve entender e reagir com eficiência a incidentes cibernéticos, considereando o grande volume de dados gerados por diversas fontes aproveitáveis. Há um volume cada vez maior de dados sobre ameaças sendo gerado em diversos ambientes, desde publicações jonralísticas, passando por softwares comerciais de segurança e auditorias forenses, até empresas de Inteligênca privada [64].

Em seu trabalho de revisão, Brown (2021) [64] discorre sobre os processos de CTI e suas formas de implementação em ambientes organizacionais. O artigo descreve CTI como informação sobre capacidades, oportunidades e intenção de adversários em conduzir ações cibernéticas ofensivas, ressaltando que se trata de "Informação"de Inteligência na acepção que corresponde a um produto gerado após um processo analítico, o que o difere do dado puro, não processado.

O ciclo de Inteligência compreende-se em um fluxo técnico, com variações decorrentes de adaptações doutrinárias, mas dotado de uma base teórica comum, que prevê o tratamento de dados previamente reunidos a partir de fontes múltiplas. O objetivo final desse fluxo é produzir e difundir conhecimento útil e oportuno para determinado processo decisório organizacional [65].

De maneira mais elaborada, Silva (2020) [2] considera que CTI é "inteligência acionável"gerada a partir de evidências sobre mecanismos, indicadores, implicações e contexto envolvendo ameaças ou eventos no Espaço Cibernético. Além de abarcar as fases de Reunião, Processamento e Análise de dados, contidas no fluxo de produção de Inteligência de Ameaças, o artigo traz uma fase final que se desdobra em utilização e disseminação da inteligência produzida, ressaltando o caráter "acionável"da CTI. O trabalho também contribuiu para construção do modelo proposto nesta dissertação ao estruturar o método geral “5W3H” (what, who, why, when, where, how, how much and how long). O método se presta a ordenar o desdobramento e detalhamento de tópicos objeto de análise e orienta a seleção dos elementos imprescindíveis ao mapeamento de ameaças e incidentes cibernéticos.

CTI, portanto, insere-se no clássico escopo defensivo da Atividade de Inteligência, que se ocupa de manter sob acompanhamento ameaças, atores, eventos e desdobramentos capazes de causar danos a determinada organização ou Estado. A partir desse monitoramento, busca-se produzir conhecimento para que o gestor organizacional não seja surpreendido e possa antecipar-se na adoção de medidas protetivas [66].

Atores dedicados ao campo de CTI concentram-se em quatro funções que replicam os níveis gerenciais e de execução comumente utilizados, com algumas variações, por organizações dotadas de maior complexidade: Estratégico, Tático, Operacional e Técnico. Essas quatro funções diferem entre si tanto na natureza das fontes utilizadas para reunião de dados, quanto no produto ofertado após a conclusão do processo. O quadrante Estratégico abarca a Informação de "alto nível", relevante para alta gestão organizacional responsável por considerar os riscos em contraponto aos objetivos estratégicos. O estrato Operacional interessa ao aparato de resposta a incidentes cibernéticos, equanto o estrato Técnico informa o pessoal responsável pela monitoramento e controle dos sistemas. Por fim, o nível Tático ocupa-se das TTPs mapeadas a partir de eventos analisados [61].

2.4 Conflitos Cibernéticos

O Modelo para Mapeamento de Ameaças Cibernéticas ora apresentado, com sua vocação para tratar de cenários complexos, ocupa-se, primordialmente, de quatro campos de conflito cibernético. Esses campos se referem a fenômenos de alcance mundial capazes de impactar significativamente governos e grandes organizações envoltas em disputas geopolíticas, quais sejam: Cibercrime; Ciberterrorismo; Espionagem, Interferência Externa e Disrupção; e Guerra Cibernética [67].

Os quatro campos citados são meios através dos quais disputas geopolíticas e ameaças criminosas com elevado potencial de dano ocorrem no Espaço Cibernético. Disputas e conflitos cujas origens encontram-se no mundo físico são levados ao Espaço Cibernético por meio de ações ofensivas cada vez mais profundas. O mundo se vê, portanto, diante de uma crescente projeção da geopolítica no Espaço Cibernético, que passou a funcionar como um campo de disputas e batalhas onde organizações e governos desdobram suas diferentes capacidades ofensivas e defensivas [68].

É seguro considerar que esses fenômenos, na ordem que foram apresentados, possuem, entre si, graus de complexidade crescentes. A complexidade a que nos referimos, todavia, não está relacionada aos recursos tecnológicos ou à capacidade técnica dos Agentes ofensivos que os compõem, mas sim à natureza dos objetivos almejados pelos patrocinadores dessas ações ou campanhas ofensivas.

No menor grau de complexidade temos os Crimes Cibernéticos perpetrados por agentes não-estatais, dedicados unicamente a ganhos financeiros contra alvos indiscriminados. Em seguida, surge o Cibercrime instrumentalizado por agentes ofensivos sofisticados e, em alguns casos, atuando sob patrocínio estatal. Nesse último caso, os agentes constituem ameaças de elevada com-

plexidade, potencialmente nocivas a sistemas governamentais e organizações privadas de valor estratégico.

O Ciberterrorismo, por sua vez, apresenta uma faceta mais simples quando utilizado como meio de ação por agentes relativamente pouco sofisticados e carentes de objetivos mediatos ou estrátégicos bem definidos. Nesses casos, não é incomum que a motivação terrorista seja demasiadamente difusa e praticamente inalcançável, tornando o objetivo imediato da ação ofensiva um fim em si mesmo, a exemplo de casos de ecoterrorismo [69]. Em um estágio posterior de complexidade, surgem organizações terroristas com objetivos políticos claros, sólida infraestrutura e crescente competência cibernética.

Espionagem, Interferencia Externa e Disrupção, tanto de matriz estatal quanto não-estatal, aparecem em seguida. No contexto específico que aqui nos interessa, ações dessas naturezas têm objetivos específicos e buscam efeitos limitados. Não se confundem com os demais campos de conflito cibernético por não integrarem campanhas mais profundas dedicadas a gerar danos extensos às organizações ou aos Estados alvejados. Tais diferenciações, registre-se, serão melhor abordadas nas Seções 2.4.4 e 2.4.3.

No último grau de complexidade, chega-se à Guerra Cibernética, dotada de maior sofisticação e cujos objetivos estratégicos bem definidos dependem de coordenação precisa com outras medidas, além de planejamento de longo prazo. Esse cenário pode ser considerado como o mais grave estágio de ameaça cibernética, uma extensão do tradicional fenômeno da Guerra travada entre Estados Nacionais [70]. Veremos na Seção 2.4.4 que os limites do que se entende como Guerra Cibernética são ainda turvos e, à primeira vista, dificilmente distinguíveis de outros fenômenos tanto mais simples quanto mais complexos.

As subseções seguintes trarão aprofundamentos e discussões acerca dos campos de conflito cibernético.

2.4.1 Cibercrime

2.4.1.1 Conceito e Escopo de Interesse

Crimes cibernéticos têm aumentado em escala global. Com o advento da pandemia de COVID-19, que empurrou sociedades e organizações ainda mais a fundo no processo de digitalização, essa marcha ganhou substancial aceleração [71]. É seguro dizer que a atividade criminosa cibernética está em franca expansão e já causa prejuízos cujo montante total é praticamente incalculável - vide o impacto global resultado do "Petya/NotPetya"ransomware de 2017 [72].

Cibercrime pode ser conceituado, em sua forma mais abrangente, como qualquer atividade criminosa que emprega computador ou rede de computadores para ações delituosas [73]. A maior parte da atividade criminosa cibernética é praticada por grupos com algum grau de organização. Tais grupos, todavia, não necessariamente seguem o padrão comumente hierarquizado das organizações criminosas convencionais, havendo coexistência de formas mais ou menos rígidas de

agregação, bem como exemplos tanto de atores puramente cibernéticos quanto híbridos, que associam cibercrimes a crimes comuns. Outro dado relevante aponta que organizações criminosas convencioanais têm cada vez mais expandido sua atuação para o mundo cibernético [74].

Criminosos cibernéticos exploram as diferentes capacidades dos países em prevenir, detectar, investigar e punir delitos cibernéticos. Atuando na zona cinzenta das legislações nacionais e internacional que tentam regular o Espaço Cibernético, esses criminosos transformaram-se em uma ameaça sem fronteiras [75]. A característica transnacional dos cibercriminosos, isolados ou organizados, aumenta sua capacidade de se evadirem das contramedidas implementadas até mesmo pelos atores mais sofisiticados [74], o que gera ainda maiores desafios nos campos da Atribuição Cibernética e da persecução criminal internacional.

As armas mais notáveis e frequentemente usadas por atacantes cibernéticos exploram vulnerabilidades surgidas com a popularização da "Internet das Coisas", ataques de *distributed denial of service* (DDoS), injeção de *Structured Query Language (SQL)*, além de variados tipos de malwares para diferentes aplicações, aqui incluídos os cada vez mais devastadores ataques de ransomware. [76] Ataques de ransomware, por serem cada vez mais frequentes, complexos e impactantes, merecem especial atenção para o escopo desta pesquisa e serão melhor explorados ainda nesta seção.

Antes de aprofundarmos a discussão sobre ransomware, todavia, cumpre reiterar que o recorte da atividade cibernética criminosa objeto desta pesquisa engloba apenas os eventos e campanhas potencialmente nocivos a grandes organizações e governos. Tal recorte se justifica pela necessidade de separarmos ações criminosas cibernéticas "quotidianas", cujo volume de ocorrências também cresceu significativamente nos últimos três anos [77], das ações de impacto nacional ou regional que ocorrem quando alvos de valor estratégico são atingidos.

Alvos com tamanha importância, quando afetados por eventos cibernéticos avançados, a exemplo de campanhas sofisticadas de ransomware contra ICs, podem causar significativo impacto de alcance nacional ou mesmo regional. [78] [79].

Ademais, são alocados como cibercrime somente os eventos e campanhas ofensivas que tenham o ganho financeiro como objetivo. Movimentos ofensivos levados a cabo por quaisquer agentes ou patrocinadores, mesmo que empregando TTPs comuns a grupos criminosos cibernéticos, serão classificados como atividade criminosa apenas se seus objetivos não ultrapassarem o limite do puro ganho financeiro [80].

Em outros termos, mesmo que enfrentemos eventos patrocinados por Estados Nacionais, grupos terroristas, organizações políticas ou grupos econômicos, na ausência de qualquer outro objetivo para aquela ação específica que extrapole o puro lucro, tratar-se-á de cibercrime. Por outro lado, mesmo agentes não-estatais que se engajem em campanhas ofensivas empregando TTPs criminosas, com objetivos outros que não apenas financeiros, fogem ao recorte de cibercrime objeto desta pesquisa e devem receber enquadramento em outras linhas de análise, como será demonstrado no decorrer deste trabalho.

Dito isso, é preciso ter cautela ao se classificar eventos cibernéticos de alta complexidade

como de natureza "meramente"criminosa. Tal afirmação se baseia no risco de se incorrer na simplificação equivocada de um fenômeno muito mais profundo, cujas características o incluiriam no cenário dos conflitos geopolíticos entre os grandes atores internacionais, estatais ou não.

2.4.1.2 Considerações sobre Ransomware

Gallo and Liska (2016) [81] define "ransomware"como um termo genérico para descrever uma classe de malware usada para extorquir digitalmente vítimas a pagarem valores de "resgate". Tipicamente, os criminosos tornam arquivos ou sistemas inteiros indisponíveis às vítimas por meio de criptografia ou alterações de credenciais de acesso, exigindo pagamento para normalização do sistema.

Em linhas gerais, o ataque de ransomware pode ser direcionado tanto aos arquivos quanto ao hardware do sistema alvo. No primeiro caso, denominado *Crypto-Ransomware*, a negação de acesso aos dados é feita por meio de criptografia dos arquivos dentro do sistema. Já a modalidade de ataque ao hardware, denominada *Locker-Ransomware*, causa a interrupção do meio de acesso ao sistema, por exemplo, pelo bloqueio de tela em dispositovos móveis, sem a criptografia do conteúdo dos arquivos. Em ambos os casos, o atacante exige o pagamento de resgate para liberação do sistema. [82]

Além da exigência de resgate, alguns ataques de ransomware passaram a ameaçar as vítimas com a publicização dos dados sequestrados [83]. Essa forma de potencialização do ataque gera maior pressão sobre as organizações e indivíduos afetados, impondo riscos de responsabilização legal aos detentores de dados pessoais expostos ou vazamento de informações valiosas. Tal modalidade de ransomware surge como uma adaptação dos agentes ofensivos às contramedidas de segurança, que aperfeiçoaram técnicas e procedimentos para criação de redundâncias em prol da disponibilidade de bancos de dados.

Na primeira metade de 2021, autoridades em Segurança Cibernética dos governos dos EUA e Austrália registraram a tendência de eventos de ransomware alvejarem grandes organizações, um tipo de campanha batizada de *big-game hunting*. Os alvos são organizações de alto valor econômico e estratégico, que não raramente fornecem serviços em segmentos críticos, a exemplo dos ataques realizados contra a *Colonial Pipeline Company* e *JBS Foods*. Em meados de 2021, entretanto, grupos de ransomware sofreram retaliações do governo dos EUA, o que levou a um redirecionamento perceptível na escolha de alvos. Aumentaram, em consequência, as ofensivas contra organizações médias, uma tentativa dos atores ofensivos de se posicionarem abaixo do radar das agências governamentais de *Cybersecurity*.

O sucesso das campanhas de ransomware ao redor do mundo levou ao surgimento de um mercado específico para negociação de códigos maliciosos dessa estirpe. A comercialização do código se dá geralmente em fóruns na *darknet*, onde os interessados têm acesso ao malware em diferentes estágios de finalização: desde códigos-fonte para compilação, até sistemas com interface pronta para receber os dados de identificação da vítima. Essa prática colaborativa trouxe ainda mais popularidade aos eventos ofensivos com emprego de ransomware e reduziu o risco para os

programadores dedicados ao desenvolvimento desse tipo de malware. Tal modalidade de ransomware, batizada de *Ransomware-as-a-Service (RaaS)*, se tornou um recurso para que criminosos com baixa capacidade de programação ingressem no lucrativo mercado de ransomware. [84].

Uma única campanha de ransomware é capaz de afetar dezenas de países, a exemplo do "WannaCry", de 2017, que atingiu 150 nações. Em 2020, vale destacar, o Brasil figurou como um dos paises cujas organizações foram mais atacadas por ransomware, ao lado de EUA, Índia e Bélgica, entre outros. Ataques dessa natureza são também destacadamente significatvos na Rússia, China e Arábia Saudita. [85]

O custo dos ataques de ransomware vai muito além do preço dos resgates exigidos. Apesar de não se tratar de ações violentas, no sentido tradicional do termo, esses ataques rotineiramente ameaçam a segurança, em diversas conotações, e mesmo a vida de pessoas ao redor do mundo. Tal constatação resta clara quando analisamos ataques contra sistemas de Infraestruturas Críticas (ICs), a exemplo dos seguintes eventos [86]:

1. Interrupção de serviços essenciais, inclusive operações militares e de segurança. Em 2019, ataque de ransomware interrompeu a operação de uma base da Guarda Costeria dos EUA por trinta horas.

2. Ataques a sitemas de distribuição de energia. Em 2020, ataque de ransomware contra o operador de um gasoduto interrompeu a distribuição de combustível por dois dias. Em 2021, ataque ao *Colonial Pipeline* parou a rede responsável pela distribuição de metade do combustível consumido na Costa Oeste dos EUA [87].

3. Hospitais e centros médicos são alvos preferenciais de ransomware. Em 2020, 560 unidades de saúde foram atacadas por ransomware apenas nos EUA. Além de custar milhoes de dólares, esses eventos causaram atraso em tratamentos e, provavelmente, levaram pacientes à morte. No mesmo ano, durante a pandemia de COVID-19, foi reportada a primeira morte causada por ataque cibernético , quando um ransomware interrompeu tratamentos no Hospital Universitário de Düsseldorf, na Alemanha [88] .

No mesmo esteio, autoridades em Segurança Cibernética dos governos dos EUA, Austrália e Reino Unido, por meio do *Joint Cybersecurity Advisory - 2021 Trends Show Increased Globalized Threat of Ransomware* [89] atestaram que quatorze dos dezesseis setores de IC dos EUA foram afetados por eventos de ransomware, inclusive Base Industrial de Defesa, Serviços de Emergência, Agricultura e Abastecimento, Sistemas Administrativos Governamentais e Setor de Tecnologia da Informação. Na Austrália, foram atingidos os setores de Saúde, Energia, Financeiro e de Pesquisa. O Reino Unido, por sua vez, considera que os eventos de ransomware são a maior ameaça cibernética ao país, figurando o setor de Educação como o setor mais afetado, seguido pelos setores empresariais, filantrópicos, Saúde, Jurídico e Sistemas Administrativos Governamentais.

Ao lado das organizações criminosas especializadas em ataques de ransomware e dos grupos ou agentes menos tecnicamente capazes que optam por emprego do Raas, grupos terroristas;

organizações políticas; grandes grupos econômicos; e governos utilizam esse e outros malwares com objetivos variados. Nesses casos, o ganho financeiro pode ser ou não o objetivo final da ação ofensiva [24] .

No grande quadro do conflito entre Estados Nacionais e organizações supranacionais, ataques de ransomware apresentam-se como uma séria ameaça cibernética à Segurança Nacional e o assunto está sendo levado para o topo da agenda de muitos governos. A maioria dos agentes APTs que desdobram campanhas de ransomware está baseada em jurisdições que os protegem da persecução criminal dos países-alvo ou da comunidade internacional [90].

Governos nacionais, por exemplo, patrocinam campanhas de ransomware como forma de suplantar sanções econômicas impostas por organismos internacinoais ou outras nações. Por outro lado, o ransomware pode também ser empregado por Estados ou atores não-estatais como TTP em campanhas com objetivo de Terrorismo ou como arma de disrupção em um contexto de Guerra Cibernética, tendo eventuais ganhos financeiros papel marginal. [86]

O *U.S. Department of the Treasury*, em 2021, tome-se como exemplo, atribuiu aos serviços de Inteligência do Estado russo campanhas cibernéticas ofensivas, homizio e associação com criminosos cibernéticos envolvidos em ataques de ransomware, vejamos:

> *The Russian Intelligence Services — specifically the Federal Security Service (FSB), Russia's Main Intelligence Directorate (GRU), and the Foreign Intelligence Service (SVR) — have executed some of the most dangerous and disruptive cyber attacks in recent history, including the SolarWinds cyber attack(...).*
>
> *(...) To bolster its malicious cyber operations, the FSB cultivates and co-opts criminal hackers, including the previously designated Evil Corp, enabling them to engage in disruptive ransomware attacks and phishing campaigns.* (USDT, 2021) [91]

A Agência Nacional de Crimes do Reino Unido, na mesma linha, atestou que a distinção entre Estados Nacionais e criminosos cibernéticos está cada vez mais turva. Por conseguinte, vem crescendo a percepção que as repostas governamentais à ameaça cibernética composta pelo Cibercrime deveriam combinar medidas diplomáticas, financeiras e legais com operações militares e de Inteligência. [92]

2.4.2 Ciberterrorismo

A criação do termo *"cyberterrorism"* é atribuída ao pesquisador Barry Collin, que, em 1980, cunhou a expressão para se referir à convergência entre o espaço cibernético e o terrorismo. [93]. Ainda existe ampla discussão sobre o tema [94], em especial quanto à abrangência, risco e perspectiva de evolução do fenômeno em si. Para alguns pesquisadores, terrorismo cibernético começou a ser discutido quando não passava de um risco remoto, cujo impacto estava distante de alcançar níveis alarmantes. Ciberterrorismo poderia, então, ser entendido como o simples uso

por terroristas de rede de computadores como meio auxiliar para suas operações e não como uma tática ou estratégia independentes. [93]

A definição de terrorismo cibernético passa, invariavelmente, pela definição do terrorismo convencional. Em que pese as discussões sobre terrorismo convencional estarem longe de ser incipientes, o tema ainda não foi pacificado. Muitos acadêmicos, entretanto, concordam que o fenômeno, em sua concepção moderna, surgiu como uma tática para incitar mudanças políticas na segunda metade do século XIX. [95].

Em linhas gerais, terrorismo consiste no emprego de violência sistemática por grupo ou partido como meio para consecução de seus objetivos [95]. Numa construção mais recente e melhor delimitada, terrorismo pode ser definido como um ataque premeditado e politicamente motivado, perpetrado por grupos subnacionais ou agentes clandestinos, contra alvos não-combatentes. [96].

A partir das definiçoes acima, extraimos três pilares conceituais do terrorismo: emprego de violência sistemática; objetivos políticos; e perpetrado por grupo ou partido. Devemos considerar, a partir desse ponto, que a mera intimidação não se enquandra no escopo do terrorismo, pois baseia-se na ameaça de emprego de violência e não no seu uso real e sistemático. No mesmo esteio, ações governamentais, ainda que violentas e politicamente motivadas, fogem à delimitação posta, em face da cobertura de autoridade legalmente constituída que seus agentes possuem. Quanto ao componente político, esse deve ser entendido amplamente como a atividade que busca realocar poder entre grupos e indivíduos, não sendo, por conseguinte, exclusividade de organizações políticas tradicionais. Essa atividade política engloba também aquelas de motivação religiosa e ideológica [97].

Há ainda menos consenso quando se trata especificamente da definição de ciberterrorismo. Alguns autores construíram a noção de ciberterrorismo alicerçados no risco de ataques cibernéticos serem perpetrados contra sistemas de Infraestruturas Críticas ou para coagir governos e populações: *"Cyber-terrorism is the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population."* (Lewis, 2002) [98]

O mesmo autor, em Lewis (2005) [99], considerou que a Internet é uma ferramenta organizacional para o terrorismo, à medida em que fornece base para financiamento, planejamento, comando, controle e comunicação entre grupos difusos com hierarquia flexivel e pouca estrutura. Serve tambem ao esforço de Inteligência, seleção e reconhecimemto de alvos, além de recrutamento, propaganda e motivação. Apesar da patente utilidade para tais grupos, a Internet não seria uma "arma"de preferência para terroristas, pois a opção por táticas as mais violentas e chocantes possíveis não se adequa ao nível factível de impactos cinéticos até então registrados em ataques cibernéticos.

Cavelty (2006) [100], por sua vez, já considerava que um ataque cibernético em larga escala, diante do grau de interpendência dos sistemas informacionais, poderia causar suficientes danos econômicos, medo e morte entre civis ao ponto de ser classificado como ato terrorista. Apesar de atestar que ataques cibernéticos realizados por extremistas políticos, à época, eram pouco sofisti-

cados, o FBI considerava que a gravidade desses fenômenos tendia a aumentar com a associação de ataques terroristas convencionais a ofensivas cibernéticas. A pesquisa citada acaba por elencar duas principais abordagens para definição do ciberterrorismo:

a. Baseado nos efeitos: ataques cibernéticos cujos impactos sejam comparáveis aos de ataques convencionais, mesmo que perpetrados por agentes criminosos;

b. Baseado nos objetivos: ataque cibernético criminoso ou politicamente motivado com o objetivo de intimidar ou coagir governo ou sociedade a avançar agenda política ou causar mal grave ou dano econômico severo.

De fato, nos últimos anos, ataques cibernéticos foram capazes de gerar efeitos cinéticos relevantes. Paralelamente, surgiram bastantes evidências de que organizações terroristas estão adotando ferramentas cibernéticas para tentar lançar ataques cada vez mais sofisticados, especialmente contra Infraestruturas Críticas. Estaríamos, portanto, observando o surgimento de agentes ofensivos cada vez mais capazes de gerar efeitos cinéticos por meio de ferramnetas cibernéticas [101].

Esse cenário de maior gravidade, contudo, teria alavancado uma percepção exagerada do risco de ciberterrorismo, em especial pela noção de que o dano advindo desses eventos poderia ser catastrófico. Lawson (2019) [102] apresenta essa exacerbação através da figura do *"cyber- doom"*. Essa retórica, fortalecida durante a gestão do ex-presidente dos EUA, Barack Obama, defende que a ocorrência de um evento cibernético catastrófico é cada vez mais provável, tomando-se por base eventos de grande impacto supostamente já registrados no mundo. Indo mais a fundo, o autor considera que tais eventos cibernéticos altamente impactantes não aconteceram de fato e põe em dúvida se um dia acontecerão.

Como exemplo da narrativa hiperbolizada do *cyber-doom*, tem-se o caso da campanha cibernética que alvejou a Estonia em 2007. Apesar de ser apresentado por alguns analistas como um caso de ataque em larga escala que desestabilizou o país, majoritariamente atribibuído à Russia num contexto de *Information Warfare*, os eventos reais se basearam em ataques de DoS e DDoS, com impactos não significativos da perspectiva de danos contra a infraestrutura do país. [102] [103]

Em meio aos debates sobre o tema, tendemos a concordar com Gulyamov (2022) [104] acerca da necessidade de colocarmos em invólucros distintos duas hipóteses para definição de ciberterrorismo, quais sejam:

a. o uso da Internet por agentes terroristas como base para o desdobramento de atividades meio ou preparatórias de atos terroristas, a exemplo dos já citados esforços de Inteligência, financiamento e recrutamento;

b. o emprego da Internet, mas precisamente de códigos maliciosos, para causar danos em sistemas informacionais capazes de impactar o mundo real por meio de resultados cinéticos.

Ao final, nos parece acertado considerar que apenas esta segunda hipótese deve ser classificada como ciberterrorismo. A distinção entre terrorismo convencional e ciberterrorismo é apenas o meio de ação empregado: meios cinéticos tradicionais e meios cibernéticos com efeitos cinéticos, respectivamente. Tanto o terrorismo cibernético quanto o convencional, por conseguinte, fundamentam-se no emprego efetivo de violência como meio de ação principal para consecução de objetivos de natureza política. Ademais, nos perfilamos à tese de que ações governamentais violentas contra populações ou organizações civis ou contra forças de outros Estados não se enquadram no rol de práticas terroristas. Tais ações, todavia, podem ser enquadradas como outras ameaças de interesse desta pesquisa.

2.4.2.1 Considerações sobre Hacktivismo

Antes de encerrarmos nossas considerações sobre ciberterrorismo e avançarmos aos demais campo de conflito cibernético, trataremos brevemente das ações de hacktivismo. A opção por trazer esse tema para a seção dedicada ao Terrorismo tem por objetivo discriminar dois fenômenos de características eminentemente políticas, mas cujas materializações diferem enormemente em meios de ação e impactos almejados.

Hacktivismo pode ser entendido como a manifestação de oposição política por meio de computadores ou redes de computadores.Trata-se de ações de natureza legal ou ilegal, que têm por objetivo dar visibilidade a demandas políticas específicas [105]. Nos dizeres de Samuel (2004): *"hacktivism is the nonviolent use o f illegal or legally ambiguous digital tools in pursuit of political ends"* (Samuel, 2004) [106].

Apesar de buscar igualmente objetivos políticos por meio de ações muitas vezes ilegais, o hacktivismo, diferentemente do ciberterrorismo, manifesta-se por meio de medidas não-violentas e não-militares. É preciso registrar, todavia, que práticas ilegais, apesar de não necessariamente violentas, continuam sendo uma forma de agressão. O universo hacktivisita, entretanto, construiu um *ethos* próprio que justifica sua conduta ao considerá-la como medida de inflexível defesa da liberdade de acesso à informação e liberdade de expressão. Ações hacktivistas que infrinjam leis ou afrontem os pilares da segurança cibernética, portanto, estariam protegidas pelo senso de que se trata de uma luta em justa causa [105].

Ademais, os meios de ação empregados por hacktivistas buscam dar visibilidade a determinado pleito político, mas não por meio de danos físicos aos alvos selecionados. Ataques de DDoS ou *defacement*, comumente empregados em campanhas de hacktivismo, por exemplo, são certamente incômodos e podem acarretar prejuízos financeiros e legais, mas é muito pouco provável que ameacem a segurança ou a vida de seus alvos ou de terceiros. Some-se a isso o fato de os impactos de campanhas hacktivistas tenderem a durar apenas o tempo da ofensiva em si, não causando, regra geral, efeitos duradouros graves sobre os sistemas afetados. [80]

Apesar das similutudes existentes entre os dois fenômenos, as distinções entre ambos são bastantes e suficientes para apartá-los como componentes de ameaças inconfundíveis, inclusive no bojo desta pesquisa. Desde que não seja parte de uma campanha mais profunda de guerra

cibernética, portanto, o hacktivismo isoladamente não alcança o grau de complexidade e risco necessários para figurar como elemento de ameaças consideradas relevantes para o Modelo de Mapeamento ora proposto.

2.4.3 Espionagem, Interferência Externa e Disrupção

Political warfare é o termo usado para definir a aplicação da doutrina de Clausewitz aos tempos de paz. Trata-se, em linhas gerais, da utilização de todos os recursos disponíveis a uma nação para alcançar de seus objetivos nacionais, desde que as ações desenvolvidas não ultrapassem os marcos teóricos que as classificariam como atos de Guerra. Tais medidas englobam desde movimentos políticos e econômicos ostensivos e propaganda aberta, até ações clandestinas, como Operações Psicológicas e suporte a organizações subversivas.

É nesse contexto de disputa, cuja intensidade permance aquém dos limites tradicionais da Guerra, que Espionagem, Interferência Externa e Disrupção se colocam como um dos potenciais "conflitos cibernéticos". Em outros termos, essas ações são empregadas pelos diversos atores em disputa como medidas ofensivas de alcance limitado. Não se trata do emprego dessas técnicas como parte de campanhas profundas de Guerra convenciaonal ou cibernética, mas de ataques com objetivos específicos e cujos danos não seriam graves ao ponto de ensejar retaliações militares cinéticas.

Antes de adentrarmos nos pormenores conceituias do tema, todavia, vale destacar que esses mesmos termos foram empregados em conotação completamente diferente na Fase I de Execução deste Modelo para Mapeamento de Ameaças Cibernéticas, vide Seção 3.2. Essa ressalva se refere especificamente ao emprego de Espionagem, Interferência Externa e Disrupção como o elmento "Objetivo"da Ameaça, a ser oportunamente detalhado na Subseção 3.2.6.

A Espionagem como meio de ação visa a objetivos variados, notadamente de natureza militar, política e econômica. Trata-se de uma ferramenta presente no bojo das disputas e conflitos humanos desde os primeiros registros históricos. Com ressalvas terminológicas que extrapolam o escopo dessa pesquisa, vale ressaltar que a Espionagem é empregada igualmente por atores governamentais e não-governamentais [107].

À medida que as operações cibernéticas têm se tornado aspecto central da Atividade de Inteligência, a Espionagem foi também carreada para o Espaço Cibernético e preservou sua importância como instrumento de política externa [108]. Espionagem cibernética, por conseguinte, é descrita como a infiltração em computadores ou outros dispositivos por meio de hackeamento, ou outras técnicas, com o objetivo de se coletar informações sem o consentimento de seu legítimo detentor [109].

É majoritário o entendimento que Espionagem não constitui um ato de Guerra. A bem da verdade, mesmo a natureza de ilegalidade da Espionagem internacional é objeto de debate, levando-se em conta as diferenças entre os arcabouços jurídicos de cada país [110].

Interferência Externa, por sua vez, no conceito cristalizado pela Política Nacional de Inteli-

gência: "É a atuação deliberada de governos, grupos de interesse, pessoas físicas ou jurídicas que possam influenciar os rumos políticos do País com o objetivo de favorecer interesses estrangeiros em detrimento dos nacionais"(PNI, 2016) [111].

Os graus de profundidade de campanhas de Interferência Externa de um Estado sobre outro variam largamente, indo desde ações de propaganda ostensivas até atuação de grupos clandestinos dedicados à sabotagem e subversão [112]. Para escopo desta pesquisa todavia, apenas ações de Interferência carreadas ao Espaço Cibernético são de interesse.

Na era dos conflitos assimétricos, as tecnologias de Informação e Comunicações elevaram significativamente a capacidade de manipulação e condicionamento da opinião pública. Por esse meio, a Interferência Externa ocorre, geralmente, de maneira discreta, em formatos que dificultam a Atribuição. Como resultados, essas campanhas ofensivas buscam minar a liberdade de convencimento e decisão da sociedade alvo sobre sua própria organização e objetivos políticos [113].

Com a cresecente digitalização dos processos e serviços públicos e privados em Estados com maior grau de liberdade individual, agentes maliciosos ofensivos exploram esse fenômeno da governança digital para enfraquecer seus adversários por meio de Operações de Desinformação [114].

Desinformação, para o escopo desta pesquisa, é o termo que abarca uma ampla categoria de tipos de informação difundida por meio digital e capaz de gerar nos destinatários distorções sobre a compreensão da realidade [115]. Desconsiderando os meios tradicionalmente empregados pelos Serviços de Inteligência no decorrer da História, em suma, é pela análise da Desinformação digital que este Modelo para Mapeamento de Ameaças Cibernética aborda o tema da Interferência Externa.

Avançando sobre o último tópico desta subseção, adotou-se nesta pesquisa o conceito de Disrupção empregado pelo NIST, qual seja: um evento não-planejado que deixa inoperante todo um sistema ou uma aplicação vital por um período de tempo inaceitável [54]. Considerando que o escopo do Modelo proposto neste trabalho não inclui eventos acidentais ou naturais, mas apenas ações humanas deliberadas, entende-se a Disrupção cibernética, na prática, como forma de Sabotagem.

Sabotagem, novamente adotando-se os termos da Política Nacional de Inteligência (2016):

> É a ação deliberada, com efeitos físicos, materiais ou psicológicos, que visa a destruir, danificar, comprometer ou inutilizar, total ou parcialmente, definitiva ou temporariamente, dados ou conhecimentos; ferramentas; materiais; matérias-primas; equipamentos; cadeias produtivas; instalações ou sistemas logísticos, sobretudo aqueles necessários ao funcionamento da infraestrutura crítica do País, com o objetivo de suspender ou paralisar o trabalho ou a capacidade de satisfação das necessidades gerais, essenciais e impreteríveis do Estado ou da população. (PNI, 2016) [111]

A partir dessa acepção de Disrupção como forma de Sabotagem, fica claro que há risco de danos significativos ao alvo. Nesse esteio, cumpre ressaltar que as ações ofensivas de Disrupção,

para que não extrapolem os limites do tipo de conflito cibernético abordado nesta Seção, não podem ser comparáveis a ações de Guerra ou Terrorismo.

Na Subseção 2.4.4, abordaremos com mais profundidade aspectos relativos a danos físicos decorrentes de ofensivas cibernéticas e parâmetros, ainda que envoltos na névoa das disputas geopolíticas e celeumas acadêmicas, que norteiam a classificação de um ataque cibernético como ato de Guerra.

2.4.4 Guerra Cibernética

O conceito de Guerra Cibernética carece ainda de pacificação no meio acadêmico. A questão que domina os debates sobre o tema é formada pela indefinição sobre o quão sistemática, violenta e destrutiva uma campanha ofensiva cibernética deve ser para ser classificada como *Cyberwarfare*. De toda sorte, para além das celeumas conceituais, é seguro assumir que o Espaço Cibernético tornou-se o "quinto campo de batalha", depois da terra, do mar, do ar e do espaço [116]. A Guerra, portanto, não pode mais ser pensada sem ao menos considerar a hipótese de que os contendores ocuparão também o "campo de batalha cibernético".

Na definição de Clarke (2016) [117], Guerra Cibernética pressupõe o engajamento de um governo no esforço de destruição de outro governo por meio do Espaço Cibernético. Ataques cibernéticos pontuais, por conseguinte, não se comparam a uma campanha duradoura, no sentido da Guerra como a entendemos no meio físico, e não podem ser consideradas ações de Guerra Cibernética.

Noutras linhas doutrinárias, a Guerra Cibernética parece ser entendida não como um formato de Guerra travado isoladamente, mas como um desdobramento das capacidades militares "tradicionais"dos contendores no "campo de batalha cibernético". As ações de Guerra Cibernética, portanto, não precisam, por si só, ser capazes de destruir o oponente, mas buscam criar facilidades e vantagens para que se alcance a vitória em conjunto com as ações de força cinéticas. Nesse contexto, a Guerra Cibernética seria travada apenas em compasso com a Guerra no mundo físico. [118].

Do ponto de vista militar, o Espaço Cibernético deve ser entendido como um "domínio", não uma missão. Nesse domínio, operações militares buscam criar efeitos específicos, com essencialmente os mesmos objetivos almejados nos demais campos de batalha. O objetivo militar cibernético fundamental é garantir a própria liberdade de ação no Espaço Cibernético, negando essa mesma liberdade ao adversário. A união dessas duas capacidades - preservar a liberdade para si e negá-la ao oponente - garantem a "superioridade cibernética militar" [119].

Em complemento à questão central abordada nos parágrafos anteriores, outros pilares teóricos ensejam discussões sobre o conceito de Guerra Cibernética, dentre os quais, destacamos [120]:

a. Guerra Cibernética como monopólio estatal ou passível de ser empregada como meio de ação por atores não-estatais;

b. os efeitos das ações cibernéticas ofensivas, para se enquadrarem como ações de Guerra Cibernética, precisam causar danos físicos a estruturas ou a pessoas, além dos inerentes efeitos cibernéticos.

O primeiro tópico em discussão, monopólio estatal sobre a Guerra Cibernética, deve ser abordado a partir da base doutrinária comum às várias formas de manifestação da Guerra em si, atividade humana cujas origens retomam, pelo menos, de 10 mil anos de história [121]. O monopólio estatal sobre a Guerra pode ser discutido somente no contexto das organizações políticas nacionais modernas, pois antes mesmo do advento dos Estados Nacionais como os conhecemos, a Guerra já era travada em variados formatos e graus de intensidade.

Datta (2021) [122], por exemplo, ao tratar da campanha ofensiva *"Solarwinds Orion Sunburst"*, estipulou que Guerra Cibernética pressupõe uma campanha direcionada, patrocinada por atores estatais e marcada pelo contínuo mapeamento e exploração de vulnerabilidades de outras nações.

Na mesma linha parece seguir Alford (2001) [123], que construiu seu conceito de Guerra Cibernética alicerçado na ideia de que a coação do oponente visa a fazer cumprir os "anseios nacionais"do atacante. O autor define Guerra Cibernética como *"any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system."*

Ainda que se adote a tese de que a Guerra foi, por algum período de tempo, um meio de ação governamental exclusivo, Izycki (2021) [124] assevera que os Estados Nacionais perderam esse monopólio e se veem cada vez mais imersos em conflitos contra atores não-estatais, cuja capacidade ofensiva os tornam ameaças reais à Segurança Nacional. Essa mesma perspectiva de quebra do monopólio estatal, por conseguinte, é passível de ser aplicada sobre a doutrina de Guerra Cibernética, enquanto subdivisão do fenômeno mais amplo da Guerra.

Com o aporte cada vez maior de tecnologia no ambiente dos conflitos geopolíticos, a infraestrutura de Informação dos Estados Nacionais passou a figurar também como alvo de ações cibernéticas avançadas, ao lado dos tradicionais segmentos de Infraestruturas Críticas, tanto em cenários de Guerra Cibernética conduzida por atores estatais e não estatais, quanto por ação de grupos criminosos e terroristas. [125]

No início do Século XXI observamos uma nova mudança na Guerra, que evoluiu da "Guerra em rede"(caracterizada pela sincronização da Informação sobre posicionamento, seleção de alvos e sistemas guiados para destruição do inimigo com altos índices de eficiência) para a "Guerra de Informação não-convencional", na qual atores, inclusive não estatais, possuem acesso a vastas fontes de Informação que, combinadas com elevada capacidade cibernética e técnicas de anonimização são capazes de negar aos adversários as vantagens até então alacançadas pelo emprego da Guerra em Rede. [126]

A análise do segundo tópico conceitual - necessidade das ações de Guerra Cibernética causarem danos físicos a pessoal ou material adversário - começa no marco teórico posto pela Carta das

Nações Unidadas de 1945, que, em seu Artigo 2(4), estipulou que os membros da ONU devem se abster do emprego de ameaça ou força contra a integridade territorial e independência política de quaisquer Estados [52].

A interpretação tradicional do enunciado da ONU grafado do Artigo 2(4) esclarece que a expressão "força"pressupõe emprego de arma, numa conotação estritamente militar, acompanhado de intenção ou efeito coercitivo. O emprego de "força"no universo cibernético estaria demostrado apenas se a ação perpetrada contra determinado sistema acarretasse dano físico a pessoal ou material. Interpretações mais extensivas desse mesmo enunciado, todavia, passaram a incluir no rol do Artigo 2(4) da ONU ações ofensivas cibernéticas que afetem sistemas de IC, causando disrupção em serviçoes essenciais, mesmo sem acarretar danos físicos. [127]. Esse entendimento se baseia na percepção que a disrupção de sistemas de IC acarreta prejuízos potencialmente graves contra sistemas essenciais e até efeitos letais contra cidadãos das regiões afetadas.

Num argumento antagônico à interpretação extensiva do Artigo 2(4), Rid (2012) [128] chega a desconsiderar a hipótese de ataques cibernéticos alcançarem níveis sufcientes de violência para serem classificados como uma faceta da Guerra. O autor classifica tais ações ofensivas, quando politicamente motivadas, como nada mais que formas sofisticadas de sabotagem, espionagem e subversão.

Lewis (2022) [129] considera que ataques cibernéticos são superdimensionados, pois não se provaram ainda capazes de trazer ganhos estratégicos consideráveis para nações em conflito. No mais das vezes, atesta o autor, o ganho de se executar ações de espionagem cibernética, levando ao conhecimento antecipado dos planos e capacidades do adversário, supera facilmente a vantagem potencialmente alcançada por ataques destrutivos.

Em igual direção, Desombre (2017) [30] afirma que é preciso diferenciar "ataques cibernéticos"de "espionagem cibernética". A maior parte dos acadêmicos concorda que a expressão "ataque cibernético"é, não raro, indiscriminadamente usada para descrever ações de espionagem cibernética - definada como o emprego de redes de computadores para acessar ilegalmente dados e informações confidenciais. Espionagem cibernética, nesse esteio, não constitui um ato de guerra, assim como a espionagem clássica, que é reconhecida como uma prática comum entre Estados, no mais das vezes, não eleva os níveis de tensão ao ponto de justificar retaliações armadas.

Essa distinção foi cristalizada nos conceitos de *computer network exploitation* (CNE) e *computer network attack* (CNA). CNE consiste na extração de dados confidenciais contra a vontade do proprietário, enquanto CNA se refere ao uso da informação para disrupção e destruição. A maioria das intrusões de alta complexidade tem a espionagem política ou econômica por objetivo, em detrimento de ações voltadas à disrupção ou sabotagem. [48].

A distinção entre CNE e CNA é digna de registro, todavia, no bojo desta pesquisa, optou-se por empregar a expressão "ataque cibernético"de maneira indiscriminada. Essa opção se fundamenta no intuito de preservar a praticidade do modelo de mapeamento de ameaças ora proposto também às esferas gerenciais e políticas de organizações e governos.

A discussão acerca da necessária ocorrência de danos físicos advindos de ataques ciberné-

ticos tem entre seus tópicos de maior expoência o amplamente debatido caso "Stuxnet", *worm* que afetou centrífugas de enriquecimento de urânio do Irã, trazido à tona em 2010. O destaque a esse evento ofensivo se explica pelo fato do Stuxnet ter ocasionado danos físicos a Sistema de Supervisão e Aquisição de Dados (SCADA) de Infraestrutura Crítica, o que lhe rendeu a posição de divisor de águas no campo da segurança cibernética. Pelo menos em relação à natureza dos danos causados, o evento Stuxnet pode ser inequivocamente classificado como uma ação de Guerra Cibernética. [127]

Outro evento significativo foi o a ataque realizado pelas Forças de Defesa de Israel contra uma instalação nuclear Síria, em 2007. As aeronaves israeleneses sobrevoaram o espaço aéreo sírio indetectáveis às defesas do inimigo, cujo radares foram tirados de ação por meio de ataque cibernético prévio. Nesse caso, não houve dano físico decorrente da ação cibernética, mas houve disrupção de uma capacidade militar vítal do inimigo, o que contribuiu sobremaneira para o sucesso da operação [130].

Mesmo que se reconheça o potencial de ataques cibernéticos causarem efeitos físicos similares aos alcançados com emprego de armas, demasiada ênfase nesse aspecto pode obscurecer outras questões operacionais e prejudicar a correta avaliação do conflito cibernético. Isso porque, há um aspecto informacional que envolve a manipulação de opiniões e do processo decisório igualmente importante na Guerra Cibernética. A bem da verdade, o principal efeito dos ataques cibernéticos no contexto de *Cyberwarfare*, pelo menos até hoje, é a manipulação de dados, conhecimento e opiniões para produzir efeitos psicológicos e políticos. Afinal, criar incertezas na cabeça de líderes militares e políticos a ponto de fazê-los hesitar e cometer erros é um objetivo militar valioso, capaz de gerar vantagens no campo de batalha. [131]

O aspecto informacional da Guerra Cibernética nos remete ao conceito de *Netwar* cunhado por Arquilla (1993) [3]. O autor, à época, trouxe à baila a estimativa que a "revolução informacional"mudaria a forma como conflitos entre as sociedades e suas respectivas forças armadas seriam travados. O autor considerou que *Netwar* e *Cyberwar* tinham escopos diferentes sobre o mesmo objeto, à medida em que ambos os fenômenos se desenvolvem em torno da informação e do conhecimento. Mais especificamente como nações adversárias produzem, controlam, empregam e protegem tais informações e conhecimento em meio aos conflitos. *Netwar*, contudo, se referiria ao conflito informacional de alto nível entre sociedades, manifestado por meio de campanhas de interferência no que uma população e a elite de uma nação concebem acerca de si mesmos e do mundo. Guerra Cibernética, por sua vez, seria o emprego da Informação como ativo associado a doutrina e a operações militares.

Voltando a Andrew (2015) [131], o autor atesta, categoricamente, que a Informação em si não é uma arma. Entretanto, afirma que uma definção muito estreita centrada apenas em efeitos cinéticos é igualmente inadequada para abarcar todo o alcance de ataques cibernéticos. Uma solução para esse impasse conceitual, ressalta o autor, é expadir o escopo do Artigo 2(4) da Carta da ONU para garantir o compromisso das nações de se eximirem de ameaçar a integriadade territorial ou "a independência política"de outros Estados, conceito alargado que incluiria ações cibernéticas.

A hipótese de conflitos cibernéticos entre Estados e grandes organizações se dar por meio de longas e persistentes campanhas de hackeamento, no lugar de ações abruptas de alta intensidade, figura, para alguns, como o meio mais plausível de materialização da Guerra Cibernética [120].

Loui (2017) [132], a propósito, defende que as ações de *Cyberwarfare* oscilam entre duas formas possiveis de materialização:

a. eventos ou campanhas massivas de alta intensidade capazes de provocar reações militares cinéticas, cenário que aproxima a Guerra Cibernética do universo da Guerra Regular, retomando as discussões sobre efeitos físicos decorrentes de ofensivas cibernéticas;

b. hackeamento constante de propriedade intelectual, suficiente para gerar, por anos a fio, prejuízos elevados e custos insustentáveis de contramedidas, criando um campo de batalha mais afeto a disputas comerciais e ideológicas que ao confronto militar aberto.

Esse segundo cenário, tradicionalmente associado a ações ofesivas Chinesas, é ilustrado pelas figuras da "*death by a thousand cuts*" e da "*hundred years' cyberwar*" [132]. Tais expressões denotam um formato de aplicação da Guerra Cibernética comparável à Guerra Irregular, marcada por assimetria de forças e evasão de um dos contendores ao conflito aberto. Nessa hipótese, a vitória se constrói em pequenos avanços acumulados em um longo conflito [133].

Ataques cibernéticos conduzidos pela China, por exemplo, são encarados como uma crescente ameaça à Segurança Nacional dos EUA. A China tem se provado capaz de infiltrar-se em sistemas de Infraestruturas Críticas de seus adversários e demonstrado habilidade para realizar ataques cada vez mais impactantes. Tais ações ofensivas são parte da estratégia de compelir seus adversários a agirem de acordo com o interesse do Estado chinês, também por meio de influência psicológica, de opinião pública e legislativa, minimizando o risco de escalada para um conflito militar aberto. [34]

Ao lado das longas campanhas de hackeamento de propriedade intelectual atribuídas ao Estado chinês, supostas operações cibernéticas russas de *Information Warfare* são um outro exemplo de campanhas cibernéticas ofensivas intencionalmente apartadas de objetivos cinéticos e conceitualmente mais próximas da visão de Rid (2012) [128] e de Andrew (2015) [131] supracitadas.

A comunidade de Inteligência dos EUA considera que a Rússia se mantém como uma das principais ameaças no Espaço Cibernético, constantemente refinando sua capacidade de executar ações de Espionagem, Interferência e ataques a Infraestruturas Críticas. As operações de influência e Interferência Externa executas pelos serviços de Inteligência russos são consideradas as mais preocupantes e vêm sendo desenvolvidas contra os EUA e outros países há décadas. A China, a propósito, tem buscado avançar suas próprias capacidades em *Information Warfare* por meio do estudo de operações russas já publicizadas. [33]

A doutrina russa de *Information Warfare* ou "Guerra de Informação"merece atenção especial no contexto deste trabalho. Apesar de longamente empregada contra o Ocidente, a Guerra de Informação russa é, em geral, mal compreendida fora dos círculos especializados de Defesa e

Inteligência. Operações dessa natureza causaram gradualmente profundos impactos, ainda que de difícil percepção, na ordem social e política das nações-alvo. [134]

Da perspectiva preponderante no Ocidente, Guerra Cibernética é um domínio especifico da Guerra, dotado de doutrina, operadores e acervo de efeitos letais e não letais próprios. Por outro lado, a Rússia percebe e aplica *Cyberwarfare* como um componente subordinado de sua abrangente doutrina de *Information Warfare*. [135]

Operações cibernéticas, na visão russa, têm como objetivo permitir que o Estado, de maneira mais ampla, domine o espectro da Informação, e não apenas busca atingir efeitos pontuais sobre sistemas de comunicação do adversário. Essa diferença de percepção é reforçada pela emprego russo da expressão *"Information Security"*, no lugar da denominação mais restrita *"Cybersecurity"* adotada pelos EUA, por exemplo. [135]

No lugar de entender a "Informação"simplesmente como o dado armazenado e transmitido pela rede, numa perspectiva centrada na teoria dos sistemas distribuídos, os russos trabalham a "Informação"como plataforma para moldar as percepções individuais e coletivas [135].Tais técnicas de desinformação vêm sendo aprimoradas e aplicadas pelos russos há decadas, atingindo resultados expressivos [136].

A manipulação da Informação busca influenciar o processo decisório governamental do adversário, constituindo-se em uma abordagem associada à *"Psychological warfare"*, que pode ser assim entendida nos termos apresentados por Linebarger (1948):

> *"Propaganda consiste no uso planejado de qualquer forma de comunicação em massa para afetar a consciência e emoção de um grupo determinado e com propósitos específicos de natureza militar, econômica ou política. Guerra Psicológica abarca o uso da propaganda contra um inimigo, associada a outras medidas de natureza militar, política ou econômica."* (Linebarger, 1948, tradução nossa) [137].

Em outras palavras, Guerra de Informação baseia-se em operações que exploram meios de comunicação com o intuito de atingir determinado objetivo sobre um adversário. Essas operações abarcam um amplo espectro de ações, incluindo intrusão em sistemas computacionais e Sabotagem; Espionagem e Operações de Inteligência; interceptação de telecomunicações; fraude; manipulação de percepções; e Guerra Eletrônica. [138]

Utilizando elementos da Guerra de Informação, agora potencializada pelos sistemas globais de mídia e informação em rede, a doutrina e as operações de desinformação russas são realizadas em atuação conjunta dos serviços de Inteligência e Propaganda, auxiliados por autoridades governamentais, [139]. Como resultado prático, a Guerra de Informação (e a desinformação) vem sendo conduzida por meio da Guerra Cibernética, tornando essas operações mais rápidas, profundas e impactantes [132].

2.4.4.1 Considerações sobre Guerra Híbrida

Além de se materializarem isoladamente como eventos relevantes no campo da Segurança Cibernética, quando combinados e somados a outros meios de ação tradicionais e inovadores no bojo dos conflitos contemporâneos, Cibercrime; Ciberterrorismo; Espionagem, Interferência Externa e Disrupção; e Guerra Cibernética, podem compor a base do formato de Guerra denominado *"Hybrid Warfare"*.

A definição de Guerra Híbrida é geralmente associada ao teórico militar Frank Hoffman, que, a partir da observação do ambiente operacional do Século XX, argumentou que a mistura de várias maneiras de travar a Guerra; os diferentes tipos de agentes e organizações em combate; e as tecnologias desdobradadas nos campos de batalha produzem um cenário altamente complexo que pode ser chamado de *Hybrid Warfare*. A Guerra Híbrida, vale ressaltar, pode ser conduzida tanto por atores estatais como não-estatais, incluindo o emprego de ações militares convencionais, Guerra Irregular, Terrorismo e criminalidade. [70]

Ainda que os meios de ação militares desdobrados fora do Espaço Cibernético escapem ao recorte desta pesquisa, o conceito de Guerra Híbrida é vital para a adequada aplicação do Modelo de Mapeamento de Ameaças proposto, notadamente quando nos debruçarmos sobre campanhas patrocinadas por Estados. Isso porque o contexto geopolítico e a natureza das relações entre os patrocinadores das ações ofensivas e seus alvos, além de questões conjunturais, são basilares para a correta análise dos diferentes componentes da Ameaça. Esses componentes serão apresentados detalhadamente no Capítulo 3.

Para efeito desta pesquisa, portanto, as áreas de conflito cibernético, com todas as nuances aqui já abordadas, são entendidas como os **campos de batalha onde nascem e se desdobram as Ameaças a serem mapeadas pelo modelo proposto. Esses fenômenos, não podemos olvidar, possuem relevância tanto em suas formas isoladas e relativamente mais simples, quanto como parte de campanhas extremamente profundas de Guerra Híbrida.**

2.5 Síntese do Capítulo

Neste capítulo foram abordados a disciplinas e conceitos que nortearam o desenvolvimento do Modelo para Mapeamento de Ameaças Cibernéticas proposto. Tratou-se, pois, dos elementos estruturais que fundamentam a metodologia para Mapeamento de Ameaças em si, extraídos e adaptados dos conceitos pertinetes a APTs, Atribuição Cibernética, Avaliação de Riscos e CTI.

Ademais, este capítulo contém as principais discussões acerca do objeto de trabalho do Modelo proposto. Em outras palavras, discorreu-se sobre os campos de conflito onde se materializam as Ameaças cibernéticas consideras pertinetes ao Modelo, quais sejam: Cibercrime; Ciberterrorismo; Espionagem, Interferência Externa e Disrupção; e Guerra Cibernética.

Capítulo 3

Discussão do Problema e Proposta

Grandes organizações e governos, cujas operações tornam-se cada vez mais dependentes dos sistemas informatizados, enfrentam o desafio de prover eficiência por meio de tecnologia e integração de redes computacionais, ao mesmo tempo que lutam contra a hiperexposição digital e os riscos de segurança dela decorrente. Em harmonia com os conceitos explicitados nos capítulos anteriores desta dissertação, nos perfilamos aos técnicos e acadêmicos que percebem a complexidade das ameaças que habitam o Espaço Cibernético, onde atores estatais e não-estatais desdobram suas ambições e replicam os conflitos nascidos no mundo físico.

Esses conflitos são transportados ao mundo cibernético por uma escolha tática e estratégica dos diversos atores envolvidos. Uma decisão fundamentada na premissa de que os recursos tecnológicos disponíveis ao ator ofensivo, as dificuldades técnicas que limitam os defensores e a ausência de regulamentação internacional e de consenso político sobre quais medidas de reação são aceitáveis, tornam as operações maliciosas no Espaço Cibernético menos arriscadas.

Um passo fundamental para o correto entendimento desse cenário de elevada complexidade é conhecer as ameaça às quais os sistemas que se deseja defender estão sujeitos. Foi diante dessa demanda premente que se desenvolveu o Modelo para Mapeamento de Ameaças Cibernéticas objeto desta dissertação, cujas principais características o incluem nos campos do conhecimento da Gestão de Risco, Inteligência e Segurança Cibernética.

Partindo das discussões travadas na Seção 2.3, entende-se a Ameaça não como um ator dotado de vontade própria, mas como o conjunto dos elementos que define um cenário ou conjuntura de maior ou menor segurança. Esses elementos, em sua dinâmica, aumentam ou diminuem a probabilidade de ocorrência de um ataque. Em outros termos, a Ameaça não se confunde com o Adversário ou o Agente de Ameaças, mas é definida como o conjunto dos vários elementos que moldam o cenário e estabelecem a probabilidade desses Adversários ou Agentes agirem contra o sistema sob proteção.

O modelo de mapeamento objeto desta dissertação, portanto, tem seu ponto de partida na delimitação dos elementos que constituem a Ameaça, apresentados nas linhas a seguir:

a. Características da organização alvo: tanto características da própria organização quanto dos

sistemas informatizados. Por exemplo, nível de informatização de sistemas e integração de redes, capacidade ofensiva e defensiva cibernética, capacidade militar, rede de apoio político internacional, conjunturas política, econômica e social internas, predisposição ao conflito.

b. Características do Adversário e do Agente: capacidade ofensiva e defensiva cibernética, capacidade militar, rede de apoio político internacional, conjuntura política interna, predisposição ao conflito, conjuntura econômica interna, entre outros.

c. Dinâmica das relações entre organização alvo e Adversário: histórico e *status* das relações diplomáticas, existência de conflitos econômicos, políticos, ideológicos, militares, entre outros.

d. Eventos externos capazes de influenciar o comportamento dos atores envolvidos: conjuntura política e econômica internacional, crises ou conflitos internacionais, entre outros.

Em seguida, os elementos que constituem a ameaça foram desdobrados em sete categorias de dados essenciais à caracterização da Ameaça, que se constituem na estrutura central do modelo ora proposto e serão devidamente detalhados na Seção 3.2. Por fim, o modelo preconiza a apresentação de impactos e um campo dedicado à avaliação e análise, a serem esmiuçados na Seção 3.3.

Em consonância com os marcos de desenvolvimento da pesquisa trazidos nos parágrafos anteriores, a execução deste Modelo para Mapeamento de Ameaças está dividido em duas fases, precedidas por um roteiro para planejamento e delimitação de escopo sob o qual o Modelo será aplicado. A primeira fase de execução estabelece os parâmetros para reunião dos dados que caracterizam a Ameaça, enquanto a segunda fase consiste na conclusão do processo com apresentação de impactos prováveis e avaliação analítica. A Figura 3.1 apresenta a ideia geral do modelo com as duas fases de execução.

3.1 Planejamento e Delimitação de Escopo

O roteiro de planejamento foi construído a partir do já citado método 5W3H [2]. O 5W3H é um método genérico, aplicável a diferentes áreas, cujo propósito é delimitar e detalhar, na medida do interesse do usuário, quais são os componentes fundamentais de um tópico a ser analisado. Do ponto de vista da metodologia de produção de conhecimento de Inteligência, o 5W3H norteia o esforço de reunião e análise da dados ao estabelecer previamente quais lacunas devem ser preenchidas para a adequada compreensão do objeto de trabalho. Vide Tabela 3.1.

Em nossa pesquisa, o 5W3H foi empregado para identificação prévia de quais dados e conhecimentos devem ser reunidos para que se alcance o mapeamnento da Ameaça em questão. Cada uma das sete categorias de dados essenciais à caracterização da Ameaça, a serem apresentadas

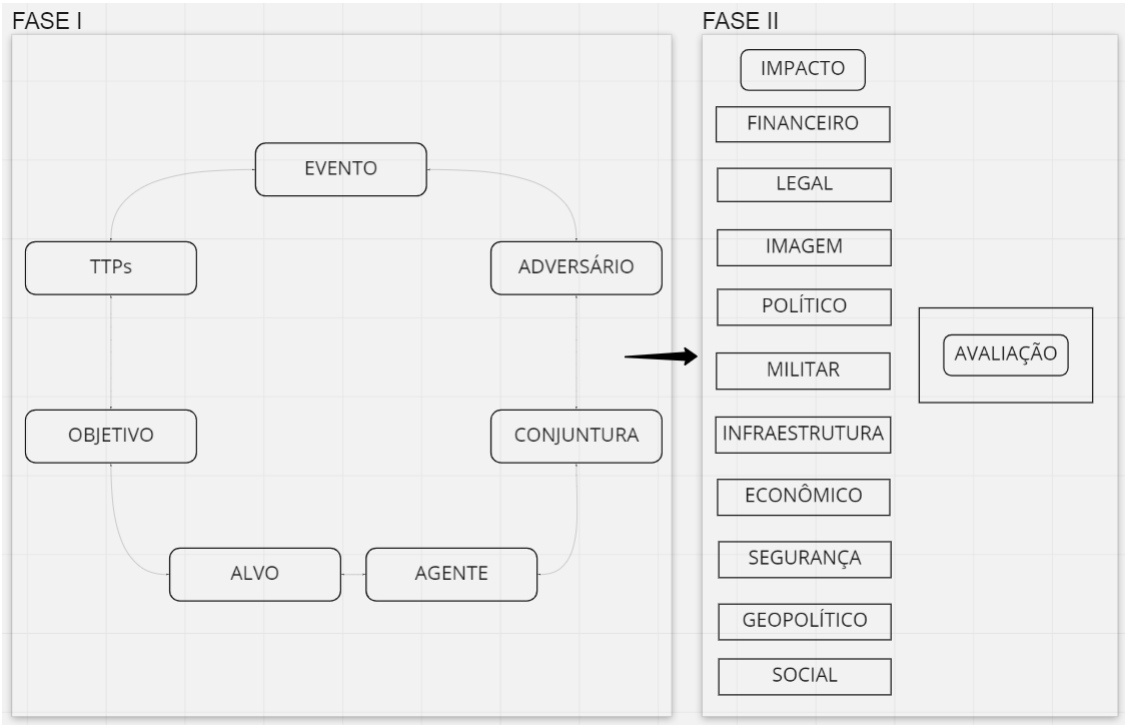

Figura 3.1: Representação gráfica das fases de execução do Modelo.

Tabela 3.1: Método 5W3H [2]

Elemento	Descrição
What	Directly describes the topic being addressed
Where	Specifies geographic references about the topic
When	Specifies relevant time frames to the topic like date and time
Who	Associates the topic with an entity capable of executing it
Why	Describes possible motivations for the occurrence of the topic
How	Describes the main characteristics and mechanisms of the topic
How much	Refers to the costs and impacts generated by the topic
How long	Description of the topic's effectiveness in terms of time

na Seção 3.2, pode ser associada a um ou mais elementos que compõem o 5W3H. Em outros termos, as categorias de dados deste Modelo de Mapeamento de Ameaças respondem as perguntas estabelecidas por cada um dos elementos do 5W3H. Vide tabela 3.2

A título de exemplo, o elemento "What"pode se referir igualmente, diante da opção do analista ou por características do objeto de análise, tanto à categoria "Alvo"quanto à "Evento", ou mesmo a ambas. Da mesma forma, o elemento "Who"pode ser associado às categorias "Agente"e "Adversário".

O registro desse processo de planejamento em um modelo estruturado é especialmente relevante para grandes organizações, cujas operações podem se dar em diferentes segmentos, recortes geográficos e recorte temporal. Cabe ao analista, portanto, definir a abrangência do trabalho de mapeamento de ameaças a ser executado, aproveitando a flexibilidade inerente do modelo 5W3H para a construção de projetos em diferentes graus de detalhamento.

Tabela 3.2: Associação ao Método 5W3H

Elemento	Categoria
What	Evento; Alvo.
Where	Evento, Alvo, Conjuntura.
When	Evento.
Who	Agente; Adversário.
Why	Objetivo; Conjuntura.
How	TTPs.
How much	Impactos.
How long	Evento; Conjuntura.

3.2 Fase I - Caracterização da Ameaça

Nesta fase, os dados essenciais à caracterização da Ameaça são reunidos e organizados em sete categorias desdobradas a partir dos já citados elementos que constituem a ameaça, vide Capítulo 3.

As sete categorias elencadas são:

a. Evento;

b. Adversário;

c. Conjuntura;

d. Agente;

e. Objetivo;

f. TTPs;

g. Alvo.

Na Fase I, cabe ao analista reunir dados para alimentar cada uma das sete categorias elencadas, executando um processo de detalhamento da Ameaça como subsídio para análise e conclusão do mapeamento em si. Os dados podem se originar das mais diversas fontes, recaindo sobre o analista a responsabilidade de seleção e julgamento dos dados de acordo com a técnica de escolha.

Em face da complexidade das Ameaças às quais o Modelo se direciona, tanto a disponibilidade quanto a confiabilidade dos dados pertinentes sobre o tema são variáveis, motivo pelo qual não há ordenação rígida de fluxo nos processos de reunião e análise.

Em outros termos, o processo de mapeamento pode ser iniciado por quaisquer das sete categorias preconizadas na Fase I, seja por opção do analista, pela natureza da demanda ou pela disponibilidade de dados. Após o início do processo, os esforços de reunião e análise passam a ser orientados pelo surgimento de novos dados ou por desdobramentos analíticos.

Dessa flexibilidade decorrem a característica "circular"da Fase I do Modelo e a possibilidade de seu emprego como método de análise *ex-post-facto* ou como ferramenta preventiva.

O emprego preventivo consiste na utilização do Modelo para mapeamento de uma Ameaça identificada antes da ocorrência de ação cibernética ofensiva direta contra o sistema sob proteção. Pressupõe a reunião de um conjunto de dados mais amplo e menos específico ao sistema sob proteção, a exemplo do histórico de atuação de Adversário ou Agente; mudança significativa de Conjuntura; ou Evento perpetrado contra terceiros países e organizações.

Hipoteticamente, o uso preventivo do Modelo pode servir ao mapeamento de uma Ameaça totalmente nova, no sentido não ter ainda se materializado em ataque contra alvo nenhum. Esse cenário, todavia, parece mais remoto, tendo em vista que já há um grande número de Adversários e Ameaças ativas contra Estados Nacionais e grandes organizações.

Já o emprego como método de análise *ex-post-facto*, pressupõe que o início do mapeamento se dê após a ocorrência de Evento direto contra o sistema sob proteção. Em caso de aplicação pós-ataque, o Modelo assumirá maior grau de especificidade, já que os dados reunidos serão desdobrados a partir da categoria Evento bem delimitada. Nesse cenário, as categorias Alvo e TTPs, em especial, tendem a se mostrar mais claras e melhor delineadas.

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

3.2.1 Evento

Reúne os dados de descrição e identificação de evento ou campanha cibernética atrelada à Ameaça sob análise. Em forma de rol exemplificativo, deve conter:

a. Denominação: Identificar o evento por meio de denominações empregadas pelas principais fontes consultadas;

b. Natureza do evento: apontar se foi um evento isolado ou uma campanha cibernética duradoura ou contra alvos diversos;

c. Alcance geográfico do evento: local, nacional, regional ou global.

d. Recorte temporal do evento: determinar a data de ocorrência do evento, tempo de duração da campanha ou data de conhecimento do fato; e

e. Resumo: Registrar características gerais do evento sob análise;

Considerando as várias bases de dados disponíveis sobre eventos cibernéticos ofensivos, notadamente as fontes de *Cyber Threat Intelligence*, haverá variações e mesmo contradições de dados e análises sobre os eventos. É muito comum, por exemplo, haver diferentes denominações dadas a grupos e campanhas APTs por empresas de segurança e agências governamentais. A consolidação desses dados e a adequada referência às fontes deve ser buscada pelo analista.

3.2.2 Adversário

O Adversário é descrito como patrocinador e principal beneficiário dos ganhos advindos de um Evento cibernético. No contexto do Modelo proposto, Adversários são, majoritariamente, Estados Nacionais patrocinadores de ações cibernéticas ofensivas, embora atores não-estatais também possam figurar como Adversários nos termos já apresentados no início do Capítulo 3.

No caso de Adversários estatais, retoma-se a escala de graus de envolvimento estatal em ataques cibernéticos construída por Egloff (2012) [1] apresentada na Tabela 2.1. Para efeito do Modelo ora proposto, a questão crucial para classificação de um Estado Nacional como patrocinador de ações ofensivas, e consequentemente como Adversário , recai não apenas sobre a natureza de sua relação com o Agente executor, mas igualmente na existência de benefícios auferidos pelo Estado em decorrência da operação ofensiva.

Imaginemos que um governo, ciente da atuação de grupo ofensivo baseado em seu território, decide ignorá-lo, colocando-se na hipótese de *State-ignored* discrita por Egloff. Nesse caso, apesar da relação entre o governo e o Agente ser passiva e não haver participação estatal direta na operação, o que vai classificar ou não o Estado em tela como Adversário é o motivo deste ter ignorado as ações do Agente de Ameaças. Caso essa motivação seja o auferimento de qualquer tipo de benefício ou vantagem, estaremos diante de uma relação de patrocínio, ainda que por meio da passividade e, portanto, diante de um Adversário estatal.

Por outro lado, se o governo não atuar contra o Agente por incapacidade técnica ou outro impedimento real e, ao mesmo tempo, não esteja se beneficiando da operação ofensiva em nenhum sentido, não há que se falar em relação de patrocínio e em Adversário estatal.

Em face da obscuridade que envolve a Atribuição Cibernética, vide a Seção 2.2, deve-se avaliar detidamente as fontes consultadas antes de se conferir qualquer grau de confiabilidade a dados que atrelem Adversários e Agentes a Eventos. Não se pode olvidar que, não raramente, há um intrincada miríade de interesses por trás da divulgação de resultados de Atribuição Cibernética, especialmente quando se trata das Ameaças permeadas por interesses estatais. Nesse esteio, é seguro considerar que a definição do Adversário se apresenta como um dos elementos mais complexos do Mapeamento de Ameaças ora proposto.

Quanto aos atores não-estatais, nos limites já estabelecidos nas primeiras linhas do Capítulo 3, podem figurar como Adversários os grandes grupos empresariais ou politícos, organizações terroristas ou grupos paramilitares e organizações criminosas.

Por outro lado, algumas Ameaças formadas por entes não-estatais não poderão ser associadas a nenhum Adversário, nos termos relevantes para este Modelo. Esses são os casos de organizaçãos criminosas em Eventos com Objetivo puramente financeiro, mas suficientemente gravosos para afetar a estabilidade e segurança de governos e grandes organizações. Grupos APT dedicados a perpetrar ataques de ransomware contra sistemas de Infraestruturas Críticas, por motivação puramente financeira, são o exemplo perfeito dessa hipótese.

Em tempo, é preciso considerar que dados confiáveis sobre a dinâmica interna de Adversários

varia largamente em função da natureza dessas organizações, que vão desde Estados autoritários empenhados no controle da informação e propaganda, passando por organizações criminosas e terroristas, até repúblicas ocidentais pautadas na transparência e abertura internacional.

Nesta categoria, portanto, devem ser reunidos e considerados para análise dados relativos às características estruturais e, igualmente, a condições mutáveis do cenário interno do Adversário, a exemplo de:

a. Cenário político, econômico e social;

b. Capacidade cibernética;

c. Capacidade militar;

d. Histórico de atuação cibernética ofensiva;

e. Predisposição ao conflito;

3.2.3 Conjuntura

A Conjuntura é formada pela soma das características da organização alvo, da dinâmica das relações entre a organização alvo e o Adversário e das condicionantes externas capazes de influenciar o comportamento dos atores envolvidos. Essa categoria constitutiva da Ameaça, portanto, é formada por uma concatenação de fatores internos e externos à organização alvo que pode agravar ou amenizar a Ameaça.

Trata-se aqui do encadeamento de características estruturais e, igualmente, de condições mutáveis do cenário interno da organização alvo; da dinâmica da relação entre as partes; e de condicionantes externas capazes de alterar o comportamento das partes. Esses fatores, somados, moldam um quadro, em determinado recorte temporal mais ou menos duradouro, que influencia sobremaneira o cenário de Ameaça. Certamente, é uma categoria de análise repleta de variáveis extremamente complexas.

As características e condições mutáveis do cenário interno do Adversário, vale ressalatar, devem ser reunidos e analisados na própria categoria "Adversário", a ser integrada aos dados da Conjuntura e demais categorias durante a execução do Modelo.

Tratando-se de Adversários estatais, a Conjuntura será primordialmente formada pelas interações geopolíticas bilaterais. Há que se considerar, entretanto, Ameaças de constituição mais genérica, formadas por Adversários estatais cuja atuação extrapola o contexto das disputas geopolíticas diretas com o país alvo. Tome-se como exemplo desse tipo de Ameaça aquelas formadas por 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, tanto de natureza estatal quanto não-estatal, também são influenciados por condicionantes externas. Arranjos internacionais para combate a crimes cibernéticos; irrupção de dis-

putas internacionais e conflitos militares; realinhamentos geopolíticos de terceiros países; graves alterações econômicas e mudanças de legislações nacionais, por exemplo, podem gerar alterações de Conjuntura capazes de afetar o comportamento dos atores envolvidos.

Ademais, tanto atores estatais quanto não-estatais estão sujeitos a mudanças abruptas de Conjuntura capazes de alterar significativamente o cenário, impulsionando o surgimento de novas Ameaças. Eventos dessa natureza, não raramente imprevisíveis, ainda que intencionais ou não, são denominados "Crises" no Modelo proposto.

Por conseguinte, o desenho da Conjuntura, sem prejuízo de outras condicionantes reputadas pertinentes, deve considerar:

a. Movimentações políticas, econômicas e sociais iternas à organização alvo;

b. Capacidade defensiva da organização alvo;

c. Status das relações diplomáticas entre organizção alvo e Adversário;

d. Disputas econômicas, políticas, ideológicas e territoriais;

e. Conflitos militares; e

f. Crises.

3.2.4 Agente

O Agente é representado pelo grupo ou indivíduo executor direto das ações ofensivas. Diante da natureza das Ameaças objeto deste trabalho, os Agentes correspondem, eminentemente, aos diversos grupos APT dedicados a ataques e intrusões sofisticados.

O Agente pode atuar isoladamente, em casos em que a Ameaça sob análise não englobe um Advesário, ou em vários níveis de proximidade e integração com uma organização ou governo patrocinador. Esses níves de integração variam em função do grau de controle exercido pelo patrocinador na operação e, consequentemente, influenciam o nível do risco de exposição do vínculo entre Adversário e Agente.

Para efeito do Modelo apresentado nesta dissertação, grupos hacker foram classificados como agentes dotados de natureza específica, excluindo os demais tipos, a exemplo de grupo ou organização criminosa ou mesmo operadores de agências governamentais e empresas legalmente constituídas. Grupos hacker se difereciam dos demais Agentes por deterem maior autonomia e, portanto, menor vinculação a patrocinadores. Tal diferenciação, vale ressaltar, se apoia em três fatores fundamentais [140] [141] [142]:

a. Existem tipos diferentes de hackers que atuam por motivações variadas, não necessariamente com objetivos financeiros ou disruptivos;

b. A atuação desses grupos os diferencia, tanto em termos acadêmicos quanto legais, de organizações envolvidas em práticas criminosas tradicionais fora do Espaço Cibernético;

c. Grupos hacker engajados em ações de alcance internacional estão sujeitos a diferentes ordenamentos jurídicos, o que pode lhes render diferentes classificações quanto à natureza de suas atividades.

Por fim, cumpre destacar que plataformas de CTI e *white papers* reúnem dados sobre Agentes em variados métodos de classificação e graus de detalhamento. Isso exige atenção do analista à ocorrência de redundâncias, contradições e diferenças terminológicas entre as diversas bases disponíveis.

Nesse esteio, dentre outros elementos considerados úteis à descrição e classificação dos Agentes, foram elencados:

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 organização criminosa, paramilitar ou terrorista; empresa legalmente constituída; e indivíduo ou grupo hacker independente;

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;

3.2.5 Alvo

Aponta o sistema atacado em Evento específico ou sistemas provavelmente visados no contexto de uma Ameaça determinada.

Entre os sistemas com maior probabilidade de sofrerem ações ofensivas de alta complexidade, merecem destaque os diversos segmentos classificados como Infraestruturas Críticas. Apesar do conceito de ICs e, por conseguinte, a lista de setores assim classificados, variar de acordo com as legislações de cada país, pode-se considerar que se trata dos setores cujos ativos, sistemas ou redes, físicas ou virtuais, se danificados, podem gerar rapidamente efeitos debilitantes à Segurança do Estado e da Sociedade. De maneira mais condensada, tem-se como exemplo de

ICs os setores: Energético; de Transporte; Abastecimento Hídrico; Alimentar; Comunicações e Informação; sistemas de Saúde; industrial de Defesa; Administrativo, Governamental e Financeiro. [132] [143] [144] [145].

O destaque dado às Infraestruturas Críticas decorre do fato desses sistemas terem se mostrado alvos atraentes para diferentes atores ofensivos nos últimos anos. Tanto Ameaças compostas por Adversários estatais quanto não-estatais têm abarcado ICs como alvos prioritários. Campanhas ofensivas com objetivos de ganho político, ganho finaceiro ou disrupção praticadas por APTs e seus patrocinadores, com destaque para Estados Nacionais e organizações criminosas, têm elevado o risco para o segmento dos serviços essenciais [146] [147].

Outros alvos não necessariamente abarcados pelo conceito de IC foram elencados como prováveis: Setor produtivo amplo - extrapola a base industrial de Defesa já inserida na lista de ICs; Centros de pesquisa científica; Entidades Políticas - tanto partidos políticos como entidades de natureza política não necessariamente associadas a partidos políticos, como *think tanks* e organizações da sociedade civil; e Empresas de Comunicação e Mídia.

Sistemas governamentais aparecem no rol de Alvos como uma categoria abrangente, formada por todos os sistemas ordinariamente encontrados nas estruturas governamentais modernas, desde sistemas administrativos até estruras de Estado, como o serviço diplomático. O aparato militar, registre-se, foi alocado em categoria própria.

Por fim, esta categoria também abarca bancos de dados com informações pessoais, independentemente de serem bases mantidas por entes governamentais ou privados. Tal inclusão está fundada no histórico de intrusões cibernéticas patrocinadas por Adversários estatais contra bases de dados pessoais, mantidas tanto por organizações públicas quanto privadas. Esses Eventos, provavelmente, têm a Espionagem como Objetivo [148] [149].

Elenca-se, finalmente, como alvos mais prováveis:

a. Setor Energético;

b. Setor de Transportes;

c. Setor de Abastecimento Hídrico;

d. Setor de Abastecimento Alimentar;

e. Setor de Comunicações e Informação;

f. Sistema de Saúde;

g. Sistemas Governamentais;

h. Sistemas de Defesa;

i. Base industrial de Defesa;

j. Sistema Financeiro;

k. Setor Produtivo amplo;

l. Centros de Pesquisa Científica;

m. Entidades Políticas;

n. Empresas de Comunicação e Mídia;

o. Bases de Dados pessoais.

3.2.6 Objetivo

Esta categoria abarca os objetivos não-cibernéticos e imediatos almejados pelo Adversário ou Agente. São “não-cibernéticos” por não se confundirem com os objetivos cibernéticos, de natureza técnica, buscados pelo Agente na execução do ataque propriamente dito. Por exemplo, o estabelecimento de um canal de comunicação com o sistema alvo é um objetivo de natureza cibernética, um meio para consecução do Objetivo não-cibernético.

São, além do mais, “imediatos” por sua utilidade tática, diferentemente do objetivo final, "mediato", que é genericamente entendido como o ganho da vantagem estratégica almejada por um Adversário. Por exemplo, a vantagem estratégica representada pela supremacia tecnológica militar é um objetivo mediato que pode ser alcançado ou mantido por meio de ações cibernéticas com Objetivo de Espionagem.

Nos casos em que a Ameaça não seja integrada por um Adversário ou se trate de Evento com o Objetivo único de Ganho Financeiro, não haveria um objetivo mediato a ser alcançado.

No Modelo proposto, foram elencados cinco Objetivos:

a. Espionagem;

b. Interferência Externa;

c. Ganho financeiro;

d. Disrupção; e

e. Terrorismo.

3.2.7 Táticas, Técnicas e Procedimentos (TTPs)

Esta categoria estabelece TTPs utilizados por Agente que compõe uma Ameaça sob análise. Nesta pesquisa, a categoria TTPs não se ocupa da observação detalhada de artefatos, códigos ou processos identificados nas ações ofensivas, mas da determinação dos meios escolhidos pelo atacante para alcançar o Objetivo proposto.

Os três componentes do acrônimo TTP, para efeito do Modelo de Mapeamento ora apresentado, podem ser assim definidos:

a. Tática - é um objetivo cibernético a ser alcançado como um meio para alcance de outro objetivo mais complexo. Pressupõe uma ordenação de emprego de recursos para alcance de objetivos cibernéticos específicos que, somados, levarão ao alcance de ulterior objetivo principal [150] [151].

b. Técnica - uma forma para execução de tarefa específica. Diversas técnicas podem ser utilizadas para cumprimento de uma mesma tarefa [151] [150].

c. Procedimento - fluxo detalhado, pré-definido, de passos para execução de uma tarefa. Pressupõe um encadeamento rígido de ações, não passível de alteração por liberalidade do executor [150].

Concatenando os três conceitos acima, concluímos que a Tática define objetivos intermediários a serem alcançados com emprego das Técnicas adequadas. A escolha da Tática depende do objetivo final. Tática difere de Procedimento por este definir um fluxo imutável de ações a serem executadas, enquanto aquela pode ser alcançada por diferentes Técnicas à discricionariedade do operador.

As TTPs do Modelo proposto, por conseguinte, são tarefas e objetivos intermerdiários, passíveis de ser executados de diversas maneiras, inclusive com auxílio de Técnicas não-cibernéticas.

Empregou-se nesta pesquisa, portanto, o termo "TTPs" em uma conotação ampla, que agrega conceitos alocados em segmentos tradicionalmente mais apartados em plataformas de CTI e *frameworks* de Atribuição Cibernética e Gestão de Risco [151]. A opção por reunir tais elementos em uma mesma categoria visa a manter o grau desejado de tecnicidade do Modelo, que se pretende útil, fundamentalmente, à instancia decisória de corporações privadas e governos.

Elencam-se, pois, 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.

3.3 Fase II - Saída do Modelo

A segunda fase de execução do Modelo traz um rol de impactos decorrentes ou potencialmente decorrentes de ações cibernéticas ofensivas materializadas ou hipotéticas. Ademais, esta fase faculta ao analista a inclusão de dados ou conclusões pertinetes ao mapeamento realizado.

A Fase II, portanto, oferece à instância gerencial informações necessárias à compreensão das Ameaças, tendo os danos e impactos decorrentes em perspectiva. Somado a isso, há a apresentação de anotações ou desdobramentos analíticos úteis ao processo decisório organizacional.

Para tanto, a Fase II foi subdividida em: Impactos e Avaliação.

3.3.1 Impactos

Impactos se referem aos danos que ultrapassam os efeitos cibernéticos sofridos pelos sistemas comprometidos e afetam quaisquer componentes organizacionais. São, por conseguinte, efeitos a serem mitigados por atuação das estruturas gerenciais e decisórias.

Os Impactos serão mensurados de acordo com a natureza da Ameaça sob análise. Dependendo da amplitude e delimitação da Ameaça, os Impactos terão abrangência e concretude variáveis em função dessa mesma amplitude. Por exemplo, no caso de Ameaça composta por Evento e Alvo bem definidos, os tipos de Impactos apresentados serão delimitados ao caso concreto. Por outro lado, em caso de Ameaças amplas, sem delimitação clara de um Evento ofensivo e Alvo pré-definidos, os Impactos apresentados serão meramente potenciais.

Ademais, mesmo a conotação do termo definidor de cada tipo de Impacto varia de acordo com a Ameaça. O Impacto de Segurança, a título de exemplo, pode se referir à Segurança na conotação de estabilidade provida por um governo à sua população, nos casos de mapeamentos de Ameaças versando sobre operações de Guerra Cibernética. Igualmente, Impacto de Segurança pode se referir à fragilização dos meios de seguranaça cibernética de uma organização empresarial, que teve credenciais de acesso roubadas em um Evento de crime cibernético.

O Modelo elenca onze tipos de impactos [60] [152] [131] [153] [154] [86]:

a. Financeiro - Perda financeira direta; Lucros cessantes; Custos judiciais; Custos por responsabilização judicial; Custos de recuperação e readaptação de sistemas e operações afetadas.

b. Legal - Alterações de legislação; Responsabilização por danos a terceiros; Responsabilização por quebra contratual;

c. Imagem - Dano à imagem no âmbito interno; Dano à imagem no âmbito internacional.

d. Político - Comprometimento do sistema representativo; Comprometimento do processo decisório; Instabilidade política interna.

e. Militar - Não atingimento de objetivo militar; Perda de vantagem militar; Perda de capacidade militar.

f. Infraestrutura - Dano físico; Dano a cadeia logística; Comprometimento de serviço crítico.

g. Econômico – Inviabilização de acordo econômico; Perda de vantagem competitiva; Enfraquecimento de setor econômico.

h. Segurança - Não atingimento de objetivo de segurança; Perda de capacidade de prover segurança.

i. Geopolítico - Crise diplomática; Perda de alinhamento diplomático; Enfraquecimento de posição política internacional.

j. Social - Instabilidade social; Perda de vidas humanas.

3.3.2 Avaliação

No segmento Avaliação, por fim, devem ser registradas conclusões ou anotações específicas para o caso sob análise. Podem se referir a desdobramentos prováveis ou concretos do caso; recomendações de ordem técnica; e discussões diversas.

Em outros termos, a avaliação traz a oportunidade ao analista de esclarecer componentes do trabalho de mapeamento julgados obscuros em face de características do destinatário da análise. Nos casos de Ameaças mais amplas, por exemplo, formadas por Adversários Estatais que operam fora da Conjuntura de conflitos geopolíticos na qual esta inserida a organização a ser protegida, a Avaliação se mostra especialemente útil para o esclarecimento da relevância da Ameaça em tela. Em um segundo exemplo, a avaliação traz a oportunidade de se aportar maior tecnicidade ao trabalho ou, ao contrário, a depender do interlocutor, esclarecer passagens técnicas exageradamente densas.

3.4 Síntese do Capítulo

Neste Capítulo se deu a apresentação do Modelo para Mapeamento de Ameaças propriamente dito. A Ameaça, para efeito desta pesquisa, foi apresentada como um conjunto de elementos cujas dinâmicas próprias moldam um cenário de maior ou menor risco e, portanto, não se confunde com o Agente de Ameaça ou Adversário. No mesmo esteio, foi estabelecido que apenas Ameaças adversariais são de interesse desta pesquisa, o que, naturalmente, exclui eventos naturais e acidentais.

A primeira Seção do Capítulo ocupou-se do roteiro de planejamento e delimitação de escopo para aplicação do Modelo, que, baseado no Método 5W3H, precede as Fases de Execução do mapeamento em si. Em seguida, a Fase I - Caracterização da Ameaça - foi apresentada em

subseção própria que detalhou cada um dos sete elementos componentes da Ameaça, quais sejam: Evento; Adversário; Conjuntura; Agente; Alvo; Objetivo; e TTPs.

Por fim, na Fase II - Saída do Modelo - discorreu-se sobre os tipos de Impactos previstos pelo Modelo em caso de concretização de evento danoso, além das explanações sobre o campo Avaliação, reservado para conter informações adicionais ao resultado do mapeamento e conclusões analíticas.

Capítulo 4

Apresentação de Resultados

Nesta seção, serão apresentados estudos de caso que ilustram a aplicação do Modelo para Mapeamento de Ameças Cibernéticas proposto. Não se deve perder de vista, contudo, que o mapeamento apresentado nas tabelas abaixo não é exaustivo, pois marca o início de um processo sempre sujeito a atualizações em face do surgimento de novos dados e evolução das Ameaças abordadas.

4.1 Visão Geral

Foram selecionados sete cenários de naturezas diferentes para aplicação experimental das Fases de Execução do Modelo para Mapeamento de Ameaças objeto desta pesquisa, atestando sua flexibilidade e abrangência nos campos aos quais se aplica. Para tanto, os cenários apresentados abarcam Ameaças formadas por atores estatais e não-estatais, envolvidos em campanhas e eventos tanto de cibercrime, quanto de comprometimento de Infraestruturas Críticas e disputas geopolíticas.

Os dados reunidos e analisados durante o mapeamento experimental são oriundos de Fontes Abertas, majoritariamente relatórios de CTI, *white papers*, artigo científicos e publicações da imprensa especializada. O grau de tecnicidade dos dados reunidos e dos resultados análiticos apresentados foram mantidos na gradação adequada aos usuários aos quais o Modelo primordialmente se destina, quais sejam, as instâncias gerencial e decisora de organizações e governos.

Os resultados apresentados nos cenários abaixo foram construídos por meio do processo de produção de Inteligência nos termos explicitados na Seção 2.3. Basicamente, pesquisas em fontes abertas permitiram a reunião de dados diversos originários de publicações de agências governamentais, empresas de segurança cibernética, pesquisadores e mídia especializada. Por ser tratar de aplicação experimental do Modelo, não foram acessadas outras fontes de dados, ordianariamente disponíveis a agências de Inteligência, a exemplo de: Operações de Busca e Fontes Humanas; Bancos de Dados internos; Bancos de Dados externos, agências de Inteligência de outros países; organismos internacionais; ou empresas contratadas.

Em seguida, por meio avaliação das fontes, comparação de dados, exclusão de falsas confirmações e avaliação de verossimilhança, foram atribuídos aos dados os graus de probabilidade ou certeza. Por fim, os dados selecionados foram inseridos nas categorias condizentes, permitindo que o subsequente processo de análise preenchesse ou indicasse as lacunas existentes e subsidiasse a delimitação dos Impactos e construção da Avaliação.

O processo de reunião e análise de dados empregado nesta pesquisa, vale ressaltar, é comumente empregado, com suas variações, em processos analíticos diversos. O Modelo de Mapeamento de Ameaças ora preconizado, não se vincula a um fluxo específico de produção de Inteligência. Ao contrário, o Modelo foi desenvolvido como um arcabouço capaz de ser inserido em qualquer metodologia de Produção do Conhecimento adota pela organização interessada.

4.2 Cenário 1

Trata-se de Ameaça de natureza provavelmente estatal, mas ainda sem atribuição de Adversário, com Objetivo de Espionagem [35]. O Mapeamento do Cenário 1 foi consolidado na Tabela 4.1.

Evento	Machete ou Ragua; Campanha regional. Iniciada anteriormente a 2011 e ainda ativa; Direcionada primordialmente a países de idioma espanhol na América Latina, mas também desdobrou ações contra o Brasil. Malware desenvolvido para infectar SO Windows por meio de e-mails de *spear-phishing* ou mídias removíveis USB. O malware é capaz de acionar câmeras e microfones, registrar teclas, localização do computador, capturar telas e coletar documentos dos sistemas infectados. Utiliza documentos previamente roubados e adaptados, ou falsos documentos confeccionados, como iscas de Engenharia Social para atração de vítimas específicas. As iscas exploram temas políticos, militares, financeiros e sexuais. Em algumas ações, haveria acesso físico às organizações alvo.
Adversário	Provável patrocinador estatal não-identificado.
Conjuntura	A América Latina atravessou, no período de atividade da Ameaça, instabilidade política em diversos países, resultando em disputas políticas e ideológicas internacionais; crises diplomáticas; crises econômicas e políticas; crises humanitárias e migratórias; sanções internacionais; e expansão da criminalidade organizada. O cenário regional de disputa e instabilidade envolve Estados Nacionais, organizações criminosas, terroristas e paramilitares, fomentando o desdobramento de campanhas cibernéticas disruptivas, criminosas e de Espionagem.
Agente	Grupo APT não nominado; Apesar da propável associação com Adversário estatal, o grupo APT que opera o malware não necessariamente é parte orgânica de estrutura governamental. Motivação desconhecida. Ativo desde, pelo menos, 2011; Tratar-se-ia de único grupo APT operando ferramenta de espionagem cibernética. A ferramenta recebe adaptações e melhoramentos para adequação a alvos diversos. Demonstra grau relativo de sofisticação técnica, suficiente para atigir objetivos propostos contra alvos na América Latina, mas aquém da técnica observada em campanhas conduzidas por grupos APT no Estado da Arte. Outras campanhas de espionagem cibernética na América Latina apresentam caracterísiticas semelhantes à linha de ação do APT em tela, todavia, incompatibilidades de TTPs indicam que não se trata do mesmo grupo.
Alvo	Dados Pessoais; Sistemas Governamentais (diplomático e político); Sistemas de Defesa; Base Industrial de Defesa; Entidades Políticas.
Objetivo	Espionagem.
TTPs	Extração de dados.
Resultado	- Impacto: Financeiro; Legal; Político; Imagem; Infraestrutura; Segurança; Militar; Econômico, Geopolítico, Segurança. - Avaliação: Os dados buscados pelo Machete seriam utéis a atores interessados em influenciar processos decisórios de adversários e alcançar vantagens estratatégicas. Não teriam valor financeiro instrínseco. A Ameaça continua ativa e o código malicioso continua sofrendo melhoramentos.

Tabela 4.1: Cenário 1

4.3 Cenário 2

O segundo estudo de caso trata da Ameaça composta pela doutrina e operações de Guerra Cibernética da Coreia do Norte. Ameaça estatal inserida numa Conjuntura ampla de disputa geopolítica e permeada por Eventos ofensivos direcionados a ganho financeiro [38] contra Alvos diversos. O mapeamento desta Ameaça foi consolidado na Tabela 4.2.

Evento	Guerra Cibernética NKPD Campanha global Ativa desde, pelo menos, 2005. Campanha de Guerra Cibernética conduzida pela Coreia do Norte. Engloba ações de Espionagem, Ransomware e outras TTPs para ganhos financeiros, além de operações de Disrupção de sistemas informatizados.
Adversário	Coreia do Norte - Estado autoritário em conflito militar direto com a Coreia do Sul e alvo de sanções internacionais. Detentor de armas nucleares e agressiva postura dissuasória, desenvolve a Guerra Cibernética como instrumento fundamental e adicional à sua capacidade militar, destacando sua natureza assimétrica. Executa campanhas de Rasomware, Espionagem e Disrupção contra alvos diversos em escala global. Recebe apoio da China em vários segmentos, inclusive militares e cibernéticos.
Conjuntura	Estado de Guerra entre Coreia do Norte e Coreia do Sul, todavia, sem engajamento aberto de forças militares. Ambiente de disputa ideológica e elevada instabilidade entre os dois países
Agente	Unidades e subdivisões da estrutura militar (General Staff Department) e de Inteligência (Reconnaissance General Bureau), totalizando pelo menos dezoito grupos especializados. Às diferentes unidades foram atribuídas denominações variadas por atores governamentais e privados, por exemplo: *Lazarus, Bluenoroff, Hidden Cobra, Andariel, Bureau 121, APT37, ScarCruft, Reaper, Group123, DarkHotel* Parte orgânica da estrutura governamental do país Adversário; Motivação ideológica; financeira; por coação; satisfação pessoal; ganho organizacional; Estrutura publicamente conhecida desde 2018; Cada unidade ou divisão é especializada em um tipo específico de ação ofensiva. Apesar do alcance global, os Agentes relacionados concentram esforços contra alvos sul-coreranos. As diferentes unidades operam tanto a partir do território norte-coreano quanto de tercerios países, em especial da China.
Alvo	Setor de transporte; Setor de abastecimento hídrico; Setor de abastecimento alimentar; Setor de comunicações e informação; Sistema de Saúde; Sistemas governamentais; Sistemas de Defesa; Base industrial de Defesa; Sistema Financeiro; Setor produtivo amplo; Centros de pesquisa científica; Entidades políticas; Empresas de comunicação e mídia; Bases de dados pessoais.
Objetivo	Espionagem, Interferência Externa, Disrupção e Ganho financeiro.
TTPs	Ransomware; Extração ou Exposição de dados; Alteração ou Destruição de dados; Negação de Serviço; Defacement; Transferência de Fundos; Destruição de Hardware ou Software.
Resultado	- Impacto: Financeiro; Legal; Político; Imagem; Infraestrutura; Militar; Econômico; Geopolítico; Segurança; Social. - Avaliação: Trata-se de Ameaça ampla composta por vários Agentes, dedicados a Objetivos diversos contra alvos espalhados pelo mundo. Apesar da predileção por operações contra a Coreia do Sul, é também uma Ameaça oposta a países alheios à zona de conflito geopolítico e militar na qual o Adversário está inserido, atacados em campanhas de Ransomware e outras TTPs com Objetivo de Ganho Financeiro. As campanhas com Objetivo de Ganho Financeiro são executadas como parte do esforço de Guerra Cibernética do Adversário, classificadas na doutrian desse Adversário, portanto, não como ações de *cybercrime*, mas de natureza militar e de inteligência. A unidade 180 é a responsável por executar ações com Objetivo de Ganho Financeiro contra outros países. Unidade opera fora do territporio norte-coreano para efeito de anonimização.

Tabela 4.2: Cenário 2

4.4 Cenário 3

O terceiro cenário parte de um Evento bem delimitado e avalia uma Ameaça formada por Grupo Hacker engajado em campanhas com Objetivo de Ganho Financeiro. O Agente tem características incomuns, empregando a TTP Ransomware com variações interessantes. Ameaça sem Adversário [155] [156] [157] [158] [159]. O mapeamento está consolidado na Tabela 4.3.

Evento	Nvidia Ransomware Evento local; Fevereiro de 2022; Ataque de Ransomware executado contra empresa multinacional de tecnologia com sede na Califórnia/USA. Roubo de dados acerca de tecnologia em desenvolvimento e credenciais de funcionários da empresa. Resgate solicitado sob ameaça de vazamentos de dados sensíveis, sem cripotografia de dados no sistema invadido. Resgate não demandou repasse financeiro direto, mas alterações em tecnologias desenvolvidas pelo alvo para exploração de criptomoedas. Resgate não cumprido e vazamento de dados sensíveis foi efetivado;
Adversário	* * *
Conjuntura	Fenômeno global de aumento de ofensivas conduzidas por grupos dedicados a crimes cibernéticos, especialmente ransomware, com diferentes graus de capacidade técnica e experiência. Aumento de casos decorrentes da acelerada digitalização implementada em vários setores durante a pandemia de COVID-19 (2020 - 2021). Risco de impactos consíderáveis em sistemas e operações de Infraestruturas Críticas.
Agente	Grupo Lapsus$ Indivíduo ou grupo hacker independente; Motivação financeira; Ativo desde, pelo menos, meados de 2021; Especializado em operações de Engenharia Social e extorsão. Executa ações destrutivas nos sistemas invadidos, inclusive sem emprego de ransomware. Ameaça as vítimas de vazamento dos dados extraídos, sem criptografia de dados ou negação de acesso aos sistemas invadidos. Resgates demandados não necessariamente envolvem repasse de recusros diretamente da vítima, mas outros meios indiretos de alcançar Ganho Financeiro. Ataca alvos no mundo todo, entre os quais: Sistemas governamentais; Setor produtivo amplo; Sistema de Saúde; Centros de pesquisa científica, Setor energético; Setor de comunicações e informação; Empresas de comunicação e mídia. Membros do grupo seriam majoritariamente jovens, com relativamente pouca experiência. Grupo busca elevada visibilidade e exposição de suas operações em mídias sociais. Associado ao grupo DEV-0537 - assim nominado pelo Microsoft Threat Intelligence Center. Ator engajado em operações de Extração ou Exposição de dados e Alteração ou Destruição de dados;
Alvo	Setor produtivo amplo; Centros de pesquisa científica.
Objetivo	Ganho financeiro.
TTPs	Ransomware; Extração ou Exposição de dados; Alteração ou Destruição de dados; Destruição de Hardware ou Software.
Resultado	- Impacto: Financeiro; Legal; Imagem; Infraestrutura; Econômico; Segurança; Social. - Avaliação: Ameaça com características incomuns. Agente de considerável agressividade, resultando em destruição de ativos em meio a ações de Ransomware. Foi atribuído a este Agente um ataque ao Ministério da Saúde do Brasil. Supostos membros do grupo foram presos no Brasil e Reino Unido.

Tabela 4.3: Cenário 3

4.5 Cenário 4

O Cenário 4 trata de Ameaça composta por diversos grupos filiados a RaaS. Engloba, portanto, vários Agentes afiliados a uma mesma estrutura de ransomware, dedicados ao Cibercrime sem patrocínio estatal. Ao contrário do mapeamento apresentado no Cenário 4.4, este caso não parte de um Evento específico, mas aborda uma campanha global permeada por diveras ações ofensivas [160] [161] [162]. Ameaça mapeada na Tabela 4.4 .

Evento	Black Matter Ransomware Campanha global. Conhecida desde julho de 2021. BlackMatter é uma ferramenta *ransomware-as-a-service* (Raas) empregada por grupos afiliados diversos, aqui denominados "BlackMatter actors". BlackMatter seria um RaaS construído por uma junção de membros e expertise dos grupos REvil e DarkSide. BlackMatter actors atacaram setores de Infraestrutura Crítica nos EUA e outros países de lingua inglesa, demandando resgates que variaram entre $80 mil a $15 milhões em Bitcoin e Monero;
Adversário	* * *
Conjuntura	Fenômeno global de aumento de ofensivas conduzidas por grupos dedicados a crimes cibernéticos, especialemnte Ransomware, com diferentes graus de capacidade técnica e experiência. Aumento de casos decorrentes da acelerada digitalização implementada em vários setores durante a pandemia de COVID-19 (2020 - 2021). Risco de impactos consíderáveis em sistemas e operações de Infraestruturas Críticas.
Agente	BlackMatter actors; Indivíduo ou grupo hacker independente; Motivação financeira; Ativos de junho a novembro de 2021; Grupos afiliados ao RaaS Black Matter, que foi desenvolvido em conjunto por membros dos grupos de ransomware REvil e DarkSide, responsáveis pelos ataques ao Colonial Pipeline e JBS. Buscam alvos de alto valor (faturamento acima de $100 milhões) em setores de IC de países de lingua inglesa - com destaque para EUA, Canadá, Austrália e Reino Unido. Selecionam alvos pela presença de vulnerabilidades, no lugar de investirem muitos recursos em um alvo de segurança mais robusta previamente definido. Evitam atacar Sistemas de Saúde, Sistemas Administrativos Governamentais e sistemas previamente comprometidos pelos grupos REvil e DarkSide. Preferem ganhar acesso inicial por meio do comprometimento de terminais vulneráveis, explorando credenciais de acesso adquiridas de outras fontes, em detrimento de ações de *Spear-phishing*. Oferecem recompensa de $ 100 mil a *insiders* ou outros hackers que forneçam acesso a novos sistemas-alvo. A estrutura do RaaS Black Matter teria sido desativada em novembro de 2021, após os desenvolvedores alegarem "pressão das autoridades".
Alvo	Setor energético; Setor de Transporte; Setor de Abastecimento Hídrico; Setor de Abastecimento Alimentar; Setor de Comunicações e Informação; Sistema Financeiro; Setor Produtivo amplo; Centros de Pesquisa Científica;
Objetivo	Ganho financeiro.
TTPs	Ransomware; Extração ou Exposição de dados;
Resultado	- Impacto: Financeiro; Legal; Imagem; Infraestrutura; Segurança; Econômico; Social. - Avaliação: Ameaça composta por vários Agentes associados, felixível e adptável a mudanças de Conjuntura. Ainda que esteja inativa, é provável que integrantes dos grupos que a compõem continuem atuantes sob diferentes denominações e TTPs.

Tabela 4.4: Cenário 4

4.6 Cenário 5

Ameaça formatada por campanha de Guerra Híbrida russa contra Alvo específico, fruto de uma Conjuntura de conflito geopolítico bilateral. Apresenta significativo emprego de ações de Guerra Cibernética e operações de Interferência Externa [129] [163] [164] [165] [166]. Mapeamento consolidado na Tabela 4.5.

Evento	Guerra Cibernética Rússia x Ucrânia Campanha regional. Iniciada em 2014 e ainda ativa. Campanha de Guerra Cibernética Russa direcionada à Ucrânia, itensificada em fevereiro de 2022 com a invasão militar do território ucraniano. Ataques cibernéticos russos explorando diferentes TTPs afetaram diversos segmentos de IC em apoio a ações militares cinéticas. Apesar do foco principal em Disrupção, ações de Espionagem também foram realizadas. Foram gerados impactos sobre a estrutura governamental, militar e a população ucranianas.
Adversário	Rússia - Dotado de elevada capacidade ofensiva cibernética. Desdobra operações de Inteligência (incluindo Desinformação e Interferência Externa) em apoio a interesses nacionais. Apresenta elevada disposição ao conflito, desdobrando campanhas militares regulares e irregulares em sua zona de influência direta.
Conjuntura	Conflito bilateral histórico entre Russia e Ucrânia, antigas repúblicas soviéticas. Eventos ofensivos cibernéticos se somam a outros meios de ação, inclusive operações de Guerra Regular, em uma campanha de Guerra Híbrida conduzida pela Rússia. OTAN tem aportado recursos em apoio ao Esforço de Guerra ucraniano.
Agente	Unidades da Divisão Cibernética do Departamento Central de Inteligência Russo (GRU). Receberam diversas nominações por atores governamentais e privados, entre as quais: Unit 26165, Unit 74445, Unit 54777, APT 28, Fancy Bear, Voodoo Bear, Sandworm, Tsar Team e outros. Parte orgânica da estrutura governamental do país Adversário; Motivação ideológica; financeira; satisfação pessoal; ganho organizacional; Data incerta de início de atividades; Parte do aparato de Inteligência Militar da federação Russa. Unidades operam globalmente com emprego de TTPs diversas e com Objetivos de Espionagem; Interferência Externa; Ganho financeiro e Disrupção.
Alvo	Setor energético; Setor de Transporte; Setor de Abastecimento Hídrico; Setor de Abastecimento Alimentar; Setor de Comunicações e Informação; Sistema Financeiro; Setor Produtivo amplo; Centros de Pesquisa Científica; Setor Energético; Sistema de Saúde; Sistemas Governamentais; Sistemas de Defesa; Base industrial de Defesa; Entidades Políticas; Empresas de Comunicação e Mídia; Bases de Dados Pessoais.
Objetivo	Disrupção e Espionagem.
TTPs	Ransomware; Extração ou Exposição de dados; Alteração ou Destruição de dados; Negação de Serviço; Destruição de Hardware ou Software.
Resultado	- Impacto: Financeiro; Legal; Imagem; Infraestrutura; Segurança; Político; Econômico; Social; Militar; Geopolítico. - Avaliação: Efeitos do conflito têm alcance global, atingindo cadeias logísiticas, de produção de alimentos e abastecimento energético. Apesar dos esforços russos, a campanha cibernética, por si só, teria se mostrado incapaz de gerar significativa vantagem estratégica. Sanções econômicas impostas à Russia por outros países e o apoio material ao Esforço de Guerra Ucraniano aumentam o risco dessas nações sofrerem ataques cibernéticos russos. Há risco de escalamento do conflito e envolvimento militar direto de outras potências mundiais. O conflito permite a observação da evolução das TTPs implementadas e dos Impactos gerados pela estrutura cibernética ofensiva Russa em apoio a ações militares de larga escala.

Tabela 4.5: Cenário 5

4.7 Cenário 6

Esta Ameaça é constituída por Evento conduzido por indivíduo ou grupo hacker independente, com TTPs de Extração ou Exposição de Dados pessoais. Destaca-se por figurar, em primeira análise, como Ameaça ordinária e sem impacto sobre sistemas críticos. Todavia, vazamento de Bases de Dados Pessoais tem potencial danoso contra vários segmentos [167] [168] [169] [170]. Mapeamento constante na Tabela 4.6.

Evento	Vazamento Free VPN Evento global. Publicizado em fevereiro de 2021. Hackeamento de dados de 21 milhoes de usuários dos aplicativos de VPN grátis para Android: SuperVPN, GeckoVPN, and ChatVPN. Juntos, os três aplicativos somam mais de 100 milhões de downloads na Google Play Store. Os dados hackeados incluiriam: e-mail, nome de usuário, nome completo, país do usuário, informações de pagamento, senhas geradas aleatoriamente, status da conta, além do número de série, marca, modelo, ID e número IMSI do telefone do usuário. Os dados foram postos à venda em fórum hacker na Dark Web em 2021 e franqueados em canal do Telegram em 2022.
Adversário	* * *
Conjuntura	Fenômeno global de aumento de ofensivas conduzidas por grupos dedicados a crimes cibernéticos com diferentes graus de capacidade técnica e experiência. Aumento de casos decorrentes da acelerada digitalização implementada em vários setores durante a pandemia de COVID-19 (2020 - 2021). Bases de Dados Pessoais tem sido alvo de Adversários e Agentes governamentais e não-governamentais, tanto como ativo comercializável, quanto como insumo para desenvolvimento de ações ofensivas mais complexas e direcionadas a outros Alvos e Objeivos.
Agente	Agente não identificado; Provável indivíduo ou grupo hacker independente; Motivações financeira e satisfação pessoal; A primeira disponibilização dos dados hackeados para compra denota a motivação financeira. O posterior franqueamento dos dados, presumindo que tenha sido feito pelo Agente e não por terceiro, além da cultura hacker de busca por visibilidade e reconhecimento, aponta para a existência de Motivação secundária de Satisfação Pessoal. Outros hackeamentos de serviços gratuitos de VPN aconteceram em 2019 e 2020, não há, todavia, indícios de se tratar dos mesmos Agentes.
Alvo	Bases de dados pessoais;
Objetivo	Ganho financeiro.
TTPs	Extração ou Exposição de dados;
Resultado	- Impacto: Financeiro; Legal; Imagem; Segurança; Social. - Avaliação: Apesar do Evento sob análise não impactar, inicialmente, ICs, grandes organizações estratégicas ou governos, o hackeamento de dados pessoais é potencialmente danoso para sistemas críticos. O vazamento desses dados facilita o desenvolvimento de outras ações ofensivas, como campanhas criminosas de *phishing* ou operações intrusivas mais complexas de Espionagem, Interferência Externa, Disrupção e Terrorismo. Dados de indivíduos específicos, ocupantes de posições-chave, podem ser buscados nas bases vazadas e serem usados na montagem de operações direcionadas a determinados Alvos. Ameaças dessa natureza ressaltam a importância da sensibilização em segurança de líderes e autoridades, neste caso específico, estimulando a escolha por serviços e aplicativos bem estruturados para emprego tanto em sistemas organizacionais quanto particulares.

Tabela 4.6: Cenário 6

4.8 Cenário 7

Ameaça composta por Evento de Cibercrime com TTP de Ransomware, sem Adversário. Considerado por alguns analistas como o ataque mais significativo já registrado contra Sistemas Governamentais brasileiros [171] [172] [173] [174] [175] [176] [177] [178] [179] [180] . Mapeamento consolidade na Tabela 4.7.

Evento	Ransomware STJ; Evento nacional; 3 de novembro de 2020; Criptografia de dados em servidores do Superior Tribunal de Justiça do Brasil, manteve o sistema total ou parcialemente indisponivel por cerca de cinco dias. Foi empregado o malware RansomExx, uma renomeação do ransomware Defray777, que ficou especialmente ativo em meados de 2020 contra alvos de alto valor. Os invasores galgaram acesso ao sistema do STJ com emprego de e-mails de phishing, dos quais três foram ativados por usuários do sistema, permitindo a instalação de trojan. RansomExx também teria sido utilizado em ataques contra o Tribunal de Justiça do Estado de Pernambuco, The Texas Department of Transportation (TxDOT), Konica Minolta, IPG Photonics, e Tyler Technologies. Os servidores foram desligados como medida de segurança e os prazos processuais foram suspensos. O STJ afirmou que os arquivos em backup não foram comprometidos e os dados dos cerca de 255 mil processo e mais os documentos administrativos tiveram sua integridade preservada. Não houve pagamento do resgate demandado de R$ 10 milhões.
Adversário	* * *
Conjuntura	Fenômeno global de aumento de ofensivas conduzidas por grupos dedicados a crimes cibernéticos com diferentes graus de capacidade técnica e experiência. Aumento de casos decorrentes da acelerada digitalização implementada em vários setores durante a pandemia de COVID-19 (2020 - 2021). No caso do sistema de Justiça, além da indisponibilidade dos dados, a interupção das sessões virtuais, assim realizadas como medida de enfrentamento à pandemia de COVID-19, aumentaram o grau de sensibilidade das redes dos tribunais. Ademais, o Brasil atravessa período de intensa disputa político-ideológica, o que colocou Sistemas Governamentais; Entidades Políticas; e Empresas de Comunicação e Mídia; entre outras organizações, também como alvos de hacktivismo, o que adiciona outras hipóteses aos processos de análise de Eventos e de Gestão de Risco.
Agente	Agente não identificado; Provável indivíduo ou grupo hacker independente; Teria realizado ataques anteriores contra o Ministério da Saúde e Governo do Distrito Federal. Motivação financeira;
Alvo	Sistemas Governamentais;
Objetivo	Ganho financeiro.
TTPs	Ransomware;
Resultado	- Impacto: Financeiro; Legal; Imagem; Segurança. - Avaliação: O ataque ao STJ foi classificado por analistas como dos mais graves já realizados contra Sistemas Governamentais brasileiros. O emprego de e-mail de phishing para ganho inicial de acesso destaca a importância de sensibilização dos usuários dos sistemas aos riscos cibernéticos. Apesar da divulgação midiática de que o Agente responsável pelo ataque foi identificado pelas autoridades policiais, não houve publicação de sua identidade ou afiliações. O uso do mesmo malware identificado em outras campanhas, inclusive em outros países, não necessariamente provam que se trata do mesmo Agente em todos os casos. Não foram encontrados indícios de se tratar de Evento patrocinado por Adversário, portanto, a classificação como Cibercrime mostra-se a mais adequada.

Tabela 4.7: Cenário 7

4.9 Síntese do Capítulo

Este capítulo ocupou-se da apresentação dos resultados alcançados na pesquisa por meio da aplicação experimental, em sete casos práticos, do Modelo para Mapeamento de Ameaças Cibernéticas objeto desta dissertação.

Os setes casos abarcam cenários de crimes cibernéticos, eventos e campanhas contra ICs, Espionagem e Ameaças de cunho eminentemente geopolítico, como Guerra Cibernética e Guerra Híbrida. Buscou-se reunir casos de variadas naturezas e complexidade com o objetivo de atestar o grau de flexibilidade do Modelo. Ademais, diferentes recortes geográficos foram abordados, aqui incluído um Evento nacional que alvejou Sistema Governamental brasileiro.

Capítulo 5

Conclusão e Trabalhos Futuros

Nesta dissertação foi apresentado um Modelo para Mapeamento de Ameaças Cibernéticas de alta complexidade com o objetivo de subsidiar o processo decisório organizacional, tanto de governos quanto de corporações privadas.

Baseado em conceitos de Gestão de Risco, *Cyber Threat Intelligence* e Atribuição Cibernética, o Modelo preconiza que o detalhamento da Ameaça se dê por meio da estruturação das atividades de reunião e classificação de dados pertinentes. Os dados são então alocados em sete categorias derivadas dos Elementos da Ameaça, orientando o fluxo de análise e culminando na apresentação de impactos e conclusões analíticas.

O modelo proposto trata a Ameaça Cibernética como um cenário mutável pela dinâmica dos elementos que a compõem. Esses elementos dizem respeito tanto aos atores ofensivos, patrocinadores e sistemas sob proteção, quanto a fatores externos conjunturais que gerem mudanças no comportamento dos atores envolvidos. A pesquisa atribui especial relevância à dinâmica que envolve adversários estatais e conjuntura internacional. Não obstante, Agentes e Adversários não-estatais, cuja capacidade ofensiva os coloca no rol de partes formadoras de Ameaças de alta complexidade, são também objeto de interesse desta pesquisa.

Os resultados do Modelo proposto trazem grau de tecnicidade compatível com diferentes perfis do corpo gerencial das organizações a ser protegidas. Para tanto, criou-se um modelo flexível, passível de ser adequado ao propósito do analista responsável por sua aplicação.

Esta pesqusia, naturalmente, não esgota o tema ao qual se propôs a abordar. A amplitude do universo da Segurança Cibernética, que engloba diferentes áreas do conhecimento, oferece variadas linhas de desdobramento para trabalhos futuros.

Uma dessas linhas de desdobramento conduz à automação do processo de reunião de dados em conformidade com as categorias elencadas no Modelo proposto. Noutra senda, vislumbra-se a utilidade de se construir um modelo para produção de alertas de Segurança Cibernética, direcionado à esfera gerencial das organizações, trazendo conhecimento antecipado sobre novos riscos e atualizações em face de alterações significativas nas Ameaças já mapeadas.

Ademais, resgatando as discussões apresentadas na Seção 2.4, vislumbra-se o potencial de especialização e aprofundamento do Modelo proposto em cada uma das áreas de conflitos cibernéticos elencados, a saber: Cibercrime; Terrorismo; Espionagem, Interferência Externa e Disrupção; e Guerra Cibernética. Há extensa produção literária sobre cada um dos campos, além da ininterrupta evolução desses fenômenos na História, motivos suficientes para que se busque continuidade dos trabalhos nesse sentido.

Considerando, ainda, a natureza deste Modelo de Mapeamento de Ameaças como um subprocesso da disciplina de Gestão de Risco, é promissora a idéia de se avançar nessa direção, adicionando aos resultados da execução do Modelo atual: níveis de gradação do risco associado às Ameaças analisadas;e medidas técnicas e gerenciais cabíveis para mitigação do risco.

Referências Bibliográficas

[1] EGLOFF, F. J.; SMEETS, M. Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, Taylor & Francis, p. 1–32, 2021. Doi:10.1080/01402390.2021.1895117.

[2] SILVA, A. de Melo e et al. A methodology to evaluate standards and platforms within cyber threat intelligence. *Future Internet*, Multidisciplinary Digital Publishing Institute, v. 12, n. 6, p. 108, 2020. Doi:10.3390/fi12060108.

[3] ARQUILLA, J.; RONFELDT, D. Cyberwar is coming! *Comparative Strategy*, Routledge, v. 12, n. 2, p. 141–165, 1993. Disponível em: <https://doi.org/10.1080/01495939308402915>.

[4] JÚNIOR, S. *A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual*. [S.l.], 2013.

[5] CARR, J. *Inside cyber warfare: Mapping the cyber underworld*. [S.l.]: "O'Reilly Media, Inc.", 2012.

[6] JUNIOR, J. A. de A. et al. Competências para os cyber red teams no contexto militar. *Revista Ibérica de Sistemas e Tecnologias de Informação*, Associação Ibérica de Sistemas e Tecnologias de Informacao, n. E26, p. 612–623, 2020. Doi:10.26512/2020.08.D.40003.

[7] KHALID, A. et al. Advanced persistent threat detection: A survey. In: *2021 3rd International Cyber Resilience Conference (CRC)*. Langkawi Island: [s.n.], 2021. p. 1–6. Doi:10.1109/CRC50527.2021.9392626.

[8] MOHAMED, N.; BELATON, B. Sbi model for the detection of advanced persistent threat based on strange behavior of using credential dumping technique. *IEEE Access*, v. 9, p. 42919–42932, 2021. Doi:10.1109/ACCESS.2021.3066289.

[9] ODNI. *A Guide to Cyber Attribution*. 2018. Disponível em: `https://www.dni.gov/index.php/cyber-threat-framework`. Acessado em: 7/02/2022.

[10] EUROPOL. *Internet organised crime threat assessment*. 2020. Disponível em: `https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020`. Acessado em: 7/02/2022.

[11] WAZID, M. et al. Hacktivism trends, digital forensic tools and challenges: A survey. In: IEEE. *2013 IEEE Conference on Information & Communication Technologies*. Thuckalay, 2013. p. 138–144. Doi:10.1109/CICT.2013.6558078.

[12] CONNELL, M.; VOGLER, S. *Russia's approach to cyber warfare (1rev)*. [S.l.], 2017. Acessado em: 7/02/2022. Disponível em: <https://apps.dtic.mil/sti/pdfs/AD1032208.pdf>.

[13] OOSTHOEK, K.; DOERR, C. Cyber threat intelligence: A product without a process? *International Journal of Intelligence and CounterIntelligence*, Taylor & Francis, v. 34, n. 2, p. 300–315, 2021. Doi:10.1080/08850607.2020.1780062.

[14] EUROPOL. *Internet Organised Crime Threat Assessment*. 2018. Disponível em: https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf;. Acessado em: 8/02/2022.

[15] DAHAN, A.; KANDEFELT, J. *Pervasive Brazilian financial malware targets bank customers in Latin America and Europe*. 2018. Disponível em: https://www.cybereason.com/blog/brazilian-financial-malware-banking-europe-south-america. Acessado em: 7/02/2022.

[16] HALL, T. et al. Economic geographies of the illegal: the multiscalar production of cybercrime. *Trends in Organized Crime*, Springer, v. 24, n. 2, p. 282–307, 2021. Doi:10.1007/s12117-020-09392-w.

[17] KSHETRI, N.; DEFRANCO, J. F. The economics of cyberattacks on brazil. *Computer*, v. 53, n. 9, p. 85–90, 2020. Doi:10.1109/MC.2020.2997322.

[18] INSIKT. *Pirates of Brazil: Integrating the Strengths of Russian and Chinese Hacking Communities*. 2019. Disponível em: https://www.recordedfuture.com/brazilian-hacking-communities/. Acessado em: 7/02/2022.

[19] LEWIS, J. *Economic Impact of Cybercrime—No Slowing Down Report*. [S.l.], 2018. Acessado em: 7/02/2022. Disponível em: <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf>.

[20] SECURELIST. *The Tetrade: Brazilian banking malware goes global*. [S.l.], 2020. Acessado em: 07/11/2022. Disponível em: <https://securelist.com/the-tetrade-brazilian-banking-malware/97779/>.

[21] TADDEO, M. Deterrence by norms to stop interstate cyber attacks. *Minds and Machines*, Springer, v. 27, n. 3, p. 387–392, 2017. Doi:10.1007/s11023-017-9446-1.

[22] PWC. *Cybersecurity + geopolitical conflict: What boards and CEOs should know and act upon*. 2022. Acessado em: 10/03/2023. Disponível em: <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cybersecurity-geopolitical-conflict-board-ceo-response.html>.

[23] BRAUE, D. *How Geopolitics Affects Cybersecurity*. 2023. Acessado em: 10/03/2023. Disponível em: <https://cybersecurityventures.com/how-geopolitics-affects-cybersecurity/>.

[24] MELO, R. C. R. D.; ALBUQUERQUE, R. D. O.; MENDONçA, F. L. L. D. Cyber threat modeling framework. In: *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*. [S.l.: s.n.], 2022. p. 1–7. Doi:10.23919/CISTI54924.2022.9866890.

[25] HEJASE, H. J.; FAYYAD-KAZAN, H. F.; MOUKADEM, I. Advanced persistent threats (apt): An awareness review. *Journal of Economics and Economic Education Research*, Jordan Whitney Enterprises, Inc, v. 21, n. 6, p. 1–8, 2020. Doi:10.13140/RG.2.2.31300.65927.

[26] ALSHAMRANI, A. et al. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, IEEE, v. 21, n. 2, p. 1851–1877, 2019. Doi:10.1109/COMST.2019.2891891.

[27] ROSENCRANCE, L. *What is advanced persistent threat (APT)?* 2021. Disponível em: https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threat-APT. Acessado em: 30/10/2022.

[28] LOCKHEEDMARTIN. *The Cyber Kill Chain*. [S.l.]. Acessado em: 28/10/2022. Disponível em: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.

[29] NSA. *NSA/CSS Technical Cyber Threat Framework v2*. 2018. Disponível em: =https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/smdsearch11747/2018/. Acessado em: 6/02/2022.

[30] DESOMBRE, W. Getting harder to catch: Analyzing the evolution of china's cyber espionage campaigns against the united states through a case study of apt1. *Sigma Iota Rho's Journal of International Relations*, v. 19, p. 85–87, 2017. Acessado em 04/11/2022. Disponível em: <https://static1.squarespace.com/static/54da238be4b0af07ca2cf7ea/t/59d10044f9a61e37e89ff986/1506869
95>.

[31] SECURELIST. *APT trends report Q3 2022*. 2022. Acessado em: 04/11/2022. Disponível em: <https://securelist.com/apt-trends-report-q3-2022/107787/>.

[32] LEMAY, A. et al. Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, Elsevier, v. 72, p. 26–59, 2018. Doi:10.1016/j.cose.2017.08.005.

[33] ODNI. *Annual Threat Assessment of the U.S. Intelligence Community*. 2022. Disponível em: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf. Acessado em: 7/11/2022.

[34] BOOZ|ALLEN|HAMILTON. *Same Cloak, More Dagger: Decoding How The People's Republic of China Uses Cyberattacks*. [S.l.], 2022. Acessado em: 03/11/2022. Disponível em: <https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html>.

[35] VALEROS, V.; RIGAKI, M.; GARCIA, S. Machete: Dissecting the operations of a cyber espionage group in latin america. In: IEEE. *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Stockholm, 2019. p. 464–473. Doi:10.1109/EuroSPW.2019.00058.

[36] CISA. *AppleJeus: Analysis of North Korea's Cryptocurrency Malware*. [S.l.], 2021. Acessado em: 7/02/2022. Disponível em: <https://www.cisa.gov/uscert/ncas/alerts/aa21-048a>.

[37] CISA. *North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector*. [S.l.], 2022. Acessado em: 04/11/2022. Disponível em: <https://www.cisa.gov/uscert/ncas/alerts/aa22-187a>.

[38] JI-YOUNG, K.; IN, L. J.; GON, K. K. The all-purpose sword: North korea's cyber operations and strategies. In: *2019 11th International Conference on Cyber Conflict (CyCon)*. [S.l.: s.n.], 2019. v. 900, p. 1–20.

[39] GOEL, S.; NUSSBAUM, B. Attribution across cyber attack types: Network intrusions and information operations. *IEEE Open Journal of the Communications Society*, IEEE, v. 2, p. 1082–1093, 2021. Doi:10.1109/OJCOMS.2021.3074591.

[40] RID, T.; BUCHANAN, B. Attributing cyber attacks. *Journal of Strategic Studies*, Taylor & Francis, v. 38, n. 1-2, p. 4–37, 2015. Doi:10.1080/01402390.2014.977382.

[41] ROMANOSKY, S.; BOUDREAUX, B. Private-sector attribution of cyber incidents: benefits and risks to the us government. *International Journal of Intelligence and CounterIntelligence*, Taylor & Francis, v. 34, n. 3, p. 463–493, 2021. Doi: 10.1080/08850607.2020.1783877.

[42] COOK, A. et al. Attribution of cyber attacks on industrial control systems. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, European Alliance for Innovation (EAI), v. 3, n. 7, 2016. Doi:10.4108/eai.21-4-2016.151158.

[43] RAIU, C. *TOP 10 unattributed APT mysteries*. 2022. Acessado em: 04/11/2022. Disponível em: <https://securelist.com/top-10-unattributed-apt-mysteries/107676/>.

[44] PAHI, T.; SKOPIK, F. Cyber attribution 2.0: Capture the false flag. In: ACADEMIC CONFERENCES AND PUBLISHING LIMITED. *ECCWS 2019 18th European Conference on Cyber Warfare and Security*. Coimbra, 2019. p. 338.

[45] SKOPIK, F.; PAHI, T. Under false flag: using technical artifacts for cyber attack attribution. *Cybersecurity*, Springer, v. 3, n. 1, p. 1–20, 2020. Doi:10.1186/s42400-020-00048-4.

[46] GOEL, S. How improved attribution in cyber warfare can help de-escalate cyber arms race. *Connections*, JSTOR, v. 19, n. 1, p. 87–95, 2020. Doi:10.11610/Connections.19.1.08.

[47] REICH, P. *Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization: Cyberterrorism, Information Warfare, and Internet Immobilization*. Information Science Reference, 2012. (Gale virtual reference library). ISBN 9781615208326. Disponível em: <https://books.google.com.br/books?id=-76EE2AtQ4AC>.

[48] JR, J. S. N. Deterrence and dissuasion in cyberspace. *International security*, Cambridge, v. 41, n. 3, p. 44–71, Cambridge, 2016. Doi:10.1162/ISECa00266.

[49] EDWARDS, B. et al. Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences*, National Acad Sciences, v. 114, n. 11, p. 2825–2830, 2017. Doi:10.1073/pnas.1700442114.

[50] TRAN, D. The law of attribution: Rules for attribution the source of a cyber-attack. *Yale JL & Tech.*, HeinOnline, v. 20, p. 376, 2018. Acessado em: 7/02/2022. Disponível em: <https://yjolt.org/sites/default/files/20$_yale_{j \cdot l \cdot t}ech._3$76.*pdf*>.

[51] LANCELOT, J. F. Cyber-diplomacy: cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*, Taylor & Francis, v. 4, n. 4, p. 240–254, 2020. Doi:10.1080/23742917.2020.1798155.

[52] ONU. *Carta das Nações Unidas,1945*. [S.l.]. Acessado em: 12/09/2022. Disponível em: <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>.

[53] NIST. *Managing information security risk: Organization, mission, and information system view*. [S.l.], 2011. Doi:10.6028/NIST.SP.800-39. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-39/final>.

[54] NIST. *Guide for Conducting Risk Assessments, NIST Special Publication 800-30 (Revision 1)*. [S.l.], 2012. Doi:10.6028/NIST.SP.800-30r1. Disponível em: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>.

[55] FFIEC. *Information Technology Examination Handbook*. [S.l.], 2016. Acessado em: 18/11/2022. Disponível em: <https://ithandbook.ffiec.gov/media/274793/ffiec$_itbooklet_information security.pdf$>.

[56] NURULLAYEV, D.; KERR, S.; KNUDSON, M. How states provoke adversaries to solicit information. 05 2022. Acessado em 23/11/2022. Disponível em: <https://www.researchgate.net/profile/Dmitriy-Nurullayev/publication/360306459$_How states provoke adversaries to solicit information/links/626ec55$
$States - Provoke - Adversaries - to - Solicit - Information.pdf$>.

[57] DAVIS, P. K. et al. *Influencing Adversary States: Quelling Perfect Storm*. [S.l.], 2021. Acessado em 23/11/2022. Disponível em: <https://apps.dtic.mil/sti/citations/AD1123253>.

[58] VIANO, E. *Global Organized Crime and International Security*. Taylor & Francis, 2018. (Routledge Revivals). ISBN 9780429843983. Disponível em: <https://books.google.com.br/books?id=OPmADwAAQBAJ>.

[59] UNODC. *"Organized Crime Has Globalized and Turned into a Security Threat"*. 2010. Acessado em: 24/11/2022. Disponível em: <https://www.unodc.org/unodc/en/press/releases/2010/June/organized-crime-has-globalized-and-turned-into-a-security-threat.html>.

[60] BODEAU, D.; MCCOLLUM, C.; FOX, D. *Cyber Threat Modeling: Survey, Assessment, and Representative Framework*. [S.l.], 2018. Acessado em: 8/02/2022. Disponível em: <https://apps.dtic.mil/sti/pdfs/AD1108051.pdf>.

[61] TATAM, M. et al. A review of threat modelling approaches for apt-style attacks. *Heliyon*, v. 7, n. 1, p. e05969, 2021. ISSN 2405-8440. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2405844021000748>.

[62] GONG, S.; LEE, C. Cyber threat intelligence framework for incident response in an energy cloud platform. *Electronics*, Multidisciplinary Digital Publishing Institute, v. 10, n. 3, p. 239, 2021. Doi:10.3390/electronics10030239.

[63] AMARO, L. J. B. et al. Methodological framework to collect, process, analyze and visualize cyber threat intelligence data. *Applied Sciences*, v. 12, n. 3, 2022. ISSN 2076-3417. Doi:10.3390/app12031205.

[64] BROWN, R.; LEE, R. M. *2021 SANS Cyber Threat Intelligence (CTI) Survey*. [S.l.], 2021. Acessado em: 8/02/2022. Disponível em: <https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt43a990b140efaa96/6112a525f0c97e3949

[65] LUBIN, A. The reasonable intelligence agency. *Yale J. Int'l L.*, HeinOnline, v. 47, p. 119, 2022. Acessado em 21/11/2022. Disponível em: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/yjil47div=7id=page=>.

[66] LOWENTHAL, M. *Intelligence: From Secrets to Policy*. SAGE Publications, 2022. ISBN 9781071806395. Disponível em: <https://books.google.com.br/books?id=NbtiEAAAQBAJ>.

[67] CAVELTY, M.; MAUER, V. *The Routledge Handbook of Security Studies*. Routledge, 2010. (Routledge handbooks). ISBN 9781780343167. Disponível em: <https://books.google.com.br/books?id=-M3ljwEACAAJ>.

[68] BUCHANAN, B. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. [S.l.]: Harvard University Press, Cambridge, MA, 2020. ISBN 9780674987555.

[69] BUELL, L. *What is called ecoterrorism*. [S.l.], 2009. Acessado em: 14/02/2023. Disponível em: <https://dash.harvard.edu/handle/1/4262048>.

[70] FRIDMAN, O. *Russian"Hybrid Warfare": Resurgence and Politicization*. [S.l.]: Oxford University Press, 2018. ISBN:0190934735, 9780190934736.

[71] KEMP, S. et al. Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during covid-19. *Journal of Contemporary Criminal Justice*, v. 37, n. 4, p. 480–501, 2021. Disponível em: <https://doi.org/10.1177/10439862211027986>.

[72] CASCAVILLA, G.; TAMBURRI, D. A.; Van Den Heuvel, W.-J. Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers Security*, v. 105, p. 102258, 2021. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404821000821>.

[73] DEORA, R. S.; CHUDASAMA, D. Brief study of cybercrime on an internet. *Journal of Communication Engineering & Systems*, v. 11, n. 1, p. 1–6, 2021. Acessado em: 27/09/2022. Disponível em: <https://www.researchgate.net/profile/Dhaval-Chudasama/publication/352121472$_{B}rief_{S}study_{o}f_{C}ybercrime_{o}n_{a}n_{I}nternet/links/60ba1082a6fdcc22ead4$ $Study-of-Cybercrime-on-an-Internet.pdf$>.

[74] BROADHURST, R. et al. Organizations and cybercrime. *Available at SSRN 2345525*, 2013. Acessado em: 27/09/2022. Disponível em: <https://deliverypdf.ssrn.com/delivery.php?ID=687101067008103018029031003075080090096055058047

[75] UN. A more secure world: our shared responsibility: report of the secretary-general's high-level panel on threats, challenges and change. UN: The United Nations, 2004. Acessado em: 27/09/2022. Disponível em: <https://digitallibrary.un.org/record/542523>.

[76] VERMA, A.; SHRI, C. Cyber security: A review of cyber crimes, security challenges and measures to control. *Vision*, v. 0, n. 0, p. 09722629221074760, 0. Disponível em: <https://doi.org/10.1177/09722629221074760>.

[77] CHECKPOINT. *Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed*. [S.l.]. Acessado em: 29/08/2022. Disponível em: <https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed/>.

[78] BEAMAN, C. et al. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers Security*, v. 111, p. 102490, 2021. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S016740482100314X>.

[79] SMITH, S. Out of gas: A deep dive into the colonial pipeline cyberattack. In: *SAGE Business Cases*. [S.l.]: SAGE Publications: SAGE Business Cases Originals, 2022.

[80] FARMER, F. Cybercrime vs hacktivism: Do we need a differentiated regulatory approach? University of Exeter, 2022. Acessado em: 17/10/2022. Disponível em: <https://ore.exeter.ac.uk/repository/handle/10871/129654>.

[81] LISKA, A.; GALLO, T. *Ransomware: Defending against digital extortion*. [S.l.]: "O'Reilly Media, Inc.", 2016.

[82] CHESTI, I. A. et al. Evolution, mitigation, and prevention of ransomware. In: *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. [S.l.: s.n.], 2020. p. 1–6. Doi:10.1109/ICCIS49240.2020.9257708.

[83] YAMANY, B.; AZER, M. A.; ABDELBAKI, N. Ransomware clustering and classification using similarity matrix. In: *2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*. [S.l.: s.n.], 2022. p. 41–46. Doi:10.1109/MIUCC55081.2022.9781655.

[84] MELAND, P. H.; BAYOUMY, Y. F. F.; SINDRE, G. The ransomware-as-a-service economy within the darknet. *Computers Security*, v. 92, p. 101762, 2020. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404820300468>.

[85] BOURNE, V. *The State of Ransomware 2020*. [S.l.], 2020. Acessado em: 24/09/2022. Disponível em: <https://www.sophos.com/en-us/medialibrary/gated-assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>.

[86] DAVIS, J. et al. *Ransomware Task Force - Combating Ransomware*. [S.l.], 2021. Acessado em: 24/09/2022. Disponível em: <https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf>.

[87] KILOVATY, I. Cybersecuring the pipeline. *Houston Law Review*, v. 60, 2023. Acessado em: 04/10/2022. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract$_id = 4070074$>.

[88] GERMANOS, G.; GEORGIOU, N. How did cybercriminals 'survive'during the pandemic?". *Urban Crime. An international Journal*, v. 3, n. 2, p. 110–123, 2022. Acessado em: 04/10/2022. Disponível em: <https://ojs.panteion.gr/index.php/uc/article/view/291>.

[89] DOD/CISA/NSA/ACSC/NCSC. *Joint cybersecurity Advisory - 2021 Trends Show Increased Globalized Threat of Ransomware*. 2022. Acessado em: 22/11/2022. Disponível em: <https://media.defense.gov/2022/Feb/09/2002935687/-1/-1/0/2021$_T RENDS_S HOW_I NCREASED_G LOBALIZED_T HREAT_O F_R ANSOMWARE_2 0220209.P$

[90] BáTRLA, M.; HARAšTA, J. Releasing the hounds? disruption of the ransomware ecosystem through offensive cyber operations. In: *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*. [S.l.: s.n.], 2022. v. 700, p. 93–115. Doi:10.23919/CyCon55549.2022.9811074.

[91] USDT. *Treasury Sanctions Russia with Sweeping New Sanctions Authority*. 2021. Disponível em: `https://home.treasury.gov/news/press-releases/jy0127;`. Acessado em: 30/09/2022.

[92] HAYES, K. Ransomware: a growing geopolitical threat. *Network Security*, Elsevier, v. 2021, n. 8, p. 11–13, 2021. Doi:10.1016/S1353-4858(21)00089-1.

[93] EMERY, N. E. The myth of cyberterrorism. *Journal of Information Warfare*, Peregrine Technical Solutions, v. 4, n. 1, p. 80–89, 2005. ISSN 14453312, 14453347. Disponível em: <https://www.jstor.org/stable/26504019>.

[94] RAMADHAN, I. Cyber-terrorism in the context of proselytizing, coordination, security, and mobility. *International Relations Department of Universitas Pertamina, Islamic World and Politics*, v. 4, n. 2, 2020. Acessado em 13/10/2022. Disponível em: <https://pdfs.semanticscholar.org/b83a/2ebb65f7920570d2bc4e6b77a3d1199515b9.pdf>.

[95] DUNNING, M. *Britain and Terrorism: A Sociological Investigation*. Springer International Publishing, 2021. (Palgrave Studies on Norbert Elias). ISBN 9783030723002. Disponível em: <https://books.google.com.br/books?id=aX80EAAAQBAJ>.

[96] HOLBROOK, D.; HORGAN, J. Terrorism and ideology: Cracking the nut. *Perspectives on Terrorism*, Terrorism Research Initiative, v. 13, n. 6, p. 2–15, 2019. ISSN 23343745. Disponível em: <https://www.jstor.org/stable/26853737>.

[97] TERRORISM (from Encyclopedia of the Social Sciences, V 14, 1934). U.S. Department of State. Disponível em: <https://www.ojp.gov/ncjrs/virtual-library/abstracts/terrorism-encyclopedia-social-sciences-v-14-1934>.

[98] LEWIS, J. A. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic & International Studies Washington, DC, 2002. Acessado em: 11/10/2022. Disponível em: <https://www.steptoe.com/a/web/4586/231a.pdf>.

[99] LEWIS, J. A. The internet and terrorism. In: CAMBRIDGE UNIVERSITY PRESS. *Proceedings of the ASIL Annual Meeting*. 2005. v. 99, p. 112–115. Acessado em: 13/10/2022. Disponível em: <https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy$_files/files/media/csis/pubs/050401_internetandterrorism.pdf$>.

[100] CAVELTY, M. D.; MAUER, V. International ciip handbook 2006, vol. ii: Analyzing issues, challenges, and prospects. *International CIIP Handbook*, Center for Security Studies (CSS), ETH Zürich, 2006. Acessado em: 13/10/2022. Disponível em: <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/490/2/eth-31123-04$_2006_2.pdf$>.

[101] SHANDLER, R. et al. Cyber terrorism and public support for retaliation – a multi-country survey experiment. *British Journal of Political Science*, Cambridge University Press, v. 52, n. 2, p. 850–868, 2022. Doi: 10.1017/S0007123420000812.

[102] LAWSON, S. *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Taylor & Francis, 2019. (Routledge Studies in Conflict, Security and Technology). ISBN 9781315505596. Disponível em: <https://books.google.com.br/books?id=nfvADwAAQBAJ>.

[103] OTTIS, R. Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. In: ACADEMIC PUBLISHING LIMITED READING, MA. *Proceedings of the 7th European Conference on Information Warfare*. 2008. p. 163. Acessado em: 14/10/2022. Disponível em: <https://www.semanticscholar.org/paper/Analysis-of-the-2007-Cyber-Attacks-Against-Estonia-Ottis/b63d7ca0eb68bb24e9b9abc5fab8b828e1f5ddcb>.

[104] GULYAMOV, S. S.; KHOJIAMONULLOKHONOV, A. I. U. The concepts of"cyberterrorism"and the problems of its definition. *Central Asian Academic Journal of Scientific Research*, «Scientific Progress Markazi», v. 2, n. 5, p. 866–875, 2022. Acessado em: 14/10/2022. Disponível em: <https://cyberleninka.ru/article/n/the-concepts-of-cyberterrorism-and-the-problems-of-its-definition>.

[105] SVYRYDENKO, D.; MOŻGIN, W. Hacktivism of the anonymous group as a fighting tool in the context of russia's war against ukraine. 2022. Acessado em: 17/10/2022. Disponível em: <https://web.archive.org/web/20220619071241id$_{/http}$: $//www.fhijournal.org/journals/2022/17/FHI_17_{S}vyrydenkoMo_{g}in.pdf$>.

[106] SAMUEL, A. W. *Hacktivism and the future of political participation*. Harvard University, 2004. Acessado em: 24/10/2022. Disponível em: <https://www.proquest.com/openview/4272e6a40239e3f2aaaf9d0fc3672bae/1?pq-origsite=gscholarcbl=18750diss=y>.

[107] PRIYANDITA, G.; HOGEVEEN, B.; STEVENS, B. State-sponsored economic cyber-espionage for commercial purposes. 2022. Acessado em: 23/02/2023. Disponível em: <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2022-12/State-sponsored%20economic%20cyber-espionage$_{0}$.pdf>.

[108] GORWA, R.; SMEETS, M. Cyber conflict in political science: a review of methods and literature. SocArXiv, 2019. Acessado em: 23/02/2023. Disponível em: <https://osf.io/preprints/socarxiv/fc6sg/>.

[109] KARA, I. Cyber-espionage malware attacks detection and analysis: A case study. *Journal of Computer Information Systems*, Taylor Francis, v. 62, n. 6, p. 1253–1270, 2022. Doi: 10.1080/08874417.2021.2004566.

[110] GIOVANNELLI, D. Extraterritorial jurisdiction over cyber espionage: A new trend in international law or just an example of lawfare. *CONTEMPORARY MILITARY CHALLENGES/SODOBNI VOJAÅ KI IZZIVI*, v. 24, n. 2, p. 49–70, 2022. Doi:10.33179/bsv.99.svi.11.cmc.24.2.3. Disponível em: <https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.3>.

[111] BRASIL. *Política Nacional de Inteligência*. 2016. Acessado em: 28/02/2023. Disponível em: <http://www.planalto.gov.br/ccivil$_{0}$3/$_{a}to2015-2018/2016/decreto/D8793.htm$>.

[112] BOUTTON, A.; DOLAN, T. M. Enemies in the Shadows: On the Origins and Survival of Clandestine Clients. *International Studies Quarterly*, v. 65, n. 1, p. 146–159, 01 2021. ISSN 0020-8833. Disponível em: <https://doi.org/10.1093/isq/sqaa096>.

[113] ROTONDO, A.; SALVATI, P. Fake news, (dis)information, and the principle of nonintervention: Scope, limits, and possible responses to cyber election interference in times of competition. *The Cyber Defense Review*, Army Cyber Institute, p. 209–224, 2019. ISSN 24742120, 24742139. Disponível em: <https://www.jstor.org/stable/26846129>.

[114] SIMPLICITY, R. O. V. Electoral regulation research network/democratic audit of australia joint. Acessado em 28/02/2023. Disponível em: <https://law.unimelb.edu.au/_data/assets/pdf_file/0007/3786127/WP74_Dowling_2.pdf>.

[115] TUCKER, J. A. et al. Social media, political polarization, and political disinformation: A review of the scientific literature. *Political polarization, and political disinformation: a review of the scientific literature (March 19, 2018)*, 2018. Acessado em 28/02/2023. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id = 3144139>.

[116] KIM, S. et al. Operation framework including cyber warfare execution process and operational concepts. *IEEE Access*, v. 8, p. 109168–109176, 2020. Doi:10.1109/ACCESS.2020.3001286.

[117] CLARKE, R. A. The risk of cyber war and cyber terrorism. *Journal of International Affairs*, Journal of International Affairs Editorial Board, v. 70, n. 1, p. 179–181, 2016. ISSN 0022197X. Acessado em 24/02/2023. Disponível em: <https://www.jstor.org/stable/90012602>.

[118] LEWIS, J. A. *"CYBER WAR: DEFINITIONS, DETERRENCE AND FOREIGN POLICY"*. [S.l.], 2015. Acessado em 24/02/2023. Disponível em: <http://www.jstor.org/stable/resrep37706>.

[119] WELCH, L. D. *Cyberspace-The Fifth Operational Domain*. [S.l.], 2004. Acessado em: 13/09/2022. Disponível em: <https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace—the-fifth-operational-domain/2011-cyberspace—the-fifth-operational-domain.ashx>.

[120] JUDA, N. Literature review: Cyberwarfare: The next dimension in inter-state conflict or a misnomer? 2021. Acessado em: 12/12/2022. Disponível em: <https://www.researchgate.net/profile/Nate-Juda/publication/356360524_CYBERWARFARE_DEFINED_2/links/61969f84d7d1af224b045d17/CYBERWARFARE-DEFINED-2.pdf>.

[121] KISSEL, M.; KIM, N. C. The emergence of human warfare: Current perspectives. *American Journal of Physical Anthropology*, Wiley Online Library, v. 168, p. 141–163, 2019. Doi:10.1002/ajpa.23751.

[122] DATTA, P. Hannibal at the gates: Cyberwarfare & the solarwinds sunburst hack. *Journal of Information Technology Teaching Cases*, SAGE Publications Sage UK: London, England, 2021. Doi:10.1177/2043886921993126.

[123] ALFORD, L. D. Cyber warfare: A new doctrine and taxonomy. *United States Air Force*, 2001. Acessado em 05/09/2022. Disponível em: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.641.8312rep=rep1type=pdf>.

[124] IZYCKI, E.; VIANNA, E. W. Critical infrastructure: A battlefield for cyber warfare? In: ACADEMIC CONFERENCES LIMITED. *ICCWS 2021 16th International Conference on Cyber Warfare and Security*. [S.l.], 2021. p. 454.

[125] ALMEIDA, V. A.; DONEDA, D.; ABREU, J. de S. Cyberwarfare and digital governance. *IEEE Internet Computing*, v. 21, n. 2, p. 68–71, 2017.

[126] TORONTO, N. W. *Military Learning and Evolutions in Warfare in the Modern Era*. Oxford University Press, 03 2021. Disponível em: <https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-1880>.

[127] ROSCINI, M. Chapter 14: Cyber operations as a use of force. In: ____. *Research Handbook on International Law and Cyberspace*. Cheltenham, UK: Edward Elgar Publishing, 2021. ISBN 9781789904246. Doi:10.4337/9781789904253.00025.

[128] RID, T. Cyber war will not take place. *Journal of Strategic Studies*, Routledge, v. 35, n. 1, p. 5–32, 2012. Doi:10.1080/01402390.2011.608939.

[129] LEWIS, J. A. *Cyber War and Ukraine*. [S.l.], 2022. Acessado em: 01/12/2022. Disponível em: <https://www.csis.org/analysis/cyber-war-and-ukraine>.

[130] MAKOVSKY, D. The silent strike: How israel bombed a syrian nuclear installation and kept it secret. *The New Yorker*, v. 17, 2012. Acessado em: 06/10/2022. Disponível em: <https://www.newyorker.com/magazine/2012/09/17/the-silent-strike>.

[131] ANDREW, J.; GEERS, K. et al. 'compelling opponents to our will': The role of cyber warfare in ukraine. In: *Cyber war in perspective: Russian aggression against Ukraine*. NATO CCDCOE, 2015. p. 39–48. Acessado em 06/10/2022. Disponível em: <https://www.usna.edu/CyberDept/$_{f}iles/documents/CyberWarinPerspective_{L}ewis_{0}4.pdf$>.

[132] LOUI, R.; HOPE, W. Information warfare amplified by cyberwarfare and hacking the national knowledge infrastructure. In: IEEE. *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*. Orlando, 2017. p. 280–283. Doi:10.1109/DASC-PICom-DataCom-CyberSciTec.2017.59.

[133] DOURADO, M. E. B.; LEITE, A. C. C.; NOBRE, F. R. F. Guerra híbrida vs. gibridnaya voyna: os diferentes significados dos conflitos híbridos para o ocidente e para a rússia. *Revista da Escola de Guerra Naval, Rio de Janeiro*, v. 26, n. 1, p. 39–64, 2020. Acessado em: 19/09/2022. Disponível em: <https://scholar.google.com.br/scholar?hl=pt-BRas$_{s}dt = 0$

[134] PATERSON, T.; HANLEY, L. Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. *Australian Journal of In-*

ternational Affairs, Routledge, v. 74, n. 4, p. 439–454, 2020. Disponível em: <https://doi.org/10.1080/10357718.2020.1734772>.

[135] WHITE, S. P. *Understanding cyberwarfare: Lessons from the Russia-Georgia war*. [S.l.]: Modern War Institute at West Point, 2018.

[136] PACEPA, I.; RYCHLAK, R. *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*. [S.l.]: WND Books, 2013. ISBN: 9781936488605.

[137] LINEBARGER, P. Psychological warfare. Infantry Journal Press, 1948. Doi:10.1177/000271624825800139.

[138] DENNING, D. E. R. *Information warfare and security*. [S.l.]: Addison-Wesley New York, 1999.

[139] LEGUCKA, A. Russian disinformation: Old tactics–new narratives. In: *Disinformation, Narratives and Memory Politics in Russia and Belarus*. [S.l.]: Routledge. p. 22–42. ISBN: 9781003281597.

[140] CHNG, S. et al. Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, v. 5, p. 100167, 2022. ISSN 2451-9588. Disponível em: <https://www.sciencedirect.com/science/article/pii/S245195882200001X>.

[141] GANDHI, F.; PANSANIYA, D.; NAIK, S. Ethical hacking: Types of hackers, cyber attacks and security. *International Research Journal of Innovations in Engineering and Technology*, IRJIET (International Research Journal of Innovations in Engineering and Technology, v. 6, n. 1, p. 28, 2022. Acessado em: 25/11/2022. Disponível em: <https://www.proquest.com/openview/99b27c29320e151b9d151305dedef0d5/1?pq-origsite=gscholarcbl=5314840>.

[142] PHILLIPS, K. et al. Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences*, v. 2, n. 2, p. 379–398, 2022. ISSN 2673-6756. Disponível em: <https://www.mdpi.com/2673-6756/2/2/28>.

[143] BRASIL. *Política Nacional de Segurança de Infraestruturas Críticas*. 2018. Disponível em: =http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acessado em: 6/02/2022.

[144] USA. *National Cyber Strategy*. 2018. Disponível em: =trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acessado em: 6/02/2022.

[145] CISA. *Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response*. [S.l.], 2021. Acessado em: 26/11/2022. Disponível em: <https://www.cisa.gov/sites/default/files/publications/essential$_{c}ritical_{i}nfrastructure_{w}orkforce-guidance_{v}4.1_{5}08_{0}.pdf$>.

[146] NSA/CISA. *NSA/CISA Control System Defense: Know the Opponent*. 2022. Acessado em: 22/11/2022. Disponível em: <https://media.defense.gov/2022/Sep/22/2003083007/-1/-1/0/CSA$_ICS_Know_the_Opponent.PDF$>.

[147] NOGUCHI, M.; UEDA, H. An analysis of the actual status of recent cyberattacks on critical infrastructures. *NEC Technical Journal, Special Issue Cybersecurity*, v. 12, n. 2, p. 19–24, 2019. Acessado em: 26/11/2022. Disponível em: <https://dr.nec.com.onenec.net/en/global/techrep/journal/g17/n02/pdf/170204.pdf>.

[148] CHEN, M. China's data collection on us citizens: implications, risks, and solutions. *Journal of Science Policy e Governance*, v. 15, 2019. Disponível em: <http://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/chen$_jspg_v15.pdf$>.

[149] OPM. *OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats*. [S.l.], 2015. Acessado em: 12/11/2022. Disponível em: <https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/>.

[150] MAYMí, F. et al. Towards a definition of cyberspace tactics, techniques and procedures. In: *2017 IEEE International Conference on Big Data (Big Data)*. [S.l.: s.n.], 2017. p. 4674–4679. Doi:10.1109/BigData.2017.8258514.

[151] MITRE. *MITRE ATT&CK Matrix for Enterprise*. [S.l.]. Acessado em: 8/02/2022. Disponível em: <https://attack.mitre.org/tactics/enterprise/>.

[152] THORNTON, R.; MIRON, M. Towards the 'third revolution in military affairs'. *The RUSI Journal*, Routledge, v. 165, n. 3, p. 12–21, 2020. Doi:10.1080/03071847.2020.1765514.

[153] MWANGI, T.; ASAVA, T.; AKERELE, I. Cybersecurity threats in africa. In: ____. *The Palgrave Handbook of Sustainable Peace and Security in Africa*. Cham: Springer International Publishing, 2022. p. 159–180. ISBN 978-3-030-82020-6. Disponível em: <https://doi.org/10.1007/978-3-030-82020-6$_10$>.

[154] DHS. *(U//FOUO) DHS Bulletin: Russia Cyber Threat Overview Substantive Revision*. 2022. Acessado em: 04/11/2022. Disponível em: <https://publicintelligence.net/dhs-russia-cyber-threat-overview/>.

[155] MITRE. *MITRE ATT&CK Groups LAPSUS$*. [S.l.]. Acessado em: 01/12/2022. Disponível em: <https://attack.mitre.org/groups/G1004/>.

[156] MSTIC. *Microsoft Threat Intelligence Center - DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*. [S.l.]. Acessado em: 01/12/2022. Disponível em: <https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/>.

[157] ARUL, A. *Lapsus$ hack leaves NVIDIA in a tight spot*. [S.l.]. Acessado em: 01/12/2022. Disponível em: <hhttps://analyticsindiamag.com/lapsus-hack-leaves-nvidia-in-a-tight-spot/>.

[158] NEWMAN, L. H. *The Lapsus$ Hacking Group Is Off to a Chaotic Start*. [S.l.]. Acessado em: 01/12/2022. Disponível em: <https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/>.

[159] THEHACKERNEWS. *Everything We Learned From the LAPSUS$ Attacks*. [S.l.]. Acessado em: 01/12/2022. Disponível em: <https://thehackernews.com/2022/05/everything-we-learned-from-lapsus.html>.

[160] CISA. *Alert (AA21-291A) BlackMatter Ransomware*. [S.l.], 2022. Acessado em: 30/11/2022. Disponível em: <https://www.cisa.gov/uscert/ncas/alerts/aa21-291a>.

[161] SASON, D. *BlackMatter Ransomware: In-Depth Analysis Recommendations*. [S.l.]. Acessado em: 01/12/2022. Disponível em: <https://www.varonis.com/blog/blackmatter-ransomware>.

[162] PAGE, C. *BlackMatter ransomware gang says it's shutting down over law enforcement pressure*. [S.l.]. Acessado em: 01/12/2022. Disponível em: <https://techcrunch.com/2021/11/03/blackmatter-ransomware-shut-down/>.

[163] JAKUB, P. *Russia's war on Ukraine: Timeline of cyber-attacks*. [S.l.]. Acessado em: 02/12/2022. Disponível em: <https://www.europarl.europa.eu/thinktank/en/document/EPRS$_BRI(2022)733549$>.

[164] GREENBERG, A. *Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless*. [S.l.]. Acessado em: 02/12/2022. Disponível em: <https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/>.

[165] BOWEN, A. S. *Russian Cyber Units*. [S.l.]. Acessado em: 02/12/2022. Disponível em: <https://crsreports.congress.gov/product/pdf/IF/IF11718>.

[166] NICHOLS, S. *Ukraine: Russian cyber attacks aimless and opportunistic*. [S.l.]. Acessado em: 02/12/2022. Disponível em: <https://www.techtarget.com/searchsecurity/news/252526575/Ukraine-Russian-cyber-attacks-aimless-and-opportunistic>.

[167] RUIZ, D. *21 million free VPN users' data exposed*. [S.l.]. Acessado em: 03/12/2022. Disponível em: <https://www.malwarebytes.com/blog/news/2021/03/21-million-free-vpn-users-data-exposed>.

[168] CYBERNEWS. *One of the biggest Android VPNs hacked? Data of 21 million users from 3 Android VPNs put for sale*. [S.l.]. Acessado em: 03/12/2022. Disponível em: <https://cybernews.com/security/one-of-the-biggest-android-vpns-hacked-data-of-21-million-users/>.

[169] NATH, O. *21 Million VPN User Records Leaked on Telegram for Free*. [S.l.]. Acessado em: 03/12/2022. Disponível em: <https://www.spiceworks.com/it-security/data-security/news/data-of-millions-of-vpn-users-leaked/>.

[170] VPNMENTOR. *10GB Database Exposing VPN Users Dumped (for Free) on Telegram*. [S.l.]. Acessado em: 03/12/2022. Disponível em: <https://www.vpnmentor.com/blog/vpns-leaked-on-telegram/>.

[171] LEGALCLOUD. *Ataque Hacker ao STJ: Principais informações*. 2020. Acessado em: 01/03/2023. Disponível em: <https://legalcloud.com.br/ataque-hacker-stj/>.

[172] GATLAN, S. *Brazil's court system under massive RansomExx ransomware attack*. 2020. Acessado em: 01/03/2023. Disponível em: <https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack/>.

[173] PETRY, G. *STJ é vítima de ransomware e tem seus dados e os backups criptografados*. 2021. Acessado em: 01/03/2023. Disponível em: <https://thehack.com.br/stj-e-vitima-de-ransomware-e-tem-seus-dados-e-os-backups-criptografados/>.

[174] GONZAGA, J. *Hacker invade sistemas do STJ e criptografa processos e e-mails*. 2021. Acessado em: 01/03/2023. Disponível em: <https://blog.unimake.com.br/hacker-invade-sistemas-do-stj-e-criptografa-processos-e-e-mails/>.

[175] PAGANINI, P. *Brazil's court system shut down after a massive ransomware attack*. 2021. Acessado em: 01/03/2023. Disponível em: <https://securityaffairs.co/110484/malware/brazils-court-system-ransomware.html>.

[176] ZANIN, H. da S.; BERNARDES, P. H. D. A. Technology and access to justice during the pandemic: online dispute resolution development in brazil and japan. *Revista Tecnologia e Sociedade*, v. 18, n. 50, p. 1–18, 2022. Acessado em: 01/03/2023. Disponível em: <https://revistas.utfpr.edu.br/rts/article/view/13443>.

[177] TADEU, E. *Ataque ao STJ visava servidores de backup, nova tendência entre hackers*. 2021. Acessado em: 01/03/2023. Disponível em: <https://www.cisoadvisor.com.br/ataque-ao-stj-visou-servidores-de-backup-nova-tendencia-entre-hackers/>.

[178] BRITO, P. *STJ foi pego pelo RansomEXX. Alvo pode ter sido escolhido*. 2020. Acessado em: 01/03/2023. Disponível em: <https://www.cisoadvisor.com.br/ransomware-ransomexx-pegou-stj-alvo-pode-ter-sido-escolhido/>.

[179] CISO. *Análise do RansomEXX indica que atacante do STJ teve tempo*. 2020. Acessado em: 01/03/2023. Disponível em: <https://www.cisoadvisor.com.br/analise-do-ransomexx-indica-que-atacante-do-stj-teve-tempo/>.

[180] PALAZOLO, G. *RansomEXX — Análise do Ransomware Utilizado no Ataque ao STJ*. 2020. Acessado em: 01/03/2023. Disponível em: <https://gustavopalazolo.medium.com/ransomexx-an%C3%A1lise-do-ransomware-utilizado-no-ataque-ao-stj-918001ec8195>.