Desafios e Complexidades da Atribuição Cibernética

Augusto de Ornellas Abreu, João José Costa Gondim

Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE, Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, Brasil

augusto.ornellas@gmail.com, gondim@unb.br

Abstract. *The attribution of state-sponsored cyberattacks constitutes one of the main challenges of contemporary international security, involving technical, legal, and political complexities that compromise the accuracy of forensic investigations. This article analyzes methodological obstacles, cognitive biases, and geopolitical pressures that influence attribution processes, examining three paradigmatic cases: Mandiant's APT1 report (2013), the TV5Monde attack (2015), and the Olympic Destroyer campaign (2018). The research demonstrates how analytical failures, false flag operations, and increasing dependence on outsourced commercial intelligence introduce systematic distortions that favor erroneous conclusions with significant diplomatic repercussions. The study identifies that methodological opacity in the private sector, combined with commercial incentives and selection biases, compromises analytical neutrality and weakens states' strategic autonomy. As a contribution, it proposes institutional reforms to strengthen governmental analytical capabilities, implement structured analytical techniques, and establish international legal frameworks that define rigorous evidentiary standards for cyber attribution.*

Resumo. *A atribuição de ataques cibernéticos patrocinados por Estados constitui um dos principais desafios da segurança internacional contemporânea, envolvendo complexidades técnicas, jurídicas e políticas que comprometem a acurácia das investigações forenses. Este artigo analisa os obstáculos metodológicos, vieses cognitivos e pressões geopolíticas que influenciam processos de atribuição, examinando três casos paradigmáticos: o relatório da Mandiant sobre o APT1 (2013), o ataque à TV5Monde (2015) e a campanha Olympic Destroyer (2018). A pesquisa demonstra como falhas analíticas, operações de falsa bandeira e a crescente dependência de inteligência comercial terceirizada introduzem distorções sistemáticas que favorecem conclusões equivocadas com repercussões diplomáticas significativas. O estudo identifica que a opacidade metodológica do setor privado, combinada com incentivos comerciais e vieses de seleção, compromete a neutralidade analítica e fragiliza a autonomia estratégica dos Estados. Como contribuição, propõe reformas institucionais para fortalecer capacidades analíticas governamentais, implementar técnicas de análise estruturada e estabelecer marcos jurídicos internacionais que definam padrões probatórios rigorosos para a atribuição cibernética.*

1. Introdução

Atribuição, no contexto da cibersegurança, se refere ao conjunto de ações e técnicas analíticas empregadas na investigação de ataques cibernéticos a fim de esclarecer sua origem e autoria[1]. Rid e Buchanan (2015) descrevem-na como um processo complexo e iterativo, que se desenrola de maneira incremental, raramente linear[2]. Mesmo que

não seja possível, muitas vezes, determinar o indivíduo ou grupo de fato responsáveis, indicadores de comprometimento coletados no decorrer da análise do incidente – domínios e IPs contatados, hashes de arquivos maliciosos, engenharia reversa de código – constituem elementos mínimos importantes para o robustecimento da segurança de ativos de rede de modo a prevenir novos ataques.

Em especial quando tem como foco campanhas maliciosas dirigidas contra infraestruturas críticas de Estado, revela ser uma atividade multifacetada que envolve aspectos técnicos complexos que exigem o emprego de equipes altamente especializadas e diversas[3]. A isso frequentemente se associam nuances estratégicas e consequências políticas significativas[4], [5].

O crescimento significativo de operações cibernéticas atribuídas a Estados diretamente ou a grupos supostamente patrocinados por esses faz com que a correta identificação dos responsáveis se torne essencial para a construção de respostas adequadas nos âmbitos diplomático, legal e militar. No entanto, o processo de atribuição permanece desafiador, devido ao anonimato típico do ciberespaço, às técnicas de dissimulação e ofuscação empregadas por grupos de ameaças avançadas persistentes (APT), e à relação complexa entre evidências técnicas e considerações políticas[6], [7].

Uma atribuição equivocada pode desencadear sanções indevidas, tensionar relações diplomáticas ou mesmo escalar para uma resposta militar contra atores inocentes[8]. Por outro lado, operações de bandeira falsa (*false flag*) podem desviar investigações na direção contrária dos reais perpetradores, provendo-lhes negação plausível suficiente para evadirem sanções. Nesse ecossistema complexo, atribuições públicas podem por si sós carregar peso político relevante, mas frequentemente são desprovidas do rigor metodológico e probatório necessário de um ponto de vista legal[9], [10].

Nesse contexto, o presente artigo elencará questões técnicas, políticas e regulatórias inerentes à atividade de atribuição cibernética, assim como desafios analíticos relevantes a serem superados. Descreverá brevemente, em seguida, três casos paradigmáticos de controvérsias ou equívocos de atribuição, em que falhas metodológicas e rigor analítico insuficiente levaram a conclusões incorretas com consequências geopolíticas significativas.

Por fim, debaterá a dependência excessiva de provedores privados de inteligência de ciberameaças, observada na tendência crescente de governos terceirizarem a coleta de indicadores, esforços analíticos e etapas críticas da atribuição a equipes e empresas privadas, não sujeitas aos limites legais do poder público, com métodos pouco transparentes, não abertos à verificação independente.

2. Atribuição cibernética: uma abordagem multidisciplinar

2.1. Indicadores técnicos

A investigação cibernética opera em múltiplas dimensões técnicas que coletivamente contribuem para a acurácia e confiabilidade das conclusões forenses. Existem diversas categorias de indicadores técnicos que devem ser coletados, documentados e analisados de forma holística para fundamentar as etapas analíticas subsequentes. Ataques cibernéticos são dinâmicos por natureza, e modelos rapidamente se tornam obsoletos por não acompanharem as mudanças constantes no cenário de ameaças.

A análise de logs de sistema, fluxos de rede, endereços IP, padrões de registro de domínios e provedores de hospedagem utilizados constitui a camada de base da

atribuição técnica. No entanto, como Tsagourias e Farrell (2020)[6] destacam, o nível de confiança das evidências frequentemente varia, e sempre existe um nível de granularidade na atribuição técnica baseada na análise de infraestruturas afetadas ou utilizadas. Grupos APT costumam explorar essa granularidade por meio de técnicas sofisticadas de ofuscação.

Atores avançados empregam arquiteturas de proxy complexas, com o uso de infraestruturas comprometidas, serviços de nuvem e ferramentas legítimas de anonimização. Especialistas do mercado [11], [12] chamam a atenção para a crescente utilização de serviços online e plataformas em nuvem (GitHub, Dropbox, AWS, Google) como meios de entrega de artefatos maliciosos, hospedagem de infraestruturas de comando e controle e repositório inicial para exfiltração de dados sensíveis. Tais atores se valem do fato de que organizações tradicionalmente implementam controles baseados na premissa de que ameaças emanam de domínios maliciosos e endereços IP suspeitos e, para evadir tais medidas, abusam da confiança depositada em plataformas legítimas, utilizando-as em todas as etapas de ataque. Aproveitam também a presença global das redes de distribuição de conteúdo (CDNs) dessas plataformas para atuar de forma mais eficiente independentemente da localização da vítima.

Uma camada adicional da investigação consiste na análise forense de malwares e demais artefatos encontrados na etapa de coleta. A análise estática e dinâmica de código malicioso pode prover indicadores cruciais de atribuição sob a forma de *timestamps* de compilação, *strings* conhecidas, escolha de linguagens de programação, estilos de escrita do código e artefatos embutidos (dados de localização linguística, codificação de teclado, etc).

A esse conjunto de dados e artefatos que descrevem e caracterizam tecnicamente um incidente cibernético dá-se o nome de “Indicadores de Comprometimento” (IoCs). Bianco (2013) os categoriza por meio do diagrama a que deu o nome de “Pirâmide da Dor”[13], reproduzido na Fig. 1 abaixo. Quanto mais próximo da base, mais fácil é para o analista descobrir o indicador, mas igualmente mais simples é para o atacante evadir a detecção ao abandoná-lo por outro da mesma classe. Por outro lado, IoCs mais acima no diagrama são incrementalmente mais complicados de se encontrar durante a investigação de um ataque, mas também são, na perspectiva do ator malicioso, mais imprescindíveis e difíceis de se substituir.

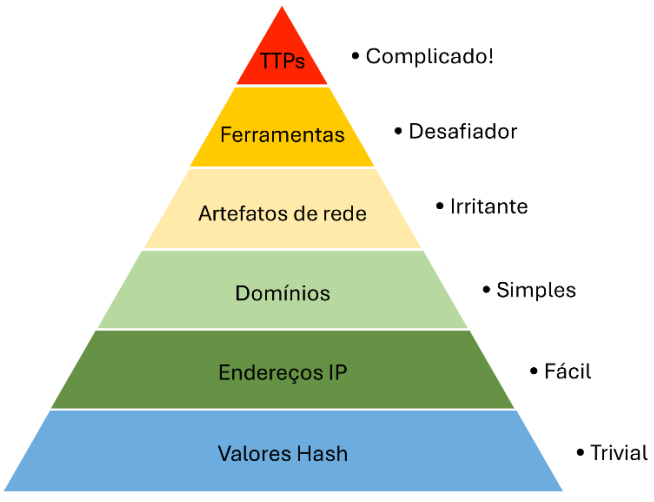

Figura 1. Pirâmide da Dor (Bianco, 2013), tradução livre

O modelo sugere, assim, que a análise técnica busca idealmente inferir, a partir do conjunto de indicadores e artefatos coletados, padrões comportamentais particulares que possam servir como assinatura específica (*digital fingerprinting*) do ator malicioso em questão. A fim de facilitar o compartilhamento dessas assinaturas comportamentais e auxiliar na atribuição de ataques por meio da comparação desses padrões ao longo do tempo, criaram-se ontologias ou taxonomias chamadas de Táticas, Técnicas e Procedimentos (TTPs) organizadas em *frameworks* analíticos, associados a extensas bases de dados de ataques e atores conhecidos, compartilhados na comunidade de inteligência cibernética. O mais difundido desses modelos é a matriz MITRE ATT&CK[1], mantida e disponibilizada gratuitamente por uma fundação financiada pelo Departamento de Defesa estadunidense.

2.2. Dimensão legal e política

As complexidades jurídicas e políticas envolvidas na atribuição precisa de ciberataques aos seus verdadeiros perpetradores decorrem, essencialmente, da ausência de padrões uniformes de prova e da falta de consenso quanto aos marcos legais que deveriam reger a responsabilidade estatal por operações cibernéticas. O direito internacional não estabelece limiares claros para a natureza e quantidade de evidências necessárias para comprovar tal responsabilidade. Isso contrasta com processos criminais domésticos, que contam com parâmetros consolidados, como o "além de qualquer dúvida razoável" (*beyond reasonable doubt*). Essa lacuna jurídica cria o que Davis (2022)[14] denomina "tolerância invertida à atribuição equivocada": um paradoxo em que o direito internacional exige perfeição na atribuição, mas não fornece diretrizes sobre como alcançá-la.

O Manual de Tallinn[4], produzido sob os auspícios da Organização do Tratado do Atlântico Norte (OTAN), embora influente no meio acadêmico, representa apenas as posições pessoais de especialistas em direito internacional, não constituindo prática estatal vinculante; por isso, sua adoção efetiva mesmo entre Estados da OTAN permanece limitada. Apesar de identificar 154 regras ou fundamentos aplicáveis a operações cibernéticas, o Manual reconhece amplas lacunas de consenso quanto a padrões de atribuição e a marcos de responsabilidade estatal. Grandes potências resistem ativamente a esforços para estabelecer padrões formais de prova na atribuição cibernética. Elas agem de tal forma para preservar suas próprias capacidades de inteligência ofensiva e manter flexibilidade em suas atribuições públicas. Utilizam-nas, no entanto, como instrumentos de *deterrence* contra seus adversários usuais, com o emprego contumaz da estratégia de *naming and shaming*[15].

No contexto das Nações Unidas, iniciativas como o Grupo de Peritos Governamentais (Group of Governmental Experts, GGE) e o Grupo de Trabalho Aberto (Open-Ended Working Group, OEWG), alcançaram consenso sobre 11 normas voluntárias e não vinculantes sobre comportamento responsável dos Estados no ciberespaço[16]. Contudo, tais normas oferecem apenas diretrizes genéricas, que requerem que os Estados "considerem todas as informações relevantes, incluindo os desafios da atribuição no ambiente das TIC", sem definir quais elementos probatórios seriam suficientes para respaldar tal atribuição. Essas normas, propostas originalmente em 2015, representam um consenso de princípios, e não de padrões operacionais, deixando os Estados vítimas sem parâmetros objetivos sobre os limiares de prova necessários para justificar contramedidas ou buscar reparação internacional. É digno de

[1] Disponível em https://attack.mitre.org/

nota que os Estados apenas concordaram que “deveriam” (*should*) exercer a devida diligência (*due diligence*), e não que “são obrigados” (*must*) a fazê-lo, o que revela a relutância em assumir obrigações vinculantes que possam limitar suas prerrogativas soberanas.

Na prática, esse vácuo jurídico resulta em um sistema *ad hoc* de atribuição política, cujos padrões probatórios variam significativamente com base em disputas geopolíticas de poder, e não em requisitos jurídicos uniformes. O regime de sanções cibernéticas da União Europeia, por exemplo, estipula expressamente que “a adoção de medidas restritivas não implica a atribuição de responsabilidade internacional por ciberataques a um terceiro Estado”, evidenciando a resistência institucional a processos formais de atribuição legal[17], [18]. Essa postura reforça o descompasso estrutural entre as capacidades técnicas de investigação forense e os mecanismos de responsabilização jurídica. Isso permite que operações cibernéticas sofisticadas causem danos expressivos, enquanto seus autores – não só em “nações párias”, mas também em potências ocidentais – exploram as lacunas de atribuição para manter a negação plausível (*plausible deniability*). Sem consenso sobre padrões mínimos de prova e sem um marco institucional robusto para avaliar alegações de atribuição, o sistema jurídico internacional mostra-se estruturalmente inadequado para enfrentar os desafios impostos por operações cibernéticas patrocinadas por Estados em um ambiente digital cada vez mais interconectado.

2.3. Desafios analíticos

Vieses cognitivos constituem um obstáculo central à produção de análises precisas em inteligência sobre ameaças cibernéticas, pois distorcem sistematicamente os processos analíticos e ampliam a probabilidade de formulação de conclusões com base em evidências insuficientes. Entre esses vieses, o de confirmação — a tendência de buscar, interpretar e privilegiar informações que confirmem crenças ou hipóteses já existentes[19] — assume relevância particular no contexto da cibersegurança, em que analistas tendem a elaborar hipóteses iniciais sobre agentes de ameaça logo nas etapas preliminares de uma investigação. Quando indivíduos exploram uma teoria para determinado problema, tendem a buscar confirmar suas convicções apenas procurando e encontrando indícios que sustentem suas suposições, ao passo que ignoram sinais contraditórios que poderiam sugerir explicações alternativas[20].

No âmbito específico da atribuição cibernética, isso se traduz, por exemplo, em situações em que analistas conferem maior atenção a dados coletados que reforcem sua hipótese inicial, negligenciando indícios que apontem que o ator malicioso esteja, de fato, voltado para outro objetivo. A amplitude desse viés é corroborada por pesquisas experimentais. Um estudo, envolvendo 65 especialistas em perícia digital de oito países, verificou que “os examinadores foram influenciados por informações contextuais” e apresentaram “baixa consistência” ao avaliar as exatas mesmas evidências[21] em outros contextos. Em estudos focados no comportamento de atacantes cibernéticos, constatou-se que o viés de confirmação leva à supervalorização de evidências que sustentam a hipótese inicial. Essa insistência, mesmo diante de provas contrárias, reflete dilemas analíticos frequentes na atuação profissional em inteligência de ameaças[22].

A lógica comercial que estrutura a indústria de inteligência de ameaças contribui para um viés de seleção sistemático, que reforça estereótipos geopolíticos e leva à superatribuição a determinados Estados-nação. Pesquisas revelam que ameaças sofisticadas contra alvos de alto perfil são priorizadas em relatórios comerciais,

enquanto ameaças contra organizações da sociedade civil tendem a ser negligenciadas ou totalmente desconsideradas[23]. Essa distorção, que privilegia alvos financeiramente relevantes em detrimento de uma cobertura abrangente, acaba por enviesar a atribuição em favor de grupos APT vinculados a grandes potências adversárias.

O viés de ancoragem, caracterizado pela dependência excessiva da primeira informação recebida, intensifica o problema quando analistas recebem estimativas preliminares sobre a identidade de um agente e passam a basear todas as análises subsequentes nessa estimativa, descartando inadvertidamente dados atualizados que poderiam indicar outras conclusões. Vieses de autoridade introduzem distorções adicionais na atribuição, ao atribuir peso diferenciado a evidências em função da reputação da fonte e não de seu mérito intrínseco. O viés de autoridade ocorre quando as opiniões de figuras de referência são tomadas como fatos e seus pedidos atendidos com pouca ou nenhuma hesitação. No contexto da cibersegurança, isso pode levar analistas a aceitar conclusões apresentadas por fornecedores comerciais de prestígio ou por agências governamentais sem realizar a devida verificação independente.

Já o viés de disponibilidade leva analistas a superestimar a probabilidade ou relevância de eventos que vêm facilmente à mente, normalmente por serem recentes, emocionalmente impactantes ou amplamente divulgados[24]. Esse mecanismo favorece sistematicamente a atribuição a agentes de ameaça ligados a incidentes de grande repercussão midiática ou ocorridos recentemente, levando a uma ênfase desproporcional em ataques recentes ou de alto perfil na avaliação de novas evidências. A combinação desses vieses com incentivos comerciais resulta no que pesquisadores denominam percepção distorcida da ameaça, na qual a inteligência de ameaças subrepresenta riscos à sociedade civil e, ao mesmo tempo, superestima riscos a organizações com capacidade de adquirir serviços de inteligência privada[23].

Técnicas de análise estruturada oferecem abordagens metodológicas baseadas em evidências para mitigar vieses cognitivos na análise de inteligência sobre ameaças cibernéticas, ainda que sua eficácia varie consideravelmente conforme a metodologia e o contexto de aplicação. A Análise de Hipóteses Concorrentes (AHC) é a técnica mais difundida, concebida para ajudar o analista a questionar seu modelo mental inicial e estimular a consideração de hipóteses alternativas, promovendo uma busca mais ampla por informações do que a que normalmente ocorreria em rotinas de trabalho intensas[25]. Entretanto, pesquisas experimentais recentes, descritas nos trabalhos ainda controversos de Martha Whitesmith[26], [27], colocam em dúvida sua real eficácia, apontando que a AHC não teria apresentado impacto mitigador estatisticamente significativo na incidência do viés de confirmação.

A técnica do Advogado do Diabo mostra-se mais promissora[28]: pesquisas empíricas demonstram que, quando aplicada corretamente, é capaz de questionar premissas e desafiar evidências apresentadas, reduzindo riscos de vieses cognitivos e fomentando perspectivas alternativas. Estudos em organizações de inteligência militar identificaram que analistas juniores tendem a aceitar mais prontamente críticas formuladas pelo advogado do diabo e que essa abordagem favorece a produção de relatórios mais equilibrados e objetivos, ao confrontar o pensamento dominante e identificar alternativas. Contudo, sua eficácia depende fortemente da reputação, experiência, status e capacidade de liderança de quem desempenha o papel.

Pesquisas recentes[29], por fim, sugerem que as agências de inteligência devem concentrar-se em melhorar globalmente a qualidade da produção analítica, e não apenas em reduzir vieses, valendo-se de métodos estatísticos pós-analíticos, como a recalibração e a agregação ponderada pelo desempenho dos julgamentos dos analistas, aliados a

programas de aperfeiçoamento humano com foco no bem-estar físico e mental dos profissionais.

3. Casos controversos de atribuição

3.1. Relatório sobre o APT1 da Mandiant (2013)

A publicação, em fevereiro de 2013, do relatório da Mandiant "*APT1: Exposing One of China's Cyber Espionage Units*"[30] constituiu um marco na atribuição comercial de operações cibernéticas, ao mesmo tempo em que expôs os riscos associados a metodologias analíticas insuficientes em avaliações de alto impacto. As críticas de Jeffrey Carr[31], [32], [33], publicadas poucos dias depois, identificaram falhas relevantes na abordagem do relatório, em particular o não uso de técnicas de análise estruturada que demonstrariam facilmente a existência de lacunas e omissões significativas. Carr argumentou que a metodologia da Mandiant se aproximava do que Richards Heuer[34] descreveu como *satisficing*: a tendência a "optar pela primeira solução que parece satisfatória, em vez de examinar todas as hipóteses possíveis e identificar qual é a mais consistente com as evidências".

Essa postura conduziu a um foco exclusivo em evidências que sustentavam a conclusão prévia de que o grupo APT1 corresponderia à Unidade 61398 do Exército de Libertação Popular (ELP) da China, enquanto demais alternativas explicativas foram sistematicamente negligenciadas. A alegação central de atribuição apoiou-se em evidências circunstanciais sumarizadas na Tabela 12 do relatório, que apontavam supostas "características correspondentes entre APT1 e a Unidade 61398". Baseou-se, especialmente, na identificação de blocos de IP utilizados pelo ator malicioso que apontavam para o distrito de Pudong em Xangai, onde haveria uma instalação da referida unidade militar do ELP.

Críticos ressaltaram, contudo, o caráter genérico dessas características — tão amplas que "poderiam ser aplicadas a praticamente qualquer grupo hacker ativo" — e apontaram que tantas correlações elementares são epistemologicamente fracas, comparáveis a "identificar um homicida pela observação de que homicidas têm dois braços, duas pernas e matam pessoas". O argumento da proximidade geográfica mostrou-se particularmente frágil: como observou Carr, a existência de uma guarnição militar na região não demonstra nada, dado o amplo espalhamento de instalações militares em todas as regiões da China. Ademais, o fato de terem sido usados endereços IP localizados no distrito de Pudong tampouco indica a correlação proposta no relatório, uma vez que essa região de Xangai conta com mais de 5 milhões de habitantes e abriga o centro financeiro e tecnológico da metrópole chinesa.

Analistas independentes[35], [36] propuseram diversas hipóteses alternativas que explicariam as evidências reunidas pela Mandiant, entre elas o uso por terceiros de infraestrutura chinesa em operações de bandeira falsa, ações de grupos criminais atuando a partir da China sem direção estatal, ou operações por procuração conduzidas por outros Estados por intermédio de servidores chineses. Ademais, o contexto comercial envolvendo o relatório suscitou dúvidas sobre sua objetividade analítica: o modelo de negócios da Mandiant, empresa posteriormente adquirida pela Google em setembro de 2022, criava incentivos para divulgar atribuições de alto perfil capazes de gerar visibilidade midiática e atrair contratos governamentais. A publicação coincidiu com um período de elevada tensão político-diplomática entre Estados Unidos e China em matéria de ciberespionagem, o que alimentou a hipótese de que fatores comerciais e políticos teriam influenciado o processo analítico. O impacto do relatório extrapolou o ambiente acadêmico: influenciou decisões governamentais e contribuiu, em maio de 2014, para a

apresentação de acusações pelo Departamento de Justiça dos EUA contra cinco supostos membros da Unidade 61398, ações essas que, em grande parte, se apoiaram na metodologia contestada da Mandiant.

3.2. Ataque à TV5Monde (2015)

O ataque cibernético de 8 de abril de 2015 contra a emissora francesa TV5Monde exemplifica o emprego sofisticado de técnicas de bandeira falsa por atores patrocinados por Estados, com o objetivo de induzir ao erro processos de atribuição e obter vantagens estratégicas. Inicialmente apresentado como uma ação jihadista[37], o incidente consistiu na tomada do site e das contas de redes sociais da emissora, na substituição de conteúdo por material pró-Estado Islâmico e na interrupção das transmissões dos onze canais da TV5Monde por aproximadamente quatro horas. Um grupo autodenominado "CyberCaliphate" reivindicou a autoria, publicando documentos supostamente pertencentes a militares franceses. Autoridades francesas, inclusive o então ministro do Interior, chegaram a atribuir o ataque ao grupo extremista[38]. O contexto geopolítico de então parecia corroborar essa conclusão: apenas dois meses antes, o jornal satírico francês Charlie Hebdo fora atacado por extremistas islâmicos, em reposta a charges do semanário que retratavam o profeta do Islã, resultando na morte de 12 pessoas. O grupo "CyberCaliphate" empreendeu outros ataques contra alvos britânicos e estadunidenses no mesmo período.

Entretanto, análises forenses posteriores[39] demonstraram que se tratava de uma operação de bandeira falsa orquestrada pelo APT28 (conhecido também como Fancy Bear, Sofacy ou Pawn Storm), grupo mais comumente ligado por boa parte das empresas de cibersegurança ao GRU, agência de inteligência militar russa. Investigadores da FireEye verificaram que o site do CyberCaliphate estava hospedado no mesmo bloco de IP de outras infraestruturas atribuídas ao APT28 e utilizava o mesmo servidor de nomes e registrador empregados em campanhas anteriores do grupo[40]. Embora também isso possa ser falsificado (como se verá no próximo estudo de caso), metadados do código malicioso indicavam que o software havia sido escrito em um teclado cirílico e compilado durante horários compatíveis com o expediente em São Petersburgo ou Moscou[41]. Fontes judiciais francesas confirmaram a identificação do malware Sednit — ligado à campanha Pawn Storm — e o rastreamento da infraestrutura para sistemas característicos das operações atribuídas ao APT28.

O caso TV5Monde evidenciou aspectos relevantes das modernas operações de bandeira falsa que agravam a complexidade da atribuição: primeiro, a capacidade dos atacantes de sustentar a dissimulação por mais de dois meses, período no qual autoridades e mídia internacional inicialmente mantiveram a atribuição a grupos jihadistas; segundo, a extensão da estratégia de engano além da mera ofuscação técnica — incluindo narrativas e provas fabricadas — com o intuito de legitimar a hipótese falsa. Esse sucesso em confundir a atribuição teria trazido benefícios estratégicos ao suposto Estado patrocinador, permitindo conduzir operações ofensivas contra um aliado da OTAN sem imediata retaliação ou repercussões diplomáticas, e demonstrou como bandeiras falsas exploram tensões geopolíticas e percepções pré-existentes para camuflar atividades de inteligência estatal. Apenas 10 anos depois, em 29 de abril de 2025, o governo francês fez a atribuição pública do ataque à inteligência militar russa[42].

3.3. Campanha *Olympic Destroyer* (2018)

O ataque conhecido como *Olympic Destroyer*, dirigido aos Jogos Olímpicos de Inverno de Pyeongchang, Coreia do Sul (2018), constitui, possivelmente, o caso mais sofisticado

de operação de dissimulação para confundir a atribuição documentado na literatura de segurança cibernética. Projetado para enganar peritos forenses, o incidente[43] paralisou temporariamente sistemas de TI durante a cerimônia de abertura — afetando o site oficial, monitores de exibição, redes Wi-Fi e transmissões — e, sobretudo, empregou múltiplas técnicas de falsa bandeira que levaram diferentes empresas de segurança a atribuir o malware a Estados distintos com base em indicadores técnicos cuidadosamente plantados[44].

Nos dias subsequentes à descoberta, firmas de cibersegurança chegaram a conclusões contraditórias[45], [46], [47]: a divisão Talos da Cisco apontou semelhanças com operações russas anteriores (p. ex., NotPetya, Bad Rabbit); a CrowdStrike identificou elementos remanescentes de ransomware russo (XData); a Intezer detectou fragmentos idênticos a ferramentas vinculadas a grupos chineses (APT3, APT10), inclusive um componente criptográfico inédito em outros registros; e a análise inicial da Kaspersky sugeriu uma correspondência perfeita entre metadados do malware e componentes associados ao grupo Lazarus, da Coreia do Norte, uma "assinatura" considerada 100% coincidente nos bancos de dados da empresa[48].

O esclarecimento posterior das técnicas empregadas no Olympic Destroyer decorreu do trabalho detalhado do pesquisador Igor Soumenkov (Kaspersky), que demonstrou tratar-se de uma falsificação sofisticada[49]: a chamada "impressão digital" do Lazarus havia sido inserida artificialmente no *rich header*, bloco de dados cifrados presente no cabeçalho do arquivo executável, mediante técnica avançada que pressupunha conhecimento pormenorizado de práticas forenses de atribuição. Como observou Vitaly Kamluk (Kaspersky), "é como se um criminoso tivesse roubado o DNA de outra pessoa e o deixado na cena do crime". A descoberta provou que os autores estudaram deliberadamente as metodologias de atribuição e confeccionaram indícios espúrios para explorar aquelas práticas[50].

O caso *Olympic Destroyer* ilustra tendências alarmantes nas operações patrocinadas por Estados: a instrumentalização da confusão de atribuição como objetivo estratégico, o domínio sofisticado de técnicas forenses por atores avançados e a capacidade de manipular analistas experientes a partir de evidências deliberadamente plantadas. Em última instância, mostra que a proliferação de bandeiras falsas compromete seriamente a credibilidade analítica e oferece aos perpetradores mecanismos para se ocultarem atrás de conclusões públicas equivocadas.

4. Governos e a dependência de inteligência de ameaças terceirizada

Diante dos desafios apresentados, os Estados contemporâneos têm delegado, em escala e profundidade inéditas, autoridade analítica em cibersegurança a provedores comerciais de inteligência sobre ameaças. Pesquisas[51] demonstram que 65% de todas as atribuições públicas entre 2015 e 2020 foram feitas por empresas, e outros 10% foram fruto de anúncios conjuntos de instituições públicas e privadas. Esse fenômeno configura um cenário preocupante: a capacidade de avaliação independente do setor público se enfraquece e vieses sistêmicos são introduzidos na formulação de políticas e decisões de segurança nacional. Estudos de Maschmeyer, Deibert e Lindsay[23] apontam que a inteligência comercial apresenta vieses estruturais que distorcem a compreensão do cenário de ameaças — "ameaças de alto nível a vítimas de grande visibilidade são priorizadas nos relatórios comerciais, enquanto ameaças a organizações da sociedade civil, que não dispõem de recursos para custear defesas cibernéticas avançadas, tendem a ser negligenciadas ou excluídas". Esse viés de seleção não decorre

apenas de preferências analíticas, mas de incentivos de mercado que favorecem clientes com capacidade de pagar por serviços *premium*, gerando, nas palavras dos autores, "uma amostra truncada do conflito cibernético que sub-representa os ataques à sociedade civil e distorce o debate acadêmico e a política pública".

A opacidade metodológica e as pressões competitivas inerentes ao mercado de inteligência comercial ampliam essas distorções e comprometem o rigor analítico[52]. Metodologias de atribuição são frequentemente tratadas como propriedade intelectual exclusiva, resultando em análises que não se prestam à verificação independente ou à revisão por pares — procedimentos essenciais para atribuir confiabilidade a avaliações de inteligência. Estudos comparativos[53] entre provedores líderes de mercado revelam inconsistências preocupantes: pesquisadores encontraram "quase nenhuma sobreposição" entre grandes fornecedores, com médias de convergência situando-se entre 2,5% e 4,0% mesmo para atores de ameaça de acompanhamento corrente. Tais discrepâncias apontam para uma cobertura analítica limitada ou desacordos fundamentais quanto à identificação de ameaças, enquanto agências governamentais passam a depender cada vez mais dessas avaliações sem mecanismos próprios de verificação. Além disso, a circulação temporal da inteligência comercial levanta dúvidas: informações competitivas frequentemente aparecem em *feeds* rivais com atraso médio de cerca de um mês, o que questiona se os fornecedores realmente proporcionam alertas precoces ou apenas reempacotam dados públicos.

A insuficiência de capacidades analíticas governamentais tem gerado dependências que fragilizam a autonomia estratégica do Estado em questões de cibersegurança. Nota-se, à guisa de exemplo, inclusive em orientações oficiais do Reino Unido[54], que "departamentos podem dispor de conhecimentos e experiência limitados em CTI, o que dificulta a aquisição de ferramentas adequadas"; pesquisas corroboram que a variabilidade da qualidade entre fornecedores comerciais produz avaliações internas inconsistentes e compromete respostas políticas coordenadas. A situação agrava-se quando análises comerciais são publicadas de forma a, inadvertidamente, comprometer operações de inteligência estatais, dado que atores privados não estão sujeitos às mesmas restrições de segurança operacional das agências governamentais. Romanosky e Boudreaux[55] alertam para outro risco: capacidades de atribuição do setor privado podem "rivalizar com as de algumas agências de inteligência governamentais", mas geralmente operam sem supervisão e mecanismos de responsabilização equivalentes.

Os incentivos de mercado que orientam a produção de inteligência tendem a conflitar com a exigência de neutralidade analítica, algo que parece ser subestimado pelos governos[56]. Estratégias de marketing motivam a divulgação de atribuições de alto impacto que atraem atenção midiática e clientes, por vezes extrapolando as evidências de fato disponíveis. Observa-se, ademais, que a dinâmica do mercado favorece os economicamente mais potentes em detrimento de uma cobertura de ameaças abrangente, criando um viés sistemático em favor de organizações capazes de pagar por serviços adicionais. A busca pela vantagem de ser o primeiro a divulgar (*first-mover advantage*) pode levar a análises apressadas destinadas a captar mídia e contratos, com custo para a acurácia. Soma-se a isso a pressão pela retenção de clientes, que pode induzir provedores a produzir inteligência que confirme vieses dos contratantes e modelos de ameaça pré-existentes, em vez de desafiá-los criticamente.

As implicações geopolíticas desse viés exigem atenção particular. Os incentivos comerciais parecem favorecer atribuições que coincidem com narrativas e expectativas de governos ocidentais[57]: provedores têm tendência a imputar ataques sofisticados a países considerados adversários — notadamente China, Rússia, Irã e Coreia do Norte — e

raramente publicam relatórios sobre atores maliciosos vinculados a governos ocidentais ou aliados[58]. Esse padrão reflete menos uma certeza analítica e mais um alinhamento com demandas de mercado e posicionamento competitivo em um setor dominado pelo Ocidente. Como resultado, as práticas de atribuição sem dúvida tendem a reforçar narrativas geopolíticas preexistentes e ocultar ameaças que não se alinham a incentivos financeiros privados, potencialmente distorcendo avaliações estratégicas e respostas políticas.

A solução dessas questões demanda ações integradas que restaurem a independência analítica estatal, sem desprezar os aportes legítimos da inteligência comercial. Entre as propostas estão a criação de órgãos de atribuição transnacionais e independentes[59], capazes de fornecer análises neutras desimpedidas por vieses mercadológicos, e a imposição de requisitos de transparência que obriguem a divulgação de metodologias e critérios de avaliação de evidências[60]. O fortalecimento das capacidades governamentais constitui a intervenção central: investir em análises independentes que funcionem como contrapeso às avaliações comerciais e, simultaneamente, estimulem a elevação de padrões por meio de competição por qualidade. Um maior engajamento com a academia também se mostra promissor: pesquisadores defendem "a incorporação de coletores de dados do meio acadêmico, que ofereçam interpretações alternativas alicerçadas em processos independentes de geração de conhecimento"[61], contribuindo para mitigar o viés comercial. Essas reformas devem abarcar não só habilidades técnicas, mas também incentivos institucionais, de modo a reorientar a relação entre setor público e inteligência comercial; esta última deve ser insumo, e não substituto, para análises governamentais rigorosas e independentes.

5. Conclusão

A atribuição de ataques cibernéticos emerge como uma das questões mais complexas e politicamente sensíveis da segurança internacional contemporânea, demandando rigor metodológico que equilibre imperfeições técnicas inerentes, lacunas jurídicas persistentes e pressões geopolíticas crescentes. Como demonstram os casos analisados, desde o controverso relatório da Mandiant sobre o APT1 até as sofisticadas manobras de bandeira falsa do Olympic Destroyer, o não uso de técnicas de análise estruturada e a dependência excessiva de evidências circunstanciais têm levado a conclusões equivocadas com repercussões diplomáticas significativas. Esses episódios ilustram que vieses cognitivos, incentivos comerciais e a instrumentalização política da atribuição cibernética comprometem sistematicamente a qualidade analítica, criando um ambiente em que operações de dissimulação se tornam cada vez mais sofisticadas e bem-sucedidas.

A crescente terceirização da inteligência de ameaças para provedores comerciais introduz distorções estruturais que privilegiam narrativas alinhadas aos interesses de mercado, negligenciando ameaças à sociedade civil e reforçando percepções geopolíticas pré-existentes. A opacidade metodológica inerente ao setor privado, combinada com pressões competitivas por divulgações de alto impacto midiático, compromete a neutralidade analítica essencial para avaliações confiáveis. Essa dependência fragiliza a autonomia estratégica dos Estados, que passam a formular políticas de segurança nacional baseadas em análises sujeitas a vieses comerciais e metodologias não verificáveis de maneira independente.

Diante de tais desafios, torna-se imperativo fortalecer as capacidades analíticas governamentais mediante investimentos em análise independente e implementação

sistemática de técnicas de análise estruturada. Somente por meio de reformas institucionais que sustentem a independência analítica estatal e estabeleçam marcos jurídicos internacionais para padrões de prova será possível mitigar os riscos de atribuições equivocadas e suas consequências para a estabilidade internacional. A inteligência comercial deve complementar, não substituir, análises governamentais robustas, garantindo que decisões estratégicas se baseiem em avaliações técnicas sólidas e não em narrativas enviesadas e moldadas por motivações comerciais.

Referências Bibliográficas

[1] R. Morgan and D. Kelly, "A Novel Perspective on Cyber Attribution," in *Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019)*, N. van der Waag-Cowling and L. Leenen, Eds., Stellenbosch, Mar. 2019, pp. 609–617.

[2] T. Rid and B. Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, vol. 38, pp. 4–37, Jan. 2015, doi: 10.1080/01402390.2014.977382.

[3] F. Skopik and T. Pahi, "Under false flag: using technical artifacts for cyber attack attribution," *Cybersecurity*, vol. 3, no. 1, p. 8, Dec. 2020, doi: 10.1186/s42400-020-00048-4.

[4] M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. Cambridge: Cambridge University Press, 2017. doi: 10.1017/9781316822524.

[5] F. J. Egloff, "Public attribution of cyber intrusions," *J Cybersecur*, vol. 6, no. 1, 2020, doi: 10.1093/cybsec/tyaa012.

[6] N. Tsagourias and M. Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges," *European Journal of International Law*, vol. 31, no. 3, pp. 941–967, Aug. 2020, doi: 10.1093/ejil/chaa057.

[7] W. C. Banks, "The bumpy road to a meaningful international law of cyber attribution," *AJIL Unbound*, vol. 113, pp. 191–196, 2019, doi: 10.1017/aju.2019.32.

[8] L. Kello, *The Virtual Weapon and International Order*, 1st ed. New Haven: Yale University Press, 2017.

[9] W. Banks, "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0," *Tex Law Rev*, vol. 95, no. 7, pp. 1487–1513, Jun. 2017, [Online]. Available: https://www.washingtonpost.com/world/

[10] A. Kastelic, "Non-Escalatory Attribution of International Cyber Incidents," 2022. Accessed: Jul. 06, 2025. [Online]. Available: https://unidir.org/wp-content/uploads/2023/05/UNIDIR_Non-Escalatory_Attribution_International_Cyber_Incidents.pdf

[11] M. Tolulope, "Examples of False Flags in Cybersecurity: Everything You Need to Know." Accessed: May 06, 2025. [Online]. Available: https://tolumichael.com/examples-of-false-flags-in-cybersecurity/

[12] Tranchulas, "The Trust Hijack: How Cybercriminals Are Weaponizing Legitimate Platforms in 2025." Accessed: Jul. 29, 2025. [Online]. Available: https://tranchulas.com/how-cybercriminals-are-weaponizing-legitimate-platforms/

[13] D. Bianco, "The pyramid of pain," Enterprise Detection & Response. Accessed: Apr. 29, 2025. [Online]. Available: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

[14] J. K. Davis, "Developing Applicable Standards of Proof for Peacetime Cyber Attribution," 2022, *NATO Cooperative Cyber Defence Centre of Excellence*. Accessed: Jul. 26, 2025. [Online]. Available: https://ccdcoe.org/uploads/2022/03/Jeremy-K.-Davis-Standards_of_Attribution.pdf

[15] M. Finnemore and D. B. Hollis, "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity," *European Journal of International Law*, vol. 31, no. 3, pp. 969–1003, Aug. 2020, doi: 10.1093/ejil/chaa056.

[16] B. Hogeveen, "The UN Cyber Norms: How Do They Guide the Responsible Development and Use of Offensive Cyber Capabilities?," *The Cyber Defense Review*, vol. 7, no. 4, pp. 123–142, 2022.

[17] S. Poli and E. Sommario, "The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions," *German Law*

Journal, vol. 24, no. 3, pp. 522–536, Apr. 2023, doi: 10.1017/glj.2023.25.
[18] I. Brunner, "Attributing cyber operations under International law: Political and legal aspects," *Questions of International Law*, vol. 110, pp. 27–43, Jun. 2025.
[19] V. Cipan, "Cognitive biases in intelligence analysis and their mitigation (debiasing)." Accessed: Jul. 28, 2025. [Online]. Available: https://viborc.com/cognitive-biases-intelligence-analysis-mitigation/
[20] M. Cunningham, "How Cognitive Bias Leads to Reasoning Errors in Cybersecurity." Accessed: Jul. 31, 2025. [Online]. Available: https://digitalisationworld.com/blogs/55821/how-cognitive-bias-leads-to-reasoning-errors-in-cybersecurity
[21] N. Sunde and I. E. Dror, "A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making," *Forensic Science International: Digital Investigation*, vol. 37, Jun. 2021, doi: 10.1016/j.fsidi.2021.301175.
[22] S. Huang *et al.*, "PsybORG+: Modeling and Simulation for Detecting Cognitive Biases in Advanced Persistent Threats," in *Proceedings - IEEE Military Communications Conference MILCOM*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/MILCOM61039.2024.10773763.
[23] L. Maschmeyer, R. J. Deibert, and J. R. Lindsay, "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society," *Journal of Information Technology and Politics*, vol. 18, no. 1, pp. 1–20, 2021, doi: 10.1080/19331681.2020.1776658.
[24] Intelligence and National Security Alliance, "Strategies for Addressing Bias in Insider Threat Programs," Jan. 2022. Accessed: Jul. 22, 2025. [Online]. Available: https://www.insaonline.org/docs/default-source/default-document-library/2022-white-papers/bias-and-insider-threat-programs-paper.pdf
[25] R. J. Heuer, "How Does Analysis of Competing Hypotheses (ACH) Improve Intelligence Analysis?," Oct. 2005. Accessed: Aug. 01, 2025. [Online]. Available: https://pherson.org/wp-content/uploads/2013/06/06.-How-Does-ACH-Improve-Analysis_FINAL.pdf
[26] M. Whitesmith, "The efficacy of ACH in mitigating serial position effects and confirmation bias in an intelligence analysis scenario," *Intelligence and National Security*, vol. 34, no. 2, pp. 225–242, Feb. 2019, doi: 10.1080/02684527.2018.1534640.
[27] M. Whitesmith, *Cognitive Bias in Intelligence Analysis*. Edinburgh University Press, 2020.
[28] E. Shewring, "The Application of the Devil's Advocacy Technique to Intelligence Analysis," *National Security Journal*, vol. 6, no. 2, Oct. 2024, doi: 10.36878/nsj20240925.03.
[29] D. R. Mandel and D. Irwin, "Beyond Bias Minimization: Improving Intelligence with Optimization and Human Augmentation," *International Journal of Intelligence and CounterIntelligence*, vol. 37, no. 2, pp. 649–665, 2024, doi: 10.1080/08850607.2023.2253120.
[30] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 2013. Accessed: May 27, 2025. [Online]. Available: https://services.google.com/fh/files/misc/mandiant-apt1-report.pdf
[31] J. Carr, "Mandiant APT1 Report Has Critical Analytical Flaws." Accessed: May 27, 2025. [Online]. Available: https://jeffreycarr.blogspot.com/2013/02/mandiant-apt1-report-has-critical.html
[32] J. Carr, "More on Mandiant's APT1 Report: Guilt by Proximity and Wright Patterson AFB." Accessed: May 27, 2025. [Online]. Available: https://jeffreycarr.blogspot.com/2013/02/more-on-mandiants-apt1-report-guilt-by.html
[33] J. Carr, "Mandiant's APT1 'Mission' Problem." Accessed: May 28, 2025. [Online]. Available: https://jeffreycarr.blogspot.com/2013/03/mandiants-apt1-mission-problem.html
[34] R. J. Heuer, *Psychology_of_Intelligence_Analysis*. Center for the Study of Intelligence, Central Intelligence Agency, 1999.
[35] O. Rochford, "Chinese Whispers, Chinese Lies: Analyzing Mandiant's APT1 Report." Accessed: May 29, 2025. [Online]. Available: https://www.securityweek.com/chinese-whispers-chinese-lies-analyzing-mandiants-apt1-report/
[36] G. Koo and L.-C. Wang, "Shoddy evidence and past hypocrisy weaken US cyber-spying charges," Global Times. Accessed: Jun. 01, 2025. [Online]. Available: https://www.globaltimes.cn/content/766334.shtml

[37] Reuters, “French broadcaster TV5Monde hit by Islamist hackers.” Accessed: Jul. 01, 2025. [Online]. Available: https://www.reuters.com/article/us-france-television-islamists-idUSKBN0N00HA20150409/
[38] A. Chrisafis and S. Gibbs, “French media groups to hold emergency meeting after Isis cyber-attack,” The Guardian. Accessed: Jul. 01, 2025. [Online]. Available: https://www.theguardian.com/world/2015/apr/09/french-tv-network-tv5monde-hijacked-by-pro-isis-hackers
[39] ANSSI, “Retour technique de l’incident de TV5Monde,” SSTIC 2017. Accessed: Jul. 17, 2025. [Online]. Available: https://www.sstic.org/2017/presentation/2017_cloture/
[40] P. Paganini, “FireEye claims Russian APT28 hacked France’s TV5Monde Channel,” Security Affairs. Accessed: Jul. 10, 2025. [Online]. Available: https://securityaffairs.com/37710/hacking/apt28-hacked-tv5monde.html
[41] J. Menn and L. Thomas, “France probes Russian lead in TV5Monde hacking: sources,” Reuters. Accessed: Jul. 10, 2025. [Online]. Available: https://www.reuters.com/article/us-france-russia-cybercrime-idUSKBN0OQ2GG20150610/
[42] TV5Monde, “Le renseignement militaire russe derrière le piratage de la campagne de Macron en 2017 et le sabotage de TV5MONDE en 2015.” Accessed: Jul. 18, 2025. [Online]. Available: https://information.tv5monde.com/international/le-renseignement-militaire-russe-derriere-le-piratage-de-la-campagne-de-macron-en
[43] K. Grohmann, “Games organizers confirm cyber attack, won’t reveal source,” Reuters. Accessed: Jul. 19, 2025. [Online]. Available: https://www.reuters.com/article/us-olympics-2018-cyber/games-organizers-confirm-cyber-attack-wont-reveal-source-idUSKBN1FV036/
[44] A. Greenberg, “The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History,” Wired. Accessed: Jul. 09, 2025. [Online]. Available: https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/
[45] Kaspersky, “OlympicDestroyer is Here to Trick the Industry,” Securelist. Accessed: Jul. 19, 2025. [Online]. Available: https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/
[46] P. Rascagnères and W. Mercer, “Who Wasn’t Responsible for Olympic Destroyer,” in *Virus Bulletin Conference 2018*, Montreal, Oct. 2018.
[47] K. Townsend, “Researchers Warn Against Knee-Jerk Attribution of ‘Olympic Destroyer’ Attack,” SecurityWeek. Accessed: Jul. 20, 2025. [Online]. Available: https://www.securityweek.com/researchers-warn-against-knee-jerk-attribution-olympic-destroyer-attack/
[48] E. Kovacs, “Sophisticated False Flags Planted in Olympic Destroyer Malware,” SecurityWeek. Accessed: Jul. 20, 2025. [Online]. Available: https://www.securityweek.com/sophisticated-false-flags-planted-olympic-destroyer-malware/
[49] Kaspersky, “The devil’s in the Rich Header,” Securelist. Accessed: Jul. 19, 2025. [Online]. Available: https://securelist.com/the-devils-in-the-rich-header/84348/
[50] Kaspersky, “The Olympic False Flag: How infamous OlympicDestroyer malware was designed to confuse cybersecurity community.” Accessed: Jul. 19, 2025. [Online]. Available: https://www.kaspersky.com/about/press-releases/the-olympic-false-flag
[51] G. Derian-Toth *et al.*, “Opportunities for Public and Private Attribution of Cyber Operations,” 2021, *NATO Cooperative Cyber Defence Centre of Excellence*.
[52] A. Zrahia, “Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views,” *J Cybersecur*, vol. 4, no. 1, pp. 1–16, Jan. 2018, doi: 10.1093/cybsec/tyy008.
[53] X. Bouwman, H. Griffioen, J. Egbers, C. Doerr, B. Klievink, and M. Van Eeten, “A different cup of TI? The added value of commercial threat intelligence,” in *29th USENIX Security Symposium*, Aug. 2020.
[54] Home Office Cyber Security Programme, “Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts,” Mar. 2019.
[55] S. Romanosky and B. Boudreaux, “Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government,” *International Journal of Intelligence and CounterIntelligence*, vol. 34, no. 3, pp. 463–493, 2021, doi: 10.1080/08850607.2020.1783877.
[56] C. Bing, “In the opaque world of government hacking, private firms grapple with allegiances,” Cyberscoop. Accessed: Jul. 31, 2025. [Online]. Available:

https://cyberscoop.com/cybersecurity-research-reports-kaspersky-symantec-microsoft-us-government/
[57] L. Yoffe, E. Matania, and U. Sommer, “The rise of responsible behavior: Western commercial reports on Western cyber threat actors,” *Contemp Secur Policy*, vol. 46, no. 3, pp. 429–454, 2025, doi: 10.1080/13523260.2025.2498711.
[58] J. Tidy, “Why is it so rare to hear about Western cyber-attacks?,” BBC. Accessed: Jul. 28, 2025. [Online]. Available: https://www.bbc.com/news/technology-65977742
[59] F. Delerue, “Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations,” *Questions of International Law*, vol. 106, pp. 5–21, 2024.
[60] J. S. Davis *et al.*, *Stateless attribution: toward international accountability in cyberspace*. RAND Corporation, 2017.
[61] F. J. Egloff and M. Dunn Cavelty, “Attribution and Knowledge Creation Assemblages in Cybersecurity Politics,” *J Cybersecur*, vol. 7, no. 1, pp. 1–12, 2021, doi: 10.1093/cybsec/tyab002.