Pontifícia Universidade Católica do Rio de Janeiro

Bernardo Beiriz Marques Barbosa

Cibersegurança mais-que-humana:

a agência dos não-humanos a partir do *spyware* Pegasus e da Teoria Ator-Rede

Trabalho de conclusão de curso

Trabalho de Conclusão de Curso apresentado ao Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) como requisito parcial para obtenção do título de bacharel em Relações Internacionais.

Orientador: Luisa Cruz Lobato
Segundo leitor: Louise Marie Hurel

Rio de Janeiro

Julho de 2024

Agradecimentos

Encontrar as palavras certas para agradecer pode parecer mais difícil que a mobilização das inúmeras ideias e conceitos que apresento ao longo deste trabalho. Agradeço inicialmente aos meus pais, Giselle e José Guilherme, meus primeiros professores. Obrigado por todo o carinho, amor, suporte e direcionamento, elementos que permitiram a minha caminhada até aqui. Aos meus avós, maternos e paternos, àqueles que conheci e aos que não pude conhecer, agradeço por terem me dado dois pais, educadores e amigos. À minha família como um todo, Hugo, Raul, Nida, Raul José, Zé, Renato, Luciana, Marcelo, Renata, obrigado por fazerem parte de inúmeros momentos que me permitiram chegar até aqui.

Aos meus irmãos, Celso Leonardo e Daniel, obrigado pelo amor, carinho e amizade. Aprendi e aprendo muito com vocês todos os dias e tenho muita sorte de poder crescer ao lado de vocês dois. Aos meus outros irmãos, Felipe e Davi, obrigado por nossa duradoura e infinita amizade, pelos momentos de alegria e de companheirismo que proporcionamos uns aos outros.

Minha trajetória no mundo acadêmico não seria possível sem os professores da Escola Parque – Barra, onde estudei por muitos anos antes de chegar na universidade. Tive ali inúmeras memórias felizes, assim como meu processo de formação enquanto cidadão.

Meu caminho nas Relações Internacionais não seria o mesmo sem o apoio de todos os professores do IRI, aos quais serei eternamente grato. Entre as várias pessoas com as quais tive a oportunidade de aprender e de trocar, gostaria de agradecer especialmente à professora Isabel Rocha de Siqueira. O Programa de Educação Tutorial, liderado de maneira brilhante pela Isabel, foi responsável por consolidar minha paixão pela pesquisa, mostrando o que podem ser as RI para fora das paredes da Academia. À minha geração do PET, Juliane, Nathan, Daniel e Maria Clara, obrigado por compartilharem essa caminhada comigo.

Aos meus colegas de curso, em especial Daniel, Pedro, Rubens e Rafaela, agradeço por terem tornado a minha jornada na universidade uma experiência baseada nos laços de um grupo. Enfrentamos juntos uma pandemia e aulas online, e, por meio de um grupo de WhatsApp, construímos uma amizade que carregarei para sempre comigo.

A composição deste trabalho não seria possível sem a orientação dos dois nomes que estampam sua capa: Luisa Lobato e Louise Marie Hurel. Agradeço à Luisa por todo seu trabalho de orientação, que envolveu muito mais que nossas trocas sobre o conteúdo presente nestas páginas. Obrigado por me ajudar a desenvolver as ferramentas necessárias para enxergar o que esse trabalho deveria e poderia ser, fazendo com que eu tenha conseguido transformar um conjunto de ideias abstratas, um desejo, em um conjunto de páginas razoavelmente coerentes.

Agradeço à Louise por ter aceitado ser a segunda leitora desse trabalho e por toda sua orientação ao longo dos últimos anos. Sua abertura para conversar com um graduando em RI, que ainda cursava seus semestres iniciais, deu início a uma caminhada no campo da Cibersegurança e da Governança da Internet que me trouxe inúmeras experiências inesquecíveis e oportunidades de aprendizado.

Parte desse trabalho foi escrita em Lyon, na França, onde moro atualmente com aquela que esteve presente tanto nos momentos de euforia na escrita, quanto nos de *writer's block*. À Rafaela, meu amor eterno, dedico minhas palavras de carinho, amor e amizade. Obrigado por todos os desafios e aventuras enfrentados lado-à-lado. Escrever é um ato de coragem e ao seu lado aprendo a ser cada vez mais corajoso.

Resumo

Beiriz Marques Barbosa, Bernardo. **Cibersegurança mais-que-humana: a agência dos não-humanos a partir do spyware Pegasus e da Teoria Ator-Rede.** Rio de Janeiro, 2024. Trabalho de conclusão de curso – Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

A cibersegurança enquanto objeto de estudos das Relações Internacionais é atravessada tanto pelos pontos fortes como pelas limitações da disciplina. As teorizações sobre agência tradicionalmente encontradas nas RI destinam um foco demasiado aos humanos, de maneira que colocam em segundo plano a relevância dos não-humanos. Isto gera implicações importantes para o estudo da cibersegurança, uma vez que essa é baseada em uma mélange entre humanos e não-humanos em interação. O presente trabalho resgata contribuições da Teoria Ator-Rede (ANT) e dos Estudos de Ciência e Tecnologia (STS) com o objetivo de demonstrar como entidades não-humanas também podem ser agentes da cibersegurança. Utilizo a metodologia de "seguir os atores" para traçar as associações realizadas pelo spyware Pegasus, argumentando que o vírus deve ser enxergado como mais do que uma ferramenta, podendo ser considerado ator e agente da cibersegurança e da Política Internacional.

Palavras-chave

Cibersegurança; Teoria Ator-Rede; Pegasus; Estudos de Ciência e Tecnologia;

Abstract

Beiriz Marques Barbosa, Bernardo. **More-than-human cybersecurity: Non-human agency as seen through the Pegasus spyware and Actor-Network Theory**. Rio de Janeiro, 2024. Trabalho de conclusão de curso – Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

Cybersecurity as an object of study in International Relations is crossed by both the strengths and limitations of the discipline. The theorisations on agency traditionally found in IR devote too much focus to humans, so that they place the relevance of non-humans in the background. This has important implications for the study of cybersecurity, which is based on a mélange of interacting humans and non-humans. This paper draws on contributions from Actor-Network Theory (ANT) and Science and Technology Studies (STS) in order to demonstrate how non-human entities can also be agents of cybersecurity. I use the "follow the actors" methodology to trace the associations made by Pegasus spyware, arguing that the virus should be seen as more than a tool, and can be considered an actor and agent of cybersecurity and International Politics.

Keywords

Cybersecurity; Actor-Network Theory; Pegasus; Science and Technology Studies

Sumário

Lista de figuras

The world is a dangerous place, Elliott, not because of those who do evil,
but because of those who look on and do nothing
Mr. Robot

1. Introdução

A cibersegurança adquiriu crescente relevância como objeto de estudos das Relações Internacionais (RI) ao longo dos últimos anos. Parafraseando Brandon Valeriano e Ryan C. Maness (2018), "a importância da cibersegurança como uma questão emergente nas Relações Internacionais (RI) não pode ser exagerada; o que pode ser exagerado é a novidade desse domínio" (p. 259, tradução nossa). Trata-se de um campo com numerosas contribuições ao longo dos anos, com diferentes escolas de pensamento das RI, metodologias e focos analíticos já tendo sido utilizados para pensar as interseções entre cibersegurança e política internacional.

As análises sobre cibersegurança desenvolvidas a partir do ferramental teórico-metodológico das RI são atravessadas tanto pelas capacidades como pelas incapacidades dessa disciplina. Características tradicionalmente encontradas em estudos de RI, como o antropocentrismo[1], (foco demasiado nos elementos humanos) e o estadocentrismo (centralidade do Estado enquanto unidade de análise) serão portanto transportadas e traduzidas para os estudos sobre cibersegurança (Fouad, 2021; Dwyer et al., 2022).

Diversos movimentos de "virada" (do inglês, *turn*) na disciplina de Relações Internacionais buscaram trabalhar sobre as limitações identificadas até então. Atualmente, as RI parecem "em meio à realização - quase simultânea - de uma série de viradas diferentes, da estética à afetiva, da histórica à prática, da dos novos materialismos à queer" (Baele, Bettiza, 2020, p. 1, tradução nossa). É no contexto dessa confluência de "viradas" que realizo o presente trabalho, buscando entender de que maneira os estudos sobre cibersegurança podem se beneficiar desses movimentos de reorientação, expandindo suas fronteiras de análise e compreensão.

---

[1] Um importante movimento de questionamento sobre o antropocentrismo das Relações Internacionais é desenvolvido também por autores dedicados ao estudo da ecologia e da Política Internacional. Um exemplo pode ser encontrado no livro organizado por Joana Castro Pereira e André Saramago, que discute o conceito de natureza "não-humana" e as RI. Os autores argumentam que uma transição da disciplina para um momento pós-antropocêntrico "deve integrar as relações entre a natureza humana e não humana em seu estudo do "internacional", buscando compreender a interconexão inerente entre a política mundial e o sistema terrestre" (2020, p. 4, tradução nossa)

As “viradas” representam a construção de perspectivas alternativas para o estudo sobre cibersegurança, afastando-se da perspectiva *mainstream* (Dwyer et al, 2022), algo que abordarei ao longo do capítulo 2. Esse movimento pode ser interpretado como a construção de uma “cibersegurança crítica”, capaz de “pluralizar e contestar o que é a cibersegurança e a quem ela se destina” (Dwyer et al, 2022, p. 3, tradução nossa). Nesse sentido, a expansão do conceito de cibersegurança responde a uma necessidade expandir sua capacidade de diálogo com novas temáticas e sujeitos, uma vez que a:

> cibersegurança, pelo menos em suas formas contemporâneas, não afeta apenas um indivíduo típico, branco, masculino e unitário no Norte Global, mas também atua em diversas comunidades, em interseção com dinâmicas de gênero, privação socioeconômica, mercados financeiros e agências não humanas (Dwyer et al., 2022, p. 3, tradução nossa).

Em meio a esse mais amplo e heterogêneo movimento de teorização, debruço-me sobre o papel dos elementos não-humanos, questão especialmente relevante para a cibersegurança. A relevância de um estudo sobre os não-humanos advém justamente da “composição” da cibersegurança, do que ela “é” de fato. Podemos entendê-la como sendo construída a partir das relações entre tecnologias e seres humanos (Dwyer et al, 2022), ou até como uma “gama multifacetada de tecnologias, processos, práticas e arranjos sociotécnicos complexos, coagulando-se em torno dessa preocupação com a segurança no e por meio do espaço cibernético” (Stevens, 2019, p. 4-5, tradução nossa).

Argumento ao longo do presente trabalho que a relevância dos não-humanos é tradicionalmente subjugada pela disciplina de RI, e por consequência, pelos estudos da cibersegurança que nascem da interseção entre esses dois campos. Segundo Fouad, analisar a agência, ou a capacidade de agir, apenas a partir da subjetividade humana é insuficiente, pois está sendo deixado de lado o “papel dos não-humanos na co-construção da segurança” (2021, p. 5, tradução nossa). Estudar a cibersegurança enquanto co-construção de humanos e não-humanos é um dos objetivos do presente trabalho, o que será possibilitado a partir da análise do *spyware* Pegasus e sua circulação global.

Para isso, recorro às ferramentas desenvolvidas em meio a uma das “viradas” nas Relações Internacionais, a aproximação da disciplina com os

Estudos sobre Ciência e Tecnologia (do inglês, *Science and Technology Studies*, STS). A introdução de ideias oriundas dos STS surge como tentativa de "descrever e compreender como a ciência e a tecnologia participam da mudança do mundo em termos materiais, sociais, tecnológicos, políticos e morais" (Liebetrau, Christensen, 2020, p. 7, tradução nossa).

"De que maneira podemos enxergar os artefatos sociotécnicos, ou não-humanos, atuando na cibersegurança" é um dos questionamentos que sustenta o presente ensaio de investigação, mas por onde podemos começar a respondê-lo?

Resgatando princípios da Teoria Ator-Rede (do inglês, *Actor-Network Theory*, ANT) apresentados por Salter (2019), o pesquisador deve buscar "'seguir os atores' - sejam esses atores humanos ou não humanos - e suspender intencionalmente a crença em 'escalas de análise pré-determinadas'" (p. 4, tradução nossa). Tal movimento de pesquisa possibilitaria que tanto atores humanos como não-humanos fossem levados em consideração nas análises, abandonando tendências antropocêntricas que conferissem vieses ao olhar do pesquisador. Seguindo os comandos de Latour (2005) descritos por Salter (2019), proponho seguir um "ator" em específico, o *spyware* Pegasus. Permito-me dar um passo atrás ao longo dos próximos parágrafos para o benefício da contextualização.

O aparelho celular de Emmanuel Macron, a esposa do jornalista saudita Jamal Khashoggi e um conjunto de escritórios em Herzliya, Israel, podem inicialmente parecer elementos distantes entre si. Um exercício de observação atenta e paciente, entretanto, pode pouco a pouco revelar algumas das conexões existentes entre esses: sua relação direta com o *spyware*[2] Pegasus, desenvolvido pela empresa israelense NSO Group. Essa ferramenta é de alta complexidade, capaz de invadir, monitorar e extrair dados de dispositivos celulares de maneira remota, muitas vezes sendo capaz de encobrir os rastros de sua atividade nesses aparelhos (Marczack et al., 2018). O nome "Pegasus" faz referência ao cavalo branco alado da mitologia grega, capaz de "percorrer distâncias impossíveis a

[2] Definição de spyware segundo a Amnesty International (2023): "Spyware é um software que permite que um operador obtenha acesso secreto a informações de um sistema ou dispositivo de computador de destino" (tradução nossa). Os materiais da Amnesty Internationaltambém podem ser utilizados como referência para mais informações sobre termos associados (disponíveis em Inglês):
https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/ (Acesso em 24 de Março de 2024)

lugares inalcançáveis e ajudar a alcançar o inalcançável" (Leander, 2021, p. 206, tradução nossa).

O *spyware* de origem israelense faz parte de um mais amplo mercado de "ferramentas de investigação"[3], ocupando posição de destaque no mesmo, justamente por sua capacidade de intrusão e adaptabilidade. Funciona com base em vulnerabilidades *zero-day* e é capaz de performar invasões no formato *zero-click* (Amnesty International, 2021). Em outras palavras, sem que sejam necessárias intervenções do usuário-alvo, falhas de segurança ainda não conhecidas pelo público são exploradas pela ferramenta, de forma que a intrusão ocorra de forma rápida, quase invisível e contornando os mecanismos de defesas até então desenvolvidos (Amnesty International, 2021).

O software de espionagem de origem israelense, entretanto, está longe de ser a única ferramenta do tipo comercializada atualmente. Dados apresentados por Steven Feldstein and Brian Kot (2023) mostram que entre 2011 e 2023 ao menos 74 governos negociaram com atores privados a compra/licenciamento de *spywares* ou "ferramentas de análise forense"[4]. No contexto brasileiro[5], o instituto de pesquisa IP.Rec constatou a existência de pelo menos 85 contratos entre órgãos de segurança pública e empresas provedoras de "ferramentas de investigação forense", com um custo de total R$54.551.313,26 no ano de 2020 (Ramiro et al., 2022).

Argumenta-se que a utilização de ferramentas semelhantes ao Pegasus por agências de segurança ao redor do mundo seria justificada por uma crescente complexidade das investigações criminais. A criptografia das comunicações digitais é muitas vezes apontada como uma das barreiras ao progresso dos investigadores que almejam identificar e capturar os responsáveis por crimes cometidos nos ambientes "físicos" e "virtuais" (Ramiro, et al., 2022). Nasce então

[3] O mercado de ferramentas de investigação é estudado em mais detalhes por Feldstein e Kot (2023), assim como por Ramiro et al. (2022)

[4] O Carnegie Democracy, Conflict, and Governance Program consolidou uma base de dados sobre a utilização de *spywares* e ferramentas correlatas a partir de informações disponibilizadas por ONGs, grupos de ativismo, centros de pesquisa e jornais. A base pode ser acessada em: https://ceipfiles.s3.amazonaws.com/pdf/Global+inventory+spyware+and+digital+forensics+11Jan23.xlsx (Acesso em 24 de Março de 2024)

[5] O próprio Pegasus esteve próximo de desembarcar no Brasil. A Polícia Federal (PF), a Procuradoria Geral da República (PGR), o Ministério Público Federal (MPF), a Agência Brasileira de Inteligência (ABIN) e Carlos Bolsonaro, filho do ex-Presidente Jair Bolsonaro, estiveram envolvidos em negociações com a NSO Group, com o objetivo de adquirir o Pegasus para o contexto brasileiro (Valença, 2021).

um competitivo e lucrativo mercado global que almeja providenciar ferramentas de investigação capazes de atravessar tais barreiras tecnológicas, movimentando bilhões de dólares anualmente (Feldstein; Kot, 2023).

O Pegasus figura como uma das principais ferramentas de "investigação" nesse mercado, capaz até mesmo de contornar estruturas de proteção como a criptografia de ponta-a-ponta (Leander, 2021). Por outro lado, ao mesmo tempo em que ocupa o posto de ferramenta cobiçada por agências de segurança ao redor do mundo, a ferramenta está imersa em inúmeros casos de abusos. Segundo os jornalistas Laurent Richard e Sandrine Rigaud, autores do livro "Pegasus: the story of the world's most dangerous spyware", "o perigoso problema do sistema Pegasus era que ele não se limitava a espionar os bandidos" (2023, p. 6, tradução nossa), sendo também utilizado em perseguições políticas a membros da oposição e organizações da sociedade civil (Access Now, 2024).

O conhecimento público sobre possíveis abusos na utilização do Pegasus iniciou-se em 2016, com investigações do Citizen Lab, departamento associado à Universidade de Toronto, no Canadá. Desde então, inúmeros casos têm sido trazidos à tona. Em 2021, por exemplo, um consórcio internacional de jornalistas liderados pela organização Forbidden Stories, chefiada por Laurent Richard e Sandrine Rigaud, revelou que ao menos 180 jornalistas em 20 países teriam sido selecionados como alvos do *spyware* (Rueckert, 2021). Emmanuel Macron, presidente da França, e Hanan Elatr, esposa do jornalista Jhamal Khashoggi, assassinado no consulado da Arábia Saudita em Istambul, na Turquia, foram todos apontados como alvos do Pegasus (Faife, 2021; Kirchgaessner, 2021; Leloup; Untersinger, 2021).

Esse *spyware*, portanto, embora possa ter surgido como mero um conjunto de linhas de código, aproxima-se cada vez mais de sua descrição mitológica, sendo capaz de atuar simultaneamente na esfera técnica como política (Leander, 2021). Entender o Pegasus como sendo apenas uma ferramenta é, portanto, insuficiente. O *spyware* surge repetidamente como peça central de fenômenos da segurança e da política internacional, ao exemplo de incidentes de cibersegurança e diplomáticos de grande relevância. Muito além de sua relevância como "peça" ou "ator individual", o Pegasus nos introduz a um debate mais amplo sobre o mercado da cibersegurança, das ferramentas de inteligência e dos *spywares*.

Embora o Pegasus seja um fenômeno importante para o campo da cibersegurança, dadas as suas capacidades técnicas e seus impactos na política internacional, sua posição de destaque no mercado de *spywares* não é eterna. Uma breve análise histórica do mercado de *spywares* mostra que outras empresas, como a italiana Hacking Team, já ocuparam o posto de destaque atualmente atribuído à NSO Group. A queda e a ascensão das empresas desenvolvedoras de ferramentas de investigação e espionagem não devem ser compreendidas apenas a partir dos (ins)sucessos das decisões humanas, mas também analisadas contanto com a participação de artefatos sociotécnicos. A derrocada da Hacking Team da posição de líder no mercado, por exemplo, está atribuída à divulgação de seus dados e documentos internos por hackers (O'Neill, 2020), o que só é possível a partir da formação de alianças entre hackers, servidores, códigos, *exploits*, entre outros elementos. O Pegasus funciona, portanto, como um buraco de fechadura a partir do qual podemos espiar as dinâmicas do mercado de *spywares* e as associações entre humanos e não-humanos.

Argumento que o Pegasus é mais que um *spyware*: pode ser considerado um ator/agente/actante da cibersegurança e da Política Internacional (Leander, 2021). Essa afirmação, entretanto, entra em choque com o antropocentrismo das RI mencionado anteriormente e sua visão sobre as tecnologias e os não-humanos de maneira mais ampla, tornando-o um interessante ponto de partida para a investigação - um ator relevante a ser seguido.

O valor do "ator" para a ANT, entretanto, só pode ser entendido no contexto da rede de associações em que está inserido. A ideia de ator não faz referência a uma unidade individual, mas "mas sim a uma entidade cuja existência depende de sua rede de alianças dentro de um campo relacional mutável, heterogêneo e expansivo" (Barry, 2013, p. 414, tradução nossa). Seguir o Pegasus, portanto, significa atentar para todo o trabalho invisível das infraestruturas que permitem que o *spyware* exista, navegue e envolva novos agentes (Leander, 2021).

Pensando nessas infraestruturas que permitem a circulação do Pegasus, a ANT e os STS levam em consideração novas formas de associação e organização, mais fluidas e flexíveis, que escapam às categorias e estruturas tradicionais

analisadas nas RI. O conceito de *assemblages*[6] no campo da cibersegurança, abordado por Egloff e Cavelty (2021), tal como por Collier (2018), tem como objetivo oferecer ferramentas para a análise desses novos arranjos e dinâmicas. Em meio às inovações analíticas permitidas pela adoção de conceitos como o de *assemblage*, pode-se destacar a capacidade de visualizar as associações que se estabelecem não apenas entre diferentes atores humanos, mas também não-humanos: práticas, objetos, textos, humanos, todos podem interagir e fazer parte dessas *assemblages*.

Reconhecendo as limitações espaço-temporais da presente obra, almejo abordar os debates sobre a sub-valorização dos não-humanos nas RI especificamente a partir do recorte da cibersegurança. Utilizo o caso do Pegasus como ponto de partida para as discussões sobre o papel da agência não-humana no contexto da cibersegurança. Destaco como um dos caminhos possíveis para a expansão das ferramentas analíticas tradicionais das RI a incorporação de ideias trabalhadas pelos Estudos de Ciência e Tecnologia e pela Teoria Ator-Rede.

Ao longo do capítulo 2 retorno aos Estudos de Ciência e Tecnologia (STS) e para a Teoria Ator-Rede (ANT), identificando suas contribuições específicas para os estudos da cibersegurança. Procurando debruçar-me sobre as ideias mais pertinentes ao presente trabalho, realizo minha investigação na interseção entre materialidade, agência não-humana e cibersegurança, tendo como referência obras e autores que realizaram percursos semelhantes (Stevens, 2019; Balzacq; Cavelty, 2016; Salter, 2019; Liebetrau; Christensen, 2021; Christensen; Liebetrau, 2019; Fouad, 2021).

Ao longo do Capítulo 3 buscarei introduzir de maneira mais detalhada o caso do *spyware* Pegasus. Seguindo as recomendações de Bruno Latour (2005), célebre sociólogo e contribuinte do campo da Teoria Ator-Rede, a pessoa pesquisadora que busque aderir a princípios da ANT deve:

> [...] 'seguir os atores em si', ou seja, tentar acompanhar suas inovações, muitas vezes selvagens, a fim de aprender com eles o que a existência coletiva se tornou em suas mãos, quais métodos eles elaboraram para fazê-la se encaixar, quais relatos poderiam definir melhor as novas

[6] A definição de *assemblages* oferecida por Egloff e Cavelty (2021) invoca a ideia de "redes complexas que nunca são estáveis, mas sempre mutáveis, montadas, desmontadas e remontadas em diferentes contextos, com múltiplas funcionalidades" (p. 2, tradução nossa). Utilizo o termo *assemblage* de maneira intercambiável com o termo rede, dando preferência ao último ao longo do texto.

> associações que eles foram forçados a estabelecer (p. 12, tradução nossa)

No contexto do presente trabalho, tal missão significa desenvolver uma metodologia de pesquisa capaz de se aproximar ao máximo do Pegasus. A partir da análise de relatórios técnicos, investigações jornalísticas e artigos científicos, procuro seguir o traçado deixado pelo Pegasus a partir de suas associações com outros atores e elementos. Esse movimento inicial de observação busca "suspender intencionalmente a crença em 'escalas de análise pré-determinadas'" (Salter, 2019, p. 4, tradução nossa), fornecendo o material necessário para que a teoria possa trabalhar sobre.

Ao longo do capítulo 4, buscarei costurar a teoria à empiria, associando as teorias discutidas anteriormente ao caso do Pegasus. Abordo os principais conceitos da ANT e dos STS, como aliança, agência, atores, actantes e mediadores. Retorno brevemente ao debate sobre determinismo tecnológico iniciado ao longo capítulo 2, apresentando os caminhos alternativos oferecidos pela ANT e pelos STS. Concluo o capítulo e sigo o capítulo final mostrando de que maneira o Pegasus pode ser uma porta de entrada tanto para o estudo do mercado de ciber vigilância que se consolida atualmente, tanto para a reorientação dos estudos da cibersegurança nas RI, prestando atenção para o papel dos não-humanos. O valor da investigação sobre o Pegasus com o auxílio da ANT e dos STS, portanto, é a consolidação de um framework teórico que pode ser estendido para os estudos sobre cibersegurança de maneira geral no campo das RI.

2. Cibersegurança e Relações Internacionais além do humano

"Os objetos também têm agência", afirma Bruno Latour no título de um dos capítulos de seu livro "Reassembling the social: an introduction to Actor-Network Theory", publicado em 2005. A afirmação de Latour (2005), embora sucinta, retoma um dos principais debates da disciplina de RI, existente desde sua institucionalização como disciplina acadêmica: "quem são os atores relevantes e o que significa atuar na Política Internacional?" (Braun; Schindler; Wille, 2019, p. 790, tradução nossa).

A definição dos atores e agentes relevantes é uma questão abordada por autores fundamentais da disciplina de RI, como Kenneth Waltz (1959), que delimita nos indivíduos, nos Estados e no Sistema Internacional, os níveis de análise que poderiam ser utilizados para pensar a Política Internacional e as RI. Desde os estudos de Waltz (1959), novos níveis/categorias de análises e atores correspondentes foram adicionais ao estudo das RI, indo além dos Estados e de seus líderes políticos como unidades analisadas (Braun; Schindler; Wille, 2019), mas a centralidade dos agentes enquanto elementos decisivos para a análise do internacional permanece presente.

O questionamento sobre quem são os agentes e como podem agir está também traduzido no estudo mais amplo da relação agente-estrutura nas RI (Cudworth; Hobden, 2013). Alexander Wendt (1987), introduzindo o estudo da questão de maneira formal nas RI, propõe considerar "agentes e estruturas como entidades mutuamente constituídas ou codeterminadas" (Wendt, 1987, p. 350, tradução nossa). Segundo o autor, "as estruturas sociais são o resultado das consequências intencionais e não intencionais da ação humana, assim como essas ações pressupõem ou são mediadas por um contexto estrutural irredutível" (Wendt, 1987, p. 360, tradução nossa). Wendt (1987) sugere, portanto, o desenvolvimento de uma perspectiva que "considera capaz de explicar as restrições que os atores internacionais enfrentam com relação às estruturas sociais, mas também o poder que esses atores possuem para transformar as estruturas nas quais estão inseridos" (Leese, Hoijtink, 2019, p. 10, tradução nossa).

Em resumo, o debate sobre agência nas RI é atravessado pelo questionamento sobre o que deve ser tido em primeiro lugar: agente ou estrutura. A dualidade formada entre agente e estrutura tende a compreender a agência enquanto um atributo, algo que "precisaria estar localizado dentro de alguém ou alguma coisa" (Leese, Hoijtink, 2019, p. 3, tradução nossa). A compreensão de agência nas RI estaria ainda tradicionalmente relacionada ao sujeito humano e sua cognição e intencionalidade. Os autores Braun, Schindler e Wille (2019), assim como Fouad (2021), apresentam uma tendência das teorias *mainstream* das RI a partir da qual "a agência tem sido vinculada ao sujeito humano, e a capacidade de agir tem sido associada à cognição, à intencionalidade, aos desejos e à tomada de decisões - qualidades consideradas exclusivas dos seres humanos" (Fouad, 2021, p. 6, tradução nossa).

Uma alternativa à concepção de agência como atributo ou produto exclusivo da ação humana, portanto possibilitando a afirmação de Latour (2005) sobre a agência dos objetos e dos não-humanos de maneira mais ampla, é a utilização de análises relacionais, baseadas na interação entre os elementos. Para essas perspectivas, as interações são o ponto de partida, sendo necessário estudar "como os padrões dessas interações (...) produzem os elementos aparentemente estáveis do mundo social, incluindo entidades com propriedades agenciais" (Braun; Schindler; Wille, 2019, p. 792, tradução nossa).

A ANT, desenvolvida também tendo como base os estudos de Bruno Latour, está mais próxima deste último grupo, enxergando nas associações entre os atores o caminho para entender a constituição da ação, que não seria um atributo fixo e permanente. Segundo a ANT, "a capacidade de agir não é uma característica intrínseca de uma entidade individual, mas deriva de sua inserção em uma rede de vínculos com outras entidades" (Braun; Schindler; Wille, 2019, p. 796, tradução nossa).

Nesse sentido, Bruno Latour (2005), ao afirmar que os objetos também podem "ter agência", incide diretamente sobre tais debates, reorientando quem podem ser os agentes e qual é a "composição" dessa agência. Com o intuito de compreender as implicações da afirmação de Latour (2005) para a teorização sobre agência nas RI, podemos inicialmente abordar o determinismo tecnológico, o social construtivismo e suas variações, pois esses apresentam diferentes perspectivas para o papel das tecnologias. O estudo do determinismo tecnológico

e do social construtivismo permite compreender de que maneira o papel das tecnologias foi estudado nas RI até os dias de hoje, e em que grau a afirmação de Latour (2005) aponta em uma direção alternativa às duas possibilidades apresentadas até então.

Abordar essas diferentes lentes analíticas, portanto, permite uma melhor compreensão do papel das tecnologias nas RI, de maneira que podemos posteriormente analisar como essas podem "ter agência", o que também possui efeitos diretos para o estudo da cibersegurança e para o caso do Pegasus abordado no presente trabalho. O presente capítulo apresenta as bases teóricas sobre as quais me debruço para estudar a cibersegurança não apenas como temática das RI, mas também enquanto terreno fértil para a proliferação dos debates que questionam os vieses e limitações que permeiam a disciplina, como o foco demasiado na figura humana e a concepção da tecnologia como elemento exógeno. Ao final, retorno ao caso do *spyware* Pegasus, apresentando caminhos iniciais para a aplicação de ideias e conceitos dos STS e da ANT no estudo de caso proposto.

2.1 A tecnologia nas RI

A tecnologia[7], de maneira ampla, é uma preocupação importante "desde o início da disciplina de RI, na segunda década do século XX", e, sendo enxergada "como uma variável causal ou como um pano de fundo, a tecnologia nunca perdeu esse lugar central" (McCarthy, 2018, p. 3-4, tradução nossa). O estudo das tecnologias nas RI, entretanto, está atravessado por duas perspectivas principais, apresentadas por Stefan Fritsch (2011) e Daniel McCarthy (2018): o determinismo tecnológico e o social construtivismo, ambas apresentando diferentes interpretações para o nexo tecnologia-sociedade (Fritsch, 2011). Analiso a seguir ambas as perspectivas, para posteriormente retornar às alternativas que surgem no ensejo das provocações oferecidas por Latour (2005).

[7] Considero que o termo tecnologia pode fazer referência "a sistemas sociotécnicos amplos, como a Internet, bem como a artefatos, padrões, rotinas e crenças específicos que compõem esses sistemas, como computadores (...)" (Dafoe, 2015, p. 1051, tradução nossa). O termo artefato pode ser empregado para fazer referência a objetos específicos, e "os sistemas sociotécnicos podem se referir às vastas configurações funcionais de todos esses componentes." (Dafoe, 2015, p. 1051, tradução nossa).

2.1.1 Os determinismos tecnológicos

O determinismo tecnológico é resumido por McCarthy (2013), quando afirma que, segundo essa lente teórica, "a tecnologia causa mudanças sociais" (p. 472, tradução nossa). A atribuição de características deterministas às tecnologias, segundo Leese e Hoijtink (2019), "é analiticamente compatível com o foco da disciplina em explicar as mudanças e a estabilidade no Sistema Internacional" (p. 9, tradução nossa). Existem, entretanto, determinismos tecnológicos distintos, o que resulta em diferentes interpretações do papel das tecnologias. Prossigo analisando as variações do determinismo seguindo a subdivisão proposta por McCarthy (2013), entre instrumentalismo e essencialismo.

A variante instrumentalista do determinismo tecnológico aproxima-se de um entendimento de "senso comum" das tecnologias de acordo com McCarthy (2013), no sentido que as tecnologias e os artefatos são meros instrumentos da ação humana. Segundo o autor, "o uso de um objeto tecnológico não leva necessariamente a nenhum resultado. As armas nucleares não reestruturam as formas de política internacional (...)" (McCarthy, 2013, p. 474, tradução nossa). Os objetos podem ser utilizados de inúmeras maneiras diferentes e o que causa mudanças "no social" é a ação humana que utiliza tais instrumentos ou ferramentas. Nas RI, portanto, o posicionamento instrumentalista coloca as tecnologias como uma variável externa que "influencia o Sistema Internacional, mas não é parte integrante desse sistema" (Leese; Hoijtink, 2019, p. 9, tradução nossa).

O debate sobre a regulação das armas nos Estados Unidos pode ser resgatado como exemplo contemporâneo que dialoga com o determinismo tecnológico e suas variantes. McCarthy (2013) apresenta o slogan da National Rifle Association (NRA), "Armas não matam pessoas. Pessoas matam pessoas", como um exemplo da interpretação instrumentalista. Sob essa perspectiva, as armas não causariam mudanças no tecido social ou em suas dinâmicas, uma vez que os efeitos são determinados a partir da agência humana, do indivíduo que resolve utilizar uma arma de fogo. O desenvolvimento do artefato tecnológico e da tecnologia em si são retirados de um contexto sócio-histórico mais amplo, pois

o que importa para as análises são as decisões humanas por trás de seu emprego (McCarthy, 2013).

Sob a ótica do instrumentalismo, às armas são "ferramentas ou instrumentos que não têm vieses a favor de posturas militares ofensivas ou defensivas" (McCarty, 2018, p. 6, tradução nossa). As tecnologias e os objetos de maneira geral, são aqui enxergados enquanto entidades "neutras" sobre as quais agem as intenções humanas, adaptando-se às intenções dessas. Não possuem, portanto, propriedades ou vieses inerentes que influenciam na construção de uma determinada realidade, pois a construção dessa depende da ação humana que as cerca e as utiliza

A segunda perspectiva, essencialista, aborda a tecnologia como detentora de propriedades inerentes. Tal como apresentado por McCarthy (2013), os artefatos e as instituições tecnológicas:

> têm uma forma necessária e, como resultado, desenvolvem-se em uma direção linear. Em vez de serem neutros em seus efeitos sociais, os objetos não humanos têm uma essência que impacta as relações sociais e políticas - a tecnologia realmente causa mudanças sociais. Para recorrer novamente à NRA, são as armas que matam as pessoas - a posse de armas altera os contextos sociais e cria resultados sociais distintos (p. 475, tradução nossa).

As variantes essencialistas, sejam essas otimistas ou pessimistas sobre o impacto das tecnologias, enxergam as mesmas como promotoras de mudanças importantes para o exercício da política (Leese; Hoijtink, 2019). Assim como no instrumentalismo, o processo de criação dos objetos tecnológicos é ofuscado pelo impacto de seu desenho final (McCarthy, 2013). Sendo assim, tanto no instrumentalismo como no essencialismo a atenção é direcionada à forma final dos objetos, com análises que majoritariamente "não levam em conta como as tecnologias surgem e como as estruturas sociais, políticas e econômicas existentes já estão sempre impressas nelas" (Leese; Hoijtink, 2019, p. 9, tradução nossa).

Ambas as perspectivas apontam em direções contrárias: a primeira colocando as tecnologias como além da agência humana; a segunda como as tecnologias como "neutras" e subordinadas à agência dos humanos. Embora apresentem ideias divergentes sobre o papel das tecnologias enquanto agentes de mudança no social, ambas as enxergam como um elemento "fechado". Em outras palavras, surgem como "caixas-pretas", sobre as quais temos poucas informações

sobre como, por que, por quem são criados, assim como quais normas e valores eles incorporam (McCarthy, 2018). A tecnologia é, em ambos os casos, tratada como algo "externo à política, e não como algo integral à forma como a política contemporânea e os assuntos mundiais são conduzidos" (Eriksson; Newlove-Eriksson, 2021, p. 5, tradução nossa).

O interesse recente de pesquisadores no campo das RI, principalmente a partir da introdução de novas ferramentas teóricas como os STS e a ANT, é de "desembrulhar", ou de abrir a caixa-preta da tecnologia, "colocando em primeiro plano sua construção, implementação e uso. Essa abordagem holística nos permitiria, então, levar em conta as políticas que entram na tecnologia, bem como as políticas que emanam da tecnologia" (Leese, Hoijtink, 2019, p. 3, tradução nossa).

A intenção aqui é de se distanciar de uma análise da tecnologia como algo que é dado, que está pronto e que é externo. Olhar dentro da caixa-preta significa também entender as tecnologias como sistemas sociotécnicos, caracterizados pela presença de elementos humanos e não-humanos (Leese, Hoijtink, 2019). Nesse sentido, um dos efeitos do determinismo tecnológico para as RI é a limitação teórica imposta pela dicotomia entre técnico e social, o que impede o desenvolvimento de perspectivas que enxerguem as tecnologias, e os artefatos de maneira geral, como co-constituintes, co-produtores da realidade social.

2.1.2 Os construtivismos

Já a corrente construtivista apresenta um primeiro desafio à perspectiva determinista sobre o papel das tecnologias, criticando posicionamentos realistas. Embora seja uma escola de pensamento que abarca diferentes correntes e posicionamentos, é possível afirmar que o construtivismo compartilha a visão de que a "tecnologia não está equipada com nenhum significado 'essencial' ou pré-estabelecido. A tecnologia é o que os atores fazem dela e, nesse sentido, é 'politicamente neutra', ou melhor, pode ser politizada de muitas maneiras diferentes" (Eriksson; Newlove-Eriksson, 2021, p.12, tradução nossa). O interesse do construtivismo reside em enxergar como diferentes identidades, normas e interesses relacionados a tecnologias são formados (Eriksson; Newlove-Eriksson, 2021).

A vertente construtivista assume que os aspectos materiais possuem um papel importante para a Política Internacional, mas estes "só adquirem significado quando relacionados às normas e identidades sociais" (Hoijtink; Leese, 2019, p. 8, tradução nossa). O impacto das tecnologias, portanto, só pode ser compreendido de acordo com os sistemas de crença e de valor nos quais estão inseridas. As mudanças sistêmicas, por exemplo, surgem a partir de alterações nas normas e valores que cercam essas tecnologias (Hoijtink; Leese, 2019).

A Teoria Ator-Rede e os Estudos de Ciência e Tecnologia estão situados em um *continuum* de perspectivas do construtivismo, porém não compartilham necessariamente dos mesmos fundamentos. As diferenças ficam evidenciadas "durante a década de 1990, os proponentes da ANT se distanciaram do construtivismo social e apresentaram a ANT como uma estrutura mais independente" (Baron; Gomez, 2016, p. 6 tradução nossa).

\ Uma conexão entre o construtivismo de maneira mais ampla e as contribuições dos STS e da ANT é estabelecida pelo movimento da "técno-política", que busca iniciar o movimento de abertura da caixa-preta. Suas ideias podem ser resumidas por alguns princípios orientadores, abordados por Johan Eriksson e Lindy M. Newlove-Eriksson (2021):

1. A tecnologia não seria nem boa, nem ruim em si mesma, nem mesmo neutra, mas sim um elemento presente em meio a um emaranhado de fatores e realidades sociopolíticas.

2. Existem múltiplas formas pelas quais a tecnologia e a política estão conectadas e interagem, moldando uma a outra, processo que muitas vezes pode ocorrer de forma imprevisível.

Diferentemente do construtivismo e de outras abordagens, a tecnopolítica caminha na direção de se afastar da agência humana como principal explicação para os resultados políticos encontrados (Eriksson; Newlove-Eriksson, 2021). Resgatando a frase de Bruno Latour (2005) que inicia o presente capítulo, abre-se o espaço para a compreensão de que os objetos também têm agência, portanto elementos outros que não os humanos também podem ter resultados sobre a realidade política e social.

A obra de Bruno Latour (2005) está então inserida em um movimento mais amplo de contestação dos dualismos encontrados pela ciência, uma realidade que também atravessa as RI, como mostrado acima. Os Estudos de Ciência e

Tecnologia, a Teoria Ator-Rede, os Novos Materialismos e a Construção Social da Tecnologia, são correntes que compartilham a missão de rejeitar o determinismo tecnológico e as divisões tradicionais entre "sociedade e tecnologia, natureza e cultura, humanos e não-humanos que permeiam a teoria social" (McCarthy, 2018, p. 232, tradução nossa).

A importação e a adaptação de discussões levantadas pelos STS, pela ANT e pela corrente tecnopolítica são imprescindíveis para a cibersegurança, campo que está a todo momento dialogando sobre as diferentes relações que se estabelecem entre política, segurança e tecnologia. Trazer essas novas ideias para o campo da cibersegurança pode então ajudar "os pesquisadores a ir além dos atos de retórica para examinar as 'realidades materiais' que precedem e moldam as percepções de ameaças e a política cibernética de forma mais ampla", sugerindo que a cibersegurança é "formada por práticas materiais-discursivas complexas" (Stevens, 2019, p. 4, tradução nossa). Inicia-se aqui uma tentativa de abrir a "caixa-preta" da cibersegurança enquanto temática, explorando sua materialidade, seus atores e dinâmicas até então ofuscados pelos vieses inseridos nas perspectivas dominantes das RI.

Esse movimento traz novas possibilidades para a cibersegurança, objeto de estudos para o qual é de suma importância a formulação de um entendimento flexível e renovado sobre o papel das tecnologias, seus efeitos e sua agência. A aplicação de conceitos da ANT e dos STS para a cibersegurança é jornada que já está em curso, representada por obras como a de Myriam Dunn Cavelty e Thierry Balzacq (2016), Noran S. Fouad (2021), Clare Stevens (2019), T. Liebetrau e C. Christensen (2020), W. wan der Wagen (2019), entre outros.

É importante notar que o uso do termo "importação" é parte de um debate importante sobre o papel da Teoria Ator-Rede enquanto "ferramenta"/framework teórico para as Relações Internacionais. Os pesquisadores Jacqueline Best e William Walters (2013), por exemplo, chamam atenção para a "síndrome da importação" das Relações Internacionais, responsável por trazer "em massa" teorias que vão desde a economia institucionalista até o construtivismo. Segundo esses:

> qualquer movimento para simplesmente "importar" a ANT perderia um dos insights mais importantes dos debates recentes na sociologia da ciência e da tecnologia. Trata-se de levar a sério a ideia de uma

> sociologia da *tradução*. Traduzir é estabelecer relações de equivalência entre ideias, objetos e materiais que, de outra forma, seriam diferentes (p. 333, tradução nossa, grifo nosso).

Idealmente, a tradução da ANT e dos STS para as RI envolve um cuidado com seus lemas e princípios gerais. Tendo em vista a amplitude da ANT e dos STS, teorias/movimentos heterogêneos, tal como as limitações do presente trabalho, concentro-me sobre algumas de suas orientações centrais, analisando sua aplicabilidade para o estudo da segurança cibernética.

2.2 Cibersegurança nas RI

"A cibersegurança é uma questão importante na política (inter)nacional. Mas o que a torna uma questão política?", questiona a pesquisadora Myriam Dunn Cavelty (2018, p. 22, tradução nossa). A cibersegurança surge inicialmente como uma questão técnica, sendo posteriormente absorvida pelos estudos de segurança e pelas RI, sendo então transformada em questão política. Esse movimento é influenciado pelas diferentes correntes teóricas da disciplina, entre elas a Teoria da Securitização, levada a frente pela Escola de Copenhague[8]. As particularidades da cibersegurança e do espaço no qual ela acontece (*mélange* entre físico e virtual) reforçam a necessidade de pensá-la como elemento não apenas técnico, mas também político, algo que a Teoria da Securitização captura com maestria.

No contexto dos estudos sobre segurança nas RI e em meio aos CSS, “os estudiosos dos Estudos Críticos de Segurança têm abordado a segurança cibernética predominantemente pelo prisma da Teoria da Securitização” (Liebetrau; Christensen, 2021, p. 8, tradução nossa). Essa teoria estuda os processos de formação de agendas das políticas sobre segurança. Tal linha de pensamento considera a segurança como um construto social (Lobato; Kenkel, 2015), argumentando que problemas não se tornam questões de segurança porque estão baseados em ameaças existenciais objetivamente mensuráveis, mas porque atores-chaves foram capazes de apresentar e estabelecer questões como fundamentadas em ameaças desse tipo (Tikk; Kerttunen, 2020).

[8] Vale ressaltar que a Teoria da Securitização aqui abordada desdobra-se em diferentes escolas de pensamento, além da Escola de Copenhague. Analisando as escolas que dialogam diretamente sobre a securitização ou sobre termos relacionados, podemos listar também a Escola de Paris e a Escola Galesa, entre outros movimentos associados. Para mais informações, ver Valença (2010).

A relação entre a securitização e a cibersegurança parte da necessidade de entender o campo da cibersegurança como um dos "setores de segurança", uma das categorias com as quais trabalha a Escola de Copenhague. Uma vez que cada setor abarca objetos referentes, atores funcionais e agentes securitizadores específicos (Lobato; Kenkel, 2015), a cibersegurança apresenta particularidades suficientes para que se constitua como um setor a ser analisado em separado (Hansen; Nissenbaum, 2009). A cibersegurança segundo a Teoria da Securitização é portanto é tida como "um ato de fala ou um discurso no qual um ator humano securitizador apresenta uma ameaça como existencial a um determinado objeto referente e, portanto, exige medidas de emergência para garantir a sobrevivência desse objeto" (Fouad, 2021, p. 4, tradução nossa).

Em suma, a Teoria da Securitização propõe que atores-chave, por meio de seus discursos e ações, são capazes de apresentar e estabelecer questões como sendo fundamentadas - problemas de segurança. Essa construção social da segurança é fundamental para entender como a cibersegurança se tornou um tema central na agenda internacional: a cibersegurança, a partir da mobilização de recursos por certos atores, é configurada como questão de segurança, deixando a esfera técnica e sendo inserida em um contexto político mais amplo.

Conforme argumentam Liebetrau e Christensen (2021), "se nos contentarmos apenas com o prisma da teoria da securitização, limitaremos de forma crítica o que pode ser a segurança cibernética" (p. 30, tradução). A aplicação dos conceitos levados a frente pela Escola de Copenhague, portanto, embora possam contribuir positivamente para construir a ponte entre os estudos de segurança, as RI e a cibersegurança (Fouad, 2021), também apresentam limitações/oportunidades interpretativas.

A primeira dessas limitações/oportunidades surge com a subordinação do papel político das tecnologias ao discurso da segurança (Liebetrau e Christensen, 2021). Ao focar em atos de fala, em discursos, questões sobre materialidade e agência deixam de ser abordadas de maneira satisfatória. Noran S. Fouad (2021) argumenta que "existem várias realidades materiais com relação à natureza das interrupções no computador, seus efeitos e o conhecimento sobre elas nas comunidades técnicas que não podem ser entendidas apenas como parte de construções discursivas" (p. 5, tradução nossa), reforçando a necessidade de desenvolver um novo olhar para a materialidade na cibersegurança, algo que ainda

não é alcançado a partir da Teoria da Securitização. Os não-humanos são então mais uma vez subordinados à atuação dos atores securitizadoras tradicionais, reforçando de maneira indireta perspectivas estado-cêntricas e antropocêntricas sobre cibersegurança.

2.3 Cibersegurança mais-que-humana: As contribuições da ANT e dos STS na cibersegurança

Sob a perspectiva das RI, podemos observar um movimento de ampliação do repertório conceitual utilizado para os estudos sobre segurança no início da década de 2010, com a virada materialista, ou movimento dos "novos materialismos" (Bellanova; Jacobsen; Monsees, 2020). Considerando a pluralidade e heterogeneidade das ideias sob a bandeira dos novos materialismos, apresento a seguir os conceitos mais importantes que podem ser traduzidos para o estudo da segurança cibernética.

Autores participantes da corrente dos novos materialismos compartilham um interesse em desenvolver novos métodos de analisar o social, o político e o econômico "como domínios que não são mais produzidos apenas por decisões e ações humanas, mas por poderes emaranhados, emergentes e geradores que incluem uma variedade de atores e efeitos não humanos" (Hoijtink; Leese, 2019, p. 12, tradução nossa). Em uma dimensão mais profunda, a construção de sentidos, portanto da intersubjetividade, sempre dependeu da interação entre relações humanas e não humanas (Salter, 2019). O papel da ANT para o estudo da cibersegurança é a ampliação da capacidade de enxergar, a partir das dinâmicas relações de co-constituição estabelecidas entre humanos e não-humanos (Liebetrau; Christensen, 2021), como a construção de sentidos é dependente de uma materialidade.

Elementos naturais, animais, humanos e artefatos tecnológicos interagem de maneiras criativas e imprevisíveis. Essa mesma lógica pode ser observada no ciberespaço e pode servir de guia na exploração das contribuições dos STS e da ANT.

2.3.1 Múltiplos agentes e agências no ciberespaço

Talvez uma das mais importantes contribuições oriundas da interação entre as RI, a ANT, os STS seja a "ampliação da gama de atores considerados relevantes para explicar a política internacional" (McCarthy, 2018, p. 224, tradução nossa). Consequentemente, associando tais contribuições ao campo da cibersegurança, temos uma nova gama de "atores em potencial" que devem ser levados em consideração ao longo da prática da pesquisa.

A partir da virada materialista, como já apresentado anteriormente, elementos não-humanos começam a ser considerados agentes em potencial, tanto quanto os humanos. Textos seminais da ANT e dos STS demonstram radicalmente a necessidade de ir além dos humanos: Latour (1988) e Callon (1984) mostram como mecanismos de fechar portas e as vieiras (moluscos) devem ser considerados potenciais atores nas redes das quais participam, cada um a partir de suas potencialidades e particularidades.

No caso da cibersegurança podemos encontrar novos atores em potencial ao ter um olhar mais atento para o "espaço" no qual a cibersegurança ocorre: o ciberespaço, um conceito de definição contestada, mas que, de maneira geral, faz referência ao "domínio das redes de computadores (e os usuários por trás delas) em que as informações são armazenadas, compartilhadas e comunicadas on-line" (Singer; Friedman, 2014, p. 13, tradução nossa). O ciberespaço é mais do que simplesmente a Internet, a rede mundial de computadores: "é tanto a Internet como o 'espaço' que ela gera (...) um espaço intangível no qual trocas desterritorializadas entre cidadãos de todas as nações ocorrem instantaneamente" (Douzet, 2014, p. 4, tradução nossa).

Dessa forma, entendemos que o "ciberespaço é composto por um domínio material e virtual - um espaço de coisas e ideias, estrutura e conteúdo (...) uma 'alucinação consensual', como Gibson (1984) o definiu famosamente, mas que não poderia existir sem a infraestrutura física que a sustenta." (Deibert, 2010, p. 16, tradução nossa). Trata-se de um conjunto de computadores conectados, cabos de fibra óptica (Nye, 2011, p.19) assim como protocolos, leis e seres humanos que desempenham diferentes papéis e que traçam entre si diferentes formas de associação.

A infraestrutura que permite a existência do ciberespaço é uma participante ativa do cibersegurança, pois "as infraestruturas não estão simplesmente lá fora, objetos passivos esperando para serem protegidos para que as sociedades funcionem sem problemas" (Aradau, 2010, p. 505, tradução nossa). Elas quebram, travam e, ainda mais importante, são parcialmente responsáveis pela produção de vulnerabilidades cibernéticas.

Lene Hansen e Helen Nissenbaum, ao debaterem a procedência das ameaças no campo da cibersegurança, afirmam que estas "não surgem apenas de agentes (geralmente) intencionais, mas também de ameaças sistêmicas" (2009, p. 1160, tradução nossa). Essas ameaças sistêmicas estariam associadas à propriedade da imprevisibilidade computacional: "as ameaças surgem de falhas de software e de falhas de hardware e não podem ser corrigidas por meio do aperfeiçoamento da tecnologia digital e da programação; há, em resumo, uma insegurança ontológica inerente aos sistemas de computador" (Hansen; Nissenbaum, 2009, 1160, tradução nossa). A própria lógica de funcionamento dos sistemas computacionais está então associada ao surgimento de vulnerabilidades, impactando a dinâmica de performance da cibersegurança. Analisando o cibercrime a partir das lentes da ANT, Wagen (2019) afirma que "no crime cibernético/espaço cibernético, obviamente várias entidades humanas e técnicas se reúnem para cometer o crime" (2019, p. 159, tradução nossa).

2.3.2 A ideia de ator e agência revigoradas

Explorar uma nova gama de agentes requer também uma renovação do que é de fato agência e o que é um ator. Bruno Latour (2005) afirma que "qualquer coisa que modifique um estado de coisas fazendo uma diferença é um ator - ou, se ainda não tiver figuração, um actante" (p. 71, tradução nossa). Essa visão está intrinsecamente relacionada ao movimento de "achatamento da ontologia", ou formulação de uma ontologia plana (em inglês, *flat ontology*) ideia apresentada por Mark B. Salter (2019), referindo-se a obra de Latour:

> Um dos princípios fundamentais da teoria ator-rede e sua vertente do novo materialismo é uma ontologia plana, ou seja, todos os atores em potencial têm a capacidade de ter um efeito político. Seres humanos, instituições, coisas, ideias, geologias, bactérias e artefatos culturais

> podem ter um efeito politicamente importante em uma determinada controvérsia ou conjunto." (2019, p. 4, tradução nossa)

A construção dessa ontologia alternativa transforma o processo de investigação ao afastar o analista de escalas de análise pré-concebidas. “Seguir os atores”, como orienta Bruno Latour em “Reassembling the Social” (2005), significa seguir e analisar os humanos e não humanos que fazem a diferença em uma determinada questão (Salter, 2019), o que inevitavelmente coloca no caminho do analista a agência não-humana.

Conceber a capacidade de atuação dos não-humanos depende de uma formulação de agência que se distancia de sua propriedade de “atributo (que deveria estar localizada em alguém ou algo) e que se aproxima de uma compreensão da agência como um produto da interação” (Hoijtink; Leese, 2019, p. 3, tradução nossa). A agência, portanto, deixa de ser propriedade, assim como a gente deixa de ser uma entidade fixa e pré-estabelecida. “Um actante é uma fonte de ação que pode ser humana ou não humana; é aquilo que tem eficácia, pode fazer coisas, têm coerência suficiente para fazer a diferença, produzir efeitos, alterar o curso dos eventos". (Bennet, 2010, p. 9, tradução nossa)”

No caso da cibersegurança mais especificamente, pode-se ainda dizer que os sistemas inteligentes possuem uma forma de atuação cada vez mais autônoma: *malwares* como o Pegasus e *ransomwares* como o WannaCry e o NotPetya possuem capacidades de replicação autônoma, tal como adaptação aos contextos informacionais que encontram. Os sistemas de Inteligência Artificial redobram os questionamentos sobre o grau de autonomia dos humanos e dos não-humanos na construção da cibersegurança (Fouad, 2021). A agência dos *malwares*, entretanto, é compartilhada: divide-se entre aqueles que o criaram, as infraestruturas pelas quais passa e atinge, modificando o estado, e até com os usuários finais atingidos.

Para Fouad (2021), é importante enxergar a especificidade da agência nos elementos da cibersegurança: “se toda a matéria em todos os setores de segurança tem agência, a segurança cibernética se distingue pela agência peculiar dos códigos/software como agentes informacionais. Ou seja, toda matéria importa, mas os códigos/softwares importam de forma diferente” (p. 9, tradução nossa).

Tal forma de agência dos *malwares* pode ser entendida como uma “agência de influência” (Fouad, 2021), ou, utilizando outro termo da ANT, como uma

mediação. Os mediadores são aqueles que "tornam o movimento do social visível para o leitor e sempre afetam o que quer que flua através dele" (Balzacq; Cavelty, 2016, p. 183, tradução nossa), portanto o papel dos mesmos não é apenas passivo, mas ativo.

A exploração dos papéis exercidos pela infraestrutura na cibersegurança deve se atentar a ideia defendida pela ANT e pelos STS de que "as coisas não humanas não são todas do mesmo tipo e não exercem a mesma forma de agência" (Fouad, 2021, p. 9, tradução nossa). Mesmo que seja possível começar a analisar a agência de cabos, servidores - e até do próprio Pegasus, a intenção dos STS e da ANT não é de equiparar a "agência" desses elementos à agência humana.

2.3.3 Ator-rede e o público-privado

A cibersegurança, entendida como um tipo de segurança que se desenvolve no ciberespaço e a partir dele (Balzacq; Cavelty, 2016) é então constituída por uma complexa rede de atores e instituições, o que inclui um vasto grupo de atores não-estatais que assumem papéis altamente relevantes (Choucri 2012; Collier, 2018). A importância dos atores privados nesse contexto advém de seu controle sobre grande parte do que conhecemos como ciberespaço (Deibert, 2018, p. 689). Dessa forma, a governança da cibersegurança não recai apenas sobre as entidades estatais (Christensen; Liebetrau, 2019), sendo uma atividade compartilhada com agentes privados (Eriksson; Giacomello, 2006).

Agentes privados constituem a rede de atores da cibersegurança tendo um papel semelhante – e até às vezes maior – que o de Estados na garantia de estabilidade para o ambiente virtual (Muller, p. 2016). Esse argumento pode ainda ser expandido para afirmar que a cibersegurança é co-produzida por todos os usuários de computadores, além de todos especialistas de Tecnologia da Informação (Balzacq; Cavelty, 2016), pois estão todos envolvidos na constituição de eventos e políticas que transformam o campo da cibersegurança, o que será explorado mais à frente.

Muito além dos envolvimentos entre humanos e não-humanos que devem começar a ser estudados, temos também a emergência e a "multiplicação de atores políticos, locais e espaços de segurança fora dos atores e instituições tradicionais do Estado" (Liebetrau; Christensen, 2020, p. 26, tradução nossa). As formas de

associação entre esses atores são ainda mais importantes. Surge um movimento dentro das RI para estudar as associações entre esses atores a partir da lógica de *assemblages*, como descrito por Collier (2018) quando diz que uma assemblage da segurança "refere-se a novas estruturas híbridas que, muitas vezes, são simultaneamente públicas e privadas, globais e locais" (p. 14, tradução nossa).

> À medida que esses conjuntos de segurança cibernética cresceram e se tornaram mais complexos, eles também representaram uma fonte crescente de tensão. Os conjuntos de segurança não são necessariamente estruturas harmônicas ou estáveis. Os conjuntos geralmente são marcados por concorrência e lutas por poder e influência, com diferentes atores apelando para visões conflitantes do que deveria ser "público" e "privado" (Collier, 2018, p. 18, tradução nossa).

Essa luta de poder é presente também no mercado de *spywares* - marcado por uma constante disputa por espaço e reorganização entre os atores relevantes, afinal de contas os fornecedores desses softwares "enfrentam uma série de desafios notáveis para legitimar seus produtos" (Harkin; Molnar; Vowles, 2020, p. 3, tradução nossa). A busca por legitimidade orienta as ações de empresas como a NSO Group, que então estabelecerá conexões com Estados, outros atores não-estatais e até mesmo com infraestruturas e pedaços de código na tentativa de estabilização de sua posição de "poder" na rede em que ocupa.

Em suma, o estudo da cibersegurança a partir da ANT e dos STS também nos oferece novas formas de enxergar a relação entre público e privado, analisando a formação de um híbrido público-privado, no qual uma série de relações humanas-não-humanas estão envolvidas na constante (re)organização de redes.

2.4 Conclusão: Cibersegurança mais-que-humana: como empregar a Teoria Ator-Rede e os conceitos dos STS no estudo do Pegasus?

A crescente atenção destinada ao tema da cibersegurança nas RI está diretamente relacionada ao desenvolvimento contínuo e à proliferação das Tecnologias de Informação e Comunicação (TICs). Tecnologias como os Sistemas de Armas Autônomas (AWS, em inglês); algoritmos de monitoramento, câmeras de reconhecimento facial inteligentes, e até mesmo os *spywares*, "têm repercussões potencialmente profundas sobre as formas como a ação na política

internacional se torna possível, as formas como as relações entre os Estados se estruturam e as maneiras pelas quais as guerras são travadas, a segurança é produzida e a paz é criada e mantida" (Leese; Hoijtink, 2019, p.1, tradução nossa).

As contestações dos STS e da ANT sobre a agência não-humana foram desenvolvidas décadas antes do desenvolvimento dos AWS, dos *ransomwares* e dos *spywares*. Essas novas tecnologias, entretanto, criam uma nova onda de possibilidades para os estudos sobre agência não-humana, uma vez que apresentam níveis cada vez mais altos de autonomia e capacidade de agir - ou como tendo *agência* (Leese; Hoijtink, 2019) Exemplos dessa capacidade de agir de forma "autônoma" podem ser observados na atuação dos *ransomwares* WannaCry e NotPetya, capazes de se adaptar ao contexto de segurança que encontram nas máquinas que infectam - adaptando sua resposta e percurso de infecção, mas também agindo de forma imprevisível (Fouad, 2021; Wagen, 2019).

Entender a atuação e os efeitos do WannaCry, do NotPetya ou até mesmo do Pegasus requer desafiar "as abordagens teóricas antropocêntricas para o estudo da segurança cibernética, que vinculam a capacidade de agir à subjetividade humana e ignoram o papel do não humano na co-construção de sua própria (in)segurança" (Fouad, 2021, p. 2, tradução nossa). Não basta, ainda, enxergar a ação humana em resposta ou a atuação dos artefatos tecnológicos como elementos separados: "um ataque cibernético só pode ser totalmente compreendido quando analisamos as várias entidades humanas e não humanas que o compõem e quando consideramos suas múltiplas associações" (Wagen, 2019, p. 153, tradução nossa)

As instruções de Bruno Latour (2005) para o emprego da ANT podem ser analisadas a partir de um pequeno conjunto de comandos centrais, tal como apresentado por Van Der Wagen (2019): seguir a ferramenta, o híbrido e a rede. Com a intenção de seguir tais comandos para a aplicação de ideias da Teoria Ator-Rede ao estudo da cibersegurança e do Pegasus, um dos primeiros movimentos a ser realizado é uma desconstrução de assimetrias, o que também pode ser entendido como a construção de uma simetria entre os diferentes elementos em análise.

Devemos abandonar determinações a priori sobre a supremacia de um ator sobre o outro em uma rede de relações, isto é, "precisamos acompanhar, ao mesmo tempo, as agências humanas e não humanas na constituição do social" (Capaverde; Fogaça; Henriqson, 2023, p. 7). Em resumo, "se quisermos saber

quem tem poder em um determinado contexto, precisamos descer ao chão e seguir a rede de associações por meio das quais o poder é exercido" (McCarthy, 2018, p. 229, tradução nossa).

Ao longo dos próximos capítulos abordarei o caso do *spyware* Pegasus a partir de relatos jornalísticos e relatórios técnicos, buscando seguir o traçado deixado pelo mesmo. Seguir o Pegasus a partir de seu rastro é um trabalho essencial de observação para a produção de uma pesquisa baseada em princípios dos STS e da ANT, pois permite redesenhar a rede de associações em que ele está inserido, sem categorias privilegiadas *a priori*. Significa, ainda, contar uma nova história sobre o caso do Pegasus, a partir da perspectiva daqueles que normalmente são ignorados ou ocultados: os não-humanos.

O próximo capítulo traz um relato do caso do Pegasus, nomeando alguns dos principais eventos, "atores" e dinâmicas observadas. O capítulo seguinte retornará então à discussão iniciada no presente capítulo, costurando as ideias da ANT e dos STS ao caso do Pegasus, focando especialmente nas ideias de agente, agência, redes e mediação.

3. O cavalo alado da cibersegurança: uma análise do Pegasus

Com o objetivo de implementar as recomendações de Bruno Latour (2005), da ANT e dos STS de maneira geral, proponho ao longo deste capítulo "seguir o ator" Pegasus, analisando as conexões que esse estabelece, as redes das quais faz parte e os efeitos que produz nessas. Parto inicialmente da "descoberta" do *spyware*, baseando-me nas investigações realizadas por um consórcio internacional de jornalistas, liderado pela organização Forbidden Stories. Baseio-me igualmente nos relatórios produzidos pelo laboratório de pesquisas Citizen Lab, da Universidade de Toronto e pelo Laboratório de Segurança da Amnesty International. Em seguida, analiso as repercussões desses relatórios e seus impactos na política internacional de maneira mais ampla. Encerro o capítulo contextualizando a atividade do Pegasus enquanto um dos elementos do mercado internacional de vulnerabilidades e de ferramentas de investigação/vigilância.

O presente capítulo é construído considerando o objetivo da ANT de "(re)traçar conexões ou associações entre diferentes tipos de atores e detectar como os atores que interagem atuam e agem, formam grupos, estabelecem estabilidade e mudam ao longo do tempo" (Wagen; Pieters, 2015, p. 6, tradução nossa). Analiso ao longo das próximas páginas os movimentos de agrupamento e reagrupamento das redes híbridas (formadas entre humanos e não-humanos) das quais o Pegasus faz parte (Wagen, 2019).

A observação dos movimentos de reorganização dessas redes, entretanto, deve ser observada em um momento de instabilidade dessas. De acordo com Balzacq e Cavelty (2016), "o sucesso de qualquer ator-rede geralmente está relacionado ao grau em que ela não parece ser uma rede que exige esforço para se manter unida, mas sim uma entidade coerente e independente (pontualização)" (p. 184, tradução nossa). A tendência das redes é a de estabilização e de aproximação de um estado de "caixa-preta", na qual não é possível enxergar sua composição. Torna-se necessário buscar momentos de "despontualização" (em inglês, *depunctualization*), isto é, de disruptura da rede a ser analisada.

Os momentos de despontualização para a ANT representam uma interrupção e alteração das performances da rede, tornando momentaneamente

visíveis os componentes da mesma para o observador (Balzacq; Cavelty, 2016). Classifico a descoberta do Pegasus como uma momento de despontualização, de disruptura da rede na qual o *spyware* está inserido, tornando possível enxergar as dinâmicas e os processos de reorganização dessa.

3.1. A descoberta do Pegasus: Ahmed Mansoor e os primeiros indícios

Nos dias 10 e 11 de agosto de 2016, Ahmed Mansoor, ativista dos direitos humanos nascido e atuante nos Emirados Árabes Unidos (EAU), recebeu mensagens instantâneas de tipo SMS (figura 1) em seu iPhone (Marczak; Scott-Railton, 2016). As mensagens em questão prometiam conter novas informações sobre torturas sofridas por emirates em prisões do Estado, assunto que seria do interesse do ativista, reconhecido por "fornecer uma avaliação confiável e independente da evolução dos direitos humanos no país" (Martin Ennals Award[9], 2015, tradução nossa).

Figura 1 - O SMS recebido por Ahmed Mansoor

Figure 3: SMS text messages received by Mansoor (English: "New secrets about torture of Emiratis in state prisons"). The sender's phone numbers are spoofed.

Fonte: Marczak; Scott-Railton, 2016

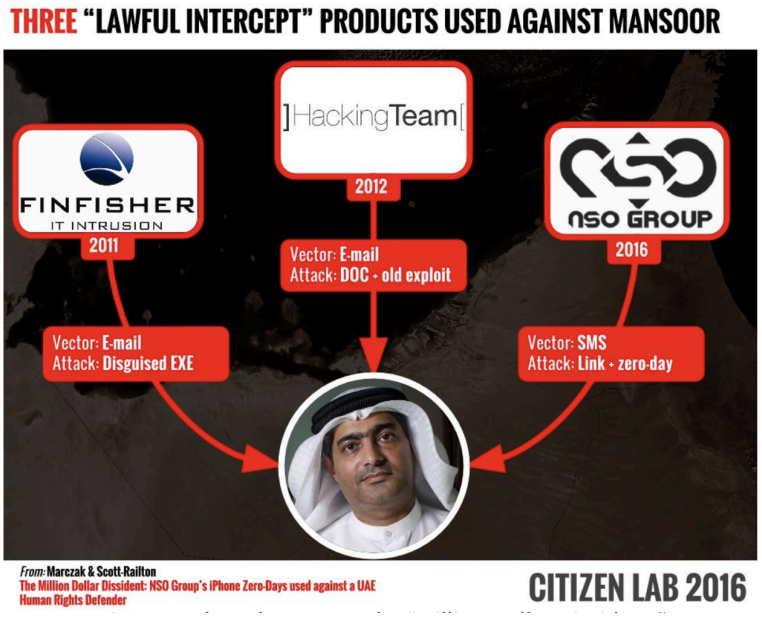
As mensagens, recebidas nos dias 10 e 11, continham links para o domínio "sms.webadv[.]co", um site que Mansoor não reconhecia. Ativista de direitos humanos em um país reconhecido por cercear a liberdade de expressão e de associação, além de ter um histórico de perseguição a opositores e manifestantes

[9] O prêmio é também reconhecido como "Prêmio Nobel dos Direitos Humanos", o qual Mansoor recebeu no ano de 2015.

contrários ao governo, Mansoor suspeitou da situação. Encaminhou os links recebidos para pesquisadores do Citizen Lab, para que pudessem averiguar se esses continham de fato informações relevantes sobre tortura ou se esses seriam mais uma tentativa de ciberataque contra o mesmo (Marczak; Scott-Railton, 2016).

O ativista emirate já havia sofrido outras tentativas de *hacking* nos anos de 2011 e 2012. Seu email havia sido alvo de *spywares* desenvolvidos pelas empresas FinFisher e Hacking Team (figura 1) (Marczak; Scott-Railton, 2016), proeminentes atores no universo da cibersegurança e do fornecimento de "ferramentas de investigação". A hipótese de que poderia se tratar de uma nova tentativa de invasão, portanto, não era inverossímil. Os pesquisadores do Citizen Lab iniciaram suas buscas e encontraram uma conexão entre os links recebidos por Mansoor e um conjunto de domínios potencialmente utilizados pela NSO Group (Marczak; Scott-Railton, 2016).

Figura 2 - As tentativas de hackear Ahmed Mansoor



Fonte: Marczak; Scott-Railton, 2016

O laboratório canadense estava naquele momento envolvido no mapeamento e análise das atividades do grupo conhecido como "Stealth Falcon"[10], "grupo que tem realizado ataques de spyware direcionados contra

[10] O grupo apresentaria conexões com o governo dos EAU, segundo relatórios posteriores do Citizen Lab. Mais informações em Marczak e Scott-Railton (2014), disponível em: https://citizenlab.ca/2016/05/stealth-falcon/

jornalistas, ativistas e dissidentes dos Emirados desde pelo menos 2012" (MITRE, 2017, tradução nossa). Ao cruzar as informações de suas investigações sobre o Stealth Falcon com os links enviados por Mansoor, os pesquisadores foram capazes de rastrear os domínios de redirecionamento até chegarem aos endereços "mail1.nsogroup[.]com" e "nsoqa[.]com", ambos registrados pela NSO (Marczak; Scott-Railton, 2016). A partir de então o processo de investigação seguiu o seguinte percurso, resumido pelos pesquisadores:

> Acessamos o link que Mansoor nos forneceu em nosso próprio iPhone 5 restaurado de fábrica (Mansoor tinha um iPhone 6) com iOS 9.3.3 (a mesma versão de Mansoor). Quando clicamos no link, vimos que ele estava de fato ativo e observamos quando um software desconhecido foi implantado remotamente em nosso telefone. Isso sugeria que o link continha um jailbreak remoto de dia zero para o iPhone: uma cadeia de explorações até então desconhecidas usadas para contornar remotamente as medidas de segurança do iPhone (Marczak; Scott-Railton, 2016, p. 9, tradução nossa).

Ahmed Mansoor havia sido, portanto, mais uma vez alvo de um ciberataque por meio de *spywares*, dessa vez com indícios de que o operador do ataque seria a NSO Group. O método de ataque também chamou a atenção dos pesquisadores por sua sofisticação: utilizava uma combinação de 3 vulnerabilidades do sistema operacional do iPhone, o iOS[11], que até o momento não eram conhecidas/não haviam sido reportadas. Abordarei a seguir o funcionamento do ataque em mais detalhes, para posteriormente retornar ao relato dos desdobramentos da descoberta protagonizada pelos pesquisadores do Citizen Lab.

3.2 Funcionamento da ferramenta

> O Pegasus é uma solução de inteligência cibernética líder mundial que permite que as agências de aplicação da lei e de inteligência extraiam remota e secretamente informações valiosas de praticamente qualquer dispositivo móvel. Essa solução inovadora foi desenvolvida por veteranos de agências de inteligência de elite para oferecer aos governos uma maneira de enfrentar os novos desafios de interceptação de comunicações no atual campo de batalha cibernético altamente dinâmico (NSO Group, 2013?, p.7 tradução nossa)

[11] A combinação de vulnerabilidades ficou conhecida como "Tridente" e seu funcionamento foi abordado em detalhes pela empresa de cibersegurança Lookout. Mais informações no relatório de Bazaliy et al. (2016), disponível em: https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

O trecho acima foi retirado de um documento cuja produção é atribuída à própria NSO[12] e que foi disponibilizado na Internet[13] pelo pesquisador de cibersegurança Claudio Guarnieri, também associado ao Citizen Lab. Desenhado como uma "solução de inteligência" para o "atual campo de batalha cibernético altamente dinâmico" (NSO Group, 2013?, p. 7, tradução nossa), o Pegasus é, efetivamente, um *spyware*, ou ferramenta de vigilância, e "contém códigos, processos e aplicativos mal-intencionados que são usados para espionar, coletar dados e informar o que o usuário faz no dispositivo" (Bazaliy et al., 2016, p. 7, tradução nossa). Mas como essa ferramenta efetivamente funciona?

O sistema de ataque do *spyware* identificado no iOS 9.3.3, versão do sistema operacional presente no aparelho de Mansoor em 2016, consiste em corromper os aplicativos já presentes no dispositivo, como o FaceTime e o calendário, de maneira que possam ser transformados em ferramentas de espionagem: comunicações de áudio e vídeo de forma geral, além mensagens SMS podem ser interceptadas e enviadas de volta para um centro de comando que opera o spyware em questão (Bazaliy et al., 2016). Ao ser infectado pelo Pegasus, o aparelho-alvo torna-se um novo ponto de coleta de informações, que posteriormente poderão ser utilizadas por agências de segurança e investigação.

Além de ser capaz de extrair os tipos de dados citados acima, a NSO descreve como pontos relevantes do Pegasus a sua: capacidade de acessar dispositivos protegidos por senhas; ser invisível para o alvo e não deixar rastros no dispositivo; ter consumo reduzido de bateria, memória e dados celulares; ser capaz de se autodestruir em caso de possível exposição; além de ser capaz de recuperar arquivos armazenados no dispositivo e enviá-los para a central de comando e controle (NSO Group, 2016).

O método de ataque descrito pelos pesquisadores do Citizen Lab e da Lookout é simultaneamente simples e silencioso em seu início: caso Ahmed Mansoor tivesse clicado nos links presentes nas mensagens SMS, seu dispositivo seria "desbloqueado" e o software seria instalado de forma remota e invisível.

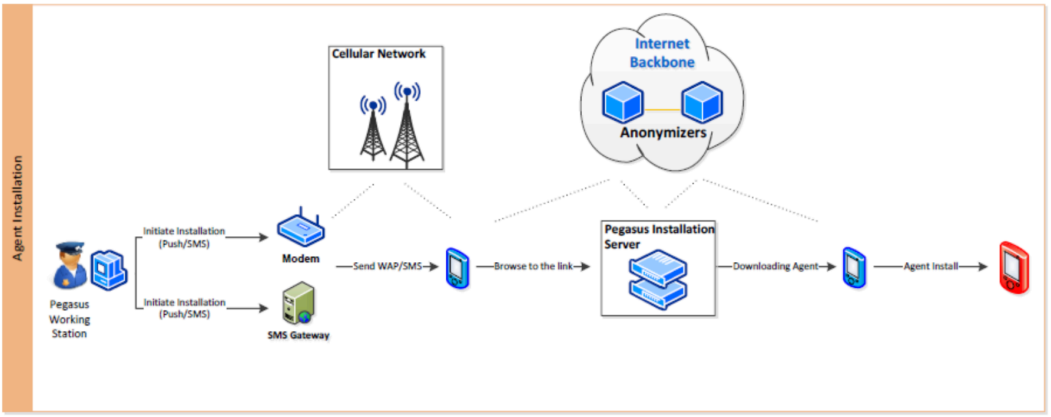
---

[12] Ao baixar o documento (disponibilizado em https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf) e extrair seus metadados, é possível ver que a criação do arquivo é atribuída a Guy Molho, anteriormente listado como "Director of Product Management at NSO Group" em seu perfil na rede social LinkedIn (Marczak, Scott-Railton 2016).

[13] Diferentes documentos relacionados à NSO Group foram divulgados em meio ao vazamento de dados sobre a empresa italiana Hacking Team em 2015. Exemplos dos documentos disponibilizados no site WikiLeaks: https://wikileaks.org/hackingteam/emails/emailid/5391

Apenas um clique é necessário para que o Pegasus possa ocupar um novo hospedeiro.

Figura 3 - Processo de instalação do Pegasus



Fonte: Marczak; Scott-Railton, 2016

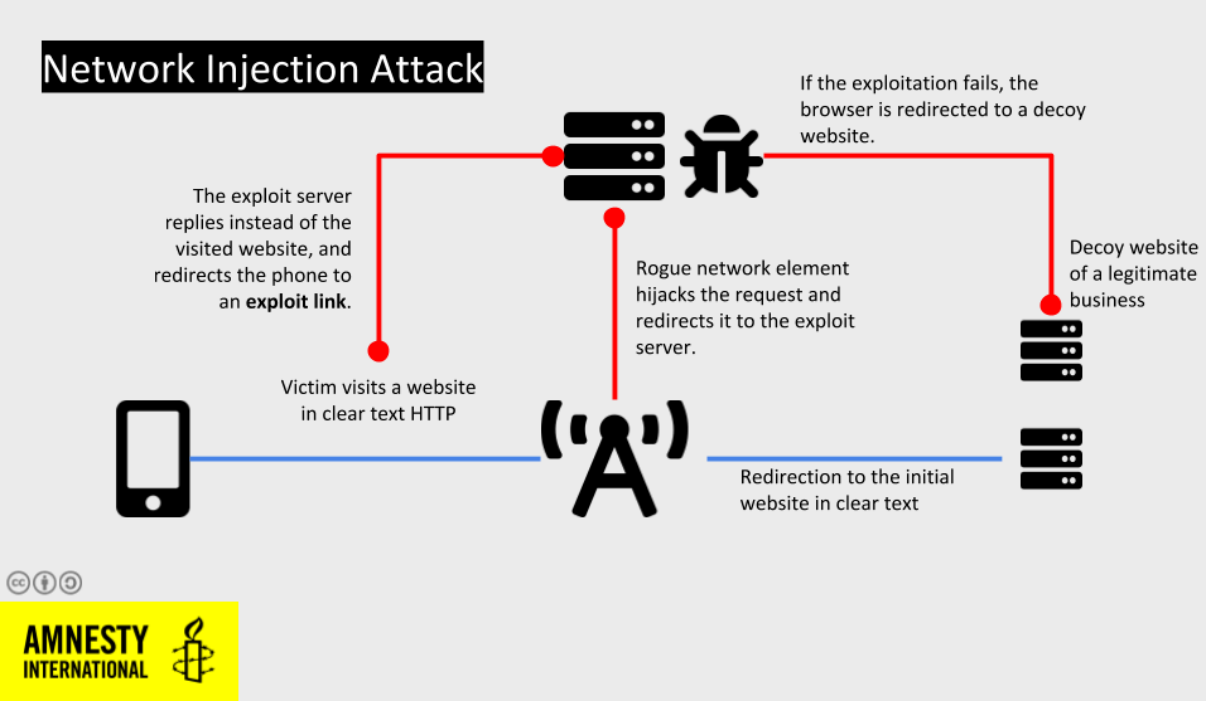
Embora esse vetor de ataque, com apenas um clique, já demonstre a complexidade e o refino do *spyware* desenvolvido pela NSO Group, os métodos desenvolvidos posteriormente são ainda mais impressionantes. Após a publicações dos relatórios do Citizen Lab (2016) e da Lookout (2016), a Apple, criadora e fornecedora do iOS, trabalhou rapidamente para que as vulnerabilidades utilizadas pelo Pegasus até então fossem resolvidas.

Após atualizações para o iOS serem disponibilizadas pela Apple, a NSO desenvolveu novas formas de acessar e "infectar" os dispositivos, agora sem a necessidade de intervenção direta do usuário. Este método é baseado em vulnerabilidades do tipo zero clique (em inglês, *zero-click*), consideradas como algumas das mais complexas e de difícil descoberta/desenvolvimento.[14] Esse novo método, analisado em detalhes pelo Laboratório Internacional de Segurança da Amnesty International(2021) e pelo Citizen Lab em 2020, permite que o Pegasus manipule processos locais dos iOS, como o *Apple's Push Notification Service* (APNs), para realizar a infecção remotamente (Marczak et al., 2020). Este novo processo de infecção está ilustrado na figura 4, abaixo.

[14] A empresa americana Zerodium atua no mercado de cibersegurança, oferecendo diferentes valores a pesquisadores que sejam capazes de encontrar novas vulnerabilidades. O site da empresa lista como possíveis valores para vulnerabilidades de zero clique no sistema iOS recompensas de até 2 milhões de dólares. Os valores oferecidos pela empresa podem ser acessados: https://zerodium.com/program.html

A consequência direta do novo vetor de invasão do Pegasus é a possibilidade de superação de um dos principais instrumentos de defesa contra ataques cibernéticos, que ainda pode ser mobilizada quando as barreiras técnicas são superadas: o conhecimento e treinamento sobre cibersegurança[15].

Figura 4 - Invasão remota do Pegasus



Fonte: Amnesty International, 2020

3.3 Projeto Pegasus: bastidores e revelações

3.3.1 A lista e o início do projeto

O Pegasus é descrito pela NSO como uma ferramenta cujo uso é destinado exclusivamente a forças de segurança pública e agências de inteligência (NSO, 2019). Seu valor seria contribuir para que alguns dos principais desafios enfrentados atualmente por agentes de segurança sejam superados, entre eles: a

[15] Faço referência ao conceito *cyber security awareness*, em inglês. A conscientização sobre a segurança cibernética envolve educar e informar indivíduos e organizações sobre os riscos associados às atividades cibernéticas e as práticas recomendadas para mitigar esses riscos. No caso do Pegasus, o vetor de ataque por meio de mensagens SMS permitia que os usuários tivessem a chance de levantar suspeitas sobre a possibilidade de serem alvos do *spyware*. No momento em que o vetor de ataque é alterado para um modelo zero clique, torna-se ainda difícil a identificação do ataque por parte dos usuários, dificultando o processo de conscientização e de proteção contra a ferramenta em questão.

difusão da criptografia; a abundância de aplicações de comunicação diferentes; a utilização de diferentes identidades virtuais; entre outros (NSO, 2016). Segundo a empresa, "até que os desafios mencionados acima sejam abordados e resolvidos, os alvos criminosos e terroristas provavelmente estarão 'a salvo' dos sistemas de interceptação padrão e tradicionais, o que significa que inteligência valiosa está sendo perdida" (NSO, 2016, p. 7, tradução nossa).

O *spyware* é, em suma, apresentado como uma ferramenta de investigação, de combate ao crime e ao terrorismo. Por outro lado, a realidade de sua utilização está distante da versão oficial oferecida pela NSO. O relatório divulgado pelo Citizen Lab em 2016 sobre Ahmed Mansoor foi responsável por levantar suspeitas sobre a possibilidade múltiplos de abusos estarem sendo praticados por meio do Pegasus, em uma escala global. Os Emirados Árabes Unidos e Mansoor seriam um pequeno recorte da atuação global do *spyware*, o que instigou jornalistas e pesquisadores ao redor do mundo a se debruçar sobre o tema. Inicia-se então um movimento investigativo internacional, liderado pela organização Forbidden Stories, chefiada pelos jornalistas franceses Laurent Richard e Sandrine Rigaud: o Projeto Pegasus[16]

A conexão de Rigaud e Richard com o Pegasus é iniciada através da organização jornalística sem fins lucrativos denominada Forbidden Stories, fundada em 2017 por Richard. A organização tem como objetivo dar prosseguimento às investigações realizadas por jornalistas que foram assassinados, o que está representado em um de seus lemas: matar o jornalista não vai matar a história[17]. Desde 2017 a organização já colaborou com mais de 150 jornalistas de ao menos 49 países ao redor do mundo, produzindo investigações que buscam expor regimes autoritários e lutar contra a censura.

Os líderes da Forbidden Stories, Richard e Rigaud, escolheram não revelar ao público maiores detalhes sobre como adquiriram uma lista contendo mais de 50.000 números telefônicos que teriam sido escolhidos como possíveis alvos de ataques por meio do *spyware* Pegasus, mencionando apenas que tal lista havia sido compartilhada por um *whistleblower* na segunda metade do ano de 2020 (Richard; Rigaud, 2023). A lista em si continha apenas números que haviam

[16] Em inglês, Pegasus Project. O site do projeto pode ser acessado em: https://forbiddenstories.org/about-the-pegasus-project/
[17] Em inglês: "Killing the journalist won't kill the story"

potencialmente sido alvos do Pegasus, algo que deveria ser checado pelos jornalistas antes que tal informação pudesse ser divulgada para o público geral. O objetivo inicial seria, portanto, a identificação dos números presentes na lista, de maneira que fosse possível posteriormente verificar, caso a caso, a possibilidade de que esses tivessem sido alvos do Pegasus.

A investigação pela Forbidden Stories envolveu mais uma vez Claudio Guarnieri, pesquisador do Citizen Lab e da Amnesty Internationalem seu laboratório sobre segurança, que já havia colaborado com a investigação de 2016 que revelou a tentativa de invasão ao aparelho celular de Mansoor. Os três encontraram-se em Berlim para reuniões sobre como o processo de investigação poderia ser organizado e, ao compararem os números de telefone presentes na lista de possíveis alvos do Pegasus com os contatos telefônicos de Laurent Richard, os primeiros resultados começaram a aparecer: um oficial do Ministério das Relações Exteriores da Turquia, Khadija Ismayilova (repórter investigativa no Azerbaijão), alguns políticos franceses e Jorge Carrasco (jornalista mexicano) (Richard; Rigaud, 2023).

A partir de então, a Forbidden Stories, o Citizen Lab, o Laboratório de Segurança da Amnesty International, além de 80 jornalistas de 17 organizações de ao menos 10 países estiveram envolvidos na missão de verificar os números telefônicos presentes na lista vazada e obtida por Richard e Rigaud, de maneira que pudessem compreender e relatar a extensão das atividades do Pegasus. A tarefa em questão incluía uma comunicação direta com os indivíduos afetados, de maneira que seus aparelhos pudessem ser submetidos a testes que comprovariam a presença de indícios da atuação do Pegasus. Para tal, a Anistia criou um kit de ferramentas de verificação móvel (MVT), disponibilizado gratuitamente para que indivíduos pudessem testar seus próprios aparelhos de maneira autônoma[18].

Simultaneamente, os investigadores da Anistia e do Citizen Lab tiveram como objetivo relacionar as evidências encontradas nos aparelhos à NSO de maneira clara e evidente, uma tarefa complexa dada a natureza suposta "invisibilidade" do *spyware*, tal como prometido pela empresa. A metodologia de investigação forense desenvolvida pela Anistia (2021), passou por uma revisão de

[18] A ferramenta disponibilizada pelo Laboratório de Segurança da Amnesty Internationalpode ser acessada em: https://docs.mvt.re/en/latest/

pares independente, realizada pelo Citizen Lab[19], garantindo que o processo seria tecnicamente sólido, sendo capaz de produzir resultados confiáveis.

Após aproximadamente seis meses de investigação, no dia 18 de julho de 2021, as 17 organizações envolvidas no Projeto Pegasus divulgaram suas primeiras matérias e relatórios de forma sincronizada. Detalharei ao longo da próxima seção alguns dos principais resultados encontrados e os impactos da mesma para a NSO e para a política internacional de forma mais ampla.

3.3.2 Principais conclusões

Entre agosto de 2016 e agosto de 2018, anos antes do Projeto Pegasus, o Citizen Lab realizou inúmeras varreduras pela Internet, buscando traços da atuação do Pegasus e mapeando a infraestrutura de servidores utilizada pela NSO. Através de técnicas de investigação próprias, o laboratório foi capaz de identificar 1091 endereços IP e 1014 domínios que estariam associados às "digitais" da NSO (Marczak et al., 2018). Agrupando os dados coletados e classificando-os de acordo com sua geolocalização, os pesquisadores encontraram 45 países nos quais a NSO e o Pegasus poderiam estar atuando (figura 5), sendo 6 deles países portadores de um histórico de utilizar spywares contra membros da sociedade civil: Bahrein, Cazaquistão, México, Marrocos, Arábia Saudita e Emirados Árabes Unidos (Marczak et al., 2018).

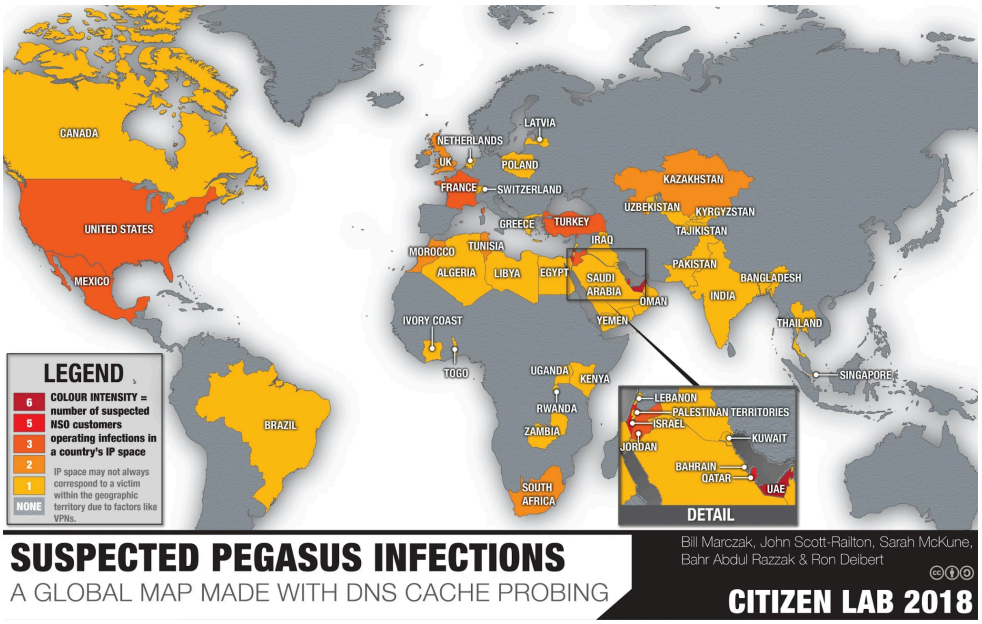
Outro resultado importante encontrado pelo Citizen Lab em 2018 foi a identificação de 10 países que estariam possivelmente envolvidos em espionagem internacional. Isto significa que entidades operadoras[20] do Pegasus poderiam estar espionando indivíduos em outros Estados, além de seu próprio território nacional. Essa dinâmica não seria inédita, pois o Citizen Lab já havia identificado um caso no qual jornalistas do Serviço de televisão por satélite da Etiópia (ESAT),

[19] O parecer do Citizen Lab sobre a metodologia de investigação da Amnesty International afirma que "A própria pesquisa do Citizen Lab chegou, de forma independente, a várias das principais conclusões da Anistia" (2021, tradução nossa). O laboratório canadense concluiu que a identificação dos processos afetados pelo Pegasus e a atribuição dessas operações à NSO teriam fundamentação técnica. O parecer completo pode ser acessado em: https://citizenlab.ca/2021/07/amnesty-peer-review/

[20] Vale reforçar a diferenciação entre os operadores do Pegasus e a NSO Group. De acordo com o relatório de transparência e responsabilidade divulgado pela empresa em 2021, "A NSO licencia o Pegasus para estados soberanos e agências estaduais, não opera o Pegasus, não tem visibilidade de seu uso e não coleta informações sobre os clientes" (p. 6, tradução nossa). O relatório de 2021 está disponível em: https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf

baseados nos Estados Unidos, haviam sido possíveis alvos de um outro *spyware*, produzido pela empresa italiana Hacking Team[21], uma das líderes do mercado de ciberespionagem antes da ascensão da NSO e do Pegasus.

Figura 5 - Mapa de possíveis infecções pelo Pegasus



Fonte: Marczack et al., 2018

A divulgação dos resultados do Projeto Pegasus corrobora os resultados das pesquisas iniciais realizadas pelo Citizen Lab. O mapeamento[22] dos números de telefones presentes na lista obtida por Richard e Rigaud permitiu a identificação de 11 países que seriam possíveis clientes da NSO, entre eles: Azerbaijão, Bahrein, Hungria, Índia, Cazaquistão, México, Marrocos, Ruanda, Arábia Saudita, Togo e Emirados Árabes Unidos (EAU) (Amnesty International, 2021). Esse mapeamento foi capaz de rastrear e identificar:

[21] A italiana Hacking Team desenvolveu o software Remote Control System (RCS), definido pelo Citizen Lab como um spyware capaz de "gravar chamadas do Skype, copiar senhas, e-mails, arquivos e mensagens instantâneas e ligar a webcam e o microfone de um computador ou telefone para espionar atividades próximas" (Marczak et al., 2014, tradução nossa). O *spyware*, tal como o Pegasus da NSO, também seria comercializado apenas para entidades governamentais, sendo também descrito como "irrastreável". Mais informações sobre o RSC da Hacking Team e seu envolvimento em espionagem transfronteiriça podem ser encontradas no relatório do Citizen Lab, disponível em: https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/

[22] O "Organized Crime and Corruption Reporting Project" disponibilizou uma plataforma online na qual é possível consultar diversos nomes e figuras identificadas como possíveis alvos do Pegasus. A plataforma está disponível em: https://cdn.occrp.org/projects/project-p/#/

> mais de 1.000 pessoas em mais de 50 países por meio de pesquisas e entrevistas em quatro continentes: vários membros da família real árabe, pelo menos 65 executivos de empresas, 85 ativistas de direitos humanos, 189 jornalistas e mais de 600 políticos e funcionários do governo - incluindo ministros de gabinete, diplomatas e oficiais militares e de segurança, bem como 10 primeiros-ministros, três presidentes e um rei (Washington Post, 2021, tradução nossa).

Evidências concretas de ataques bem-sucedidos do Pegasus foram identificadas em 37 aparelhos telefônicos de jornalistas, ativistas dos direitos humanos e empresários, o que foi possível graças à ferramenta MVT desenvolvida pela Amnesty International (Mekhennet; Priest; Timberg, 2021). Figuras públicas proeminentes como Emmanuel Macron, presidente da França, também foram identificados como possíveis alvos, (Leloup; Untersinger, 2021) o que reabriu debates importantes sobre soberania e cibersegurança no contexto da espionagem digital.

Ronald Deibert (2023), professor candadense de ciência política, fundador e diretor do Citizen Lab, chama atenção para o fato de que não são apenas governos ditatoriais que figuram como clientes da NSO. Democracias como a Espanha, o México e até mesmo os Estados Unidos já estabeleceram negócios com a empresa israelense. A União Europeia, por exemplo, também esteve em meio ao escândalo envolvendo o *spyware*, figurando não apenas como possível alvo dos ataques, o que pode ser observado na presença de Macron na lista de supostos alvos do Pegasus, mas também como tendo 14 Estados-membros que teriam adquirido a ferramenta de origem israelense.

Após a divulgação do Projeto Pegasus, foi estabelecido a Comissão de Inquérito do Parlamento Europeu para investigar o uso do Pegasus e de spywares de vigilância equivalentes (Comissão PEGA)[23]. As análises realizadas pela comissão foram posteriormente abordadas pelo Comitê de Assuntos Jurídicos e Direitos Humanos do Conselho da Europa, o qual afirma por meio de uma de suas resoluções que:

> Sabe-se que o Pegasus foi vendido para pelo menos 14 países da União Europeia, incluindo Polônia, Hungria, Espanha, Holanda, Alemanha (em uma versão modificada), Bélgica e Luxemburgo. Há fortes evidências de que o Azerbaijão também o utilizou, inclusive durante seu conflito com a Armênia. Outros Estados membros

[23] Os relatórios da Comissão PEGA (em inglês, PEGA Committee) estão disponíveis em: https://www.europarl.europa.eu/committees/en/pega/documents/latest-documents

> adquiriram ou usaram ferramentas de spyware semelhantes, como o Candiru e o Predator. Essas ferramentas não foram usadas apenas dentro da jurisdição dos Estados membros, mas também foram exportadas para países terceiros com regimes autoritários e alto risco de violação dos direitos humanos, incluindo a Líbia (sob o regime de Gaddafi), o Egito, Madagascar e o Sudão. Essas exportações podem ter violado as regras de exportação da UE (2018,

O artigo de Deibert para a revista Foreign Affairs, corrobora e resume os resultados das investigações do Projeto Pegasus e da Comissão PEGA, indicando a utilização do Pegasus nos seguintes contextos: monitoramento de movimentos de oposição, principalmente no período que antecede as eleições; infiltração em organizações da sociedade civil e instituições governamentais; rastreamento e agressão física de dissidentes que vivem no exílio; enfraquecimento de autoridades judiciais e organizações da sociedade civil; perseguição a advogados que representam vozes dissidentes; espionagem em nome de clientes privados em todo o mundo (Deibert, 2023).

Richard e Rigaud resumem os achados de sua investigação ao afirmarem que "o problema mais grave do sistema Pegasus era que ele não se limitava a espionar os bandidos" (p. 6, tradução nossa). Essa interpretação dos fatos é frontalmente refutada pela empresa israelense. Há de um lado a afirmação da NSO Group de que não havia jamais desviado de sua missão de "tornar o mundo um lugar mais seguro, auxiliando investigações legais realizadas por autoridades estatais para proteger a segurança dos cidadãos contra crimes graves e terrorismo" (2021, p. 5, tradução nossa). De outro, inúmeros casos da utilização da ferramenta como forma de perseguição a opositores dos governos contratantes do Pegasus, que habilmente classificam seus alvos como ameaças em potencial, portanto legitimando o uso da ferramenta como medida de segurança.

Exploro a seguir de maneira breve o caso de Jamal Khashoggi, ilustrando os efeitos práticos dos abusos que podem ser cometidos a partir do *spyware*, o que coloca à prova as afirmações da NSO sobre sua ferramenta.

3.3.3 Anatomia de uma invasão: Jamal Khashoggi, suas mulheres e o vírus

O jornalista de origem saudita Jamal Khashoggi entrou no consulado da Arábia Saudita na Turquia às 13:14 (horário local) do dia 2 de outubro de 2018,

sem nunca mais ter retornado (BBC, 2021). Investigações posteriores ao fato revelaram que o jornalista saudita foi assassinado e possivelmente esquartejado por indivíduos que estavam dentro do consulado. O jornal turco Daily Sabah divulgou no dia 9 de setembro de 2019, quase um ano após a morte do jornalista, transcrições de gravações que teriam sido realizadas dentro do consulado, possivelmente originadas de grampos pela agência de inteligência turca[24] (Simsek; Karaman, 2019). Segundo o jornal, às 13:39 seria possível ouvir o som de uma serra de autópsia, possivelmente utilizada para esquartejar o corpo do jornalista durante aproximadamente 30 minutos.

O relato brutal dos últimos minutos de Khashoggi está diretamente relacionado ao *spyware* Pegasus e seus efeitos. Após o assassinato do jornalista saudita, a análise forense dos aparelhos telefônicos de pessoas próximas ao mesmo revelou que sua esposa egípcia Hanan Elatr, assim como sua noiva turca, Hatice Cengiz, haviam sido alvos do *spyware* (Kirchgaessner, 2021). Não é possível afirmar com precisão de que maneira o Pegasus teria sido utilizado no caso de Khashoggi, porém é possível imaginar que o monitoramento do círculo de pessoas próximas ao jornalista tenha sido instrumental para arquitetar o seu assassinato.

Contrariando as conclusões da análise forense realizada pela Amnesty International, a NSO afirmou por meio de nota em seu website que "nossa tecnologia não foi associada de forma alguma ao hediondo assassinato de Jamal Khashoggi. Podemos confirmar que nossa tecnologia não foi usada para ouvir, monitorar, rastrear ou coletar informações sobre ele ou seus familiares mencionados na investigação" (2021, tradução nossa).

O envolvimento do Pegasus no assassinato de Khashoggi é ilustrativo das capacidades destrutivas do *spyware* e de sua utilização como ferramenta de vigilância, monitoramento e perseguição[25]. Analiso a seguir de que maneiras a NSO Group conseguiu permanecer relevante e funcional enquanto empresa, mesmo em meio a inúmeros escândalos sobre seu principal produto, o Pegasus.

---

[24] Turkey's National Intelligence Organization (MIT)

[25] Ahmed Mansoor, citado no início do capítulo, segue sob custódia das autoridades dos Emirados Árabes Unidos até a publicação do presente trabalho. Mais informações podem ser encontradas no artigo do Jersulem Post (2024), disponível em: https://www.jpost.com/middle-east/article-781120

3.4 Cavalo-camaleão: respostas da NSO e sua mutabilidade

3.4.1 Reações da empresa ao Projeto Pegasus

> O relatório da Forbidden Stories está repleto de suposições erradas e teorias não corroboradas que levantam sérias dúvidas sobre a confiabilidade e os interesses das fontes. Parece que as "fontes não identificadas" forneceram informações que não têm base factual e estão longe da realidade. Depois de verificar suas alegações, negamos firmemente as falsas alegações feitas em seu relatório. Suas fontes forneceram informações que não têm base factual, como fica evidente pela falta de documentação de apoio para muitas de suas alegações. Na verdade, essas alegações são tão ultrajantes e distantes da realidade que a NSO está considerando um processo por difamação (NSO, 2021, tradução nossa).

A reação por parte da NSO Group após a divulgação dos relatórios iniciais do Citizen Lab e do Projeto Pegasus foi de, majoritariamente, negar seu envolvimento em situações de "mau uso" de seus produtos. Simultaneamente, a empresa afirma em seu relatório de transparência de 2023 que "reconhecemos plenamente que ferramentas sofisticadas de inteligência cibernética, como o Pegasus, podem ser mal utilizadas para afetar negativamente o direito à privacidade dos indivíduos, reprimir a liberdade de expressão e prejudicar o discurso público" (NSO, 2023, p. 9, tradução nossa).

Os relatórios divulgados pela empresa trazem também dados que podem complementar as pesquisas anteriores do Projeto Pegasus. Se no ano de 2018 o Citizen Lab reportou que operadores do Pegasus poderiam estar espalhados por 45 países, a NSO confirmou em 2023 as suas operações em 31 países (NSO, 2023), com 56 clientes distintos.

Há uma necessidade de reposicionamento da empresa, afastando-a da associação com governos autoritários, assassinatos e perseguições a jornalistas. A NSO afirma ainda em seu relatório de 2023 que desde 2021 já abriu 19 investigações sobre potenciais casos de mau uso de suas ferramentas, além de argumentar que nos últimos dois anos teria suspendido ou terminado as operações de 6 clientes como resultados dessas investigações, o que teria resultado em uma perda de 57 milhões de dólares (NSO, 2023). Desde 2021 teriam também declinado 10% dos potenciais novos clientes por preocupações com direitos humanos.

A divulgação de relatórios de transparência pela empresa pode ser classificada como uma das estratégias de sobrevivência do ponto de vista mercadológico. Por meio desses, reafirma seu comprometimento com os direitos humanos, chama atenção para alguns de seus "feitos" importantes, além de esclarecer "equívocos" sobre o Pegasus e suas reais capacidades. A produção de relatórios de transparência, de uma política para *whistleblowers*[26], além de uma política própria de direitos humanos[27], faz parte da capacidade de adaptação e mutabilidade da empresa.

Uma das principais argumentações utilizadas pela NSO para defender as negociações que estabelece com diferentes governos e agências de inteligência baseia-se no fato de que o Pegasus seria um "artigo de defesa", isto é "a tecnologia Pegasus está sujeita a rigorosas leis de controle de exportação. Por exemplo, a NSO Group é obrigada a obter licenças de marketing e exportação da Defense Exports Control Agency ("DECA") do Ministério da Defesa de Israel para se envolver em qualquer discussão de vendas" (NSO, 2023, p. 8, tradução nossa).

A chancela de Israel para as negociações da NSO transformou o *spyware* em uma moeda de troca importante na política internacional. Relatos do jornal inglês The Guardian sobre a política envolvendo o Pegasus questionam a aquisição da ferramenta logo após a visita do Primeiro Ministro de Israel, Benjamin Netanyahu a países como Índia e Hungria (Kirchgaessner; Holmes; Walker, 2021). Ademais, países considerados "inimigos" de Israel, como a Turquia, parecem não ter adquirido o software espião, o que não seria uma coincidência, mas sim uma movimentação política de Israel, utilizando a NSO e o cobiçado Pegasus como uma ferramenta diplomática.

3.4.2. Estrutura empresarial em transformação

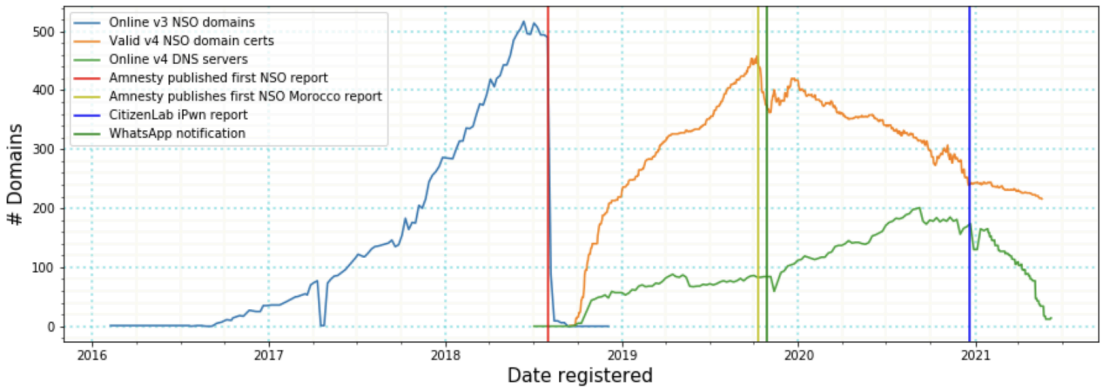
A compreensão do caso Pegasus depende de uma investigação sobre a infraestrutura técnica e jurídica da NSO Group, pois são essas que permitem a continuidade das operações da empresa e de suas ferramentas de vigilância. A

[26] A política de *whistleblower* da NSO Group pode ser acessada em: https://www.nsogroup.com/governance/whistleblower-policies/
[27] A política de direitos humanos da NSO Group pode ser acessada em: https://www.nsogroup.com/governance/human-rights-policy/

análise da infraestrutura técnica utilizada pela NSO revela uma rede complexa de servidores e protocolos projetados para evitar a detecção e a rastreabilidade do *spyware*. O relatório inicial do Citizen Lab sobre Mansoor mostra que a empresa israelense utiliza uma rede *proxy* para anonimizar e mascarar suas operações, a Pegasus Anonymizing Transmission Network (PATN) Marczak; Scott-Railton, 2016. Dessa forma a identidade dos operadores pode ser preservada, efetivamente ofuscando a identidade do governo associado a uma infecção em particular. Essa estratégia já havia sido utilizada por outras produtoras de *spywares*, como a italiana Hacking Team e pela anglo-germânica Gamma International, desenvolvedora do FinFisher (Marczak; Scott-Railton, 2016).

A análise da infraestrutura técnica da NSO revela uma rede complexa de servidores e protocolos projetados para evitar a detecção e a rastreabilidade. No entanto, os esforços contínuos de organizações como o Citizen Lab e a Amnesty International têm se mostrado eficazes na desarticulação parcial dessa rede. Esses esforços resultaram na identificação e mapeamento de servidores ativos associados ao Pegasus, como representado na figura 6, que ilustra uma queda significativa no número de servidores ativos após cada relatório publicado por essas entidades. Uma queda no número de servidores ativos identificados após cada relatório demonstra uma reação da NSO, efetivamente mostrando que os pesquisadores de ambas as organizações foram capazes de mapear, ao menos em parte, elementos importantes da estrutura técnica utilizada pelo *spyware*.

Figura 6 - Gráfico de servidores associados à NSO Group



Fonte: Amnesty International, 2021

A reação da NSO Group à divulgação desses relatórios demonstra uma tentativa de adaptação e ocultação de suas operações. Cada relatório publicado não apenas aumenta a conscientização global sobre o uso do spyware, mas também pressiona a NSO a modificar suas práticas e infraestrutura para escapar da detecção. Essa dinâmica de "gato e rato" evidencia a eficácia das investigações conduzidas pelo Citizen Lab e pela Amnesty International, cujos pesquisadores foram capazes de mapear, ao menos em parte, elementos cruciais da estrutura técnica utilizada pelo Pegasus. A queda no número de servidores ativos é um indicativo claro de que as estratégias de mapeamento e exposição têm impactos reais na capacidade operacional do Pegasus.

Além da infraestrutura técnica, é crucial considerar a infraestrutura jurídica que sustenta as operações da NSO Group. A empresa opera em um ambiente regulatório que, até certo ponto, permite a proliferação de suas ferramentas de vigilância. A análise das bases legais e das políticas de exportação de tecnologia de segurança cibernética de Israel é fundamental para compreender como a NSO continua a fornecer seus serviços a governos e outras entidades ao redor do mundo.

Uma investigação realizada em conjunto pela Amnesty International, Privacy Internacional e pelo The Centre for Research on Multinational Corporations (SOMO) revela que a “falta de transparência em relação à estrutura corporativa do NSO Group e a falta de informações sobre as jurisdições relevantes em que opera são barreiras significativas na busca da prevenção e responsabilização por violações de direitos humanos relacionadas aos produtos e serviços do NSO Group” (Amnesty International, 2021, p. 6, tradução nossa).

Baseando-se em bancos de dados de registros de empresas e em pesquisas anteriores realizadas por jornalistas e organizações da sociedade civil, o relatório publicado pela Amnesty International Inicia seu rastreamento da NSO Group com base em sua criação em Israel em 25 de Janeiro de 2010, sob o nome de NSO Group Technologies Ltd[28] (Amnesty International, 2021). Desde sua fundação em

[28]O relatório observa que embora a “NSO Group Technologies Ltd. seja uma empresa limitada incorporada e registrada em Israel, “NSO Group” também é um termo genérico usado pela empresa e pela mídia para se referir às várias empresas relacionadas” (Amnesty International, 2021, p. 31, tradução nossa).

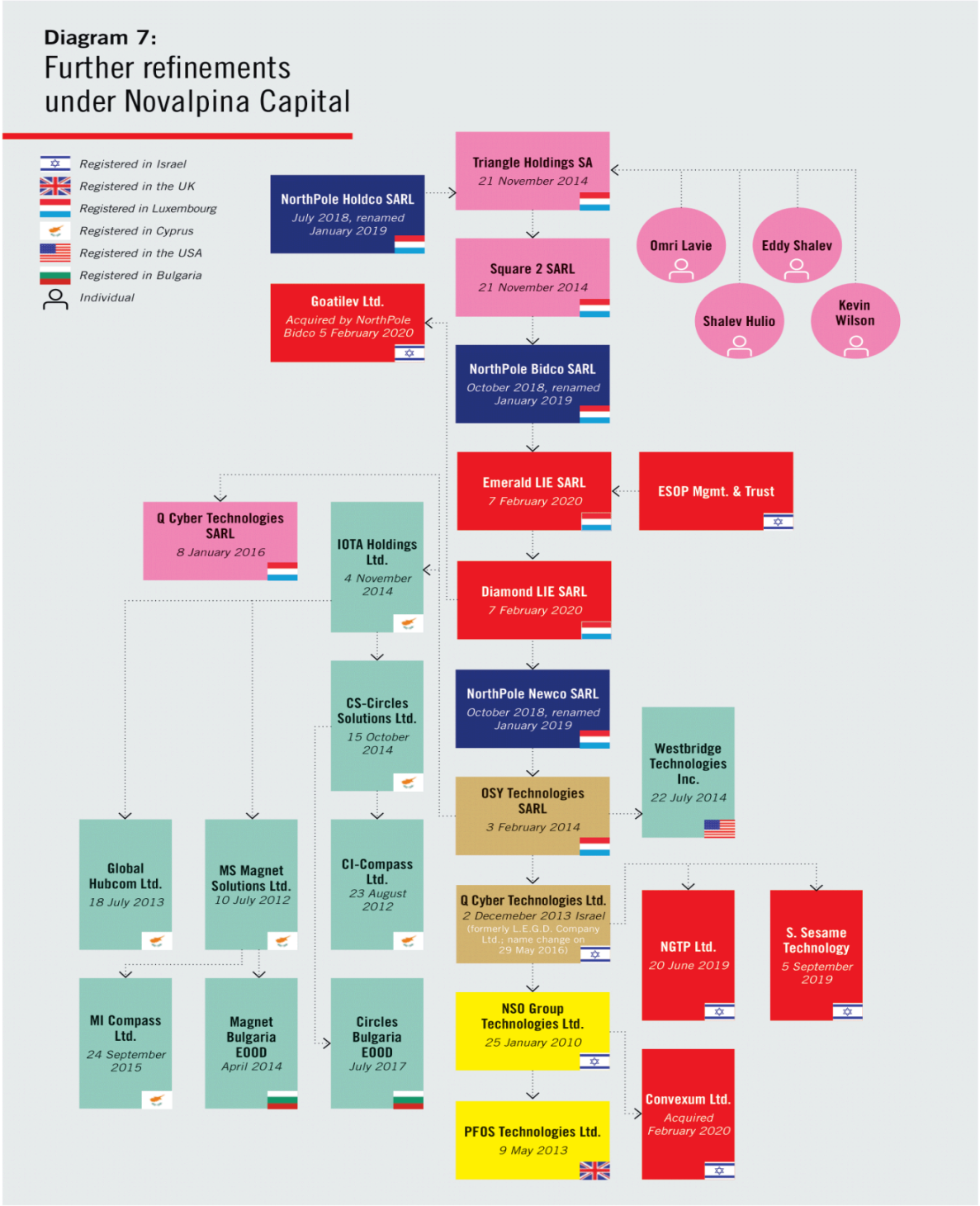
2010, a empresa vivenciou aquisições por empresas de *private equity* e expansão para diversos países.

Em 2014, a Francisco Partners, firma de private equity americana, adquiriu uma participação majoritária no NSO Group. Em 2019, a empresa passou por uma aquisição por parte da administração com o apoio da Novalpina Capital, firma de *private equity* do Reino Unido. Atualmente, o NSO Group opera em diversas jurisdições, incluindo Ilhas Virgens Britânicas, Bulgária, Ilhas Cayman, Chipre, Israel, Luxemburgo, Reino Unido e EUA.

É importante notar que o NSO Group possui licenças de exportação em Israel e Bulgária, e suas entidades corporativas exportam produtos e serviços a partir de Israel, Bulgária e Chipre. Entre os investidores do NSO Group, encontram-se fundos de pensão públicos do Reino Unido (South Yorkshire Pensions Authority e East Riding Pension Fund) e dos EUA (Oregon Public Employees Retirement System e Alaska Permanent Fund Corp).

A transformação da estrutura jurídica da empresa tem como objetivo protegê-la de pressões internacionais, tornando de difícil compreensão as jurisdições às quais estaria submetida. Além disso, o contínuo processo de reinvestimentos na empresa é uma resposta às crises financeiras que a empresa enfrentou ao longo dos últimos anos. Após a empresa ser colocada na lista de empresas com restrições comerciais (U.S. Department of Commerce, 2021), a NSO começou a adquirir dívidas na casa de 400 milhões de dólares (Ronalds-Hannon; Scigliuzzo, 2022).

Figura 7 - Estrutura jurídico-empresarial da NSO Group



Fonte: Amnesty International; Privacy International; Somo, 2021.

3.5. Conclusão

O Pegasus é apenas um entre os vários *spywares* que são atualmente adquiridos por agências de segurança ao redor do mundo, um mercado que foi impulsionado por tendências como: uma cultura digital hiperconectada; a necessidade de atravessar barreiras como a criptografia de ponta-a-ponta; o surgimento de protestos e movimentações no ambiente digital; além da privatização da segurança de uma maneira mais ampla (Deibert, 2023). O estudo do Pegasus em particular serve como porta de entrada para uma análise mais ampla sobre a cibersegurança internacional e a privacidade na era digital.

Um dos principais do Projeto Pegasus pode ser identificado na atenção que este foi capaz de evocar para o tema da vigilância, da cibersegurança e da perseguição a indivíduos por meio do ciberespaço. A investigação global retoma de maneira concreta e robusta as perguntas deixadas em aberto por Edward Snowden, com as revelações sobre o sistema de espionagem em massa desenvolvido pela Agência Nacional de Segurança (NSA) dos Estados Unidos.

Ao longo do presente capítulo busquei "seguir" o *spyware* através das investigações realizadas pelo consórcio internacional de jornalistas envolvido no Projeto Pegasus, inspiradas em revelações iniciais do Citizen Lab. Observa-se no funcionamento da ferramenta analisada uma capacidade de adaptação e mutabilidade, o que é também encontrado na estrutura jurídica e organizacional da NSO Group, sua desenvolvedora. Apresentei até então o Pegasus enquanto ferramenta, seguindo a perspectiva dos relatos jornalísticos e das investigações forenses. Ao longo do próximo capítulo retornarei aos fundamentos teóricos da ANT e dos STS enunciados no capítulo 2, de forma a entender o Pegasus não apenas como ferramenta, mas como ator da cibersegurança e da política internacional.

4. Complexificando: Pegasus como introdução a um universo complexo

A política e a segurança internacional são complexas e multifacetadas. Os instrumentos analíticos *mainstream* das RI[29], abordados ao longo do capítulo 2, não dão conta de analisar essas temáticas enquanto elementos compostos pelo entrelaçamento entre elementos humanos e não-humanos. Os autores Mayer, Carpes e Knoblich (2014) argumentam que temas e conceitos como "a segurança internacional, a condição de Estado, a guerra, bem como a diplomacia, o poder e a governança global estão fortemente entrelaçados e incorporados a elementos materiais, instrumentos técnicos e práticas científicas" (p. 2, tradução nossa). Apesar disso, a disciplina de RI ainda não estaria preparada para lidar com esse entrelaçamento e incorporação que atingem suas principais temáticas, pois ainda tende a estudar a matéria como um elemento exógeno à política (Mayer; Carpes; Knoblich, 2014).

Lidar com a complexidade de temas como a política e a segurança internacional requer, portanto, imprescindivelmente abordar o entrelaçamento entre elementos humanos e não-humanos, reconceitualizando a relação entre matéria e política. Acompanhando o raciocínio desenvolvido por Mayer, Carpes e Knoblich (2014), que propõem a teorização no entorno da "tecnopolítica"[30] como uma alternativa ao determinismo tecnológico e ao social construtivismo, apresentei ao longo do presente trabalho os STS e a ANT como possibilidades de superação da dicotomia entre "o social" e "o material", pois oferecem *frameworks* analíticos capazes de reestruturar a relação entre matéria e política.

A introdução dos STS e da ANT nas RI possibilita uma maior sensibilidade às complexidades, contingências, hibridismos e dinamismos que atravessam temas desde a diplomacia até a cibersegurança (Mayer; Carpes; Knoblich, 2014). A complexificação da política internacional e da cibersegurança a partir dos STS e da ANT é um movimento desejado, pois possibilita a introdução de questionamentos originais e de novas definições para termos

[29] Mayer, Carpes e Knoblich (2014) fazem aqui referência às correntes deterministas e social construtivistas, apontando que seria necessário o desenvolvimento de um pensamento que estivesse na interseção entre ambos os extremos, o que permitiria novas formas de estudar a ciência e a tecnologia por meio das RIs.

[30] Segundo Mayer, Carpes e Knoblich (2014), a tecnopolítica "implica uma compreensão da ciência e das tecnologias além da estrutura do construtivismo social, por um lado, e do determinismo tecnológico, por outro" (p. 2, tradução nossa).

fundacionais do campo, como ocorre em relação ao conceito de agência. Esse movimento pode ser interpretado, ainda, como um resgate de "vozes", agências e histórias apagadas até então: a dos não-humanos.

Ao longo do capítulo 3 apresentei o caso do *spyware* Pegasus, ilustrando algumas das associações, alianças e redes nas quais a ferramenta esteve envolvida. O presente capítulo tem como objetivo retornar aos princípios da ANT e dos STS e associá-los ao caso do Pegasus, analisando as dinâmicas de co-construção entre elementos humanos e não-humanos presentes tanto no processo de desenvolvimento da ferramenta, como também em sua circulação.

O Pegasus, assim como diversos outros elementos não-humanos, não devem ser enxergados apenas como figurantes que compõem o pano de fundo dos eventos listados anteriormente. Os artefatos sociotécnicos que abordo ao longo do presente capítulo desempenham papéis centrais nas redes que se formam no entorno do Pegasus, e sua agência pode ser enxergada a partir dos desenhos de pesquisa e *frameworks* analíticos possibilitados a partir dos STS e da ANT. Sendo assim, uma das tarefas do capítulo 3 é demonstrar que "o Pegasus não é apenas uma ferramenta (o que obviamente também é), mas um "actante" político que importa para a política de segurança" (Leander, 2021, p. 206, tradução nossa).

4.1 Analisar depois de seguir: análise do Pegasus a partir da ANT e dos STS

4.1.1 Das caixas pretas às alianças e às associações

As operações da NSO Group, centradas no desenvolvimento e na venda do Pegasus, eram relativamente estáveis e invisíveis até o recebimento de um SMS pelo ativista Ahmed Mansoor (Marczak; Scott-Railton, 2016). Até o momento de divulgação do relatório de 2016 sobre as atividades do Pegasus no smartphone de Mansoor pelo Citizen Lab, poucas informações sobre a empresa e sobre sua ferramenta eram conhecidas[31]. A publicação do relatório pelo laboratório de pesquisas canadense pode ser vista como o acontecimento que desencadeia a

[31] O relatório do Citizen Lab de 2016 aponta como umas das poucas matérias jornalísticas sobre o Pegasus e a NSO existentes até então o artigo do jornal La Prensa, do Panamá. O artigo de 2015 investiga a aquisição do Pegasus pelo governo panamenho, apontando alguns dos principais personagens envolvidos nas negociações. Mais informações em: https://www.prensa.com/impresa/panorama/Virzi-ligado-compra-equipo-Pegasus_0_4267073341.html

subsequente investigação global sobre o *spyware* e sobre a NSO Group. A partir de então, são levantadas questões sobre a legalidade das operações da NSO Group, sobre a capacidade técnica e o funcionamento do Pegasus, tal como sobre o envolvimento da ferramenta em perseguições a jornalistas e em abusos dos direitos humanos de maneira mais ampla.

Sob a ótica da ANT, o momento de descoberta e revelação do sistema Pegasus para o público geral, representa uma despontualização, isto é, um momento no qual os componentes de uma determinada rede se tornam visíveis (Balzacq; Cavelty, 2016). É a partir desse momento de despontualização da rede associada ao Pegasus que temos visibilidade o suficiente para enxergar as associações traçadas pelo *spyware* em questão, momento oportuno para o início da tarefa de "seguir os atores" proposta por Bruno Latour (2005).

O processo de despontualização pode ser melhor contextualizado a partir do exemplo oferecido por Latour (1999) em seu livro "Pandora's Hope". O autor francês faz alusão ao projetor de imagens, utilizado em escolas e faculdades como acessório durante aulas e palestras. Enquanto o projetor funciona normalmente, é apenas "um intermediário silencioso e mudo, considerado como natural, completamente determinado por sua função" (Latour, 1999, p. 183, tradução nossa), portanto sem maiores questionamentos sobre sua natureza, política ou funcionamento.

A construção do projetor enquanto um elemento único é descrito por Latour (1999) como um processo de "*blackboxing*", a partir do qual são tornados "totalmente opacos a produção conjunta de ações, fatos ou artefatos" (p. 183, tradução nossa). O mesmo processo, quando abordado por John Law (1992), pode ser descrito como uma simplificação: "se uma rede atua como um bloco único, ela desaparece, sendo substituída pela ação em si e pelo autor aparentemente simples dessa ação" (p. 385, tradução nossa). Essa simplificação, *blackboxing* ou pontualização, escondem as redes que produzem as entidades como o projetor, dando visibilidade apenas ao produto ou ação final.

No momento em que o mesmo projetor, silencioso e invisível, deixa de funcionar, reúnem-se ao seu entorno os técnicos humanos, que analisam e testam suas diferentes partes em busca de encontrar e resolver o problema, isto é, fazê-lo voltar a funcionar (Latour, 1999). O projetor, que era um elemento, ou uma

"caixa-preta"[32], é decomposto em inúmeras partes, humanas e não-humanas, que vão desde as lâmpadas e fios até os técnicos envolvidos na investigação e reparo do mesmo. No momento em que o projetor, ou uma televisão, por exemplo, deixa de funcionar, "transforma-se em uma rede de componentes eletrônicos e intervenções humanas" (Law, 1992, p. 384, tradução nossa), sendo cada um desses elementos uma caixa-preta em si mesmo (Latour, 1999).

O momento em que a caixa-preta é aberta é, enfim, o processo de despontualização, inverso ao de pontualização, simplificação ou *blackboxing*. Retornando ao momento de despontualização do Pegasus, com revelação do *spyware* ao público, podemos afirmar que este diretamente relacionado à tarefa de organizações como a Amnesty International, o Citizen Lab e a Lookout Security, que analisam em detalhes técnicos o funcionamento da ferramenta.

Corroborando as constatações de Stevens (2019) sobre o papel da empresa de segurança Symantec na análise do *malware* Stuxnet, adaptando-as para o caso do Pegasus, afirmo que esses estudos detalhados sobre as capacidades técnicas do Pegasus o tornam um artefato inteligível, sobre o qual podemos desenvolver nossas análises. O trabalho dos pesquisadores é de tornar o Pegasus comensurável, "traduzindo o que eles 'estavam vendo no código' em eventos inteligíveis" (Stevens, 2019, p. 14, tradução nossa). A análise técnica é um dos componentes do processo de abertura da caixa-preta do Pegasus, porém não é suficiente em si mesma.

Ao longo do capítulo 3 mobilizei relatórios técnicos, matérias jornalísticas e documentos da NSO Group com o objetivo de retraçar a trilha de associações realizadas pelo Pegasus, efetivamente seguindo-o em múltiplas instâncias espaço-temporais. Complementando a análise técnica, os relatos jornalísticos auxiliam no processo de ilustração e mapeamento da rede que se esconde por trás da "caixa-preta" do Pegasus. Entre os materiais utilizados e fontes consultadas, recorri aos documentos provenientes de vazamentos de dados da Hacking Team e outros disponibilizados por *whistleblowers*, como a lista de possíveis alvos do *software* espião. Essas fontes e materiais ocupam um papel central no movimento

[32] Uma definição de caixa-preta é oferecida por Nawararthne e Storni (2023) ao descreverem o conceito como aplicado aos momentos nos quais uma "rede de atores humanos e não humanos heterogêneos se alinha e estabiliza sua associação para agir como um todo, de modo que seja aceita como um único ator" (p. 1634, tradução nossa)

de mapeamento das alianças e dos mediadores em um caso como o do Pegasus, que aborda diretamente questões de segurança nacional e vigilância.

O trabalho do pesquisador em contextos que envolvem "questões de segurança" é similar ao dos jornalistas investigativos, que devem aprofundar-se para descobrir a verdade que não está necessariamente acessível, uma vez que "a névoa do sigilo é especialmente espessa quanto mais nos aproximamos do cerne das questões de segurança nacional. A caixa-preta é uma caixa trancada, uma caixa oculta ou um *arcanum*" (Best; Walters, 2013, p. 346, tradução nossa). Uma das estratégias possíveis para facilitar a abertura da caixa-preta que havia sido estabelecida ao entorno do Pegasus é justamente a utilização de fontes e materiais que subvertem a lógica do segredo e da confidencialidade. De acordo com Best e Walters (2013):

> o pesquisador deve agora seguir o rastro dos mediadores que assumiram a tarefa de nomear e abrir mundos de sigilo. Personagens como o jornalista investigativo e o denunciante, técnicas como solicitações de acesso à informação ou *wikileaking* agora se tornam parte da rede que se estuda (p. 346, tradução nossa).

A mobilização de diferentes fontes teve também como objetivo desenvolver uma visão mais ampla e transversal do objeto de análise, revelando suas dimensões sociais e políticas (Kaufmann, 2019)[33]. Durante o processo de rastreio das múltiplas associações estabelecidas pelo Pegasus, encontramos alianças de diferentes naturezas, como materiais[34], textuais[35], conceituais[36] e

[33] A ideia de que apenas *softwares* ou algoritmos teriam uma "vida própria" (Fouad, 2021) pode ser contrastada com a imprevisibilidade aos quais estão sujeitos os materiais de marketing (secretos) da NSO Group, por exemplo. As consequências não previstas de sua criação também fazem parte do quadro de composição do caso Pegasus e devem ser levadas em consideração. Seria possível afirmar, no limite, que materiais como fotos e relatórios acabam tendo também uma "vida própria" a partir das associações que realizam? Ver Salter (2019) para uma discussão mais ampla sobre o papel dos objetos na construção de questões de segurança a partir da perspectiva da ANT.

[34] Podemos enxergar algumas das alianças materiais nos servidores da NSO Group e da Apple pelos quais o Pegasus transita, além dos próprios aparelhos celulares que são afetados pelo *spyware*.

[35] As matérias jornalísticas, documentários e relatórios produzidos pelo consórcio internacional de jornalistas envolvido no Projeto Pegasus podem ser alguns dos exemplos, além da comoção internacional transformada em meios de publicações em redes sociais.

[36] As alianças conceituais mobilizadas pelo Pegasus podem ser encontradas na argumentação da NSO Group sobre sua missão e capacidade de garantia da segurança, portanto mobilizando diretamente a ideia de segurança individual, porém também indiretamente mobilizando conceitos como privacidade, risco e o papel das empresas privadas na garantia da cibersegurança de maneira mais ampla.

sociais[37] (Stevens, 2019; Fouad, 2021). Essa observação pode ser comparada às conclusões dos estudos de Clare Stevens (2019) e Noran S. Fouad (2021) sobre o Stuxnet e o WannaCry, respectivamente.

De acordo com Stevens (2019), "o sucesso de malwares complexos, bem como a legitimidade política das empresas comerciais como agentes de segurança, exige a mobilização de várias alianças" (p. 2, tradução nossa). A NSO Group e o Pegasus[38] mobilizam inúmeras alianças, materiais, técnicas, políticas e textuais que garantem que ambos sejam enxergados como peças importantes no campo da cibersegurança. O Pegasus torna-se, a partir de sua circulação e da mobilização de inúmeras alianças, uma ferramenta bem-sucedida tanto no sentido técnico como econômico.

Entre os elementos mobilizados pelo Pegasus, garantindo sua atuação de sucesso, podemos listar: os pesquisadores de tecnologia envolvidos em seu desenvolvimento (tanto os empregados pela NSO como os que desenvolveram vulnerabilidades posteriormente adquiridas pela empresa); as legislações internacionais e locais que permitiram a aquisição da ferramenta por diferentes governos e entidades ao redor do mundo; os códigos e as falhas de segurança de segurança exploradas pelo *spyware* nos sistemas da Apple, da Google e do WhatsApp. Deve-se considerar esta uma lista não-exaustiva das alianças mobilizadas pelo Pegasus e que permitiram a sua atuação.

A análise sobre as alianças estabelecidas pelo Pegasus não é um objetivo final, mas sim um ponto de partida para o estudo dos atores e da agência. Kaufmann (2019) afirma que:

> Assim como nas RI, as relações estão de fato em foco quando a agência é estudada. No entanto, as relações não são apenas um ponto de entrada metodológico, mas são o núcleo ontológico da agência. Elas são o lugar de onde emergem os atores e as ações humanas e não-humanas. Esse método de rastrear a agência por meio das relações não é, então, empregado para criar conhecimento reproduzível, mas para abordar a questão do que conta como conhecimento (p. 160, tradução nossa)[39].

[37] Encontradas na associação entre indivíduos afetados e jornalistas, além de indivíduos que se manifestam contra a empresa de forma pública.

[38] A distinção entre a NSO Group e o Pegasus é proposital, pois trata-se de unidades e/ou entidades distintas a serem analisadas, embora possam fazer parte de uma mesma rede.

[39] É importante ressaltar a crítica sobre esse mesmo ponto, realizada por Nexon e Pouliot (2013): "a ANT, talvez deliberadamente, não possui os conceitos mais holísticos que as abordagens alternativas de construção social propõem para capturar os fenômenos macro: propriedades estruturais na análise de redes sociais, dinâmica de campo em Bourdieu ou formações discursivas

O movimento de mapeamento das alianças realizados pelo Pegasus após segui-lo é, portanto, a porta de entrada para a compreensão sobre a sua possibilidade de agência e classificação enquanto actante, o que analiso a seguir.

4.1.2 Actantes, mediadores e agência distribuída

A lista de alianças formadas pelo Pegasus nos oferece também uma noção do desenho da rede[40] na qual este está inserido, composta por pessoas, organizações, agentes, máquinas, portanto por entidades tanto humanas como não-humanas. Antes de avançar sobre a discussão de agência é necessário atentar para a definição de rede apresentada pela ANT, evitando seu papel como "falso-cognato teórico".

John Law (1992) oferece um esclarecimento sobre a definição de rede ao afirmar que aquilo que entendemos como um indivíduo humano é "um efeito gerado por uma rede de materiais heterogêneos que interagem" (p. 383, tradução nossa). O uso do termo ator-rede na ANT é derivado da constatação de que "um ator é também, sempre, uma rede" (Law, 1992, p. 384, tradução nossa). O ator-rede para Bruno Latour (2005) é "aquilo que é feito agir por uma grande rede em forma de estrela composta por mediadores que entram e saem dela" (p. 217, tradução nossa). Bueger e Stockbruegger (2017) oferecem um resumo desses conceitos ao afirmarem que:

> Um ator pode ser decomposto, e seus componentes podem ser desmontados e remontados. A agência é distribuída em uma rede ou "coletivo". Quem ou o que age é sempre um problema empírico que só pode ser determinado pela investigação da rede por meio da qual um efeito está sendo produzido (p. 49, tradução nossa).

O Pegasus, por consequência, não apenas está inserido em diferentes redes, como também é, efetivamente, uma rede heterogênea, uma caixa-preta que

em Foucault. Por esse motivo, não está claro exatamente como se pode '*scale up*' em um *framework* ANT. Essa limitação parece problemática em uma disciplina como as RI, em que a maioria dos fenômenos de interesse - da guerra às organizações internacionais - têm dimensões de nível macro" (p. 344, tradução nossa)

[40] A utilização do termo "rede" no singular tem como objetivo a simplificação. A ANT de maneira geral desenvolve suas análises baseando-se na existência de múltiplas redes heterogêneas, uma vez que os elementos (humanos e não-humanos) estão em constante interação com outros, em processo de contínua reorganização (Law, 1992)

se abre com o processo de investigação iniciado. Uma segunda consequência das afirmações de Law (1992), Latour (2005) e Bueger e Stockbruegger (2017) é a necessidade de ir além do *spyware* Pegasus em si na análise sobre agência. Dado que a agência é algo distribuído em uma rede, devemos buscar em quais outras entidades além da ferramenta é possível encontrar agência, sejam essas entidades humanas ou não-humanas.

Segundo Latour (2005), "qualquer coisa que modifique um estado fazendo uma diferença é um ator - ou, se ainda não tiver figuração, um actante" (p. 71, tradução nossa). Seguir os atores (ou actantes) significa, portanto, seguir aqueles que fazem a diferença, que modificam o estado de seus arredores. Com o objetivo de orienANT o processo de busca por aqueles que fazem a diferença, dois papéis principais são delimitados por Latour (2005): intermediários e mediadores. De maneira bastante resumida, intermediários e mediadores são os papéis que podem ser assumidos pelos actantes[41] de uma rede.

Os intermediários são aqueles que transportam um significado ou força sem uma transformação, enquanto os mediadores "transformam, traduzem, distorcem e modificam o significado ou os elementos que devem carregar" (Latour, 2005, p. 39, tradução nossa). Os papéis de mediador e agente não são irreconciliáveis. Bruno Latour (2005) afirma que os objetos, dada a sua natureza de conexões com os humanos, "rapidamente deixam de ser mediadores e passam a ser intermediários, (...), independentemente de sua complexidade interna" (p. 79, tradução nossa). Saem de um papel de mudança ativa em uma rede para transformarem-se em transmissores de ação e sentido, tal como um projetor que funciona normalmente.

A classificação definitiva para os actantes como mediadores ou intermediários não é possível (ou desejada) com base nos princípios da ANT. Argumento, portanto, que o Pegasus assume ambos os papéis, definidos de acordo com o contexto analisado. Considerando as limitações espaço-temporais do presente capítulo, focarei a seguir no aspecto da mediação performada pelo *spyware*[42].

---

[41] Segundo Davis (2020), o termo "'actante' substitui o termo ator porque 'ator' geralmente possui uma conotação humana" (p. 77, tradução nossa).

[42] O artigo de Fouad (2021) chama atenção para a distinção entre "código" e "software", o que pode ser utilizado para pensar a composição do *spyware* Pegasus, que pode ser entendido como ambos. Segundo Fouad (2021), "Os códigos são artefatos textuais que especificam determinadas instruções que os dispositivos digitais devem seguir para executar suas tarefas designadas. O

Seu papel como mediador é evidenciado por sua atuação ao alterar o comportamento dos dispositivos que infecta, permitindo o acesso não autorizado a informações confidenciais, como mensagens, chamadas e dados de localização (Marczak; Scott-Railton, 2016). Altera também o comportamento dos usuários que entram em contato com seus primeiros indícios ou com a notícia de sua existência. Sandrine Rigaud e Laurent Richard (2023) relatam que ao longo de suas reuniões com membros da organização Forbidden Stories resolveram colocar seus aparelhos telefônicos desligados em uma sala ao lado, pois se estivessem infectados com o *spyware* poderiam atuar como espiões infiltrados, revelando o conteúdo das investigações.

A mediação do Pegasus, entretanto, não está restrita ao nível do funcionamento dos aparelhos ou das formas que os indivíduos lidam com sua possível presença. Em uma perspectiva mais abrangente, a descoberta do Pegasus desencadeia um processo mais amplo de re-orientação do ativismo contra os abusos praticados por meio de *spywares* e ferramentas de vigilância. Sendo assim, desempenha um papel de mediador nas práticas de privacidade e vigilância, tanto por possibilitar novas ações por meio de agência de segurança, como por colocar em pauta novas questões sobre privacidade e criptografia.

Simultaneamente, podemos enxergar o *spyware* como um ator/agente/actante, capaz de afetar as redes que ocupa. Atribuir agência ao Pegasus depende de um movimento anterior de observação de suas ações, uma vez que para a ANT a agência não é um atributo, mas um produto da interação entre diferentes entidades. De acordo com Leesee e Hoijtink (2019), "a agência não precede a ação, mas a ação constitui a agência" (p. 3, tradução nossa). A caracterização do Pegasus enquanto ator/agente/actante é, portanto, algo que só pode ser realizado posteriormente ao movimento de segui-lo.

A rede na qual o Pegasus está inserido e as dinâmicas de cibersegurança que nela circulam, entretanto, não conta apenas com o *spyware* como actante. Analisando novamente a lista de associações traçadas pelo Pegasus, observamos a presença de inúmeros actantes em potencial, muito além de humanos como Laurent Richard, Sandrine Rigaud, Claudio Guarnieri ou até mesmo Ahmed

---

software, por outro lado, transforma códigos estáticos em programas processuais por meio da engenharia de software e, por sua vez, atua como mediador entre os códigos e a execução no mundo real" (p. 3, tradução nossa).

Mansoor. Inúmeros iPhones infectados, servidores da NSO e documentos vazados obtém sucesso no "teste" de para a definição de actantes proposto por Bruno Latour (2005), e posteriormente resgatado por Salter (2019).

Observa-se no caso Pegasus, portanto, a mobilização de um conjunto de entidades não-humanas, como as tecnologias, enquanto actantes na rede, o que contrasta com associação de agência com capacidades humanas de agir ou com a intencionalidade (Fouad, 2021). Em outras palavras, nos termos da ANT a agência está dissociada de uma capacidade intrinsecamente humana, uma vez que não é fruto de uma intenção, mas da produção de uma relação entre duas ou mais entidades distintas.

As afirmações de Latour (2005) sobre os atores, entretanto, podem gerar um erro fundamental no emprego da ANT, que seria considerar humanos e não-humanos como "iguais" absolutos. Segundo Latour (2005) "a ANT não é, repito, não é, o estabelecimento de alguma absurda 'simetria entre humanos e não humanos'. Ser simétrico, para nós, significa simplesmente não impor a priori alguma assimetria ilusória entre a ação intencional humana e um mundo material de relações causais" (p. 76, tradução nossa). A afirmação de que inúmeras entidades não-humanas ou elementos materiais são actantes no caso do Pegasus não significa o abandono da observação de suas particularidades e *affordances*. Mesmo entre as entidades não-humanas observamos diferenças, pois "não são todas do mesmo tipo e não exercem a mesma forma de agência" (Fouad, 2021, p. 9, tradução nossa)[43].

A principal contribuição do mapeamento da rede de atores e da agência no caso do Pegasus para os estudos da cibersegurança e da segurança e de maneira mais ampla é a constatação de que a agência é distribuída entre inúmeros actantes. Essa está dispersa entre elementos humanos e não-humanos, artefatos sociotécnicos e tecnologias e não está apenas concentrada na figura de elementos humanos ou de atores tradicionais como os Estados ou agências de segurança, tradicionalmente tidos pelas RI enquanto principais unidades de análise. Retomarei mais à frente a discussão sobre ANT, assemblages e cibersegurança e os atuais desdobramentos que atravessam a disciplina de RI.

[43] Um estudo mais aprofundado sobre as diferentes formas de agência presentes no caso do Pegasus foge ao escopo do presente trabalho.

4.2 Destinado ao desastre? O desenho do Pegasus, consequências não previstas e tecnologias de duplo-uso

A interpretação do Pegasus enquanto mediador concorda com os estudos de Balzacq e Calvety (2016) quando esses afirmam que ver os *malwares* como mediadores ou atores nos permite dar a eles "uma agência transformadora própria, separada da 'intenção' da pessoa que escreveu o código" (Balzacq; Cavelty, 2016, p. 183, tradução nossa). Não é possível afirmar que os desenvolvedores do código do Pegasus compartilhavam entre si o desejo, ou ainda que detivessem o controle sobre a utilização da ferramenta enquanto instrumento de perseguição política contra jornalistas e membros da sociedade civil. Davis (2020) reitera a ideia de que "um artefato não faz apenas uma coisa, ele faz várias coisas, muitas das quais nunca foram imaginadas" (p. 53, tradução nossa).

É importante ressaltar que "a 'bondade' ou 'maldade' do *software* não pode ser determinada antes de sua performance e de sua interpretação, pois ele sempre incorpora uma gama de possíveis manifestações em seu código" (Balzacq; Cavelty, 2016, p. 7, tradução nossa). Definir a natureza do Pegasus antes de sua atuação e interação com outros elementos e entidades não é, portanto, uma possibilidade a partir dos princípios da ANT.

Afastando-nos momentaneamente da radicalidade relacional da ANT , a partir da qual as entidades e seus sentidos só passam a existir quando relacionadas a outras entidades, podemos invocar o pensamento de Langdon Winner (1980) sobre a política embutida nos artefatos, uma lógica que contém em si traços deterministas sobre o papel das tecnologias. Winner (1980) questiona a associação entre o desenho das tecnologias e dos artefatos e a produção de "um conjunto de consequências lógicas e temporalmente anteriores a qualquer um de seus usos declarados" (p. 125, tradução nossa). Em outros termos, o desenho de certos objetos influenciaria a ocorrência de determinados resultados e cenários, atendendo a certos interesses sociais.

O Pegasus é desenhado[44] como uma ferramenta capaz de manipular processos dos aparelhos celulares de maneira que possa tomar o controle dos mesmos. A natureza de sua operação não está, necessariamente, associada a uma atividade maliciosa (interpretada como ferramenta de vigilância ou *spyware*) ou como produtora de segurança (protegendo cidadãos contra o terrorismo, como afirma a NSO Group em seus documentos). Há, entretanto, elementos na sua composição que indicam um determinado uso, que facilitam sua utilização para determinados fins. Uma simples cerca, por exemplo, não "impõe fronteiras impenetráveis, eu disse, mas permite a restrição espacial" (Davis, 2020, p. 55, tradução nossa)[45]. Em resumo, "mesmo que uma tecnologia tenha uma origem e tenha sido projetada para uma finalidade específica, isso não a limita a essa origem ou a essa finalidade" (Leander, 2013, p. 815, tradução nossa).

Argumento, em um momento de flexibilização[46] dos princípios da ANT, que o desenho do Pegasus, manifestado nas possibilidades oferecidas a partir de suas funcionalidades, incentivam uma linha de ação que tende à extrapolação dos limites inicialmente estabelecidos para a sua utilização. Segundo Davis (2020):

> os objetos tecnológicos incentivam alguma linha de ação quando essa linha de ação é facilitada e atraente. Em geral, a ação é óbvia, esperada e fácil de ser executada. Essas linhas de ação que são incentivadas geralmente representam exatamente o que uma tecnologia foi criada para realizar. Os usuários precisam empregar pouca ou nenhuma criatividade, desvio ou subterfúgio para envolver a tecnologia de maneiras incentivadas. [...]. Em alguns casos, no entanto, um objeto pode incentivar linhas de ação sobre as quais o designer pouco ou nada pensou (p. 62, tradução nossa).

O desenho do Pegasus e seu conjunto de funcionalidades torna o monitoramento de ativistas, jornalistas e cidadãos comuns uma ação "óbvia" e "fácil de ser executada", mesmo que ela não seja necessariamente esperada por

---

[44] O termo "desenho" pode ser substituído por outros como "projetado" (fazendo referência ao termo *engineered*, em inglês). Fouad (2021) traz uma discussão interessante sobre a distinção entre os termos "*designed"* e "*engineered"*: "códigos/softwares são principalmente projetados em vez de desenhados, pois nem sempre seguem o que os programadores determinam. Os programadores quase têm uma "experiência ignorante" ao lidar com códigos/software que ajudaram a produzir" (p. 12, tradução nossa).

[45] O termo "permite" é traduzido do inglês *affords*, que faz referência ao conceito de *affordance*.

[46] Mostrarei a seguir que a ANT não é contrária à ideia de que os objetos podem facilitar um determinado curso de ação. O emprego do termo flexibilização tem como objetivo ressaltar a introdução a um argumento que pode aparentar ser inicialmente contraditório, mas que se mostrará posteriormente embasado nas ideias de Bruno Latour (2005).

seus desenvolvedores[47]. A extrapolação de seu papel como mera ferramenta de garantia da segurança, utilizada apenas fins "legais" parece estar diretamente relacionada às suas características inerentes[48]. Essa visão está respaldada no arcabouço jurídico internacional sobre tecnologias de dupla utilização.

O Acordo de Wassenaar, mencionado no capítulo 3, adicionou em 2013, "os sistemas de vigilância de IP e itens relacionados aos softwares de invasão [...] na lista de controle de dupla utilização do Acordo" (Korzak, 2020, p. 297, tradução nossa). O termo dupla utilização faz referência a itens e tecnologias "que podem ser usados tanto para fins civis quanto militares," (União Europeia, 2021, p. 8, tradução nossa)[49]. Como consequência, as empresas que desenvolvem e vendem esses tipos de ferramentas passaram a precisar de licenças para a venda e exportação de produtos como os *spywares* e o próprio Pegasus (Korzak, 2020).

Seria então possível afirmar que o Pegasus e outros *spywares* são ferramentas desenhadas/projetadas de maneira que facilitam e/ou incentivam a extrapolação dos limites legais? Aderindo aos princípios básicos da ANT não é possível afirmar que os *spywares*, suas características, possibilidades e capacidades, determinam o curso de ação a ser adotado. Os martelos não determinam que os pregos sejam martelados (Latour, 2005), da mesma maneira que o Pegasus não define de maneira definitiva o curso de ação a ser adotado por seus operadores. A afirmação de que o Pegasus definiria um curso de ação possível retoma a veia determinista, apenas invertendo os papéis dos humanos e não-humanos.

Por outro lado, Latour (2005) argumenta que "além de 'determinar' e servir como 'pano de fundo para a ação humana', as coisas podem autorizar, permitir, proporcionar, incentivar, permitir, sugerir, influenciar, bloquear, tornar possível, proibir e assim por diante (p. 72, tradução nossa). Esta afirmação engaja diretamente com a ideia de *affordance* e a multiplicidade das capacidades de ação

---

[47] Vale ressaltar que a NSO Group reconhece em seu relatório de transparência de 2023 que "como qualquer outra tecnologia, a tecnologia de inteligência cibernética também pode ser mal utilizada ou abusada para violar outros direitos humanos importantes, como os direitos à privacidade e à liberdade de expressão" (NSO Group, 2023, p. 3, tradução nossa).

[48] É importante reforçar que o Pegasus é utilizado como exemplo por ser o objeto de estudos do presente trabalho, porém o argumento pode ser expandido para diversos outros *spywares* e ferramentas similares.

[49] Lena Riecke (2023) chama atenção para o fato de que "a dualidade criada pelo termo se expandiu para além da divisão entre 'militar' e 'civil', levando a uma investigação mais ampla sobre a legitimidade de um determinado uso final por um determinado ator" (p. 706, tradução nossa), portanto requisitando uma avaliação caso a caso.

ao engajar com as tecnologias (Latour, 2005), trazendo a ideia de que os objetos poderiam incentivar os cursos de ação em uma direção ou outra. A introdução do martelo, segundo Latour (2005), representa uma mudança significativa no curso da ação de pregar um prego, da mesma maneira que a introdução dos *spywares* pode representar uma alteração significativa no curso da vigilância e da investigação. Existe, ainda, uma outra "solução baseada na ANT" que pode ser aplicada ao ao casos do Pegasus e dos *spywares*, remetendo ao trabalho de Bruno Latour (1994) sobre a relação que entre humanos e armas.

"Armas matam pessoas" e "pessoas matam pessoas, não armas" são slogans utilizados nos debates sobre a regulamentação da venda de armas nos Estados Unidos, como apresentado por Latour (1994), questionando a seguir "quem ou o que é responsável pelo ato de matar? A arma é apenas uma espécie de tecnologia mediadora?" (p. 31, tradução nossa). Santaella e Cardoso (2015) abordam o estudo de Latour (1994) associando os slogans apresentados a vertentes deterministas distintas sobre o papel das tecnologias:

> Por um lado, o slogan 'armas matam pessoas' parece dar poder predominante à técnica (e pode, portanto, ser entendido como um determinismo tecnológico), por outro lado, o slogan 'pessoas matam pessoas; não armas' parece conferir poder exclusivo ao lado humano (determinismo humanista) (p. 169, tradução nossa).

Latour (1994) apresenta uma classificação similar, relacionado o primeiro slogan a uma perspectiva materialista e o segundo a uma visão sociológica. Segundo o relato materialista sobre as armas, essas permitiriam, instruiriam e direcionariam os humanos em posse das mesmas (Latour, 1994). Segundo essa interpretação das armas (o que pode ser expandido para a tecnologia de forma geral), "cada artefato tem seu roteiro, sua *affordance*, seu potencial para se apoderar dos transeuntes e forçá-los a desempenhar papéis em sua história" (Latour, 1994, p. 31, tradução nossa). Apenas ao aplicar a visão materialista no caso do Pegasus seria possível afirmar que seu *script*, seu desenho ou engenharia teria relação direta com a ação na qual este está envolvido.

A solução encontrada por Latour (1994) baseia-se na análise do híbrido que se forma a partir da associação entre homem e arma. O ator que age ao atirar não é o homem ou a arma, mas o híbrido homem-arma/arma-homem. O homem não é mais apenas o homem e a arma não é mais apenas a arma, ambos

transformam-se em algo diferente do que a entidade inicial que eram (Latour, 1994). Em suma, Latour (1994) afirma que "não são as pessoas nem as armas que matam. A responsabilidade pela ação deve ser compartilhada entre os vários atores" (p. 34, tradução nossa), entre eles o híbrido formado. Mas e o Pegasus em meio a tudo isso?

A posse do Pegasus por um Estado ou por uma agência de inteligência não determina que essa agirá de uma forma particular, mas confere a essa entidade tanto a capacidade como o potencial de agir de maneiras diferentes do que agiria se não tivesse em posse do mesmo (Irvine-Smith, 2016). Entre essas novas possibilidades e potenciais de ação estão igualmente situadas a possibilidade de empregar o *spyware* em investigações "legítimas" contra o terrorismo, tal como na perseguição a jornalistas e ativistas como Mansoor e Khashoggi. Estuda-se, portanto, o híbrido "Estado-Pegasus", que possui um conjunto de possibilidades e capacidades de ação diferentes da entidade inicial Estado ou Pegasus, podendo ser considerado uma nova entidade diferente das duas primeiras (Irvine-Smith, 2016).

Inúmeros temas das RI podem ter seus estudos reformulados e/ou revolucionados a partir da introdução dos princípios da ANT discutidos por Latour (1994). Altera-se o ponto de partida (não mais arma ou homem, por exemplo), destinando-se a atenção ao híbrido formado, uma entidade terceira. Analiso em mais detalhes os impactos da ANT para a segurança internacional e para as RI ao longo da seção seguinte.

4.3 Apenas um nó na rede: o que a ANT e o Pegasus contribuem para o estudo das RI

Analisando o papel desempenhado pelo Pegasus no setor de vigilância cibernética, Lena Riecke (2023) entende o *spyware* como sendo apenas a ponta de um iceberg. Segundo Korzak (2020), "o caso da NSO destaca uma questão que se tornou uma preocupação duradoura de segurança cibernética: o uso e o possível uso indevido de ferramentas de vigilância e intrusão, geralmente chamadas de 'spyware'" (p. 297, tradução nossa)

Proponho um reaproveitamento da figura do iceberg apresentada por Riecke (2023) para pensar o campo das RI de maneira mais ampla. O Pegasus nesse contexto é a ponta de um iceberg teórico ainda pouco explorado, cuja parte

submersa é composta por inúmeras temáticas da cibersegurança e das RI que podem ser transformadas pelo emprego da ANT ou, ainda, a diversidade de temas que podem ser discutidos a partir do Pegasus.

Se a política e a segurança internacional mostram-se complexas, precisamos desenvolver ferramentas analíticas capazes de estudá-las a partir de suas complexidades, o que a ANT e os STS se propõem a fazer. Contrariamente a um movimento de reducionismo e generalização presentes nas proposições *mainstream* das RI, a ANT e os STS oferecem uma complexificação da política e da segurança internacional, o que é feito por diferentes caminhos.

Entre esses, temos a adição de novos atores, como os não-humanos, novas formas de associação e organização entre esses, além de uma nova conceituação para a ideia de agência, distribuída entre diferentes entidades, portanto não mais restrita aos humanos e que se distancia da ideia de intencionalidade.

Além disso, a intenção de pesquisas realizadas sob as orientações da ANT e dos STS não deve ser associada a uma vontade de "explicar" a realidade, mas sim de relatar o que pode ser observado, com o benefício de poder resgatar elementos que poderiam ter sido deixados de lado por outras abordagens. Esse movimento não pode ser ignorado, pois representa um contraste fundamental com as origens das RI e suas principais correntes, destinadas a, por meio de estruturas rígidas e bem definidas, explicarem o que é e como funciona o Internacional e suas dinâmicas. Mas de que maneira a missão de "complexificação" da ANT e dos STS pode ser aplicada concretamente no estudo de um fenômeno?

"Seguir os atores" é uma das soluções encontradas pela ANT, pois possibilita um entendimento contextual da questão, que considera as múltiplas condições e arranjos encontradas em um determinado momento e/ou lugar. O ator a ser seguido pela ANT realiza múltiplas associações e alianças temporárias, tanto com humanos como não-humanos, reforçando a necessidade de análises cada vez mais próximas de seu objeto de estudo. Valoriza-se a compreensão das dinâmicas específicas, mesmo que efêmeras, que afetam os atores e suas relações, em detrimento de visões deterministas e generalizantes.

O objetivo da ANT é produzir análises que vão além da lógica "*x* causa *y*". Segundo Balzacq e Cavelty (2016), "vincular um *malware* a efeitos políticos amplos não é aconselhável nem possível - claramente, não há uma única relação de causa e efeito a ser encontrada aqui" (p. 195, tradução nossa), o que pode ser

traduzido para a análise do Pegasus aqui realizada. A ambição do presente trabalho limita-se a explorar as associações realizadas pelo *spyware*, de maneira que a cadeia de mediadores possa ser identificada e suas transformações momentâneas de sentido e práticas possam ser ilustradas.

Os princípios da ANT nos mostram que *x* e *y* apresentam-se como entidades múltiplas, construídas a partir da associação (temporárias) entre diferentes elementos. Ademais, a ideia de causa não é o principal interesse da ANT, uma vez que a afirmação de que "*x* causa *y*" apresenta um caráter tendendo ao infinito e à generalização. Não seria possível, segundo a ANT, afirmar que *x* sempre causará *y*, isto porque não podemos afirmar a permanência de *x* enquanto *x*, dada a sua composição dinâmica e contextual. Além disso, a certeza de que "*x* sempre causa *y*" dependeria de uma mesma forma de associação entre *x* e *y*, imutável, o que a ANT opta por não afirmar ser uma possibilidade dada a relevância da constante reorganização dos elementos.

5. Conclusão

> (...) há uma necessidade urgente de uma avaliação sistemática da escala, do alcance e do caráter das práticas de vigilância contemporâneas, bem como das justificativas que elas atraem e das controvérsias que provocam. Precisamos saber se essas práticas marcam uma reconfiguração significativa, por exemplo, das relações entre a coleta de inteligência e a vigilância da Internet e de outros sistemas de telecomunicações, ou se elas marcam desafios contínuos aos direitos fundamentais na esfera digital. E precisamos prestar muita atenção às implicações de longo prazo das práticas que já levantaram questões muito sérias sobre transgressões generalizadas de princípios legais e normas democráticas de maneiras que falam de mudanças históricas no local e no caráter da autoridade soberana e da legitimidade política (Bauman et al., 2014, p. 122, tradução nossa).

As revelações de Edward Snowden sobre os programas de vigilância em massa desenvolvidos pela NSA provocaram reações de proeminentes autores das RI, como pode ser observado no trecho de Bauman et al. (2014) citado acima. Naquele momento, tanto questões práticas, como sobre o uso de criptografia em dispositivos móveis e em aplicativos de mensagens instantâneas, quanto teóricas, como a possibilidade de uma reorientação para os estudos de vigilância e estudos críticos de segurança, foram levantadas por diferentes autores da disciplina.

O movimento realizado por Snowden é o de revelar dinâmicas que já existiam, que já estavam presentes, mas que ainda não eram enxergadas de maneira adequada por um público mais amplo. Dinâmica semelhante pode ser encontrada no caso do *spyware* Pegasus, não apenas pela revelação de que ferramentas de espionagem e vigilância estavam sendo utilizadas de forma indevida, mas também por ser um momento de se tornar capaz de enxergar algo que estava próximo, mas não podia ser enxergado.

As principais vertentes de concepção e entendimento sobre agência nas RI dificultam a visualização da agência não-humana, ou, ainda, desconsideram-na como uma possibilidade. As contribuições de Bruno Latour (2005), dos autores da ANT e dos STS de maneira geral, tal como de Snowden, Richard e Rigaud, oferecem novos caminhos para enxergar o que já estava em curso mas que ainda não era analisado de maneira própria.

O determinismo tecnológico e o construtivismo, abordados no segundo capítulo, são fundamentais para entender o papel das tecnologias no seio das RI, de modo que posteriores contribuições da ANT e dos STS representam uma

quebra de paradigma com o *mainstream*. A agência deixa de estar aqui ou ali, deixa de ser um atributo e se torna emergente, produto da relação entre duas partes. Conceitos importados da ANT e dos STS, como a simetria ontológica, podem ter impactos positivos e transformadores para o campo das RI, possibilitando novos ângulos de análise e possíveis reformulações para assuntos já considerados como fundamentais para a disciplina.

O estudo da cibersegurança, portanto, é atravessado não apenas pelas mudanças trazidas pelo desenvolvimento tecnológico da contemporaneidade, mas também pelas inovações teóricas permitidas pelo intercâmbio de ideias entre as RI e disciplinas correlatas. A cibersegurança deixa, pouco a pouco, de ser enxergada como "única" e homogênea, uma área sobre a qual os humanos comandam máquinas em uma direção ou outra. Transforma-se em um múltiplas ciberseguranças, baseadas na constante e necessária interação entre humanos e não-humanos, algo que até então não poderia ser enxergado de maneira satisfatória com as lentes *mainstream* das RI.

O *spyware* Pegasus, analisado ao longo do trabalho, serve ao papel de ilustração e contextualização, mas representa apenas um dos inúmeros casos de de atentado contra os direitos individuais por meio das tecnologias digitais. Muito além de servir como teste para a aplicação dos conceitos desafiadores da ANT e dos STS, o Pegasus chama atenção para um mercado de espionagem, vigilância e vulnerabilidades ainda pouco conhecido e com grande potencial de destruição.

Os argumentos apresentados ao longo do trabalho permitem um distanciamento do leitor das colocações radicais: "os *sywares* espionam pessoas" ou "são pessoas que espionagem pessoas (por meio dos *spywares*)". A relação é um tanto quanto mais complexa do que isso, pois o que deve ser analisado é a condição de capacidades e possibilidades que surge do híbrido humano-*spyware*, diferente de ambas as partes em separado.

Reconhecendo a limitação espaço-temporal do presente trabalho, assim como a diversidade de termos e conceitos que poderiam aqui ser empregados para tratar da ANT e dos STS, busquei dedicar maior atenção a alguns dos principais termos do campo, como agência, ator, actante e mediação.

6. Referências bibliográficas

ACCESS NOW. How Pegasus spyware crushes civic space in Jordan. Access Now, 2024. Disponível em: <https://www.accessnow.org/publication/between-a-hack-and-a-hard-place-how-pegasus-spyware-crushes-civic-space-in-jordan/>.

AMNESTY INTERNATIONAL. Moroccan journalist targeted with network injection attacks using NSO Group's tools. Amnesty International, 2020. Disponível em: https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/. Acesso em: 16 jun. 2024.

AMNESTY INTERNATIONAL. Forensic methodology report: How to catch NSO Group's Pegasus. Amnesty International, 2021. Disponível em: https://www.amnesty.org/en/documents/doc10/4487/2021/en/. Acesso em: 16 jun. 2024.

AMNESTY INTERNATIONAL. The Predator Files: Caught in the net. Amnesty International, 2023. Disponível em: https://www.amnesty.org/en/documents/act10/7245/2023/en/. Acesso em: 16 jun. 2024.

ARADAU, Claudia. Security That Matters: Critical Infrastructure and Objects of Protection. **Security Dialogue**, v. 41, n. 5, p. 491-514, out. 2010. Disponível em: https://doi.org/10.1177/0967010610382687. Acesso em: 16 jun. 2024.

BAELE, S.J.; BETTIZA, G. 'Turning' everywhere in IR: on the sociological underpinnings of the field's proliferating turns. **International Theory**, v. 13, n. 2, p. 314-340, 2021. doi:10.1017/S1752971920000172. Disponível em: https://doi.org/10.1017/S1752971920000172. Acesso em: 16 jun. 2024.

BALZACQ, T.; CAVELTY, M. D. A theory of actor-network for cyber-security. **European Journal of International Security**, Cambridge, v. 1, n. 2, p. 176-198, 2016. DOI: 10.1017/eis.2016.8. Disponível em: https://doi.org/10.1017/eis.2016.8. Acesso em: 16 jun. 2024.

BARRY, A. The Translation Zone: Between Actor-Network Theory and International Relations. **Millennium**, London, v. 41, n. 3, p. 413-429, 2013. Disponível em: https://doi.org/10.1177/0305829813481007. Acesso em: 16 jun. 2024.

BAUMAN, Zygmunt; BIGO, Didier; ESTEVES, Paulo; GUILD, Elspeth; JABRI, Vivienne; LYON, David; WALKER, R. B. J. After Snowden: Rethinking the Impact of Surveillance. **International Political Sociology**, v. 8, n. 2, p. 121-144, jun. 2014. DOI: https://doi.org/10.1111/ips.12048. Acesso em: 24 jun. 2024.

BAZALIY, Max et al. Technical analysis of Pegasus spyware: An Investigation Into Highly Sophisticated Espionage Software. LOOKOUT, 2016. Disponível em:

https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf. Acesso em: 16 jun. 2024.

BBC NEWS. Jamal Khashoggi: All you need to know about Saudi journalist's death. Disponível em: https://www.bbc.com/news/world-europe-45812399. Acesso em: 16 jun. 2024.

BELLANOVA, R.; JACOBSEN, K. L.; MONSEES, L. Taking the trouble: science, technology and security studies. Critical Studies on Security, v. 8, n. 2, p. 87-100, 2020. Disponível em: https://doi.org/10.1080/21624887.2020.1839852. Acesso em: 16 jun. 2024.

BENNETT, Jane. Vibrant Matter: A Political Ecology of Things. Durham: Duke University Press, 2010. Disponível em: JSTOR https://doi.org/10.2307/j.ctv11jh6w. Acesso em: 16 jun. 2024.

BEST, Jacqueline; WALTERS, William. "Actor-Network Theory" and International Relationality: Lost (and Found) in Translation: Introduction. International Political Sociology, v. 7, n. 3, p. 332-334, setembro 2013. DOI: 10.1111/ips.12026_1. Disponível em: https://doi.org/10.1111/ips.12026_1. Acesso em: 16 jun. 2024.

BRAUN, B.; SCHINDLER, S.; WILLE, T. Rethinking agency in International Relations: performativity, performances and actor-networks. Journal of International Relations and Development, v. 22, p. 787–807, 2019. Disponível em: https://doi.org/10.1057/s41268-018-0147-z. Acesso em: 23 jun. 2024

BUEGER, Christian; STOCKBRUEGGER, Jan. Actor-Network Theory: Objects and actants, networks and narratives. In: McCARTHY, Daniel R. (Ed.). Technology and World Politics: An Introduction. 1st ed. London: Routledge, 2017. p. 18. eBook. DOI: https://doi.org/10.4324/9781317353836. ISBN 9781315666013.

CALLON, Michel. Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. **The Sociological Review,** v. 32, n. 1_suppl, p. 196-233, 1984. DOI: 10.1111/j.1467-954X.1984.tb00113.x. Disponível em: https://doi.org/10.1111/j.1467-954X.1984.tb00113.x. Acesso em: 16 jun. 2024.

CAVELTY, Myriam Dunn. Cybersecurity Research Meets Science and Technology Studies. **Politics and Governance**, [S.l.], v. 6, n. 2, p. 22-30, jun. 2018. ISSN 2183-2463. Disponível em: https://www.cogitatiopress.com/politicsandgovernance/article/view/1385. Acesso em: 16 jun. 2024. doi: https://doi.org/10.17645/pag.v6i2.1385.

CAPAVERDE, C. B.; FOGAÇA, L.; HENRIQSON, É. Teoria ator-rede para as ciências da segurança: reagregando elementos sociais e técnicos. **Revista de Administração de Empresas,** v. 63, n. 3, e2021-0530, 2023. Disponível em: https://doi.org/10.1590/S0034-759020230302. Acesso em: 16 jun. 2024.

CHRISTENSEN, K. K.; LIEBETRAU, T. A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry. **Intelligence and National Security**, Abingdon, v. 34, n. 3, p. 395–408, 2019. DOI: 10.1080/02684527.2019.1553704. Disponível em: https://doi.org/10.1080/02684527.2019.1553704. Acesso em: 16 jun. 2024.

COLLIER, James. Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision. **Politics and Governance,** [S.l.], v. 6, n. 2, p. 13-21, 2018. DOI: 10.17645/pag.v6i2.1324. Disponível em: https://doi.org/10.17645/pag.v6i2.1324. Acesso em: 16 jun. 2024.

CUDWORTH, Erica; HOBDEN, Stephen. Of Parts and Wholes: International Relations beyond the Human. **Millennium**, v. 41, n. 3, p. 430-450, 2013. Disponível em: https://doi.org/10.1177/0305829813485875. Acesso em: 24 jun. 2024.

DAVIS, Jenny L. How artifacts afford: the power and politics of everyday things. Cambridge, Massachusetts: The MIT Press, 2020.

DOUZET, Frédérick. La géopolitique pour comprendre le cyberespace. **Hérodote**, n. 152-153, p. 3-21, 2014. DOI: 10.3917/her.152.0003. Disponível em: https://www.cairn.info/revue-herodote-2014-1-page-3.htm. Acesso em: 16 jun. 2024.

DWYER, Andrew C. et al. What can a critical cybersecurity do? **International Political Sociology**, v. 16, n. 3, setembro 2022. Disponível em: https://doi.org/10.1093/ips/olac013. Acesso em: 16 jun. 2024

EGLOFF, Florian J.; DUNN CAVELTY, Myriam. Attribution and knowledge creation assemblages in cybersecurity politics. **Journal of Cybersecurity**, v. 7, n. 1, 2021. Disponível em: https://doi.org/10.1093/cybsec/tyab002. Acesso em: 16 jun. 2024.

ERIKSSON, Johan; NEWLOVE-ERIKSSON, L. Chapter 1: Theorizing technology and international relations: prevailing perspectives and new horizons. In: Technology and International Relations. Cheltenham, UK: Edward Elgar Publishing, 2021. Disponível em: https://doi.org/10.4337/9781788976077.00007. Acesso em: 16 jun. 2024.

ERIKSSON, Johan; GIACOMELLO, Giampiero. The Information Revolution, Security, and International Relations: (IR)relevant Theory? **International Political Science Review**, v. 27, n. 3, p. 221-244, 2006. DOI: 10.1177/0192512106064462. Disponível em: https://doi.org/10.1177/0192512106064462. Acesso em: 16 jun. 2024.

FAIFE, Corin. New analysis further links Pegasus spyware to Jamal Khashoggi murder. The Verge, 2021. Disponível em: <https://www.theverge.com/2021/12/21/22848485/pegasus-spyware-jamal-khashoggi-murder-nso-hanan-elatr-new-analysis>. Acesso em: 16 jun. 2024.

FELDSTEIN, Steven; KOT, Brian; Carnegie Endowment for International Peace. Why does the global spyware industry continue to thrive? Trends, explanations, and responses. [s.l.]: Carnegie Endowment for International Peace, 2023. Disponível em: https://carnegie-production-assets.s3.amazonaws.com/static/files/Feldstein_Global_Spyware.pdf. Acesso em: 16 jun. 2024.

FOUAD, N.S. The non-anthropocentric informational agents: codes, software, and the logic of emergence in cybersecurity. **Review of International Studies**, v. 48, n. 4, p. 766-785, 2022. doi:10.1017/S0260210521000681. Disponível em: https://doi.org/10.1017/S0260210521000681. Acesso em: 16 jun. 2024.

GIBSON, William. Neuromancer. New York: Ace Science Fiction Books, 1984.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quarterly**, v. 53, n. 4, p. 1155-1175, dezembro 2009. DOI: 10.1111/j.1468-2478.2009.00572.x. Disponível em: https://doi.org/10.1111/j.1468-2478.2009.00572.x. Acesso em: 16 jun. 2024.

HARKIN, D.; MOLNAR, A.; VOWLES, E. The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. **Crime, Media, Culture,** v. 16, n. 1, p. 33-60, 2020. DOI: 10.1177/1741659018820562. Disponível em: https://doi.org/10.1177/1741659018820562. Acesso em: 16 jun. 2024.

IRVINE-SMITH, Sally. From Object to Mediator: The Agency of Documents. Proceedings from the Document Academy, vol. 2, iss. 1, Article 4, 2015. DOI: 10.35492/docam/2/1/4. Disponível em: https://ideaexchange.uakron.edu/docam/vol2/iss1/4. Acesso em: 16 jun. 2024.

JERUSALEM POST. UAE trying 84 people on terrorism charges, including rights activists. The Jerusalem Post, 2024. Disponível em: https://www.jpost.com/middle-east/article-781120. Acesso em: 16 jun. 2024.

KERTTUNEN, Mika; TIKK, Eneken. Introduction. In: TIKK, Eneken; KERTTUNEN, Mika (Eds.). Routledge Handbook of International Cybersecurity. 1st ed. London: Routledge, 2020, p. 8. eBook. DOI: 10.4324/9781351038904.

KIRCHGAESSNER, Stephanie. Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests. The Guardian, 2021. Disponível em: <https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>. Acesso em: 16 jun. 2024.

KIRCHGAESSNER, Stephanie; HOLMES, Oliver; WALKER, Shaun. Pegasus project turns spotlight on spyware firm NSO's ties to Israeli state. The Guardian, 2021. Disponível em: <https://www.theguardian.com/world/2021/jul/20/pegasus-project-turns-spotlight-on-spyware-firm-nso-ties-to-israeli-state>.

KORZAK. Export Controls: The Wassenaar Experience and Its Lessons for International Regulation of Cyber Tools. In: TIKK, Eneken; KERTTUNEN, Mika (Eds.). Routledge Handbook of International Cybersecurity. 1st ed. London: Routledge, 2020. p. 297-299.

LATOUR, Bruno. On technical mediation: Philosophy, Sociology, Genealogy. **Common Knowledge**, v. 3, n. 2, p. 29-64, 1994.

LATOUR, Bruno. Reassembling the social: an introduction to actor-network-theory. Oxford: Oxford University Press, 2005.

LAW, John. Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. **Systems Practice**, v. 5, p. 379-393, 1992. DOI: 10.1007/BF01059830. Disponível em: https://doi.org/10.1007/BF01059830. Acesso em: 16 jun. 2024.

LEANDER, Anna. Parsing Pegasus: An Infrastructural Approach to the Relationship between Technology and Swiss Security Politics. **Swiss Polit Sci Rev**, v. 27, p. 205-213, 2021. Disponível em: https://doi.org/10.1111/spsr.12441. Acesso em: 16 jun. 2024.

LEESE, Matthias; HOIJTINK, Marijn. How (not) to talk about technology. In: HOIJTINK, Marijn; LEESE, Matthias (Eds.). Technology and Agency in International Relations. 1st ed. London: Routledge, 2019. Capítulo 1, p. 23. eBook. DOI: 10.4324/9780429463143. Disponível em: https://doi.org/10.4324/9780429463143. Acesso em: 16 jun. 2024.

LELOUP, Damien; UNTERSINGER, Martin. « Projet Pegasus » : un téléphone portable d'Emmanuel Macron dans le viseur du Maroc. Le Monde.fr, 2022. Disponível em: <https://www.lemonde.fr/projet-pegasus/article/2021/07/20/projet-pegasus-un-telephone-portable-d-emmanuel-macron-dans-le-viseur-du-maroc_6088950_6088648.html>. Acesso em: 16 jun. 2024;

LIEBETRAU, T.; CHRISTENSEN, K.K. The ontological politics of cyber security: emerging agencies, actors, sites, and spaces. **European Journal of International Security**, v. 6, n. 1, p. 25-43, 2021. doi:10.1017/eis.2020.10. Disponível em: https://doi.org/10.1017/eis.2020.10. Acesso em: 16 jun. 2024.

LOBATO, L. C.; KENKEL, K. M.. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, v. 58, n. 2, p. 23–43, jul. 2015.

MARCZAK, Bill et al. Hacking team and the targeting of Ethiopian journalists. Citizen Lab, 2014. Disponível em: https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/. Acesso em: 16 jun. 2024.

MARCZAK, Bill et al. Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Citizen Lab Research Report No. 113, University

of Toronto, setembro 2018. Disponível em: https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf. Acesso em: 16 jun. 2024.

MARCZAK, Bill et al. Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware. 2021. Disponível em: https://citizenlab.ca/2021/07/amnesty-peer-review/. Acesso em: 16 jun. 2024
.
MARCZAK, Bill; SCOTT-RAILTON, John. Keep calm and (Don't) enable Macros: A new threat actor targets UAE dissidents - The Citizen Lab, 2014. Disponível em: https://citizenlab.ca/2016/05/stealth-falcon/. Acesso em: 16 jun. 2024.

MARCZAK, Bill; SCOTT-RAILTON, John. The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. Citizen Lab Research Report No. 78, University of Toronto, agosto 2016. Disponível em: https://tspace.library.utoronto.ca/bitstream/1807/96976/1/Report%2378--Million-Dollar-Dissident.pdf. Acesso em: 16 jun. 2024.

MCCARTHY, D. R. Introduction: Technology in World Politics. In: MCCARTHY, D. R. (Ed.). Technology and World politics: an Introduction. [s.l.] London New York Routledge, Taylor & Francis Group, 2017.

MEKHENNET, Dana; PRIEST, Craig; TIMBERG, Souad. Private spy software sold by NSO Group found on cellphones worldwide. Washington Post, 2021. Disponível em: https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/?itid=lk_inline_manual_2. Acesso em: 16 jun. 2024.

MITRE. Stealth Falcon, group G0038. MITRE ATT&CK®: Tactics and Techniques. Disponível em: https://attack.mitre.org/groups/G0038/. Acesso em: 17 jun. 2024.

MULLER, Lilly P. How to govern cyber security? The limits of the multi-stakeholder approach and the need to rethink public–private cooperation. In: FRIIS, Karsten; RINGSMOSE, Jens (Ed.). *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. 1st ed. London: Routledge, 2016. p. 14. eBook. DOI: https://doi.org/10.4324/9781315669878. ISBN: 9781315669878. Acesso em: 16 jun. 2024.

NSO GROUP. Pegasus – Product Description. [s.l.]: NSO Group, 2018. Disponível em: <https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf>. Acesso em: 16 jun. 2024.

NSO GROUP. Transparency and Responsibility report. [s.l.: s.n.], 2021a. Disponível em: https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf. Acesso em: 16 jun. 2024.

NSO GROUP. Following the publication of the recent article by Forbidden Stories, we wanted to directly address the false accusations and misleading allegations presented there. NSO Group, 2021b. Disponível em: https://www.nsogroup.com/Newses/following-the-publication-of-the-recent-article-by-forbidden-stories-we-wanted-to-directly-address-the-false-accusations-and-misleading-allegations-presented-there/. Acesso em: 16 jun. 2024.

NYE, Joseph S., Jr.; Belfer Center for Science and International Affairs. Cyber Power. [S.l.]: Belfer Center for Science and International Affairs, 2010. Disponível em: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf. Acesso em: 16 jun. 2024.

OCCRP. Who's on the list? – The Pegasus Project. OCCRP, 2021. Disponível em: https://cdn.occrp.org/projects/project-p/#/. Acesso em: 16 jun. 2024.

O'NEILL, Patrick Howell. The fall and rise of a spyware empire. MIT **Technology Review**, 2020. Disponível em: https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/. Acesso em: 16 jun. 2024.

RAMIRO, André et al. Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil. Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em: 16 jun. 2024.

RIECKE, Lena. Unmasking the Term 'Dual Use' in EU Spyware Export Control. **European Journal of International Law**, v. 34, n. 3, p. 697-720, ago. 2023. DOI: 10.1093/ejil/chad039. Disponível em: https://doi.org/10.1093/ejil/chad039. Acesso em: 16 jun. 2024.

RONALDS-HANNON, E.; SCIGLIUZZO, D. Spyware scandal rocking NSO Group is a $400 million debt problem. Bloomberg Law, [S.l.], [s.d.]. Disponível em: https://news.bloomberglaw.com/mergers-and-acquisitions/israels-nso-takes-drastic-measures-to-survive-spyware-scandal. Acesso em: 16 jun. 2024.

RUECKERT, Phineas. Pegasus: The new global weapon for silencing journalists. Forbidden Stories, 18 jul. 2021. Disponível em: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/. Acesso em: 16 jun. 2024.

SALTER, Mark B. Security Actor-Network Theory: Revitalizing Securitization Theory with Bruno Latour. **Polity**, v. 51, n. 2, p. 349-364, 2019. Disponível em: https://www.journals.uchicago.edu/doi/10.1086/701885. Acesso em: 16 jun. 2024.

SANTAELLA, Lucia; CARDOSO, Tarcísio. O desconcertante conceito de mediação técnica em Bruno Latour. **Matrizes**, São Paulo, v. 9, n. 1, p. 167-185,

2015. ISSN 1982-2073. Disponível em: https://www.redalyc.org/articulo.oa?id=143039560010. Acesso em: 16 jun. 2024.

SIMSEK, Abdurrahman; KARAMAN, Nazif. Saudi hit squad's gruesome conversations during Khashoggi's murder revealed. Daily Sabah, 2019. Disponível em: https://www.dailysabah.com/investigations/2019/09/09/saudi-hit-squads-gruesome-conversations-during-khashoggis-murder-revealed. Acesso em: 16 jun. 2024.

SINGER, Peter Warren; FRIEDMAN, Allan. Cybersecurity and cyberwar: what everyone needs to know. 1. ed. New York: Oxford University Press, 2014.

STEVENS, C. Assembling cybersecurity: the politics and materiality of technical malware reports and the case of Stuxnet. **Contemporary Security Policy**, v. 41, n. 1, p. 129-152, 2019. Disponível em: https://doi.org/10.1080/13523260.2019.1675258. Acesso em: 16 jun. 2024.

VALERIANO, Brandon; MANESS, Ryan C. International relations theory and cyber security: threats, conflicts, and ethics in an emergent domain. In: BROWN, Chris; ECKERSLEY, Robyn (eds.). **The Oxford Handbook of International Political Theory**. Oxford Handbooks, 2018. Edição online. Oxford Academic, 5 abr. 2018. Disponível em: https://doi.org/10.1093/oxfordhb/9780198746928.013.19. Acesso em: 16 jun. 2024.

VAN DER WAGEN, W. The Significance of 'Things' in Cybercrime: How to Apply Actor-network Theory in (Cyber)criminological Research and Why it Matters. **Journal of Extreme Anthropology**, v. 3, n. 1, p. 152–168, 2019. Disponível em: <https://journals.uio.no/JEA/article/view/6895>.

VAN DER WAGEN, W.; PIETERS, W. From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. **British Journal of Criminology**, v. 55, n. 3, p. 578-595, 2015. DOI: 10.1093/bjc/azv009. Disponível em: https://doi.org/10.1093/bjc/azv009. Acesso em: 16 jun. 2024.

VALENÇA, Marcelo Mello. Novas guerras, estudos para a paz e Escola de Copenhague: uma contribuição para o resgate da violência pela segurança. 2010. 327 f. Tese (Doutorado em Relações Internacionais) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2010. Orientador: Kai Michael Kenkel. Inclui bibliografia.

WENDT, Alexander E. The Agent-Structure Problem in International Relations Theory. **International Organization,** v. 41, n. 3, p. 335-370, Summer 1987.

WINNER, Langdon. Do artifacts have politics? **Daedalus**, vol. 109, no. 1, pp. 121-136, 1980. JSTOR. Disponível em: http://www.jstor.org/stable/20024652. Acesso em: 16 jun. 2024.