JIM SCIUTTO

ÂNCORA E CORRESPONDENTE-CHEFE DE SEGURANÇA NACIONAL DA CNN

A GUERRA NAS SOMBRAS

OPERAÇÕES SECRETAS DA RÚSSIA E DA CHINA PARA DERROTAR OS ESTADOS UNIDOS

ALTA CULT
EDITORA

A Guerra nas Sombras
Copyright © 2021 da Starlin Alta Editora e Consultoria Eireli. ISBN: 978-65-5520-450-6

Impresso no Brasil — 1ª Edição, 2021 — Edição revisada conforme o Acordo Ortográfico da Língua Portuguesa de 2009.

Produção Editorial Editora Alta Books **Gerência Editorial** Anderson Vieira **Gerência Comercial** Daniele Fonseca	**Produtor Editorial** Thiê Alves	**Coordenação de Eventos** Viviane Paiva eventos@altabooks.com.br **Assistente Comercial** Filipe Amorim vendas.corporativas@altabooks.com.br	**Editor de Aquisição** José Rugeri j.rugeri@altabooks.com.br **Equipe de Marketing** Livia Carvalho Gabriela Carvalho marketing@altabooks.com.br

Equipe Editorial Ian Verçosa Illysabelle Trajano Luana Goulart Maria de Lourdes Borges Raquel Porto	Rodrigo Ramos Thales Silva	**Equipe de Design** Larissa Lima Marcelli Ferreira Paulo Gomes	**Equipe Comercial** Daiana Costa Daniel Leal Kaique Luiz Tairone Oliveira Vanessa Leite

Tradução Carolina Gaio **Copidesque** Alessandro Thomé	**Revisão Gramatical** Hellen Suzuki Thaís Pol	**Diagramação** Lucia Quaresma **Adaptação para formato e-book** Catia Soderi	**Capa** Larissa Lima

Publique seu livro com a Alta Books. Para mais informações envie um e-mail para autoria@altabooks.com.br

Obra disponível para venda corporativa e/ou personalizada. Para mais informações, fale com projetos@altabooks.com.br

Erratas e arquivos de apoio: No site da editora relatamos, com a devida correção, qualquer erro encontrado em nossos livros, bem como disponibilizamos arquivos de apoio se aplicáveis à obra em questão.

Acesse o site **www.altabooks.com.br** e procure pelo título do livro desejado para ter acesso às erratas, aos arquivos de apoio e/ou a outros conteúdos aplicáveis à obra.

Suporte Técnico: A obra é comercializada na forma em que está, sem direito a suporte técnico ou orientação pessoal/exclusiva ao leitor.

A editora não se responsabiliza pela manutenção, atualização e idioma dos sites referidos pelos autores nesta obra.

Ouvidoria: ouvidoria@altabooks.com.br

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

S359g Sciutto, Jim

A Guerra nas Sombras: Operações Secretas da Rússia e da China para Dominar os Estados Unidos / Jim Sciutto ; traduzido por Carolina Gaio. - Rio de Janeiro : Alta Books, 2021
320 p. : 16cm x 23cm.

Inclui índice
ISBN: 978-65-5520-450-6

1. Geopolítica. 2. Rússia. 3. China. 4. Estados Unidos. I. Gaio, Carolina. II. Título.

2021-68 CDD 320.12
CDU 911.3-32

Elaborado por Vagner Rodolfo da Silva - CRB-8/9410

ALTA BOOKS
EDITORA
Rua Viúva Cláudio, 291 — Bairro Industrial do Jacaré
CEP: 20.970-031 — Rio de Janeiro (RJ)
Tels.: (21) 3278-8069 / 3278-8419
www.altabooks.com.br — altabooks@altabooks.com.br
www.facebook.com/altabooks — www.instagram.com/altabooks

AGRADECIMENTOS

Este livro se baseia na crítica perspicaz, honesta e, em alguns casos, consciente de líderes de inteligência, militares e políticos dos Estados Unidos e da Europa. Agradeço ao ex-DNI James Clapper; ao ex-diretor da NSA e da CIA Michael Hayden; ao ex-secretário de defesa Ashton Carter; ao ex-vice-secretário de defesa Bob Work; ao ex-chefe do MI6 John Scarlett; ao ex-vice-diretor da NSA Rick Ledgett; ao ex-chefe do FBI Bob Anderson; ao general John Hyten, atual chefe do Comando Estratégico; ao ex-chefe de Comando Espacial da Força Aérea dos EUA general William Shelton; ao ex-assessor de Segurança Nacional Tom Donilon; e ao ex-embaixador dos EUA na Ucrânia (e atual embaixador na Grécia) Geoffrey Pyatt. Na Estônia, a presidente Kersti Kaljulaid, o ministro das Relações Exteriores, Sven Mikser, e o ex-ministro da Defesa, Jaak Aaviksoo, me apresentaram generosamente à experiência, muitas vezes chocante, das relações de seu país com seu vizinho gigante do leste. Alexander Hug, até pouco tempo integrante da OSCE, fez-me um relato único do abate do MH17 sobre a Ucrânia, que ainda é um dos atos mais chocantes da Guerra nas Sombras. O capitão da Marinha dos EUA, Ollie Lewis, agora membro do Estado-maior Conjunto e ex-comodoro do Esquadrão Submarino 12, me deu informações fundamentais sobre o papel vital dos submarinos em um novo "grande jogo" sob as ondas.

Preciso agradecer à CNN por me enviar em uma série de missões pelo mundo — da Ucrânia ao Mar da China Meridional e ao Ártico —, pelas comunidades de defesa e inteligência dos EUA, o que abriu meus olhos para a Guerra nas Sombras. Jeff Zucker, Rick Davis e Allison Gollust me apoiaram desde o início, mesmo em meio ao infindo ciclo nacional de notícias. Um agradecimento especial a

minha produtora de longa data, Jennifer Rizzo, que me acompanhou nas linhas de frente desse conflito, incluindo vários lugares em que não fomos bem-vindos.

Agradeço a Gail Ross, da Agência Ross Yoon, por ajudar a transformar uma questão complexa em uma história que vale a pena contar; e a Eric Nelson, da HarperCollins, por considerá-la e apoiá-la completamente.

Em toda parada de minha saga global pela Guerra nas Sombras, encontrei militares e funcionários públicos dos EUA dedicando a vida à promoção dos interesses do país e o defendendo de uma série de ameaças de nossos dias. Na Guerra nas Sombras, esses norte-americanos são, ao mesmo tempo, humanos e gladiadores; porém seus papéis, essenciais à proteção dos Estados Unidos, são desconhecidos.

Uma atenção especial vai para as equipes que abriram suas portas para mim, com generosidade e honestidade. Aos comandantes e às tripulações do *USS Hartford* e do *USS Missouri*, obrigado por me receberem a bordo. E a todos os submarinistas, obrigado por se sacrificarem tanto. Vocês não são chamados de "serviço silencioso" só por se esconderem de adversários sob as ondas, mas por fazerem sacrifícios que a maioria dos norte-americanos nem sequer conhece. Como filho de militar da Marinha, ser membro da "Order of the Blue Nose", ou seja, reconhecido como marinheiro que cruzou o Círculo Polar Ártico, é uma grande honra.

Quero agradecer à Marinha dos EUA e ao esquadrão de patrulha marítima VP-45 (os "pelicans" [pelicanos]) por convidar meus colegas da CNN a bordo de uma aeronave de vigilância P-8 Poseidon sobre o Mar da China Meridional — a primeira vez que jornalistas foram autorizados em uma missão operacional do P-8.

Seus pilotos e suas tripulações de voo conseguem ser tranquilos, gente boa e comedidos em um ambiente de tensão extrema.

O Comando Espacial da Força Aérea dos EUA abriu suas portas para mim e para meus colegas da CNN em várias bases em todo o país e, ao fazê-lo, me apresentou ao iminente conflito no espaço e aos "guerreiros espaciais" que se preparavam para ele. Eles realmente cumprem seu lema: "Guardiões da Alta Fronteira." Sou particularmente grato aos homens e às mulheres da Base da Força Aérea de Schriever e da Base Aérea de Peterson, em Colorado Springs, Colorado; da Base da Força Aérea Buckley, em Aurora, Colorado; da Vandenberg AFB, na Califórnia; e da Offutt AFB, em Nebraska, sede do Comando Estratégico dos EUA. Agradeço também às unidades altamente capacitadas na linha de frente desse conflito, incluindo a 50ª Ala Espacial da Base Aérea Schriever, conhecida como "Masters of Space", e a 460ª Ala Espacial da Base Aérea de Buckley.

A AGI (Analytical Graphics, Inc.) nos recebeu em seu amplo centro de operações fora da Filadélfia e compartilhou análises e ideias ao longo deste projeto, para me manter atualizado sobre as últimas atividades russas e chinesas no espaço. Agradecimentos especiais vão para Paul Graziani, CEO da AGI, e para Bob Hall.

A NSA recebeu minha equipe no Centro de Operações de Ameaças Cibernéticas (NCTOC, da sigla em inglês) da agência, descrito como a alma de sua "missão de operações de segurança cibernética 24/7/365". Dentro da NCTOC, percebi que essa era uma descrição precisa para a batalha espacial, na qual os ataques acontecem aos milhares todos os dias.

A Agência de Inteligência da Defesa concedeu, aos meus colegas da CNN e a mim, acesso ao seu Centro de Inteligência de Mísseis e Espaço, em Huntsville, Alabama, algo raríssimo. A área de

Huntsville está se infiltrando na história do programa espacial dos EUA, com alguns de seus lendários foguetes organizados em um horizonte de outro mundo. Os homens e as mulheres do MSIC foram os especialistas altamente bem preparados que determinaram, em poucas horas, que foi um foguete russo, disparado de território controlado pela Rússia, que derrubou o voo MH17 sobre a Ucrânia.

Bob Anderson, ex-diretor assistente executivo da divisão Criminal, Cibernética, de Resposta e Serviços do FBI, expôs claramente o constante roubo de segredos de segurança nacional da China e a extensão e agressividade de suas iniciativas generalizadas para debilitar os EUA.

Andrew Erickson, professor de estratégia da Escola de Guerra Naval dos EUA, fez uma análise perspicaz e precisa da estratégia da China para a Guerra nas Sombras muito além do Mar do Sul da China. De maneira reveladora, Erickson traça os fundamentos históricos dos objetivos de Pequim até a fundação da China comunista.

Austin Lowe, analista da China e linguista mestre em Estudos Asiáticos pela Walsh School of Foreign Affairs, da Georgetown University, e bacharel em Línguas e Culturas da Ásia Oriental pela Columbia (e que, aliás, é meu sobrinho), fez uma análise e uma pesquisa essenciais sobre a China. O tempo em que viveu e estudou no continente fez toda a diferença.

CrowdStrike e FireEye compartilharam em primeira mão informações sobre suas experiências, para ajudar a acompanhar e explicar a interferência russa nas eleições de 2016.

Meus sinceros agradecimentos a Julie Tate, por sua ajuda na verificação dos fatos. Por fim, e o principal, este livro não teria se

concretizado sem o apoio de minha família. Agradeço a minha esposa, Gloria Riviera, que acreditou neste livro desde a concepção das ideias até a conclusão e ajudou a transformar algumas das primeiras cópias imprecisas em uma história interessante. Quero agradecer também a nossos filhos, Tristan, Caden e Sinclair. Nossa família já me dá forças para lidar com a demanda diária de cobrir as notícias, então poder me entregar às cerca de 90 mil palavras sobre as complexidades das guerras modernas foi um grande presente. Um brinde às aventuras que viveremos ao redor do mundo pelos próximos anos.

Jim Sciutto
Washington, D.C.
Fevereiro de 2019

SUMÁRIO

CAPÍTULO 1

Nas Sombras da Guerra

O alto funcionário do governo ficava quieto sempre que o garçom se aproximava da mesa, esperando ele se afastar para retomar o assunto. Ele foi minha fonte mais difícil de conhecer. Era eu quem o procurava, e, na maioria das vezes, recebia uma resposta negativa, quando recebia. Desta vez, no entanto, ele havia solicitado a reunião. Como se mostrava muito discreto, eu sabia que tinha algo a dizer. Sua escolha para o almoço foi estranha para uma conversa particular. O Café Milano é uma caricatura dos restaurantes seletos de Washington: comida e carta de vinhos caras demais, equipe subserviente e uma clientela composta de figurões de Washington e corretores internacionais de energia. E, no entanto, ali estávamos nós, discutindo o que era, sem dúvida, a operação mais audaciosa e assustadora da Rússia no exterior desde a Guerra Fria.

Minha fonte me disse que a inteligência ocidental estava muito confiante de que o próprio Vladimir Putin havia mandado e coordenado o envenenamento do ex-agente da KGB Sergei Skripal e de sua filha, Yulia, em Salisbury, Inglaterra, no início daquela primavera. A tentativa de assassinato com o poderoso agente nervoso produzido na Rússia, o Novichok, chocou o Reino Unido e

a Europa. O uso de Novichok foi particularmente alarmante. Mais letal do que o VX, o agente nervoso mais poderoso de todos os tempos do arsenal norte-americano, que fora banido por décadas, o Novichok destrói os sinais nervosos de todo o corpo, causando contrações musculares repetidas e incontroláveis. As vítimas têm convulsões dolorosas, vômitos e espumam pela boca, mesma forma como testemunhas encontraram os Skripals naquele dia em um banco de um parque em Salisbury. Nos meses seguintes ao ataque, todas as autoridades europeias que conheci o descreveram em termos assustadores. Ao realizar uma operação potencialmente letal no solo de um aliado da OTAN, argumentavam, a Rússia estabeleceu um padrão novo e assustador para suas atividades malignas no exterior.

As agências de inteligência do Ocidente logo supuseram que tal operação não poderia ter acontecido sem o conhecimento dos altos líderes russos, e, no alto do Kremlin, Putin era o único grande líder que importava. No entanto, uma ordem direta do presidente russo para assassinar alguém em solo britânico elevaria as apostas, e minha fonte me dissera que as agências de inteligência ocidentais concluíram que era "altamente provável" que Putin tivesse feito isso. Com a operação Skripal, Putin parecia ter enviado duas mensagens ousadas: aos britânicos e, mais amplamente, ao Ocidente, de que ele não via limites territoriais para as ações violentas da Rússia no exterior; e aos dissidentes russos e outros críticos, a de que eles não estavam seguros em nenhum lugar do mundo.

Meu contato se inclinou para compartilhar mais um detalhe perturbador: investigadores britânicos determinaram que os dois agentes da inteligência militar russa que realizaram a operação

levaram o Novichok à Grã-Bretanha para matar milhares de pessoas.

"Milhares?", perguntei, para confirmar.

"Sim, milhares", repetiu ele.

A inteligência ocidental não acreditava que a equipe russa de ataque planejasse matar milhares de cidadãos, mas o descaramento de transportar uma substância extremamente perigosa, em uma quantidade tão imensa, no Reino Unido surpreendeu os líderes ocidentais. Até mesmo uma pequena quantidade de Novichok acarretaria enormes riscos para quem entrasse em contato com ele. Isso ficou claro quando dois moradores de Salisbury, sem conexão com os Skripals — Charlie Rowley e Dawn Sturgess —, encontraram um frasco da substância inocentemente disfarçado de perfume Nina Ricci, descartado na tentativa de assassinato dos Skripals. Depois de pulverizar a substância no punho, acreditando ser perfume, Sturgess ficou doente em poucos minutos e morreu em dias; Rowley sobreviveu por pouco. Skripal e sua filha sobreviveram também, mas depois de semanas hospitalizados. O contrabando de enormes quantidades de Novichok para o Reino Unido aumentou o risco de mais baixas. Moscou parecia nem se importar e, principalmente, não dar a mínima para a reação da Grã-Bretanha e do restante do Ocidente. Aquele foi um grave ataque com armas químicas ao Ocidente pela Rússia. Foi sem precedentes. Será?

Tão chocante quanto o envenenamento de Skripal era o fato de que nenhum detalhe me era estranho. Doze anos antes, quando estava em Londres como principal correspondente estrangeiro da ABC News, cobri o assassinato do dissidente russo Alexander Litvinenko. Em uma trama que parecia ter saído das páginas de um romance de John le Carré, dois agentes russos envenenaram

Litvinenko com polônio-210 radioativo em sua xícara de chá. Uma partícula da substância é poderosa o suficiente para matar várias pessoas, e sua radioatividade é tão forte que os investigadores britânicos conseguiram rastrear todo o caminho até a Grã-Bretanha, dos assentos 26E e 26F no jato russo em que os dois agentes tinham voado para Londres a seu quarto no hotel Best Western, na Shaftesbury Avenue, em Piccadilly, para o estádio de futebol do Arsenal, onde assistiram a uma partida, ao restaurante japonês Itsu, onde conheceram Litvinenko, até o Pine Bar do Millennium Hotel, em Mayfair, onde lhe deram a dose letal.

O alvo e a arma eram diferentes dos usados no envenenamento de Sergei Skripal, mas o padrão era o mesmo: um assassinato extraterritorial — este, com sucesso — de um homem que o Kremlin via como inimigo do Estado. Como Skripal, Litvinenko era ex-agente do FSB, o sucessor da KGB. Ele fora expulso do FSB em 1998, depois de fazer denúncias públicas de atividades ilegais realizadas pelos serviços de inteligência russos. Sua acusação mais bombástica saiu em um livro afirmando que fora o presidente russo quem promoveu uma série de ataques terroristas a prédios residenciais de Moscou em 1999, e não os terroristas chechenos, que o Kremlin responsabilizara. O objetivo: garantir a eleição de Putin em 2000 e justificar a segunda intervenção militar da Rússia na Chechênia.

Em 2000, Litvinenko fugiu da Rússia, com sua esposa e seu filho, para o Reino Unido, onde pediu asilo político. Um ano depois, recebeu o asilo e se tornou cidadão britânico. Em sua nova casa, no Ocidente, em um aliado da OTAN, ele pensou que estaria seguro, e continuou seu trabalho expondo o que alegou serem crimes da liderança russa. Ele se aliou a outro dissidente russo em Londres, e crítico de Putin, Boris Berezovsky. Pouco antes de sua morte,

Litvinenko acusou Putin de ordenar o assassinato, em 2006, da jornalista russa Anna Politkovskaya. No final, ele, como Skripal, ainda estava ao alcance do FSB.

A operação de 2006 foi excepcionalmente ousada. O hotel onde Litvinenko foi envenenado — o Millennium — ficava a apenas meio quarteirão da embaixada dos EUA em Londres. Mais alarmante, a arma era extremamente poderosa. Na época, autoridades britânicas, alarmadas, descreveram-no para mim como o primeiro ataque de armas químicas do país, comparando-o com a detonação de uma bomba suja nas ruas de Londres. E, como aconteceu com o envenenamento de Skripal, os agentes russos colocaram milhares de pessoas em perigo.

"Milhares de civis, incluindo residentes britânicos e visitantes, estão em risco de exposição à radioatividade", disse um advogado investigador do inquérito britânico sobre o envenenamento de 2016.

Na sequência do ataque, as autoridades britânicas testaram contaminação em cerca de 800 pessoas, e foram encontradas dezenas com altas doses de radiação. Algumas, como a esposa e o filho de
Litvinenko, foram contaminadas ao entrar em contato direto com ele. A partir desses e de outros civis contaminados, a radiação se espalhou como um surto epidêmico de um patógeno letal. Pessoas que tiveram apenas um contato passageiro com sua família também foram contaminadas, assim como aquelas que entraram em contato com essas vítimas secundárias. A teia de contatos primários, secundários, terciários, e assim por diante, cresceria, atingindo centenas.

Cobrindo a história, também me tornei uma vítima em potencial. Como em minhas reportagens eu visitara muitos dos locais em que

se acreditava que Litvinenko fora exposto ao polônio-210, incluindo o restaurante japonês Itsu e o Millennium Hotel, a ABC News me enviou para exames de radiação. Os detalhes do processo são grosseiros, mas envolviam beber contraste, muita água e enviar galões de amostras de urina, para detectar a contaminação radioativa. Foram dias tensos para mim e minha esposa, apenas alguns meses após nos casarmos. Felizmente, minhas amostras deram negativo.

Ainda assim, em seu discurso de encerramento do inquérito britânico, um advogado que representava a polícia de Londres descreveu a trama como "um ataque nuclear nas ruas de Londres".

"Quem se mete em um esquema para levar o polônio-210 ao centro da cidade não tem um pingo de consideração pela vida humana", declarou Richard Horwell. "Nunca saberemos os perigos da exposição do grande público ao polônio e quais efeitos de longo prazo visitarão os londrinos."[1]

O polônio-210 é uma arma vil de assassinato, que encobre bem o crime. Um especialista nuclear que testemunhou o inquérito britânico traçou a origem da substância até uma instalação nuclear russa na cidade de Sarov, quilômetros ao sul de Moscou, e os investigadores descobriram traços dele em todos os lugares nos quais os suspeitos tinham ido, conferindo uma teia indelével de impressões digitais radioativas. As maiores concentrações foram encontradas na mesa do Pine Bar, do Millennium Hotel, onde Litvinenko e seus supostos assassinos, Andrei Lugovoy e Dmitry Kovtun, encontraram-se para o chá, contaminado ainda dentro do bule.

No entanto, apesar das nítidas evidências, a Grã-Bretanha levaria uma década inteira para culpar oficialmente a Rússia pelo envenenamento. Um inquérito público de 2016 concluiu o que a

inteligência ocidental avaliou nas semanas seguintes ao ataque: que a Rússia ordenara o assassinato de Litvinenko, enviando dois agentes, um deles ex-guarda-costas da KGB, para envenená-lo com polônio-210, proveniente de um reator nuclear russo. Como ocorreu com Skripal, tal operação, descobriu a investigação, provavelmente fora ordenada pelo próprio Putin.

Sir Robert Owen, que liderou o inquérito, concluiu: "Tenho certeza de que o Sr. Lugovoy e o Sr. Kovtun colocaram o polônio-210 no bule de chá no Pine Bar, em 1º de novembro de 2006. Também tenho certeza de que fizeram isso com a intenção de envenenar o Sr. Litvinenko."[2]

Em 2006, 12 anos antes de o envenenamento de Skripal alarmar o mundo, o Kremlin já calculara que poderia se livrar do assassinato em solo ocidental, o que, em grande parte, se provou correto. A resposta tardia da Grã-Bretanha foi expulsar quatro diplomatas russos, uma década após a morte de Litvinenko. Em 2017, sob a Lei Magnitsky, o Congresso impôs sanções a Lugovoy, único cidadão russo a ser alvo dos Estados Unidos. As penalidades para a operação de 2006 — delicadamente avaliadas e adiadas — foram claramente insuficientes para mudar o comportamento russo, talvez lançando as bases para uma repetição nas ruas de Salisbury, em 2018. Para acrescentar um insulto às graves lesões, Lugovoy foi eleito membro do estado russo Duma, onde serve até hoje.

Duas operações mortíferas em solo ocidental, com armas que ameaçaram a vida de milhares de pessoas, realizadas sob ordem do presidente russo, com 12 anos de intervalo. Para a Rússia, é difícil identificar um único ataque como o lançar fogo de sua Guerra nas Sombras contra o Ocidente. Porém os acontecimentos da última década mostraram duas frentes coerentes e perturbadoras: a crescente agressividade russa e as persistentes ilusões ocidentais

sobre suas intenções. O mesmo padrão é perceptível na China, que lançou as próprias batalhas inaugurais em outra, talvez mais perigosa, Guerra nas Sombras contra os Estados Unidos.

Para a Rússia, os meses que se seguiram ao assassinato de Litvinenko acarretaram uma série de atos hostis, de audácia cada vez mais acentuada: seu ciberataque à Estônia em 2007, sua invasão à Geórgia em 2008. Em fevereiro de 2014, a Rússia invadiu e anexou a Crimeia, na Ucrânia, segmentando uma nação europeia soberana sem disparar um tiro. Logo depois, lançou uma guerra no leste da Ucrânia, armando "voluntários" para combater as Forças Armadas ucranianas e desestabilizar ainda mais o país. No ciberespaço, de 2014 a 2015, a Rússia realizou um longo e expansivo ataque ao sistema de e-mail do Departamento de Estado dos EUA — uma operação que funcionários da Agência de Segurança Nacional identificaram como um precursor dos ciberataques da eleição presidencial de 2016. A interferência da Rússia em 2016 levou sua atividade hostil a um novo nível de agressão, descrito como um ataque surpresa à democracia norte-americana — um "Pearl Harbor político", que chegou sem aviso e, portanto, compreensivelmente, pegou a comunidade de Segurança Nacional desprevenida. Mas, na verdade, houve vários alertas, antes de 2016, de uma nova e agressiva estratégia russa para minar o país aos poucos, com uma combinação de potência coercitiva e poder branco.

A China, outro grande concorrente dos EUA em nível internacional, seguia uma estratégia semelhante, talvez mais sutil, mas não menos agressiva. Em meados dos anos 2000, o esforço nacional da China para roubar a tecnologia e os segredos de Estado dos EUA já estava em alta velocidade e registrava sucessos alarmantes nos setores público e privado. Em 2014, a China

desafiou tanto o direito internacional quanto as leis da física para produzir um território soberano no meio do Mar do Sul da China, iniciando a construção de uma série de ilhas artificiais em águas reivindicadas por vários de seus vizinhos do sudeste asiático. A China também estava expandindo suas forças e bases militares de dentro das ondas até o espaço, com a intenção expressa de superar os Estados Unidos e, se necessário, derrotá-los em uma guerra.

Dentro do governo dos EUA e da comunidade de inteligência, inicialmente, essas investidas bárbaras foram negligenciadas e, depois, subestimadas. Autoridades norte-americanas, lideradas pelo presidente Barack Obama, aceitaram as garantias da China de não militarização de suas ilhas artificiais no Mar da China Meridional — garantias que Pequim renegou quase que no ato. Mais tarde, Obama aceitaria as garantias chinesas de que Pequim reduziria o roubo cibernético dos segredos corporativos dos EUA, atividades maliciosas que continuam desenfreadas e brutais nos dias de hoje. Mesmo depois de, finalmente, reconhecer esses atos de agressão, muitas autoridades dos EUA e especialistas em suas políticas continuaram a encará-los como fugazes e reversíveis.

Quanto à Rússia, os sucessivos líderes dos EUA persistiram na convicção de que tudo ficaria bem, atendo-se aos pontos em que seus antecessores fracassaram. O malfadado "reset" do governo Obama com a Rússia ocorreu poucos meses após sua invasão à Geórgia. A imagem da então secretária de Estado, Hillary Clinton, apresentando seu homólogo da Rússia, o ministro das Relações Exteriores Sergei Lavrov, com um botão vermelho de reset em Genebra sobreviveu por muito tempo como um símbolo da péssima interpretação que o Ocidente faz de Moscou. Os hackers russos controlaram a rede de e-mails do Departamento de Estado meses

antes de serem detectados. Mais tarde, nenhuma agência de inteligência dos EUA previu a anexação da Crimeia pela Rússia.

A visão desdenhosa que o governo Obama tinha do Kremlin persistiria até quase o final de seu mandato. Na cúpula do G7, em 2014, Obama relegou a Rússia ao status de "poder regional", dizendo que suas ambições territoriais "pertenciam ao século XIX". Seus comentários de 2014 ecoaram seu desdém pelas prioridades da política externa de Mitt Romney no debate presidencial de outubro de 2012: "Quando lhe perguntaram qual era a maior ameaça geopolítica enfrentada pelos EUA, você disse Rússia, não Al-Qaeda. Você disse que a Rússia e a década de 1980 estão pedindo a devolução de sua política externa, porque a Guerra Fria acabou há 20 anos."

A resposta de Romney a Obama agora parece presciente. "A Rússia indicou que é um inimigo geopolítico", disse ele. "Não usarei lentes cor-de-rosa quando se trata da Rússia ou do Sr. Putin."

No entanto, em 2016, o desprezo de Obama foi substituído pela visão cor-de-rosa do próprio presidente Donald Trump sobre Moscou e Putin. Se o período que antecedeu 2016 foi dividido entre alertas despercebidos e reações hesitantes, com sua resposta à interferência da Rússia na eleição presidencial de 2016, os Estados Unidos correram o risco de passar da inércia equivocada para a negligência voluntária.

No centro desses reiterados erros cometidos por ambas as administrações, havia uma impressão errônea das metas e intenções russas e chinesas, marcadas pela esperança — em última análise, falsa — de que os interesses da Rússia e da China estariam alinhados com os dos EUA.

"Conheci Vladimir Putin na década de 1990", disse Ashton Carter, que serviu como secretário de defesa de 2015 a 2017, e como oficial da defesa na década de 1990. "Ficou claro para mim, mas não para todos da defesa e nem, sem dúvida, para a comunidade estratégica, que Vladimir Putin [...] estabeleceu o objetivo de arruinar o Ocidente em si. E isso era uma barreira intransponível para lidar com ele de forma construtiva."

Carter diz que a visão predominante do governo dos EUA sobre a China sofreu de uma situação análoga ao espelhamento.

"A China, que, na década de 1990, achamos que pelo menos se dedicaria a um maior envolvimento com o sistema de segurança que os EUA criaram e de que se beneficiara", disse Carter, "na verdade, assumiu uma postura de conquistar um lugar ao sol para o Reino do Meio".

Além do equívoco fundamental em relação às intenções dos adversários dos EUA, não houve uma percepção da mudança crucial sobre o que a Rússia e a China estavam dispostas a fazer para atingir suas metas — e em como o fariam. Com efeito, os principais adversários dos EUA conceberam — e, então, empreenderam — um tipo inteiramente novo de guerra no Ocidente, com foco nos Estados Unidos.

Hoje, as principais autoridades de segurança nacional dos EUA, que lideram a instituição, após essa ameaça ter tomado corpo, reconhecem que não entenderam a profundidade e a amplitude do que agora identificam como a maior ameaça à segurança nacional dos EUA.

"Precisamos estudar suas táticas a fundo, porque, obviamente, não estamos preparados", disse-me o general Michael Hayden, diretor da CIA de 2006 a 2009. "Entendo de combate aéreo. E de

ataques de segundo e terceiro escalão, porque temos que saber, mas não usamos isso."

"Isso" é a guerra híbrida, em suma, uma estratégia de atacar um adversário ficando logo abaixo do limiar da guerra convencional — o que os comandantes e estrategistas militares chamam de "zona cinzenta" — e usando uma série de táticas de poder branco: de ciberataques a infraestruturas críticas, para ameaçar ativos espaciais, a operações de informação destinadas a desencadear a divisão doméstica, a aquisições territoriais logo após uma invasão formal. Essa é uma guerra conduzida pelas sombras — uma Guerra nas Sombras —, embora suas consequências sejam tão concretas e duradouras quanto as da guerra completa.

Este livro conta o que aconteceu quando os inimigos do Ocidente perceberam que, embora seja improvável ganharem uma guerra a ferro e fogo, eles têm meios de vencer. O Ocidente se condicionou a interpretar mal o que seus inimigos fazem, a ver suas ações através das lentes do passado. Com frequência, as motivações russas e chinesas são mal interpretadas, seus objetivos são mal interpretados; e as consequências de longo prazo, também. Além disso, Rússia e China estão minando ou transformando em fraquezas o que o Ocidente vê como seus maiores pontos fortes: sociedades abertas, inovação militar, domínio da tecnologia na Terra e no espaço e liderança de longa data em instituições globais.

Os Estados Unidos precisam de um novo guia para o conflito internacional, porque os métodos antigos não estão funcionando. É como se a China e a Rússia tivessem iniciado uma nova Guerra Fria que ninguém notou. As táticas são novas e estão em constante transformação, mas as metas são as mesmas. Esses países querem se tornar soberanos no cenário mundial enfraquecendo e

desestabilizando o Ocidente, seus aliados e os sistemas dos quais dependem. Esses dois adversários também estão pastoreando outros países, com o Irã e a Coreia do Norte encabeçando a jornada. A mira não está só sob os Estados Unidos: todas as nações que não os auxiliam são alvos em potencial.

Em algum momento, os Estados Unidos entenderão essa Guerra nas Sombras como seu principal problema de política externa, embora a maioria dos cidadãos norte-americanos ainda não saiba de nada disso. Quanto mais cedo tal guerra se tornar foco de debates políticos e reuniões internacionais, mais brilhante — e seguro — será o futuro do Ocidente.

A Guerra nas Sombras não é resultado de um plano secreto, espreitando nas vielas dos serviços de inteligência russos e chineses. Tanto a tática quanto o pensamento por trás dela se ocultaram. Em fevereiro de 2013, o general Valery Gerasimov, chefe do Estado-maior da Federação Russa, detalhou a estratégia de seu país em um ensaio, para quem quisesse ver no semanal *Military-Industrial Kurier.*

"No século XXI, vimos uma tendência a embaçar as fronteiras entre os estados de guerra e paz", escreveu Gerasimov no artigo intitulado, de forma um tanto ingênua, "O valor da ciência está na previsão". "As guerras não são mais declaradas, e, tendo começado, avançam seguindo um modelo desconhecido."[3]

Embora Gerasimov estivesse ostensivamente descrevendo como a Rússia acreditava que seus adversários estavam conduzindo a guerra na era moderna, seu ensaio definia a própria estratégia russa de travar guerra contra seus adversários, principalmente os Estados Unidos, formando a base daquilo a que os oficiais de

inteligência ocidentais agora se referem como a "Doutrina Gerasimov", englobando métodos militares e não militares.

"As próprias 'regras da guerra' mudaram", escreveu ele. "O papel dos meios não militares para alcançar objetivos políticos e estratégicos cresceu, e, em muitos casos, tais meios excederam o poder [...] das armas em eficácia."[4]

Para um alto comandante russo traçando a estratégia militar de seu país em um fórum público, Gerasimov era extraordinariamente específico, identificando as táticas exatas que a Rússia empregaria no próximo ano na Crimeia e no leste da Ucrânia, incluindo forças especiais que se apresentavam como alheias aos soldados da Federação Russa.

"O uso aberto de forças — muitas vezes sob o disfarce de manutenção de paz e regulação de crises — é empregado apenas em um determinado estágio, para alcançar o sucesso derradeiro no conflito", escreveu Gerasimov.

Eram os "homenzinhos verdes" que apareciam nas ruas da Crimeia, aparentemente, a pedido dos russos étnicos, temendo os ataques dos compatriotas, cidadãos ucranianos. Hoje, o general Hayden vê o ensaio de Gerasimov, em toda sua franqueza e clareza, como um dos mais óbvios alertas perdidos.

"Esse foi um ataque contra uma fraqueza inédita, de uma direção inesperada", disse Hayden. "Inesperado porque estamos olhando para o lado errado, enquanto Gerasimov — embora tenha escrito, não o lemos, realmente — foi certeiro."

A doutrina da guerra híbrida da China — sua estratégia para vencer na zona cinzenta — tem um nome diferente: "vencer sem lutar", ou o que a Estratégia de Segurança Nacional dos EUA de 2017 descreve como "competição contínua", com os dois lados nem

em paz nem em guerra. Suas ilhas artificiais no Mar do Sul da China são exemplos dessa estratégia em ação. Como a Rússia na Crimeia, a China conseguiu assegurar a soberania territorial em águas disputadas sem disparar um tiro.

No entanto, autoridades dos EUA com experiência direta em confrontos com a inteligência chinesa alertaram que Pequim não se esquiva de conflito e violência que julga necessários. Bob Anderson liderou a divisão de contrainteligência do FBI até 2015, e identificou e capturou dezenas de espiões chineses operando dentro dos Estados Unidos.

"Os chineses são até mais cruéis do que os russos", disse-me Anderson. "Eles vão matar pessoas num piscar de olhos. Vão matar famílias num piscar de olhos. Farão isso silenciosamente dentro da China ou em seus territórios, mas eles absolutamente o farão, se precisarem."

"Os chineses são uma cultura de inteligência muito cruel", acrescentou.

Hoje, encorajadas por seus sucessos, a Rússia e a China travam uma guerra híbrida contra uma série de adversários, grandes e pequenos. O ex-secretário de Defesa Carter a vê em ação em toda a extensão de sua fronteira com a Europa, incluindo inúmeros aliados da OTAN.

"Na verdade, segue por toda a sua costa ocidental com a Europa", disse Carter. "Tentam comprometer e devastar países, e intimidá-los por meio do planejamento, e, em alguns casos, realizam operações nas quais é fácil maquiar o que está acontecendo com uma grande mentira."

Em todas as frentes, "a grande mentira" é uma parte essencial da estratégia. Com a invasão da Crimeia e da Ucrânia, isso

representava negar que as tropas eram russas. Com a intromissão na eleição presidencial de 2016, representava divulgar fake news por redes sociais e meios de comunicação tradicionais russos para semear dúvidas sobre o papel da Rússia e para dar voz aos políticos norte-americanos que endossavam essas dúvidas, incluindo o próprio presidente Donald Trump.

"Putin é um dos especialistas da grande mentira: você faz alguma coisa, nega e cria incerteza suficiente para que pelo menos o povo russo não acredite que você está fazendo o que está fazendo", disse Carter.

No caso da interferência eleitoral da Rússia, alguns norte-americanos também acreditavam na grande mentira, liderada por um candidato à presidência dos EUA, agora presidente, cuja retórica imitava a da Rússia, às vezes palavra por palavra.

"Eles pegavam os memes criados nos Estados Unidos para fazer ataques nas redes sociais; geralmente, usando a direita alternativa; eventualmente, o presidente", disse o general Hayden.

A China conduz as próprias operações de informação, inclusive por meio da presença internacional, cada vez mais representativa, de sua mídia estatal. No final de 2016, o país renomeou sua rede televisiva central (CCTV) como rede global de televisão chinesa (CGTN), a ala internacional controlada pelo governo que firmou forte presença nos EUA como RT Network da Rússia, mas com pouca demonstração do respaldo do governo. Segundo a cobertura da CGTN, muitas vezes feita por repórteres e âncoras norte-americanos, as ilhas artificiais não são uma ocupação de terras, mas uma questão de soberania, desafiada sob tratados que, a CGTN observa, nem os Estados Unidos ratificaram.

A Guerra nas Sombras começou há anos, mas a China e a Rússia começaram a tomar território quando os Estados Unidos estavam preocupados com outra ameaça e outro tipo de guerra — no Oriente Médio, nos anos seguintes aos ataques do 11 de Setembro.

"Na época em que a primeira guerra do Iraque começou", disse Carter, "a Rússia e a China já haviam estabelecido suas bases estrategicamente. Mas aquele foi o exato momento em que nos deparamos com algo maior do que uma década de preocupação em outros lugares".

"Acho que durante esse período, que durou duas administrações, havia uma falta de motivação para encarar o fato de que duas grandes dores de cabeça adicionais estavam se desenvolvendo durante nossas outras lutas. E nossas Forças Armadas estavam preocupadas com as ameaças concretas no momento, que eram o terrorismo e a contrainsurgência no Afeganistão e no Iraque", disse Carter.

Hoje, bastante tardia, a guerra híbrida e os meios de defesa e de vencer os conflitos na zona cinzenta ocupam a mente dos militares dos EUA e dos oficiais da inteligência. A partir de 2015, a OTAN desenvolveu um plano de guerra para defender a Europa da agressão russa — que, pela primeira vez, identifica e até mesmo incorpora táticas híbridas de guerra.

"Não tínhamos um plano de guerra há 25 anos", disse Carter. "Achávamos que não precisávamos de um."

Esse pensamento ainda não é unânime na Casa Branca. Oficiais da defesa e da inteligência, que serviram nas administrações de Obama e na de Trump, disseram-me que os EUA não podem se defender com eficácia e confiança desse novo tipo de guerra sem lideranças nos níveis mais altos e, mais importante, do presidente.

"Simplesmente não entendo por que nosso governo está tão engajado com questões relativas a comportamentos censuráveis da Coreia do Norte, do Irã e até mesmo da China, que considero questões legítimas, mas quieto em relação à Rússia", disse Carter. "Não consigo entender."

O advento da Guerra nas Sombras não deveria surpreender ninguém. Em termos militares, a guerra híbrida é um produto natural de um mundo com uma única superpotência e outras potências em ascensão ou declínio ansiosas para desafiá-la. Para a China, a Rússia e outros adversários norte-americanos e ocidentais em geral, a guerra híbrida é a única maneira de enfrentar um país como os Estados Unidos, com um poderio militar incontestável. Em outras palavras, a chamada zona cinzenta é o único campo de conflito em que esses adversários acreditam ter uma chance de vencer.

John Scarlett foi chefe do serviço de inteligência internacional da Grã-Bretanha, o MI6, de 2004 a 2009 e, antes disso, chefe de sua estação de Moscou. Ele explica a motivação — na verdade, a necessidade — para a guerra híbrida do ponto de vista da Rússia.

"Não é muito difícil entender o que está acontecendo", contou-me Scarlett. "Em pouco tempo vimos a humilhação, o ressentimento, a sensação de que as coisas estão acontecendo sem que os interesses da Rússia sejam levados em conta e a forte consciência da diferença de poder entre os EUA e a Rússia."

"Se você quer ser tratado como igual, tem que encontrar outra maneira de expressar isso", disse. "[A guerra híbrida] permitiu que países muito mais fracos assumissem países muito mais fortes. Há uma assimetria natural."

Apesar de empregar estratégias semelhantes, a Rússia e a China são adversários distintos. A China é uma potência em ascensão, com grandes ambições territoriais, econômicas e militares destinadas a conflitar com as do país mais poderoso do mundo. Pequim se vê em uma longa guerra com os Estados Unidos pelo domínio global.

A Rússia é uma potência em declínio. Com uma economia menor, em termos de PIB, do que alguns estados norte-americanos, o Kremlin sabe que nunca competirá, de fato, com os Estados Unidos pela liderança global. A competição é mais um jogo de soma zero: a derrota dos Estados Unidos é a vitória da Rússia e vice-versa.

"Com a União Soviética, estamos falando de um colapso", disse Scarlett. "Com a China, de mudanças rápidas, desenvolvimento e progresso, bem como de uma alta consciência da natureza frágil do progresso."

"Nesse crescimento, era previsível que [a China] passaria da autocomiseração para — em nível internacional — a autoconfiança", continuou Scarlett. "Vemos um grau de afirmação e assertividade chegando, começando de forma regional e ganhando proporções internacionais."

A Rússia e a China, acredita Scarlett, acabam enfrentando os Estados Unidos em termos semelhantes, embora tenham chegado de lugares diferentes e estejam seguindo trajetórias particulares.

No entanto, a Guerra nas Sombras da Rússia e da China nos Estados Unidos é impulsionada pelas mesmas forças cruciais e imutáveis, e essas semelhanças podem acarretar resultados desastrosos.

A primeira semelhança é estratégica: o domínio desafiador dos EUA na Europa e na Ásia serve tanto às ambições russas quanto às

chinesas de exercer uma influência maior nas próprias regiões. Cada uma inveja a Doutrina Monroe — isto é, o exercício do poder absoluto dentro dos arredores dos EUA — e trabalha para estabelecer a própria versão.

A segunda força comum é política. Moscou e Pequim sofrem de uma crise de legitimidade em casa. Seus líderes não são eleitos pelo seu povo e, portanto, têm pouca reivindicação de poder além do fato de que o possuem. Na era moderna, não há censura e propaganda que impeça os cidadãos russos e chineses de observar que os norte-americanos escolhem os próprios líderes. Portanto, sua melhor defesa contra os próprios povos é retratar o sistema político dos EUA como falido e corrupto — pelo menos, mais do que o sistema chinês e do que o russo.

A terceira força é indiscutivelmente a mais poderosa. Ao enfraquecer os EUA, tanto a China quanto a Rússia tentam corrigir erros históricos e restaurar o que consideram as posições legítimas de seus países como potências mundiais. Para a Rússia, o pecado é recente: o colapso da União Soviética, seguido por aquilo que os russos consideram sua subjugação pelo restante da Europa e pelos Estados Unidos. Para a China, o pecado remonta a gerações, começando com sua humilhação em uma série de guerras do século XIX, o que, com o tempo, a seu ver, levou seu território e sua economia a ser igualmente subjugados pelo Ocidente.

Em suma, a Guerra nas Sombras tem todos os ingredientes de uma verdadeira guerra a ferro e fogo.

Os líderes russos e os chineses são extremamente conscientes da história uns dos outros. Estudar o colapso da União Soviética é obrigatório para os líderes do Partido Comunista Chinês. E Mikhail Gorbachev é uma figura tão difamada em Pequim quanto em Moscou. Diferentemente dos Estados Unidos, onde ele é visto como

um líder russo que ajudou a evitar a Terceira Guerra Mundial; na Rússia e na China ele é visto como um líder que permitiu que seu país desmoronasse — e que o Ocidente juntasse as peças.

Hoje, os planejadores militares em Moscou e Pequim discutem abertamente toda uma gama de meios não convencionais para reduzir a vantagem militar e a influência dos EUA em tempos de paz e, se necessário, de guerra. Para eles, a guerra híbrida não é apenas assimétrica, é interminável. Como o general Gerasimov escreveu, ameaçadoramente, a estratégia da Rússia envolve a criação de "uma frente permanente em todo o território do Estado inimigo".

A interferência da Rússia na eleição presidencial de 2016 estendeu a "frente permanente" para o processo político dos EUA. Hoje, os investigadores da inteligência e os congressistas dos EUA estão percebendo que a interferência está muito mais entranhada do que se pensava. Além de hackear e liberar e-mails e outras comunicações do Partido Democrata e de funcionários de campanha de Clinton, a Rússia preparou grandes comunidades de trolls para influenciar milhões de eleitores indecisos com fake news e histórias divisivas. Com a aproximação das eleições em 2018 e 2020, a Rússia tomou medidas mais alarmantes, ameaçando o próprio processo eleitoral.

As autoridades norte-americanas de defesa e de inteligência agora falam abertamente sobre o perigo de repetir os erros dos anos 1930, isto é, observar a agressão de adversários na Europa e na Ásia, enquanto impõem limites frouxos a suas ambições. Esse medo de repetir os erros do passado alimenta o chamado para se defender da Guerra nas Sombras agora ou enfrentar o perigo de um conflito mais amplo nos próximos anos. E, ainda, sem um compromisso em todos os níveis do governo dos Estados Unidos, a

perspectiva alarmante é a de que o país saia da Guerra nas Sombras encolhido e derrotado.

---

11 "The Litvinenko Inquiry: Report into the death of Alexander Litvinenko", Chmn, Sir Robert Owen, janeiro de 2016, 192.

2 Ibid.

3 "Valery Gerasimov, the General with a Doctrine for Russia", *Financial Times*, 15 de setembro de 2017.

4 "The Gerasimov Doctrine: It's Russia's new chaos theory of political warfare. And it's probably being used on you", Molly McKew, *Politico Magazine*, setembro/outubro de 2017.

CAPÍTULO 2

Abrir Fogo

(RÚSSIA)

Os cidadãos da Estônia, o pequeno país báltico precariamente assentado na fronteira com a Rússia, zombam de si mesmos por serem os homens e mulheres entediantes do norte da Europa.

"Nossos vizinhos têm inúmeras piadas sobre sermos lerdos e frios", disse-me um jornalista estoniano, Jaanus Lillenberg.

Assim, no final de abril de 2007, quando Tallinn, a capital estoniana, foi abalada por violentos protestos de rua, o caos foi um choque. Naqueles dias frios e chuvosos de abril, Tallinn foi engolida pela violência.

"Eles quebraram janelas, atacaram carros estacionados à beira da estrada, jogaram pedras, garrafas e tudo mais", disse Lillenberg, que trabalhava com tecnologia para o matutino *Postimees*. "Foi algo que nunca havia acontecido em nossa história."

Para os moradores de Tallinn, as cenas nas ruas pareciam de outro mundo. A Estônia é um país de baixa criminalidade. As ruas são limpas. Os estonianos são apaixonados... por tecnologia, não por protestos. As manifestações públicas são assuntos sérios. O caos parecia emprestado de um conto de fadas sombrio, ou — mais provavelmente — das ruas de seus aliados e vizinhos "não tão frios".

"Vimos isso na TV — em Paris, Estocolmo ou nos Estados Unidos —, mas nunca na Estônia", disse Lillenberg. "Foi quase como uma história oriunda do Polo Norte."

A tropa de choque lutou para restaurar a ordem, mas não conseguiu controlar a multidão. Quase 200 pessoas ficaram feridas, e mais de 1.000 foram presas — um número considerável em uma cidade com menos de meio milhão de habitantes.

A Estônia tem uma longa história, mas ainda é uma nação jovem, que só reconquistou a independência após o colapso da União Soviética, uma geração atrás, em 1991. Sua separação da Rússia, junto dos parceiros bálticos Letônia e Lituânia, enfureceu Moscou, remexendo amargamente memórias de um império perdido. A ferida ainda se agita no Kremlin. Quando as batalhas de rua se desdobraram, as testemunhas notaram que os desordeiros tinham um nome — um país — na ponta da língua.

"A multidão gritava: 'Rossiya, Rossiya', que significa Rússia, é claro", disse Lillenberg.

A faísca para os protestos foi a decisão do governo estoniano de mover um memorial de guerra soviético de décadas. O Soldado de Bronze, como era conhecido, homenageava as tropas do Exército Vermelho soviético que morreram combatendo forças nazistas na Estônia durante a Segunda Guerra Mundial. O memorial se tornara um ponto de encontro para os nacionalistas russos e estonianos em manifestações por vezes violentas nas semanas e meses anteriores. Para os russos, representava a vitória sobre os nazistas e o passado orgulhoso do país. Para os estonianos, era uma lembrança dolorosa de décadas de repressão após a anexação de seu país à União das Repúblicas Socialistas Soviéticas, ou URSS.

Após mover a estátua de Tallinn, o governo planejava colocá-la em um cemitério militar, afastado do centro da cidade, e exumar os corpos dos soldados soviéticos não identificados, enterrados nas proximidades, para lhes dar um enterro digno. Porém muitos russos étnicos na Estônia, e seus compatriotas do outro lado da fronteira, interpretaram a iniciativa como um insulto à herança russa e, pior, como uma demonstração extra da independência da Estônia da influência russa. Para inflamar ainda mais as tensões, a mídia russa circulava histórias falsas nas redes sociais e em sites de notícias alegando que a Estônia planejava destruir o memorial.[1]

O então ministro das Relações Exteriores da Estônia, Sven Mikser, um jovem membro do parlamento, lembrou um crescente sentimento de medo entre os compatriotas.

"A gravidade, trocentos carros de cabeça para baixo. Quero dizer, as pessoas ficam exaltadas quando coisas assim acontecem", disse Mikser.

Poucos estonianos acreditavam que os tumultos eram espontâneos. Eles suspeitaram que foram orquestrados pelo governo russo. "Absolutamente", disse Lillenberg. "Não, isso não acontece assim do nada."

Conforme as horas se passavam e a confusão aumentava, a violência nas ruas se reduziu a apenas uma frente de um ataque mais amplo. Silenciosamente, no ciberespaço, um exército invisível formava uma ofensiva que prenunciaria ataques cibernéticos posteriores na Europa Ocidental e nos Estados Unidos. As primeiras pistas foram confusas e difíceis de relacionar. Lillenberg e sua equipe assistiram ao ataque cibernético se desdobrar em ondas de interações online aparentemente inócuas. O alvo? A seção de comentários de seu jornal, que estava sendo inundada.

"Recebíamos comentários anônimos, de 8 a 9 mil por dia. Mas, de repente, foi como chegar a mais de 10 mil em 10 minutos", disse ele. "Eu estava meio: 'Quê?!'"

Além do ritmo sem precedentes, Lillenberg notou uma estranha uniformidade nos comentários que chegavam. Ele e seus colegas identificaram e contaram um punhado de mensagens idênticas que estavam sendo repetidas aos milhares. Estava ficando claro que esse trabalho vinha de bots de computador, em vez de leitores reais.

"Houve uma variação de cerca de 30 mensagens", disse ele. "Elas se repetiam. E parecia que não havia pessoas por trás, porque as pessoas não conseguem enviar comentários tão rapidamente."

"Foi o primeiro sinal para entendermos que havia algo errado", falou.

Tanto o ritmo quanto a proporção do ataque se acelerariam rapidamente. Em uma hora, o número de comentários que inundavam o site de seu jornal saltou para 100 mil a cada 10 minutos.

O ataque ao site do *Postimees* estava sendo replicado nos setores privado e público. Jaak Aaviksoo, com apenas duas semanas de trabalho como ministro da Defesa, imediatamente tomou nota. Como todos na Estônia, ele foi educado sob o domínio da tecnologia.

"Olhei diferentes portais de notícias, e eles tinham caído. Eu me perguntei o que estava acontecendo, então soube que os sites dos bancos e do governo também tinham caído", disse Aaviksoo.

Sentado em um escritório do qual ele ainda tinha que remover a mobília e a decoração de seu antecessor, Aaviksoo suspeitava de um ataque coordenado do exterior.

"Ficou claro que não era apenas um incidente ruim", disse ele. "Eram pessoas ruins lá fora."

Os estonianos, talvez a população mais conectada do mundo, de repente viram-se desligados — sem acesso a notícias ou sites do governo e, portanto, sem informações sobre o que estava acontecendo. Os bancos eletrônicos, que àquela altura eram responsáveis pela maioria das transações financeiras da Estônia, também ficaram inacessíveis. O ataque explorou uma vulnerabilidade gritante para o país. A pequena Estônia, conhecida pelas muralhas medievais e ruas de paralelepípedos de sua capital antiga, é uma potência tecnológica: o primeiro país a permitir a votação online e o berço do Skype. Mas, agora, um dos países mais conectados estava sob um dos ciberataques mais incapacitantes que o mundo já vira.

A Estônia foi a primeira vítima de um ataque cibernético patrocinado por um Estado para outra nação. Ele tomou a forma de um ataque distribuído de negação de serviço, ou DDoS, na sigla em inglês [distributed denial of service]. Os ataques DDoS não eram novidade, mas a proporção deste foi sem precedentes. Hackers russos sequestraram milhares de computadores em mais de 100 países e os colocaram, sem o conhecimento dos donos, sobre alvos em toda a Estônia.

"Pense em um enorme shopping center", explicou Lillenberg. "As pessoas entram, fazem compras e saem. O mesmo vale para os servidores da web. Um usuário entra, faz pedidos, o servidor dá alguns retornos, e o usuário sai. É assim que o fluxo segue."

"Imagine que seu shopping comporte 10 ou 15 mil pessoas. Mas, agora, imagine 2 milhões de caras pressionando a porta da frente sem nenhuma intenção de comprar nada, apenas para bloqueá-la. Isso é um ataque DDoS", disse Lillenberg.

A Estônia se tornou tão vulnerável justamente por ser muito avançada.

"Descobrimos que o ciberespaço constitui uma parte — essencial — da infraestrutura crítica", disse Mikser. "Portanto, temos que defender e manter esses sistemas funcionando mesmo em tempos de crise, mesmo em tempos de ataques."

O ataque, no entanto, estava acontecendo em várias frentes: tumultos nas ruas, botnets na web. Foi uma guerra híbrida em ação. Juntos, esses exércitos secretos pareciam encarregados de paralisar o país. Como estudante de táticas militares soviéticas, o ministro da Defesa, Aaviksoo, reconheceu a mão do vizinho russo.

"Tumultos de rua, até certo ponto, nunca tínhamos visto. Ataques coordenados e concentrados no ciberespaço... Esse foi o alerta para a Estônia", disse-me Aaviksoo. "Claro, descobrimos que esses ataques não eram tão espontâneos quanto demonstravam. Coordenados, focados, globais. Indícios claros de que havia recursos consideráveis os viabilizando."

O ciberataque foi o maior já lançado por um Estado a outro, e o acréscimo de tumultos orquestrados em terra incluiu um elemento alarmante de violência física. O fato de a Estônia ser membro da OTAN fez daquele um desafio aberto não apenas ao país, mas também aos Estados Unidos e à Europa. O ataque à Estônia em 2007 foi o abrir fogo da Guerra nas Sombras.

Alguns estonianos temiam que os motins e ataques cibernéticos estivessem preparando o terreno para uma invasão em grande escala. Os estonianos estavam bem conscientes da profunda insatisfação de seus vizinhos com a perda dos estados clientes na Europa Oriental. Os países bálticos, incluindo a Estônia, que fazem fronteira com a Rússia eram particularmente sensíveis, tendo sido

os primeiros a ser anexados pela União Soviética e os primeiros a declarar independência após seu colapso.

"O propósito de um DDoS muito forte é esse mesmo, um ataque em grande escala para derrubar um país por um tempo, no que concerne à informação", observa Lillenberg.

Como seus semelhantes na Ucrânia, na Geórgia e em outras ex-repúblicas soviéticas, os estonianos há muito tempo eram alvo da propaganda russa. Os defensores da independência eram destituídos como nacionalistas e fascistas, e os russos étnicos eram retratados como vítimas que precisavam da ajuda russa. Quase 16 anos desde que a Estônia recuperara a independência, as lembranças da dominação soviética ainda estavam frescas, e as feridas, abertas.

"Houve algo que percebi. Todos estavam tentando ser fortes, mas todos ainda são humanos. Houve um nível de preocupação muito pessoal", disse Lillenberg. "Estavam preocupados com eles mesmos e com suas famílias. Nós estávamos muito, muito preocupados."

"Se você conhece a doutrina russa, sabe que é uma questão de progressão. Em alguns pontos, há tanques; em outros, armas nucleares, mas tudo faz parte do mesmo plano, que começa com a criação e a distribuição de fake news e, em seguida, aumenta de proporção", acrescentou.

Tal pânico não foi exclusivo do público. O ministro da Defesa, Aaviksoo, fez apelos urgentes aos seus comandos de combate. Eles não relataram incursões no espaço aéreo estoniano e nem no território da Estônia, incluindo sua fronteira leste, bem defendida, com a Rússia. Ainda assim, o Ministério da Defesa se colocou em pé de guerra contra um inimigo que ainda não tinha sido identificado.

"O ponto era que, pelo menos psicologicamente, o ataque representava uma ameaça à segurança nacional", disse-me Aaviksoo. "Uma grande parte da população estava com medo, desestabilizada. Não houve vítimas humanas nem perdas materiais, mas o entendimento de que estávamos sob ataque era claro."

"A batalha real está acontecendo no espaço psicológico — entre as orelhas das pessoas, na mente delas", disse ele.

Esse foi um ataque à psicologia de uma nação e seu povo: confundir, dividir, antagonizar, amedrontar e semear dúvidas sobre seus líderes.

"As pessoas passaram a duvidar do poder do governo", acrescentou. "O que estava acontecendo?"

Enquanto o governo lutava para acalmar o público, restaurar a ordem e repelir o ciberataque, foi confrontado com uma série de questões críticas, ainda sem respostas. Um inimigo sem rosto estava sistematicamente silenciando seu país. A Estônia estava sofrendo o equivalente a um bloqueio cibernético, limando os estonianos de praticamente todos os serviços públicos e privados, e, em breve, cortando o contato do país com o mundo exterior. O público e o governo tinham apenas um suspeito na Rússia. No entanto, nem os manifestantes nas ruas e nem os bots na web usavam uniformes. A Estônia estava em guerra? E, se sim, contra quem?

Para o ministro da Defesa, Aaviksoo, uma guerra não precisa de tropas invasoras e mísseis.

"Um entendimento comum é o de que a guerra não depende dos meios para você realizar um ataque, mas do impacto. Se houver

dano material extenso, perda de vidas, lesões", explicou Aaviksoo. "Então, se o impacto está nessa escala, é um ato de guerra."

"Não importa se foi um míssil ou um ataque cibernético", acrescentou.

A Rússia, com todas as suas capacidades militares de primeiro mundo, incluindo um arsenal nuclear maior que o dos Estados Unidos, estava pegando emprestado táticas de Estados e atores não estatais desonestos. Ela estava atacando a pequena Estônia por meios assimétricos. As autoridades estonianas comparam 2007 aos ataques do 11 de Setembro.

"Muitas pessoas chamaram o 11 de Setembro de ataque de baixa tecnologia e alta execução", disse Mikser. "O que acontece em um ataque cibernético como esse é que, quando você baixa a guarda, quando não é cuidadoso, obviamente, os invasores abusam. Eles se aproveitam disso."

Os líderes da Estônia ponderaram minuciosamente essas questões ao mesmo tempo em que tentavam defender o país. Mas elas não eram questões exclusivas da Estônia. A Estônia pertence à OTAN, cujos membros são obrigados, por um tratado, a entender um ataque armado a uma nação como um ataque armado contra todas e a se mobilizar para defender seus aliados.

O Artigo 5 do Tratado estabelece: "As Partes concordam em que um ataque armado contra uma ou várias delas na Europa ou na América do Norte será considerado um ataque a todas, e, consequentemente, concordam em que, se um tal ataque armado se verificar, cada uma [...] prestará assistência à Parte ou Partes assim atacadas, praticando sem demora, individualmente e de acordo com as restantes Partes, a acção [sic] que considerar

necessária, inclusive o emprego da força armada, para restaurar e garantir a segurança na região do Atlântico Norte."[2]

A Estônia estava sendo forçada a definir e interpretar as leis da guerra moderna em tempo real. Um ataque cibernético, junto a protestos orquestrados nas ruas, desencadearia uma resposta da OTAN, se houvesse perdas significativas de vidas e danos a propriedades? Alguns acreditavam que a ação não militar só se qualificaria se desencadeasse uma perda de vidas equivalente à decorrente das ações militares. Essa questão demandava uma definição nova, ou adaptada, para ameaças inéditas em uma era inédita de guerra.

No fim das contas, a Estônia não pediu a seus aliados da OTAN para responder militarmente. Aaviksoo disse que eles apenas os mantiveram informados.

"Nossa resposta foi dizer a todos que estávamos sob ataque. Compartilhamos nossa experiência, informamos nossos amigos e vizinhos", disse Aaviksoo.

Por sua vez, a Estônia optou por não fazer retaliações. Seu governo e a instituição de defesa estavam focados em repelir o ataque cibernético, apaziguar os ânimos nas ruas e reposicionar o país no mundo digital.

"Nunca fizemos uma retaliação no sentido estrito da palavra", disse ele. "Mas acho que em todo conflito deve haver a possibilidade de represália. Você precisa demonstrar, de forma crível, sua capacidade de reagir. Esse é um elemento integrante. Você não pode abrir mão dessa capacidade crível de reagir."

Cinco dias depois do ataque, a Estônia deu um passo ousado: nomeou publicamente, e envergonhou, a poderosa vizinha Rússia como culpada. O ministro das Relações Exteriores da Estônia à

época, Urmas Paet, disse que seu país tinha evidências eletrônicas que levavam até o Kremlin.

"Descobriu-se que os ataques cibernéticos terroristas contra os sites de instituições governamentais da Estônia e do Gabinete do Presidente foram feitos de endereços de IP de computadores e indivíduos concretos de órgãos governamentais russos, incluindo a administração do presidente da Federação Russa", disse Paet, ministro das Relações Exteriores, em um comunicado oficial divulgado em 1º de maio de 2007.[3]

Paet considerou o ciberataque um atentado, e não apenas à Estônia, mas a toda a Europa.

"Consideramos que a União Europeia está sob ataque da Rússia, porque ela está atacando a Estônia", continuou Paet. "Os ataques são psicológicos, virtuais e reais."

Psicológicos, virtuais e reais. As palavras de Paet eram uma descrição poderosa da Guerra nas Sombras em ação. A experiência da Estônia assombrou e mobilizou os planejadores militares da Estônia para defendê-la de ataques semelhantes no futuro, e para alertar seus aliados da OTAN, incluindo os EUA, sobre o que provavelmente aconteceria em seguida.

O foco da Estônia continuou na defesa e recuperação. No *Postimees*, Jaanus Lillenberg e seus colegas lançaram uma pequena, porém ágil, retaguarda cibernética. Com as redes de e-mail fora do ar e antes do amplo uso das mensagens do Twitter e do Facebook, eles coordenaram sua estratégia por meio de mensagens de texto, começando com ferramentas cibernéticas simples.

"Primeiro de tudo, limitamos a quantidade de comentários que poderiam ser enviados de um endereço IP", lembrou ele. "Então

construímos em poucas horas esse sistema de filtragem muito rápido e inteligente."

O sistema que eles desenvolveram filtrou comentários que incluíam certas palavras-chave e frases que Lillenberg notou na enxurrada de comentários gerados por botnets, como "fascistas" e "SS". Os bots, como os trolls russos do Twitter de hoje, alimentavam teorias da conspiração, incluindo histórias falsas sobre o governo da Estônia planejar destruir o memorial de guerra soviético. Lillenberg e sua equipe estavam escrevendo o código para esses novos programas de filtragem em tempo real, enquanto seus sistemas estavam sob ataque. Foi uma operação feita a várias mãos.

"Tinha um cara", lembra Lillenberg, "um desenvolvedor de software, que estava gripado e me ligou às 3h da manhã para dizer: 'Sim, acho que consegui fazer funcionar'".

Seu sistema reduziu enormemente o tráfego online.

"Aquele último sistema foi arrasador", disse-me Lillenberg com um sorriso.

Lillenberg e sua equipe desenvolveram outra ferramenta para confundir os bots. Julgando — corretamente — que o ataque fora arquitetado por falantes de russo, em vez de falantes nativos de estoniano, ele teve uma ideia: aplicar um teste simples para os visitantes dos sites.

"Não queríamos usar um que fosse público, porque eles saberiam as formas de contorná-lo", explicou ele. "Então escrevemos outro que era muito, muito estúpido, mas não era algo que se encontrava na internet."

"Você tem três ícones", disse ele. "Vamos dizer, tesoura, relógio e avião. E há uma ordem em estoniano: 'Clique no avião.' Se o

visitante — ou o bot, na verdade — não entender estoniano, vai se perguntar o que fazer com esses ícones."

Não foi bem como a antiga instalação militar secreta de Bletchley Park quebrando o código Enigma. No entanto, sua correção simples funcionou, pressagiando o tipo de correção que os especialistas em cibersegurança implementariam para derrotar ataques DDoS semelhantes nos meses e anos que se seguiram.

"Demorou um pouco. Eu diria de 48 a 50 horas de trabalho para que conseguíssemos controlá-lo", disse ele. "Nós resolvemos as coisas, colocamos os caras para trabalhar e esperamos os resultados."

O reparo de Lillenberg foi uma pequena vitória em uma pequena batalha em um longo ataque cibernético. Os ataques de baixa tecnologia e alto impacto continuaram por semanas. Por fim, os líderes da Estônia chagaram a uma opção punitiva para impedi-los: bloquear todo o tráfego internacional na web, desconectando temporariamente do resto do mundo um dos países, até então, mais conectados.

"Ninguém do mundo exterior conseguiria obter nenhuma informação da Estônia. Acho que esse também era o objetivo do ataque", disse Jaanus Lillenberg. "Se você tem uma área fechada, na qual as informações não entram nem saem, pode fazer muitas coisas por lá. Operações militares, operações de informação..."

Olhando para trás, o ataque cibernético da Rússia à Estônia em 2007 incorporou elementos que caracterizariam ataques semelhantes, nos anos que se seguiram, aos ex-Estados soviéticos, como a Geórgia, e — mais tarde — a nações ocidentais, incluindo os Estados Unidos.

Primeiro, a Rússia empregou armas cibernéticas expansivas, mas relativamente simples, para ataques DDoS projetados para sobrecarregar as redes e tirá-las do ar. A proporção era sem precedentes: sequestrar milhares de computadores em mais de cem países. No entanto, as ferramentas estavam longe de ser sofisticadas.

Além disso, mesmo que a Rússia não declarasse guerra, era fácil identificar sua mão no ataque. Por um lado, a parte cibernética da investida coincidiu com a ação física em terra, no caso, protestos pró-russos, que as autoridades estonianas acreditavam ter sido coordenados com a ajuda de autoridades russas. E, apesar de os botnets operarem a partir de dezenas de países, foram marcados por impressões digitais eletrônicas, incluindo ligações com endereços de IP russos e código escrito em russo.

Mais amplamente, a Rússia estava revelando uma parte essencial de seu grande plano na Guerra nas Sombras: minar o Ocidente, enfraquecendo a confiança no sistema ocidental como um todo.

"A Rússia tem os próprios interesses estratégicos, que são — e que eles assim o definem — diametralmente opostos à visão estratégica da aliança ocidental", disse Mikser. "Portanto, eles vêm usando maneiras diferentes de dividir o Ocidente, criar conflito e, basicamente, minar a confiança das sociedades e das pessoas nos processos democráticos."

Hoje, mais de uma década depois, 2007 continua sendo um momento decisivo para a Estônia e seus líderes. Assim como os ataques do 11 de Setembro transformaram a abordagem da comunidade de inteligência dos EUA em relação ao terrorismo, o ataque cibernético sem precedentes da Rússia gerou uma forte reflexão sobre as vulnerabilidades cibernéticas da Estônia e de como atenuá-las.

"Foi a primeira vez na história em que alguém empreendeu [um ataque desse tipo]", disse-me Kersti Kaljulaid, presidente da Estônia. "E foi possível porque a Estônia é um Estado digital. Você não poderia atacar nenhum outro Estado dessa maneira, nesse ponto. Então foi um momento histórico, sem dúvidas."

Com apenas 46 anos, Kaljulaid é a mais jovem presidente da Estônia. Pessoalmente e em público, a mãe de 4 filhos transmite a atitude sensata da Estônia ao enfrentar o vizinho muito maior e cada vez mais agressivo. Como muitos oficiais e cidadãos da Estônia que conheci, ela não expressa nenhum medo, apenas um senso de propósito e convicção. Esse senso de propósito é latente nas inúmeras medidas e investimentos que a Estônia fez desde 2007 para se defender. O país se tornou uma espécie de "cyber Beirute" — perpetuamente cercada pela Guerra nas Sombras e sob a ameaça de ser engolida por ela, mas, ainda assim, consegue sobreviver e até mesmo prosperar.

Ataques de negação de serviço, como o que paralisou o país em 2007, são agora comuns, mas as defesas da Estônia os tornaram ineficazes.

Ataques DDoS, me disse a presidente Kaljulaid com confiança, tornaram-se "garoa". "Ninguém nem percebe as gotas caindo em nossos sistemas", acrescentou.

Claro, dez anos é uma vida em termos de tecnologia. Rússia, China, Coreia do Norte e outros atores cibernéticos adaptaram e aprimoraram suas capacidades cibernéticas. E, com esses recursos avançados, ocorreram ataques cibernéticos ainda mais agressivos.

"Isso mostra como a tecnologia e as defesas se desenvolveram, mas também o quanto essas ações agressivas [se tornaram] mais ativas na esfera da internet", disse ela.

E, no entanto, à medida que a sofisticação dos ataques cibernéticos avançou, o mesmo aconteceu com sua capacidade de se defender deles. Seu registro fala por si. A situação da Estônia é atípica, por ela não ter sofrido grandes perdas em dois dos ataques cibernéticos mais prejudiciais dos últimos anos: o ataque ransomware de 2017, "WannaCry", que os EUA atribuíram à Coreia do Norte, e um ataque global à infraestrutura de rede em 2018, pelo qual culparam a Rússia.

"Na verdade, eles não causaram danos à Estônia porque nossos profissionais são melhores em higiene cibernética do que os de qualquer outro lugar. Eles sabem manter a segurança na esfera digital", disse Kaljulaid. "Na verdade, acredito que estamos vendo menos atividades cibernéticas obstrutivas, porque a sociedade estoniana está no nível mais alto de higiene cibernética, então somos mais difíceis de atacar."

Notavelmente, Kaljulaid disse que a Rússia encontrou as defesas cibernéticas da Estônia tão impenetráveis que nem está mais tentando.

"Estamos nos preparando... para evitar esses ataques. E, adivinhe, não sofremos um sequer há tempos", disse ela.

Seu sucesso, enfatizam os líderes estonianos, não seria possível sem uma consciência nacional da ameaça nem sem um esforço nacional para se defender dela.

"Você tem a responsabilidade nacional de explicar às pessoas que elas precisam assumir sua responsabilidade individual", enfatizou Kaljulaid. "Na realidade, a tecnologia nunca as protegerá."

Todas as autoridades da Estônia demonstram a sabedoria e a necessidade da "higiene cibernética". Uma ironia dos ataques

cibernéticos mais prejudiciais da última década, incluindo a interferência da Rússia nas eleições de 2016, é que eles usaram ferramentas relativamente simples, que exigem erros simples do usuário. Os ataques de phishing, como o bem-sucedido da campanha de Hillary Clinton, exigiram que o presidente de campanha clicasse em um link. Os estonianos são treinados — intimidados, até — a nunca cometer o mesmo erro.

"Higiene cibernética, higiene cibernética e higiene cibernética", repetiu a presidente Kaljulaid. "Nós ensinamos nosso povo. É essencial."

Sua educação cibernética começa nas escolas, com a chamada política da web, que educa as crianças para evitar agentes desconhecidos na internet com a mesma cautela relativa a um estranho no parquinho. Como Kaljulaid disse, a tecnologia não pode proteger as pessoas contra as ameaças cibernéticas. As pessoas precisam aprender a se proteger.

O sucesso da Estônia é notável, considerando quantas atividades os estonianos fazem online, desde receber pagamentos de apoio público até serviços bancários e eleições. Mesmo com a subsequente interferência da Rússia nas eleições em toda a Europa e nos Estados Unidos, a Estônia nunca desistiu de seu sistema de votação online. As apostas não podem ser maiores. Uma violação cibernética minaria a confiança nas eleições e no sistema financeiro da Estônia. Como resultado, as assinaturas digitais são norma para todos os tipos de transações online.

"Nosso povo sabe que, se algo não for assinado digitalmente, não é seguro", disse Kaljulaid. "Se alguém assinou digitalmente algo com a identidade digital e lhe enviou as informações, você pode ter certeza de que é seguro e de que foi criptografado no momento da

assinatura. A internet segura existe. Todo o resto, nosso povo sabe, é perigoso."

Contudo, o governo da Estônia não deposita toda sua fé na vigilância dos civis. A Estônia está tomando medidas agressivas não apenas para evitar futuros ataques, mas para assegurar que eventuais ataques não consigam paralisar o país, como a Rússia fez em 2007. Uma dessas medidas é o estabelecimento das chamadas embaixadas de dados.

Uma embaixada de dados é uma coleção fortemente protegida de servidores localizados fora do país, com uma cópia de segurança digital gigante de todos os dados e comunicações do governo, dados de eleitores e registros financeiros e de saúde. A ideia é ter essa cópia para que a Estônia possa acessá-la no caso de um ciberataque incapacitante. Ao anunciar seus planos, em junho de 2017, o governo disse, esperançosamente, que "seu projeto piloto poderia, novamente, dar um exemplo ao resto do mundo".[4] A Estônia abriu sua primeira embaixada de dados, em Luxemburgo, em 2018.

"Ela goza de todos os direitos, segundo o acordo bilateral entre a Estônia e o outro país em que a embaixada está", explicou a presidente Kaljulaid. "Assim, como qualquer embaixada, ela é tecnicamente nosso território; só nós podemos entrar e conceder permissão para entrarem."

As empresas do setor privado da Estônia também estão buscando ajuda externa.

As agências de notícias, por exemplo, contrataram parceiros estrangeiros para resguardar imagens espelhadas de sites de notícias da Estônia em servidores fora do país. A Rádio Pública da

Estônia é uma delas, embora, por motivos de segurança, não divulgue em quais países as cópias de segurança estão.

"Não posso dizer os lugares, mas temos boas casas de mídia, que agora têm espelhos geográficos de nossos sites de notícias", disse Lillenberg, que agora trabalha para a Rádio Pública da Estônia.

Lillenberg, agora um veterano grisalho do ciberataque de 2007, descreve esses postos avançados digitais em termos militares.

"Então, se eles disparam um novo míssil de cruzeiro e atingem o prédio de notícias, nada acontece, porque outro prédio, em outra localização geográfica, está em pleno funcionamento", disse ele.

No atual conflito cibernético com a Rússia, o setor privado da Estônia está na linha de frente. Na verdade, o governo da Estônia depende de empresas privadas como soldados cidadãos.

"Outra coisa que aprendemos foi que, na verdade, grande parte do conhecimento necessário para lidar com essas ameaças está no setor privado", disse o ex-ministro da Defesa, Aaviksoo. "E é importante que a cooperação entre o governo e o setor privado seja boa."

Para destacar essa parceria e o papel essencial dos cidadãos estonianos na defesa cibernética, a Estônia se destacou na "Unidade Cibernética" da Liga de Defesa da Estônia, composta de voluntários especialistas em tecnologia da informação e com habilidades de segurança cibernética, além de especialização em direito, economia e muito mais, que treinam regularmente para ajudar a combater um ciberataque incapacitante em caso de crise. A unidade também propiciou que o governo recorresse a talentos do setor privado a que nunca se associaria em tempo integral.[5]

A Liga de Defesa da Estônia é uma milícia voluntária que foi fundada em 1918 e restabelecida com a independência da Estônia

após o colapso da União Soviética, em 1991. Os estonianos dizem que a Liga foi inspirada nos Minutemen da Guerra de Independência dos Estados Unidos. E, hoje, as unidades de milícias armadas da Liga treinam regularmente para evitar um ataque convencional. Os membros da Unidade Cibernética são os Minutemen do campo de batalha cibernético, operando como uma unidade de reserva de voluntários do setor privado que aguarda a convocação para defender o território cibernético. Os aliados da Estônia na OTAN têm estudado a Unidade Cibernética como um modelo para os próprios países.[6]

Apesar do sucesso em sobreviver em 2007, os líderes estonianos enfatizam que a Guerra nas Sombras extrapola o ciberespaço. E os ataques da Rússia se dão também por outros meios, dos quais é mais difícil se defender, particularmente operações de informação, como ataques a eleições ocidentais.

"Isso é muito mais perigoso do que no ciberespaço convencional, porque, nele, os problemas se resolvem com sistemas técnicos e boa higiene cibernética", disse-me a presidente Kaljulaid. "Temos que nos esforçar — temos que explicar ao nosso pessoal qual é o X da questão."

"Os cenários híbridos estão em voga após a anexação da Crimeia e a agressão à Ucrânia Oriental", disse Mikser. "Na verdade, vivemos esse tipo de pressão híbrida desde que recuperamos nossa independência."

"Sempre houve uma combinação de pressão política, guerra psicológica, se entendermos assim, medidas econômicas sendo aplicadas e tentativas de interferir em nossos assuntos políticos internos", disse ele.

Em meio à Guerra nas Sombras, Kaljulaid diz que o Ocidente deve olhar para os ataques da Rússia como um todo, não isolados — e combatê-los como um todo.

"Todas as ações russas, cibernéticas ou físicas, começaram com a ocupação de parte da Geórgia, passando para a Ucrânia, então testando nossas defesas cibernéticas e atacando democracias", disse ela. "Tudo isso é elemento e sinal da tentativa de virar a mesa do nosso [sistema] baseado em regras. Precisamos entendê-lo de maneira holística, como um processo conectado."

Essa abordagem requer unidade entre os aliados ocidentais e uma disposição para identificar e punir o comportamento russo. Como um exemplo poderoso, Kaljulaid citou o momento em que o presidente francês Emmanuel Macron confrontou o presidente russo Vladimir Putin na escadaria do Palácio do Eliseu, em Paris, sobre a interferência russa nas eleições presidenciais da França.

"Você vê o presidente Macron ao lado do presidente Putin dizendo: 'Você fez isso com nossa eleição democrática'", lembrou ela. "Isso as pessoas veem. São coisas grandes o suficiente para chamar a atenção."

Mesmo com tais avisos, a Rússia realizou ataques ainda mais agressivos contra o Ocidente, abrindo novas frentes na Guerra nas Sombras. Muitos diplomatas e oficiais europeus reagiram com particular alarme ao envenenamento promovido pela Rússia ao ex-espião russo Sergei Skripal e a sua filha, Yulia, nas ruas de Salisbury, Inglaterra, em março de 2018. A arma, que a polícia acreditava estar lambuzada na maçaneta do apartamento de Skripals, era o agente nervoso russo Novichok. Três meses depois, um casal britânico, Dawn Sturgess e Charlie Rowley, que não tinha parentesco com os Skripals, foi envenenado com o mesmo agente

nervoso, segundo a polícia, depois de manusear um contêiner contaminado. Mais tarde, Sturgess também faleceu.

"Essas foram ações físicas no território de um país da OTAN sem precedentes em sua história", disse-me Kaljulaid. "Minha pergunta é: qual será o próximo? Precisamos sempre pensar nisso. E estar prontos."

LIÇÕES

O ataque cibernético da Rússia contra a Estônia em 2007 proporcionou duas lições importantes para os Estados Unidos, especificamente, e para o Ocidente, como um todo. Primeiro, mostrou que até mesmo uma arma cibernética apenas relativamente contundente pode paralisar uma nação inteira. O "ataque distribuído de negação de serviço", ou DDoS, da Rússia à Estônia demandou custos e complicações mínimas, e é uma tática que pode ser facilmente replicada e implementada por uma série de agentes estatais e não estatais menores. Segundo, o ataque de 2007 mostrou que a Rússia estava disposta a lançar armas cibernéticas contra nações ocidentais com a intenção de perturbá-las e arrasá-las em larga escala, o que, até certo ponto, nunca tinha sido feito. Junto a uma elaborada operação de influência em terra, sob a forma de protestos orquestrados e disseminação de informações falsas, a Rússia criou pânico e divisão em um adversário estrangeiro, um indício inicial da campanha de ruptura que mais tarde lançaria contra a Europa Ocidental e os Estados Unidos.

Os Estados Unidos e seus aliados ocidentais, em grande parte, não perceberam essas lições em 2007 e, portanto, deixaram passar sinais do que estava por vir na década que se seguiu. Esse padrão

de alertas perdidos continuaria, mesmo com esses avisos se tornando mais claros e ameaçadores. Por toda parte, os líderes e formuladores de políticas do Ocidente insistiram em sua visão errônea de que os líderes russos queriam, em grande medida, o mesmo que o Ocidente: um relacionamento amistoso governado pela ordem internacional, baseado em regras criadas e definidas pelo Ocidente. Isso incluiu a adesão a tratados destinados a minimizar o perigo de confrontos militares e a instaurar a cooperação militar. Essa expectativa equivocada se sedimentou como senso comum a respeito da Rússia. Porém os eventos que se seguiram mostraram o quanto essa perspectiva era ilusória.

---

1 Estonian Public Radio ("ERR"), 25 de abril de 2017.

2 North Atlantic Treaty Organization, official text, The North Atlantic Treaty, 4 de abril de 1949.

3 Statement by the foreign minister Urmas Paet, *Eesti Paevaleht* (newspaper), 1º de maio de 2007.

4 e-Estonia, Government of Estonia, junho de 2017.

5 Estonian Defence League ("Kaitseliit").

6 Ibid.

CAPÍTULO 3

Segredos Roubados

(CHINA)

Para seus amigos e contatos norte-americanos, Stephen Su era um homem de negócios afável e um sujeito sociável.

"As pessoas gostavam dele", disse-me Bob Anderson, ex-chefe de contrainteligência do FBI. "Elas não o achavam um otário. E, sei que parece estúpido, mas sabe como as pessoas são, e foi assim que tudo começou."

Stephen Su, que também usava o nome chinês, Su Bin, morava em sua China natal, mas viajava com frequência para os EUA e para o Canadá, para fazer negócios nos setores de aviação e aeroespacial. Sua empresa, a Lode-Tech, era uma pequena participante em um campo de gigantes. Ele se concentrava na fabricação de chicotes de cabos para aeronaves, um produto seguro na extremidade de baixa tecnologia do setor de aeronaves militares. No entanto, em cerca de cinco anos, de 2009 a 2014, Su teceu uma rede de contatos comerciais próximos dentro das contratantes da defesa norte-americana e canadense, com alguns dos contratos militares mais sigilosos dos EUA. Como Anderson explicou, Su fez questão de conhecer as pessoas que tinham acesso

a essas tecnologias, ou que conheciam quem tivesse, e "fazer com que confiassem nele".

Seus contatos o descreviam como o sócio ideal, que buscava fechar acordos que beneficiassem todos os envolvidos. Ele era muito focado em negócios, mas também era uma boa companhia. Ao longo dos anos, desfrutou de incontáveis jantares caros regados a vinho nos melhores restaurantes de Seattle, Vancouver e Los Angeles.

"Ele era muito cativante", lembrou Anderson. "Mal conhecia alguém e já dizia: 'Em que você trabalha? O que tem feito? Rapaz, isso é muito interessante.' Então, em muitos desses casos, ele falava: 'Bem, você sabe, tem uma ótima maneira de ganhar dinheiro com isso' ou 'Podíamos fechar uma ótima parceria. Conheço muita gente que se interessaria por informações como essa'".

As informações que, de fato, interessavam a Su se relacionavam a três das mais avançadas aeronaves militares dos EUA já construídas: os caças "invisíveis" Lockheed Martin F-35 e F-22, e a aeronave de transporte Boeing C-17 Globemaster. Embora fossem produtos de dois dos maiores empreiteiros militares do Pentágono, cada um precisou de milhares de componentes de dezenas de fornecedores menores. Essa cadeia de suprimentos dava a Su informações sobre incontáveis envolvidos — bem como uma explicação conveniente para eventuais sócios que se preocupassem com o tipo de informação que Su procurava.

"Su diria algo como: 'Não estou pedindo para você me fornecer o F-35, mas qual é o problema de eu conseguir um sistema para vendê-lo a um amigo ou possível cliente?'", disse Anderson. "E assim ia."

Seus contatos não sabiam, mas Su não trabalhava sozinho. Na verdade, ele fazia parte de uma equipe transnacional de três pessoas: ele agia na América do Norte, e seus dois parceiros — identificados na queixa criminal do FBI, em 2014, apenas como "coconspirador não encarregado 1" e "coconspirador não encarregado 2"—, na China continental. De acordo com o FBI, Su identificava arquivos de valor inestimável nos computadores das empresas-alvo, então os transmitia para os parceiros na China, que invadiam os sistemas dessas empresas-alvo para roubá-los. A equipe então vendia esses arquivos roubados para as partes interessadas da China, ou seja, empresas estatais do setor militar. Como a acusação criminal observou, eles não fizeram isso só a pedido do governo chinês, mas também "para seu lucro pessoal". A espionagem servia tanto ao país quanto a suas contas bancárias.[1]

Os e-mails que o FBI levantou mostraram que seu *modus operandi* era simples e eficiente. A equipe se reuniu pela primeira vez no verão de 2009, quando Su enviou os primeiros e-mails para os coconspiradores identificando possíveis alvos dentro dos EUA. Em um e-mail datado de 6 de agosto de 2009, Su anexou uma planilha do Excel protegida por senha com endereços de e-mail, números de telefone e posições de cerca de 80 engenheiros e outros funcionários que trabalhavam em um novo projeto militar. A espionagem de Su era de baixa tecnologia, até mesmo desajeitada. O assunto do e-mail de 6 de agosto era "My Cell Phone Number" ["Meu Número de Telefone], o que, o FBI descobriu mais tarde, indicava que a senha do arquivo protegido do Excel era o número de seu celular.[2]

Quatro meses depois, em 14 de dezembro de 2009, Su enviou um e-mail similar, dessa vez com o assunto "Target" [Alvo], listando os nomes e cargos de outros quatro executivos, incluindo o

presidente e os vice-presidentes de uma empresa que fabricava armas e sistemas de guerra eletrônicos para os militares dos EUA. Posteriormente, a análise do FBI determinou que as divisões identificadas nesses primeiros e-mails correspondiam a alvos que a equipe de Su hackeou.[3]

O próximo passo dos hackers se assemelhou aos métodos usados pelos hackers russos para invadir o Partido Democrata na eleição presidencial dos EUA de 2016. Eles enviaram os chamados e-mails de phishing para funcionários específicos da empresa-alvo, como explicou o FBI: "Para parecer que vieram de um colega ou contato comercial." Se o destinatário clicasse no link contido no e-mail ou abrisse o anexo, uma "conexão de saída" era estabelecida entre o computador da vítima e outro na China, sob controle dos hackers. Eles então instalavam malwares no computador da vítima, para que o controlassem remotamente e — o mais alarmante — explorassem toda a rede da empresa.[4]

Su e sua equipe tomavam medidas cuidadosas para esconder a origem da invasão cibernética. Para isso, a conexão de saída dos hackers da empresa-alvo era roteada por uma série de servidores em diversos países do mundo. Esses "hop points", como são conhecidos, obscureceriam quem eram os hackers e sua localização — se e quando fossem descobertos.

Como escreveram em um relatório interno de 2013, obtido pelo FBI, "para evitar complicações diplomáticas e legais, o trabalho de vigilância e a coleta de inteligência são feitos fora da China. A inteligência coletada é enviada primeiramente a um oficial da inteligência por um servidor temporário pré-ordenado, de fora da China, ou por um jump server, que fica em um terceiro país, antes de finalmente chegar às regiões/áreas circunvizinhas ou a uma estação de trabalho de Hong Kong ou Macau".[5]

A etapa final do roubo — ou seja, o último "salto" de volta para os clientes na China continental — não passava por nenhuma rede de computador. Su e seus parceiros montaram o que chamavam de "salas de máquinas" em Hong Kong e em Macau, onde a inteligência roubada seria coletada e depois levada para a China.

"A inteligência é sempre captada e transferida para a China pessoalmente", escreveram em um e-mail de 2013.[6]

Acontece que Su e seus parceiros tiveram acesso irrestrito à rede da Boeing por 3 anos antes que a invasão fosse descoberta. Durante o período, eles alegaram ter roubado cerca de 630 mil arquivos digitais — totalizando monstruosos 65 gigabits de dados — apenas do C-17. E roubaram dezenas de milhares de arquivos do F-22 e do F-35.[7]

Embora a equipe de Su Bin tenha tido um enorme sucesso, ela foi apenas uma pequena parte de um enorme exército de hackers chineses dedicados a roubar os segredos mais importantes do governo e do setor privado dos EUA. Nas últimas duas décadas, a China construiu uma enorme infraestrutura encarregada de espionagem cibernética. O Escritório do Representante de Comércio dos EUA (USTR) estima que o país tenha perdido até US$600 bilhões por ano em propriedade intelectual. Uma vez que considera a China "o principal detentor de IP do mundo", o USTR acredita que ela é responsável pela maior parte dessas perdas.

O roubo de segredos norte-americanos é uma das frentes mais insidiosas da Guerra nas Sombras: constante, profundamente prejudicial à segurança nacional e à vista de todos. Quando fui chefe da equipe da embaixada dos EUA em Pequim, as empresas norte-americanas — embora cientes do roubo — muitas vezes se

recusavam a pedir ajuda do governo, ou mesmo a identificar ciber-rupturas, por medo de alienar seus parceiros chineses ou perder o acesso ao mercado chinês. De fato, a estratégia da China depende desse medo — e o cultiva.

Um alto funcionário da lei dos EUA descreveu o aparato de espionagem da China como uma "tênia", alimentando dezenas de milhares de instituições e indivíduos dos EUA para extrair seu bem mais precioso: sua engenhosidade. O objetivo de Pequim é ultrapassar os Estados Unidos como superpotência mais poderosa e tecnologicamente mais avançada do mundo. Os líderes chineses preferem fazê-lo pacificamente, mas, se houver uma guerra, eles nivelarão o campo de batalha.

Isso não é simplesmente conjectura, mas se reflete na retórica dos mais altos níveis de liderança chinesa. O presidente Xi Jinping prevê a China na vanguarda da inovação até 2035 e, além disso, como a potência global líder até 2050. Objetivos nobres a serem concretizados, mas, para tal, a liderança demonstrou que será preciso implementar o leapfrogging — e até a espionagem cibernética — no caminho.

"Isso se resume à dominação mundial, e, se e quando houver um conflito — e, infelizmente, é provável que haja —, eles querem estar mano a mano, se não melhor que os EUA, e é para isso que estão se preparando nos últimos 30 ou 40 anos", explicou Anderson.

A espionagem cibernética parece uma frente branca e menos sangrenta da Guerra nas Sombras. Porém Anderson diz que os serviços de segurança chineses operam tão brutalmente no ciberespaço quanto em qualquer outro campo de batalha.

"Os chineses são até mais cruéis do que os russos", disse-me Anderson, parando para ter certeza de que eu estava ouvindo. "Eles vão matar pessoas num piscar de olhos. Vão matar famílias num piscar de olhos. Farão isso silenciosamente dentro da China ou em seus territórios, mas eles absolutamente o farão, se precisarem."

Bob Anderson foi parar na contrainteligência de aplicação da lei, onde "brutal" é acessório de fábrica. Ele começou como policial estadual de Delaware, fiscalizando crimes de motoristas imprudentes a traficantes de drogas ilícitas e homicídios. Entrou para o FBI em 1995, em um esquadrão antidrogas no sudeste de Washington, D.C., quando a capital tinha uma das maiores taxas de tráfico e consumo de drogas e crimes violentos do país.

"Comprávamos cocaína, crack, metanfetamina, heroína", lembra Anderson. "D.C. foi a capital do assassinato dos EUA na época."

Subindo na hierarquia, ele serviu em uma equipe da SWAT e de resgate de reféns, antes de ser promovido a supervisor da contrainteligência do FBI, em 2001. Sua experiência nas ruas foi um treinamento vital para lidar com a espionagem internacional. Agentes estrangeiros, lembra Anderson, eram tão violentos e perigosos quanto os traficantes que perseguia pelas ruas de Washington. Os russos eram implacáveis.

"Ah, merda! Eles odeiam sua coragem", disse Anderson. "Eles o odeiam porque você é norte-americano, e não é porque você é branco, negro, homem ou mulher. Eles o odeiam porque é norte-americano."

Anderson me contou que certa vez se sentou com um alto funcionário do serviço de inteligência estrangeira da Rússia (SVR)

para uma troca de espiões. Foi a primeira vez que o diretor assistente de contrainteligência do FBI se sentou com o inimigo russo em solo norte-americano.

"Ele trouxe dois secretários — obviamente, dois caras gigantes da GRU [agência de inteligência militar da Rússia] — que estavam de terno, prontos para quebrar o pescoço de qualquer pessoa no restaurante a que fomos", disse ele. "Foi uma cena saída de um romance policial."

O funcionário russo, de 72 anos, sentado a sua frente para a troca, era, como Putin, um veterano da antiga KGB.

"Esse cara provavelmente matou a maior parte do próprio pessoal e estava me encarando do outro lado da mesa sem dar a mínima para o fato de eu ser um agente do FBI", disse-me Anderson. "Ele simplesmente me odiava por eu ser norte-americano."

O ódio continua sendo uma constante, mas, em seu posto na contrainteligência, ele observou como a própria natureza da espionagem mudou, sobrecarregada pelo advento e pela expansão das ferramentas cibernéticas.

"Eu estava prendendo um monte de espiões e comecei a perceber uma mudança em seu padrão de ação", disse Anderson. "Em vez das tradicionais quedas de uma ponte, tudo estava em um pen drive. Tudo estava na nuvem, e, nessa época, as pessoas nem sabiam de que porra eu estava falando."

Anderson conta suas histórias de espionagem com a indiferença de um policial veterano e com um toque de bravura. Para ele, um traficante de drogas ilícitas de Washington, D.C., compartilha mais do que você imagina com um ladrão cibernético da China. Ambos estão dispostos a mentir, enganar, lutar e até mesmo matar para

conseguir o que querem. Com suas credenciais de rua, Anderson se viu como o principal investigador do que viria a ser um dos ataques cibernéticos mais devastadores nos Estados Unidos, incluindo a violação extensiva da NSA, por Edward Snowden; o hack da Coreia do Norte na Sony Pictures; e a penetração da China no Escritório de Administração de Pessoal dos EUA, que exporia as informações pessoais de milhões de funcionários do governo que detinham, ou mantinham, autorizações de segurança (inclusive minhas, fui descobrir depois).

"Eram 600 pessoas de 123 países", disse Anderson. "E, quando você começa a ver essa merda, começa — pelo menos eu — a entender tudo de uma perspectiva criminosa; como cartéis, eles usam dinheiro, mas agora é a moeda virtual. E eles podem lavá-la, sei lá, em 50 países em uma hora. Quero dizer, como acompanhar isso?"

O número exato de espiões como Stephen Su é difícil de definir, mas Anderson estima que, a qualquer momento, existirão dezenas de equipes como a dele agindo nos Estados Unidos. E atrás deles, na China, diz Anderson, há muito mais hackers trabalhando; alguns, em tempo integral, pelos serviços de segurança chineses; outros, em regime de meio período. Entenda esse sistema como um programa cibernético de "serviço nacional" para jovens chineses de alto nível.

"Você iria para a cadeia aqui, mas os chineses têm milhares de jovens — como os melhores do MIT ou de Stanford — contra os EUA", diz Anderson. "Eles recebem para fazer isso, é uma rotina para eles."

"E são muito calculistas no que fazem, têm requisitos, como a comunidade de inteligência dos EUA tem exigências", disse Anderson.

Também são extremamente ambiciosos em seus objetivos. Em um e-mail de 2011, a equipe de Su afirmou com um floreio que as informações que estava roubando "nos permitiriam alcançar rapidamente os níveis dos EUA [...] usando seu conhecimento para superá-los".[8]

Em busca de seu objetivo grandioso, Su e seus coconspiradores mantiveram registros meticulosos — ansiosos para provar sua utilidade aos clientes do governo chinês e para melhorar seus resultados. E, assim, com uma série de autoavaliações brilhantes em e-mails, teceram um relato exaustivo de seus crimes. Eles eram defensores ferrenhos de seus arquivos roubados. Afinal, sua missão não era apenas roubar informações confidenciais, mas vendê-las pelo maior preço possível. Para isso, enviavam por e-mail atualizações regulares de seu trabalho — atualizações que pareciam propagandas, cheias de elogios e floreios.

Em 7 de julho de 2011, cerca de um ano após a infiltração na segura rede da Boeing, o "coconspirador 1 não declarado" de Su Bin enviou um relatório a seu supervisor, o "coconspirador 2 não declarado", intitulado "Past Achievements" [Conquistas Passadas], que incluiu uma longa lista de materiais roubados de empresas de defesa dos EUA. Eles alegaram ter ganhado o controle dos servidores de um contratado e roubado 20 gigabytes de dados tecnológicos. Além de roubar arquivos relacionados às aeronaves C-17 e F-22 e F-35, eles se gabaram de realizar "reconhecimento" em arquivos relacionados a um veículo aéreo não tripulado (UAV) fabricado nos EUA.

"Coletamos uma grande quantidade de informações e caixas de e-mail do pessoal relevante", estava no e-mail de 7 de julho. "Também obtivemos a senha para o sistema de gerenciamento de clientes do fornecedor e controlamos as informações dos clientes dessa empresa."

Outras "conquistas passadas" incluíam alvos fora dos EUA. "Por meio de reconhecimento e infiltração de longo prazo, asseguramos a autoridade para controlar o site do [...] míssil desenvolvido em conjunto pela Índia e pela Rússia", escreveu um dos coconspiradores chineses de Su. Ele citou a tecnologia militar roubada de Taiwan e informações políticas roubadas do "Movimento Democracia" e do "Movimento da Independência Tibetana", dentro da China. Eles se concentravam em todas as informações que acreditavam que o governo chinês gostaria de saber — e que estariam dispostos a pagar para ter.[9]

Contudo, os EUA foram, de longe, seu principal alvo. Em 27 de fevereiro de 2012, um dos coconspiradores enviou um e-mail com o assunto "Complete Listing" [Listagem Completa]. Um anexo documentou cerca de 32 projetos militares dos EUA alvejados, com a quantidade de dados tecnológicos que alegavam ter roubado de cada um deles.

Segundo a acusação criminal do FBI de 2014, ao lado de "F-22", estava "220M", indicando 220 megabytes de dados. Os números ao lado dos outros 31 projetos visados foram seguidos por um "G", que um especialista do FBI concluiu se referir a gigabytes de dados. Um gigabyte equivale a 1.000 megabytes, o equivalente a cerca de 5 mil livros.[10]

Foi uma extraordinária coleção de informações sobre alguns dos projetos militares mais avançados e sigilosos dos EUA. Mais tarde, a análise do FBI confirmou que os diretórios de arquivos, esquemas