A Huawei na história: grandes potências e risco de telecomunicações, 1840-2021

Rush Doshi e Kevin McGuiness

Brookings Institution, março de 2021

Resumo executivo

No fim de 2018, enquanto os EUA se perguntavam se o Canadá receberia a Huawei nas suas redes de telecomunicações, o primeiro-ministro canadense Justin Trudeau fez uma série de declarações que resumiram a sabedoria popular de grande parte do mundo. "Essa não deveria ser uma decisão política", ele declarou na época, e o Canadá não "deixaria a política se envolver nas decisões" sobre o papel da Huawei na sua rede.[1]

A noção de que as potências poderiam deixar a política de fora das questões sobre telecomunicações não era apenas otimista, mas também estava em descompasso com a história das telecomunicações. Este relatório explora essa história e mostra como as potências e as telecomunicações estão quase sempre estreitamente conectadas. Quando os Estados ignoravam essas conexões e eram mais indiferentes à segurança das suas redes, os resultados não eram vantajosos e, às vezes, eram até desastrosos.

Este relatório examina vários casos importantes de concorrência entre grandes potências na área de telecomunicações, que remontam ao início mais precoce das telecomunicações elétricas, na década de 1840. Esses casos demonstram que muitas das perguntas que os legisladores enfrentam hoje têm análogos próximos no passado. Embora o presente debate sobre segurança da rede e infraestrutura do 5G possa parecer novo, na verdade, ele ecoa discussões já esquecidas, que datam do início das telecomunicações elétricas, há cerca de 150 anos. Além disso, muitos dos elementos familiares atuais da concorrência no setor das telecomunicações, como a utilização de agências normativas, subsídios estatais, distribuição de cabeamento, guerra da informação, mercados em países em desenvolvimento e criptografia para obter vantagens, foram desenvolvidos há mais de um século, com lições importantes para os debates atuais.

Fornecemos abaixo uma lista dessas lições principais:

1. **O controle sobre as redes de telecomunicações globais é uma forma de poder político.** Espera-se que as redes de 5G formem a base de uma economia conectada e mais inteligente, conectando inúmeros dispositivos e sensores. Ávida para construir essas redes em todo o mundo, a China subsidiou suas principais empresas e projetos de 5G em todo o mundo como parte da iniciativa "Digital Silk Road" (ou Rota da Seda Digital). Esse esforço é análogo à busca, pela Grã-Bretanha, de um domínio de rede no início da telegrafia elétrica. A Grã-Bretanha construiu sua vantagem ao longo de seis décadas aumentando constantemente a dependência de outros países pelas redes britânicas, chegando até mesmo a abster-se de taxas e benefícios econômicos para convencê-los a passar os cabos pela Grã-Bretanha, ao mesmo tempo em que reduziu a dependência de

redes estrangeiras por parte da Grã-Bretanha. O resultado foi que a Grã-Bretanha acabou controlando mais da metade do tráfego de cabos no mundo, a maior rede de rádio e a maior frota de navios de cabeamento. A "hegemonia da informação" da Grã-Bretanha permitiu que ela isolasse a Alemanha de praticamente todas as telecomunicações globais na primeira Guerra Mundial, forçando Berlim a encaminhar o tráfego por meio das linhas de propriedade britânica suscetíveis ao controle britânico, o que mais tarde se mostrou decisivo na derrota da Alemanha nesse conflito.

2. **Longos períodos de paz e prosperidade geralmente resultam em negligência quanto aos riscos de telecomunicação.** Nos últimos 30 anos, a paz no período pós-Guerra Fria e a globalização econômica coincidiram com o rápido progresso das telecomunicações, o que levou os países a priorizar benefícios comerciais revolucionários em relação aos riscos políticos e de segurança, incluindo até mesmo a propriedade ou o funcionamento das redes por entidades estrangeiras. Um desenvolvimento semelhante ocorreu nos primórdios das telecomunicações, na década de 1840, que coincidiu também com um período de relativa paz e globalização que continuou até a primeira Guerra Mundial. Durante grande parte dessa era, o desejo de captar o potencial comercial aparentemente milagroso de novas tecnologias de comunicações obscureceu questões relacionadas à dependência de redes ou empresas estrangeiras. A Grã-Bretanha aproveitou a tranquilidade de outros, construindo e depois explorando uma posição nodal inatacável nas redes globais, com a maioria das outras grandes potências dependentes das redes britânicas.

3. **Quando os Estados são negligentes quanto à segurança de suas telecomunicações, os resultados, além de desastrosos, podem remodelar a política mundial.** Décadas de negligência da Alemanha quanto à dependência alemã das linhas de telecomunicações britânicas significaram que, quando Berlim despertou para os riscos dessa dependência, já era demasiado tarde para mudar. Quando a Primeira Guerra Mundial foi deflagrada, a Grã-Bretanha cortou todos os cabos da Alemanha e forçou Berlim a rotear o tráfego por meio das redes britânicas, apesar do risco de intercepção, o que levou à descoberta do "telegrama Zimmerman", que ajudou a fazer com que os Estados Unidos entrassem na guerra. Da mesma forma, a indisciplina russa envolvendo transmissões de rádio sem fio na Primeira Guerra Mundial permitiu que os alemães interceptassem as comunicações, "vissem" o movimento das tropas da Rússia em tempo real e impingissem a elas uma derrota decisiva na Batalha de Tannenberg. Posteriormente, na segunda Guerra Mundial, a exacerbada confiança nazista nos códigos alemães levou a esforços mínimos para atualizá-los, permitindo que a Grã-Bretanha os quebrasse e obtivesse informações de inteligência. Acredita-se que isso encurtou a guerra entre dois e quatro anos. Considerando o poder da informação, mesmo os ataques ocasionais de indisciplina ou negligência da intercepção de sinais podem alterar a história.

4. **Novas tecnologias sempre vêm acompanhadas de novos esforços de interceptação.** O surgimento de cabos subaquáticos veio acompanhado de esforços para cortar e desviar essas linhas já na Guerra Hispano-Americana. Com a transmissão de rádio vieram os esforços de rivais para capturar nós de rede e interceptar transmissões. O surgimento de códigos sofisticados de criptografia resultou em esforços de escala industrial para quebrá-

los. Ao longo do tempo, houve quem acreditasse que um novo salto nas comunicações poderia ser menos vulnerável do que aqueles que o precederam. Porém, todas as vezes, o ciclo de inovação e exploração não foi interrompido.

5. **As redes de telecomunicação nunca foram politicamente neutras, especialmente em tempos de tensão.** Em 2019, executivos da Huawei se comprometeram com um compromisso do tipo "sem porta dos fundos, sem espionagem" e prometeram que a empresa permaneceria fora da política, com o governo da China se comprometendo a respeitar este compromisso. No entanto, há mais de um século, as empresas de telecomunicação e seus governos anfitriões fizeram promessas semelhantes em público ao mesmo tempo em que as rompiam secretamente e trabalhavam juntas tanto em tempos de paz quanto de guerra. Por exemplo, a dominação britânica dos cabos submarinos levou franceses, alemães e americanos a defender que as linhas deveriam permanecer neutras, mesmo durante guerras. As empresas britânicas declararam publicamente sua neutralidade, mas, na realidade, submeteram-se aos interesses políticos britânicos, especialmente em momentos de grande tensão, e desistiram inteiramente da neutralidade durante os períodos de guerra. Com frequência, o poder que surge da interrupção ou da interceptação de fluxos de informações tem sido atraente o suficiente para permitir que reivindicações sinceras de neutralidade perdurem.

6. **Os países geralmente buscam desenvolver suas próprias empresas campeãs da área de telecomunicações assim que reconhecem a vulnerabilidade de se depender de empresas concorrentes ou adversárias.** Atualmente, os Estados Unidos carecem de um grande fabricante de estações de rádio base de 5G, o que tem levado a debates sobre se o país deve investir nas empresas domésticas ou depender de aliados. Eles também estimularam a discordância em relação ao grau em que a Huawei é, por si só, uma *champion* estatal *de facto*. Esses debates têm precedentes. No início do século XX, muitos Estados dependentes de outros no quesito "equipamentos ou redes de telecomunicações" começaram a construir seus próprios sistemas. A Alemanha, por exemplo, forçou a Siemens & Halske e a AEG – empresas domésticas com operações de rádio concorrentes – a se juntar para estabelecerem uma alternativa alemã ao domínio britânico no setor de radiotransmissão. Muitos outros países importantes apoiaram empresas que, embora ostensivamente privadas, estavam envolvidas com os governos que as apoiavam.

7. **A luta pelos padrões aplicáveis às telecomunicações, que geralmente requer a inclusão de aliados e parceiros, pode determinar quais Estados terão poder nas redes.** Países cuja tecnologia se torna o padrão dominante podem exercer essa influência sobre os outros. Dessa forma, a corrida atual por padrões na tecnologia de comunicação da informação é semelhante à corrida anglo-alemã por redes de rádio. A Grã-Bretanha, por meio da Marconi Company, empresa apoiada pelos britânicos, era tão dominante no setor de rádio sem fio que todas as outras grandes potências tinham que passar mensagens através da rede sem fio da Grã-Bretanha, que se recusava a se conectar a qualquer outra estação sem fio. Com o tempo, a Alemanha conseguiu quebrar essa dominância em um órgão normativo que proibia esta política de "não intercomunicação" com a ajuda de outras potências, incluindo os Estados Unidos e a França. Esta foi uma demonstração de

como abordagens de coalisão semelhantes podem ser usadas hoje pelos Estados liberais para definir ou preservar padrões favoráveis de tecnologia da informação e das comunicações (TIC) se trabalharem em conjunto.

8. **Os Estados se voltam à criptografia conforme a interceptação das suas comunicações fica mais fácil, mas, em geral, a criptografia tem limites devido a determinados adversários ou erro de usuário.** Alguns argumentam que a preocupação com o papel da Huawei nas redes ou a vulnerabilidade geral dos dispositivos conectados à Internet é atenuada pela criptografia moderna. Esse tipo de argumento vem de longa data. Há um século, quando as telecomunicações começaram a surgir, a possibilidade de que as mensagens de telégrafo podiam ser lidas por outros que controlavam os nós da rede, ou que o rádio poderia ser interceptado por equipamentos de escuta passiva, levou a grandes avanços de criptografia, que ocasionalmente levavam a um excesso de confiança. Acreditava-se que as complexas máquinas de criptografia com códigos rotativos da Alemanha eram invencíveis, mas os erros de usuários e os esforços britânicos em escala industrial permitiram à Grã-Bretanha desvendar os códigos alemães. Atualizações baratas dos equipamentos e codificadores alemães poderiam ter cancelado essa vantagem britânica, mas a confiança excessiva de Berlim na sua criptografia impediu a execução de tal manutenção. O resultado foram comunicações de inteligência interceptadas e uma mudança no curso da guerra. A criptografia de ponta a ponta é significativamente mais avançada que as tecnologias que a precederam, mas a história sugere que ter um pouco de humildade é necessário.

9. **Muitos Estados não consideram totalmente o quanto um adversário pode fazer esforços extraordinários para comprometer suas redes.** Em meio a debates sobre as telecomunicações modernas, vale a pena observar que os Estados que priorizaram a conveniência ou o comércio e, portanto, usaram atalhos de segurança, muitas vezes não tiveram surpresas agradáveis no que diz respeito aos esforços que um determinado adversário fez para comprometer suas redes. Na Primeira Guerra Mundial, a Alemanha surpreendeu-se com a velocidade e a voracidade com que a Grã-Bretanha cortou todos os cabos usados pelo líder da Tríplice Aliança para acessar o mundo exterior. De forma parecida, os comandantes russos ficaram surpresos quando sua indisciplina com relação ao rádio levou a uma derrota desastrosa em Tannenberg. Na Segunda Guerra Mundial, a Alemanha não esperava que os britânicos formassem uma operação de quebra de código altamente centralizada e em escala industrial que pudesse explorar os erros de comunicação alemães, não importa o quanto fosse trivial ou fugaz, para quebrar os códigos alemães. E, durante a Guerra Fria, os soviéticos deixaram de criptografar uma linha telefônica subaquática interna que acreditavam estar fora do alcance dos Estados Unidos e, como consequência, Washington descobriu uma maneira de grampeá-la, conquistando uma fonte inestimável de informações.

10. **A segurança de rede não se trata apenas de interceptação, mas também de negação.** Uma parte do debate sobre o papel da Huawei nas redes foca questões envolvendo a segurança de dados, deixando de dar mais importância a situações de negação de serviço de rede, que tem sido uma parte importante da concorrência no setor de telecomunicações por parte das grandes potências. No início da telegrafia, as grandes potências procuraram

cortar cabos e negar comunicações, culminando na operação sem precedentes e bem planejada da Grã-Bretanha de cortar todos os cabos ao redor do mundo que pudessem conectar a Alemanha ao exterior. Às vezes, um Estado pode se prejudicar na busca de estratégias de negação de serviço de rede, mas sem que isso o impeça de continuar se acreditar que o dano será maior para o oponente.

As grandes potências e as telecomunicações

"Grandes impérios fizeram grandes esforços para acelerar o fluxo de informações", registra a história das telecomunicações. "Os romanos construíram estradas, os persas e mongóis estabeleceram revezamentos de cavalos, os britânicos subsidiaram o transporte postal a vapor."[2] No entanto, apesar do grande desejo que os Estados tinham por informações, os fluxos delas permaneceram limitados até o início da telegrafia moderna. A eletrificação dos fluxos de informação criou as telecomunicações modernas e com elas, padrões familiares de rivalidade sobre elas por parte das grandes potências.

O período das primeiras décadas das telecomunicações modernas, que se estendeu de 1840 até a Primeira Guerra Mundial, tem características importantes e semelhantes às da atualidade. Esse período, como a atual era pós-Guerra Fria, foi de relativa paz entre as grandes potências, mas também de "menor sensibilidade", por parte dos principais Estados, às questões de política e segurança nas redes de telecomunicações.[3] Grandes potências construíram redes nacionais e internacionais no século XIX e, inicialmente, contentaram-se em deixar esta área sob o comando das indústrias, ignorando, assim, a nacionalidade das empresas privadas e subestimando os riscos de um adversário controlar as redes de telecomunicações. Os benefícios das mudanças revolucionárias nas telecomunicações – o que alguns na época chamavam de "a aniquilação do tempo e do espaço"[4] – eram tão óbvios e esmagadores que "a propriedade dos cabos era vista como um problema menor".[5] A telegrafia consistia mais em negócio do que em política nesse período, registra um historiador em uma observação que poderia ter sido aplicada facilmente a algumas das emoções iniciais sobre a moderna tecnologia da informação e sua mais recente encarnação: o 5G.[6]

O período de relativa tranquilidade das grandes potências não duraria. Países como o Peru, em 1879 e, em seguida, os Estados Unidos, em 1898, foram alguns dos primeiros a cortar as redes de telecomunicações de um rival. À medida que as tensões entre as grandes potências aumentavam, os países em todo o mundo passaram a perceber que alguns – a saber, a Grã-Bretanha – tinham administrado bem o longo período de paz e, por meio de suas empresas privadas, haviam conquistado domínio sobre as comunicações internacionais.

Cada vez mais temerosos da dependência das redes de cabos submarinos britânicas, países como França e Alemanha subsidiaram fortemente o desenvolvimento de suas próprias redes, em um desenvolvimento não tão diferente que o próprio subsídio e proteção que a China oferece às suas campeãs de tecnologia da informação, como Alibaba, Baidu, Tencent e Huawei. Como a historiadora Heidi Tworek documenta, os rivais britânicos também apostaram alto na próxima geração de tecnologia de telecomunicações – "telegrafia sem fio", mais conhecida como rádio – esperando diminuir a dependência dos cabos de telégrafo submarinos de propriedade britânica.[7] Enquanto os britânicos lideravam nessa área, a Alemanha se recusou a confiar nas redes britânicas. O país construiu uma rede própria, com empresas campeãs apoiadas pelo Estado operando em partes menos conectadas do mundo, como América Latina, África e Ásia, no que hoje poderia ser o equivalente à expansão das empresas de tecnologia chinesas no mundo em desenvolvimento e a determinação de Pequim de lançar as bases para as redes 5G.

Ao longo desse período, muitos dos elementos da concorrência no setor das telecomunicações das grandes potências, por vezes negligenciados hoje, com frequência eram levados bem a sério pelos países naquela época. A Alemanha, frustrada com o domínio britânico nas redes de rádio, usou um órgão normativo para romper com o domínio britânico, em uma tática que demonstra que esses organismos não tão importantes no passado quanto são agora. E, agora que as telecomunicações se tornaram sem fio e ainda mais fáceis de interceptar, as grandes potências acreditam na criptografia, às vezes abstendo-se de promover o uso disciplinado das suas redes, pressupondo que os "códigos" – etapas detalhadas para criptografar ou descriptografar mensagens – resolveriam o problema, uma crença que quase sempre se mostrou errônea devido a erros que usuários cometem. Essa visão tem paralelos notáveis com os pressupostos modernos sobre insegurança geral das redes de telecomunicações e a crença articulada por alguns em debates sobre a Huawei de que a criptografia neutralizaria em grande parte o risco de a China acessar alguma rede de telecomunicações terceira.

Quando a paz entre as grandes potências terminou e a guerra irrompeu, a importância política das telecomunicações – nem sempre clara em tempo de paz – de uma hora para outra ficou evidente. O sucesso alemão na intercepção das transmissões russas na Primeira Guerra Mundial produziu uma vitória tão definitiva na Batalha de Tannenberg que ela mudou o curso da guerra e ajudou a acelerar a saída da Rússia do conflito. O domínio britânico dos cabos submarinos na Primeira Guerra Mundial foi tão completo a ponto de apartar a Alemanha do sistema global de telecomunicações, rotear o tráfego de cabos alemães através de suas redes e, por fim, descobrir o telegrama Zimmerman, ajudando a trazer os Estados Unidos para o conflito. Na Segunda Guerra Mundial, a Grã-Bretanha alcançou mais um sucesso em termos de inteligência, quebrando a criptografia alemã supostamente inquebrável e obtendo informações inigualáveis, o que, de acordo com a historiografia oficial da Grã-Bretanha, encurtou a guerra na Europa em anos. Esses casos demonstram que a segurança das telecomunicações não é apenas uma questão de táticas de campo de batalha, mas de concorrência política, algo que pode ditar o destino de grandes potências e moldar a história mundial.

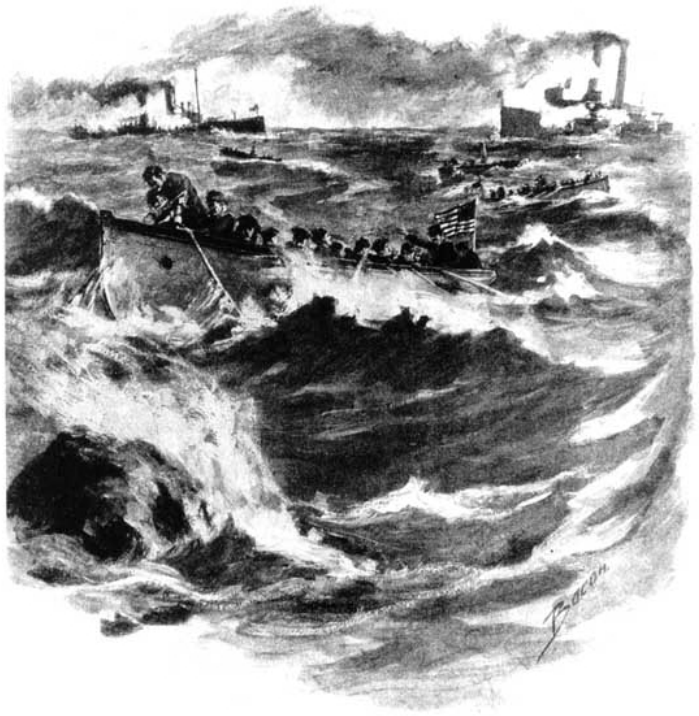
À medida que o mundo avançou para uma Guerra Fria entre os EUA e a União Soviética, as vantagens britânicas foram desfeitas não só pela potência norte-americana, mas pelas mudanças na tecnologia que fizeram com que as redes mais antigas fossem se tornando menos relevantes, demonstrando a importância de grandes potências permanecerem na vanguarda da tecnologia. Nessa nova era, a concorrência nas telecomunicações continuou seguindo por caminhos familiares. Por exemplo, os Estados Unidos foram pioneiros em maneiras de grampear cabos subaquáticos que estavam enterrados tão profundamente que eram considerados tão seguros que as mensagens que passavam neles eram muitas vezes deixadas descriptografadas. A concorrência também avançou para outros domínios, como satélites e infraestrutura de Internet, ainda que grande parte dessa história ainda esteja sendo escrita e, na maioria dos casos, permaneça sob sigilo.

Como demonstrado por estes breves casos, as telecomunicações sempre foram uma matéria de cunho político. A exploração dessas tecnologias e recursos geralmente evoluiu simultaneamente ao seu desenvolvimento. Sempre que novos métodos de comunicação chegaram, as grandes potências procuraram maneiras de interceptá-los ou interrompê-los. "A comunicação elétrica tem sido, muitas vezes, descrita como uma das grandes realizações da humanidade", observa um

historiador das telecomunicações, "mas, quando o analisamos do ponto de vista da segurança, vemos uma imagem totalmente diferente, pois a segurança não é uma característica técnica, mas sim social e política." E, "como a política não melhorou", ele observa, "as telecomunicações têm um lado obscuro".[8]

Passemos agora para um resumo dos principais temas em quase dois séculos de concorrência no setor das telecomunicações.

1. A Guerra Hispano-Americana: os limites da neutralidade dos cabos



Uma representação da expedição de corte de cabos dos EUA em Cienfuegos, publicada em 1907. A operação demonstrou que os cabos de telégrafo submarinos não seriam tratados como neutros durante os conflitos armados, mesmo por uma grande potência que já defendia a neutralidade dos cabos.

Fonte: Biblioteca On-line do Centro Histórico Naval[9]

À medida que os cabos submarinos começaram a cruzar o mundo no século XIX, várias potências, incluindo a França, a Alemanha e os Estados Unidos, clamaram para que eles ficassem fora da política internacional. Em 1858, em um dos primeiros telegramas transatlânticos enviados, o presidente dos EUA, James Buchanan, pediu à Rainha Vitória que mantivesse as novas linhas de telégrafo mundiais "sempre neutras… mesmo em meio a hostilidades".[10]

No entanto, uma vez que as hostilidades tiveram início, os estimados princípios de neutralidade foram abandonados. Duas décadas depois da mensagem de Buchanan, o Peru cortou linhas de cabos chilenas que passavam por território disputado.[11] Essa disputa recebeu pouca atenção. Mas, quando os Estados Unidos, antigo defensor de neutralidade de cabos, cortaram cabos tanto no Atlântico como no Pacífico durante a Guerra Espanhol-Americana, o mundo ficou em alerta.

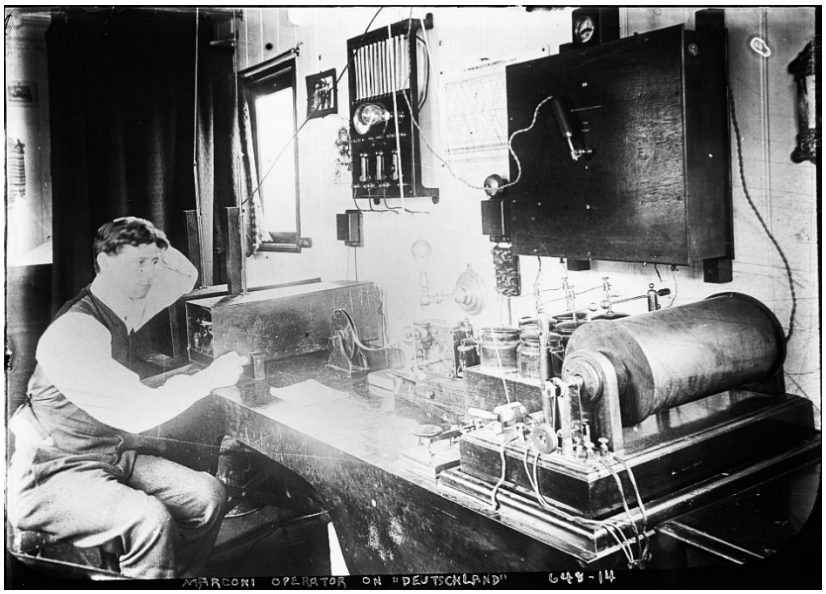
O corte de cabos pelos EUA foi planejado antes do conflito. No palco do Atlântico, os Estados Unidos esperavam cortar o contato entre a Espanha e o exército espanhol em Cuba. "O isolamento de Havana era, naturalmente, de grande importância", lia-se em um relato de uma revista norte-americana da época, e isso exigia que os Estados Unidos "cortassem toda a comunicação telegráfica entre Havana e o mundo externo".[12] Primeiro, os Estados Unidos

cortaram o tráfego espanhol que atravessava o território norte-americano na Flórida. Depois, o país enviou uma pequena unidade militar norte-americana para destruir um nó-chave de telecomunicações em Cienfuegos, cortando a comunicação entre a cidade de Havana e de grande parte do oeste de Cuba e a Espanha. Posteriormente, os Estados Unidos atacaram vários cabos a leste de Cuba, bem como cabos no Caribe que conectavam Porto Rico à Espanha.[13] Juntos, os cortes de cabos degradaram significativamente a capacidade de a Espanha orientar e comandar forças em Cuba.[14]

No Pacífico, os Estados Unidos cortaram o único cabo submarino entre Manila e Hong Kong, separando, na prática, as Filipinas da Espanha.[15] A decisão também prejudicou as comunicações dos EUA, mas teoricamente impôs um custo ainda maior à Espanha, e os Estados Unidos puderam compensar esse fato enviando regularmente um navio a Hong Kong para fazer a conexão com Washington.[16] As forças norte-americanas também cortaram cabos submarinos dentro das Filipinas, diminuindo ainda mais a capacidade de a Espanha comandar suas forças.

A Guerra Hispano-Americana talvez tenha sido o primeiro conflito global que abrangeu vários palcos nos quais as telecomunicações elétricas foram importantes. Também marcou a primeira vez em que uma grande potência buscou negar acesso de outra parte aos cabos submarinos. Antes do conflito, a telegrafia ainda era vista principalmente como um domínio comercial, e muitos esperavam que os cabos permanecessem fora da concorrência política e militar. O conflito pôs em xeque os limites dessas perspectivas e indicou que o controle sobre a infraestrutura de telecomunicações e a capacidade de negar essas vantagens a rivais geopolíticos sempre foram de imensa importância política.

2. A rivalidade anglo-alemã: criação de redes e definição de padrões



Operador de rádio da Marconi Company no "Espaço Marconi" do transatlântico alemão SS Deutschland. A influência da Marconi Company foi tão grande que seus funcionários operavam em espaços de rádio alemães, mesmo que a Alemanha estivesse preocupada com os riscos de interceptação e negação de serviço.

Fonte: Biblioteca do Congresso, Coleção George Grantham Bain[17]

A definição de padrões tecnológicos e seus respectivos efeitos nas redes são há tempos uma arena velada de concorrência entre grandes potências. Os países cuja tecnologia se torna o padrão dominante podem exercer essa vantagem sobre os outros – uma questão que recebe atenção das potências em crescimento, que trabalham muitas vezes para reduzir sua vulnerabilidade, criando sistemas paralelos. Na verdade, a presente concorrência sino-americana sobre TIC espelha uma corrida centenária entre a Alemanha e a Grã-Bretanha pelo domínio da infraestrutura de TIC no passado, com paralelos excepcionais e lições importantes para o presente.

No fim do século XIX, o engenheiro italiano Guglielmo Marconi, com o apoio da Marinha Real Britânica, criou a telegrafia sem fio.[18] A invenção foi revolucionária. Embora haja casos de grandes potências cortando os cabos umas das outras no passado, e embora as comunicações entre navios e entre o navio e o continente já tenham enfrentado problemas, o sistema de Marconi resolveu esses problemas e estava menos propenso a interferências.[19] Marconi acabou fazendo uma parceria com a Grã-Bretanha, dando ao país um monopólio sobre as transmissões de rádio. Junto da parcela de 60% que a Grã-Bretanha tem na rede de cabos submarinos do mundo todo, a região dominava as transmissões internacionais. A vantagem britânica incomodava a Alemanha, mas a concorrência em relação às tecnologias sem fio também "apresentou uma oportunidade para a Alemanha exercer o controle sobre uma nova infraestrutura internacional" e "contornar os cabos britânicos"; o resultado foi uma primazia da grande potência.[20]

Sentindo-se vulnerável, o imperador Wilhelm II autorizou o apoio estatal direto a cientistas e engenheiros alemães, à medida que copiavam com sucesso os projetos de Marconi, patenteavam-nos na Alemanha e construíam redes de rádio próprias financiadas por contratos com as forças armadas alemãs.[21] Mesmo assim, a vantagem superior do rádio de alcance mais longo e do pioneirismo de Marconi estabeleceu sua empresa apoiada pelo Reino Unido como o padrão global, e Marconi aproveitou esses efeitos de rede para perseguir uma política de "não intercomunicação" com operadores de rádio que não fossem Marconi. As empresas e os transatlânticos alemães não queriam ter sua comunicação global interrompida, por isso preferiram o sistema apoiado pela Grã-Bretanha aos sistemas alemães.

O imperador Wilhelm II intensificou a política industrial alemã para fazer frente ao padrão britânico. Ele rapidamente determinou que Siemens & Halske e AEG, duas grandes companhias elétricas alemãs com operações de rádio concorrentes, se juntassem para estabelecer a alternativa alemã definitiva, a Telefunken. "A rivalidade [doméstica] no campo da telegrafia sem fio enfraquece a competitividade da Alemanha", explicou o imperador, "e dá à Marconi Company a oportunidade de alcançar um monopólio mundial" que "não era do interesse da Alemanha".[22] Sob o comando do imperador Wilhelm II, a Alemanha buscou o protecionismo, chegando a proibir os sistemas Marconi em alguns casos. Buscou mercados emergentes, vendendo sua tecnologia para a América do Sul e África, para definir o padrão nessas regiões e garantir a receita.

Quando esses esforços se revelaram insuficientes, a Alemanha descobriu o sucesso em órgãos normativos multilaterais. Em 1906, a Alemanha reuniu as grandes potências na primeira Convenção Internacional de Radiotelegrafia, uma conferência sobre padrões de rádio. Na ocasião, os membros em conjunto proibiram a política de "não intercomunicação" da Marconi, rompendo com o monopólio britânico e estabelecendo, na prática, um duopólio anglo-alemão.[23]

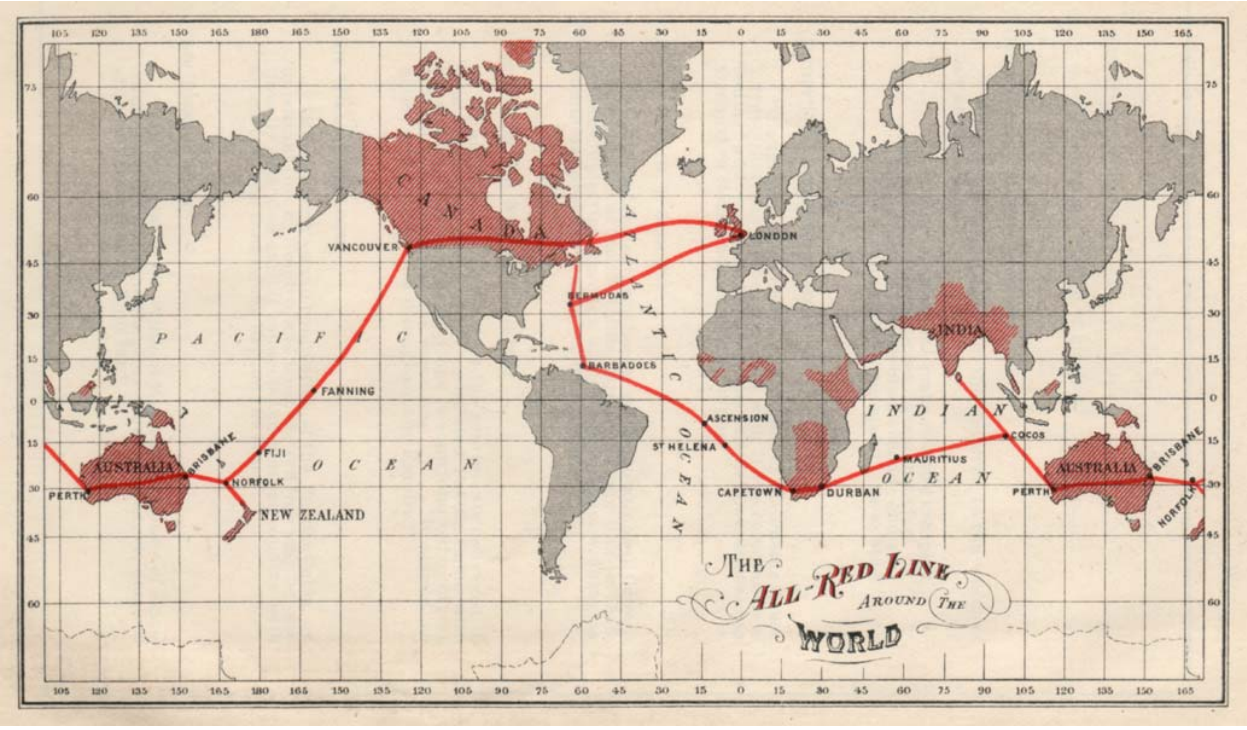
A concorrência anglo-alemã revela que os órgãos normativos têm enormes implicações estratégicas. A China usa hoje muitas das técnicas que a Alemanha usou há um século – política industrial orientada pelo Estado, proteção estatal, contratos estatais generosos, integração civil e militar, proibições de produtos rivais, fusões forçadas, busca de mercados emergentes e até mesmo tratados internacionais para estabelecer seus padrões – tudo isso ajudou empresas de tecnologia chinesas, como Alibaba e Tencent, proprietárias do WeChat e do Alipay, a se tornarem campeãs locais. Desde então, essas empresas vêm se expandindo para o exterior, muitas vezes tendo como alvo não o mercado norte-americano, mas – como a alemã Telefunken antes deles – mercados emergentes, com lucros mais baixos e concorrência reduzida.[24]

A China também está lutando por padrões na rígida infraestrutura de conectividade via Internet. Seu governo está investindo bilhões para que os fabricantes chineses de chips possam superar os rivais norte-americanos na corrida pelos padrões de Internet móvel 5G. Da mesma forma, empresas chinesas, como a Huawei e a ZTE, recebem empréstimos do governo para construir uma rígida infraestrutura de conectividade via Internet por todo o mundo em desenvolvimento. Como o exemplo britânico demonstra, esses esforços não só transformam a tecnologia chinesa no padrão, mas também oferecem oportunidades de vigilância. Enquanto isso, a iniciativa da Nova Rota da Seda aumenta a possibilidade de que os padrões para a "infraestrutura inteligente"

na Ásia, especialmente os sensores e softwares relevantes, possam ser estabelecidos pela China, o que pode levar à negação da interoperabilidade de outras empresas, afastando-as, assim, de veículos autônomos e outros setores.

A rivalidade anglo-alemã na telegrafia mostra que Washington precisa levar a sério o desafio estatal na China em termos de padrões. Ela também oferece um caminho a seguir. Da mesma forma que a Alemanha utilizou conferências internacionais para quebrar o monopólio britânico da telegrafia, os Estados Unidos poderiam estabelecer ou preservar padrões favoráveis em matéria de TIC por meio de acordos multilaterais. Isso pode impedir a China de estabelecer padrões unilaterais por meio de acordos de livre comércio, das companhias estatais campeãs ou dos projetos de infraestrutura.

3. Grã-Bretanha na Primeira Guerra Mundial: implantação da hegemonia das informações



A "All Red Line", uma dispendiosa rede britânica de linhas de cabo submarinos construída e organizada de modo que nenhuma parte passasse pelo território de um rival. O investimento inadequado da Alemanha em sua própria rede global de telecomunicações resiliente permitiu que a Grã-Bretanha a apartasse das comunicações globais, enquanto a Grã-Bretanha, de forma geral, não foi afetada.

Fonte: George Johnson, ed., The All Red Line: The Annals and Aims of the Pacific Cable Project/Internet Archive[25]

Os esforços da Alemanha para quebrar o domínio britânico sobre as telecomunicações no início do século XX não nasceram de uma paranoia. Assim que a Primeira Guerra Mundial eclodiu, a Grã-Bretanha logrou conquistar sua considerável influência nas redes de telecomunicação e acabou mudando o curso da guerra. Ela cortou cabos alemães, monitorou as transmissões do país e forçou seu tráfego em redes controladas pela Grã-Bretanha, desvendando o Telegrama Zimmerman, que ajudou a trazer os EUA para a guerra.[26]

A Grã-Bretanha não foi a primeira grande potência a cortar ou manipular redes de telecomunicação: o Peru cortou uma ligação entre Chile e Bolívia, os Estados Unidos cortaram cabos espanhóis e a Grã-Bretanha apartou os bôeres de seus apoiadores europeus em uma situação de crise e manipulou o tráfego de cabos para a França em outra.[27] Mas esses esforços foram levados ao extremo na Primeira Guerra Mundial.

A Grã-Bretanha foi a primeira a apartar um país inteiro das principais redes globais de telecomunicações, implantando, no primeiro dia da guerra, um plano cuidadosamente elaborado em tempos de paz.[28] No espaço de um ano, a Grã-Bretanha destruiu os cabos alemães em todo o

mundo: no Canal da Mancha, no Mar do Norte, no Atlântico Norte, na América do Sul, em grande parte da África, no Extremo Oriente e até mesmo em países neutros que hospedavam a infraestrutura alemã.[29]

Para compensar, a Alemanha tentou expandir a rede de rádio que a Telefunken construiu década antes na América Latina e no "Sul Global" para que ela cobrisse o mundo. Em um esforço com paralelos modernos na Nova Rota da Seda Digital da China, Berlim ofereceu empréstimos e investimentos a governos interessados nos "benefícios de desenvolvimento do rádio" para que hospedassem nós de comunicação alemães. Em resposta, a Grã-Bretanha persuadiu ou induziu a maioria desses países a renunciar ao apoio a nós de rádio alemães ou a sabotá-los ativamente.[30]

Deixada sem redes próprias, Berlim não tinha outra opção senão depender da rede britânica durante a guerra. No início, os britânicos começaram a monitorar silenciosamente todo o tráfego que passava por seus cabos e usaram essa vantagem para combater a guerra de informações contra a Alemanha, vazando seletivamente o embaraçoso tráfego alemão para prejudicar suas relações com países neutros. Quando a Alemanha enviou um telegrama propondo uma aliança militar com o México contra os Estados Unidos – o vergonhoso telegrama Zimmerman –, a mensagem atravessou uma rede britânica e foi interceptada e descriptografada pela Grã-Bretanha, que a compartilhou com o governo dos Estados Unidos, que, por sua vez, a compartilhou com seu povo.[31] Esse incidente ajudou a levar os Estados Unidos à guerra, moldando a história mundial e, por fim, selando a derrota da Alemanha.

A guerra de informação britânica contra a Alemanha revela os perigos de se conceder a uma potência rival a capacidade de monitorar o tráfego ou de encerrar o acesso das telecomunicações. Revela, igualmente, que as redes que as grandes potências consideram corriqueiras em tempo de paz são frequentemente desprezadas em tempos de guerra, e que a luta pelos nós de comunicação envolverá inevitavelmente terceiros e países neutros.

4. A vitória alemã em Tannenberg: os perigos da interceptação

Uma estação de telégrafo de campo sem fio alemã durante a Primeira Guerra Mundial. A incapacidade de a Rússia criptografar adequadamente suas comunicações em suas estações de campo levou a uma derrota desastrosa, que remodelou o curso da guerra.

Fonte: C. O. Nordensvan e Valdemar Langlet. Det stora världskriget *[A Grande Guerra Mundial]*[32]

A Alemanha não estava totalmente desprovida de recursos próprios na guerra das informações. Ela cortou cabos terrestres e submarinos da Rússia que fazia a conexão com seus aliados ocidentais, bem como vários cabos transatlânticos utilizados pelos britânicos, sendo pioneira no uso de submarinos para essas missões.[33] Dada a redundância das redes britânicas, esses esforços foram, em última análise, menos debilitantes do que os alemães esperavam. O que se revelou muito mais significativo foi o uso da inteligência de rádio por parte da Alemanha contra a Rússia durante a Batalha de Tannenberg, em agosto de 1914, o primeiro mês da guerra, desencadeando uma derrota desastrosa para os russos. Um oficial da inteligência alemã na época chamou o incidente de "o primeiro na história do homem em que a interceptação do tráfego de rádio inimigo desempenhou um papel decisivo".[34]

A batalha ocorreu em meio a vitórias russas na frente oriental. À medida que a Rússia avançava mais no território da Prússia Oriental, seus militares encontraram um desafio de comunicação relevante, que criou o cenário para uma derrota desastrosa. Os alemães, quando bateram em retirada, cortaram suas próprias linhas de telégrafo, e os russos, no seu avanço, não tinham pessoal treinado o suficiente para estabelecer comunicações por fio por toda a sua formação, que se espalhava pelo país. A transmissão de rádio forneceu uma alternativa, mas, embora os russos tivessem adotado novas tecnologias de rádio para seu comando e controle militar, eles não as tinham protegido como deveriam. Diferentes códigos foram atribuídos a grupos diferentes. A maioria tinha pouco treinamento com codificação e decodificação de sinais, alguns códigos eram conhecidos por terem sido quebrados pelos britânicos e os manuais de código eram limitados ou ininteligíveis para muitos dos recrutas analfabetos.[35] O resultado foi que os comandantes russos

sentiram que precisavam correr o risco de utilizar mensagens de rádio não codificadas e esperar que os alemães não as estivessem monitorando de perto.

Os alemães, no entanto, estavam monitorando os sinais meticulosamente. Tendo já observado a indisciplina russa no rádio nos combates contra os japoneses, sabiam que as transmissões não codificadas russas não faziam parte de uma campanha de simulação e engano. Então, utilizaram seus conhecimentos sobre as comunicações russas em tempo real para levantar a "neblina da guerra" e derrotar decisivamente a força superior. A Rússia perdeu um exército inteiro, com mais de 100 mil vítimas e 92 mil presos, em comparação com apenas 13 mil vítimas alemãs.

5. A Grã-Bretanha na Segunda Guerra Mundial: os limites de criptografia

Rotores mecânicos da máquina de codificação Lorenz, considerados inquebráveis de facto durante a Segunda Guerra Mundial. Os esforços britânicos para quebrar o código deram aos oficiais acesso a comunicações alemãs de alto nível.

Fonte: Matt Crypto / Wikimedia Commons[36]

As invenções da telegrafia sem fio e do rádio significaram mais conveniência em comparação aos cabos físicos, mas traziam maior risco de interceptação. Nas Primeira e Segunda Guerras Mundiais, as grandes potências existiam em um mundo em que as comunicações de rádio eram consideradas acessíveis a outros. E, nesse mundo, não tão diferente das hipóteses atuais sobre a vulnerabilidade dos modernos sistemas de telecomunicações e computadores, a criptografia era considerada essencial para a segurança. O resultado, como um historiador militar americano observou, foi uma "luta entre o criptografista e o criptoanalista".[37] Quando as grandes potências estavam no lado errado dessa luta, os resultados podiam ser catastróficos.

Para evitar esse resultado, as organizações utilizaram códigos cifrados para reduzir o risco de a interceptação comprometer a segurança. Também exercitaram a "disciplina de rádio" para evitar que adversários coletassem insights sobre padrões de uso por meio da análise do tráfego de ondas.

A maioria das grandes potências investiu em um esforço verdadeiramente industrial para analisar o tráfego adversário e, se possível, quebrar os seus códigos. A Grã-Bretanha focou muito mais a análise de códigos adversários do que a Alemanha, exercendo atividades correlatas em várias

agências. E, tal como os sucessos britânicos na interceptação de sinais de comunicação e na criptoanálise tinham moldado o curso da Primeira Guerra Mundial, moldaram também o curso da Segunda Guerra Mundial, quando a operação britânica em Bletchley Park quebrou as máquinas codificadoras alemãs Enigma e Lorenz.

Os sistemas de codificação Enigma e Lorenz usaram máquinas de rotor extraordinariamente complexas para criptografar mensagens que a Alemanha acreditava que "permaneceriam invulneráveis".[38] Cada tecla pressionada substituiria um caractere por outro com base em configurações exclusivas para a máquina, e aquelas configurações – que, para o sistema Lorenz, excediam o número total de átomos no universo – precisavam ser de conhecimento do remetente e do receptor para que a mensagem fosse lida.[39] O Enigma era usado pelos militares, pela Gestapo e pelos diplomatas; o Lorenz, ainda mais complexo, era usado por Adolf Hitler, altos funcionários nazistas e militares para comunicação mútua.

O sucesso britânico em quebrar o Enigma e o Lorenz foi resultado de vários avanços. Em primeiro lugar, foi resultado da cooperação de inteligência aliada com a Polônia, que tinha explorado alguns erros alemães para quebrar algumas máquinas Enigma mais simples.[40] Como um criptoanalista britânico da época comentou, o esforço deles "nunca teria decolado" sem as contribuições polonesas.[41]

Em segundo lugar, era um resultado da confiança exacerbada alemã. A Alemanha nunca suspeitou que os códigos haviam sido quebrados e, portanto, proibia modificações razoavelmente fáceis que teriam forçado a Grã-Bretanha a recomeçar seu trabalho.[42] Mesmo assim, a Alemanha tinha fé que a invulnerabilidade de suas máquinas "era quase certa", relatou um oficial sênior de Bletchley Park.[43]

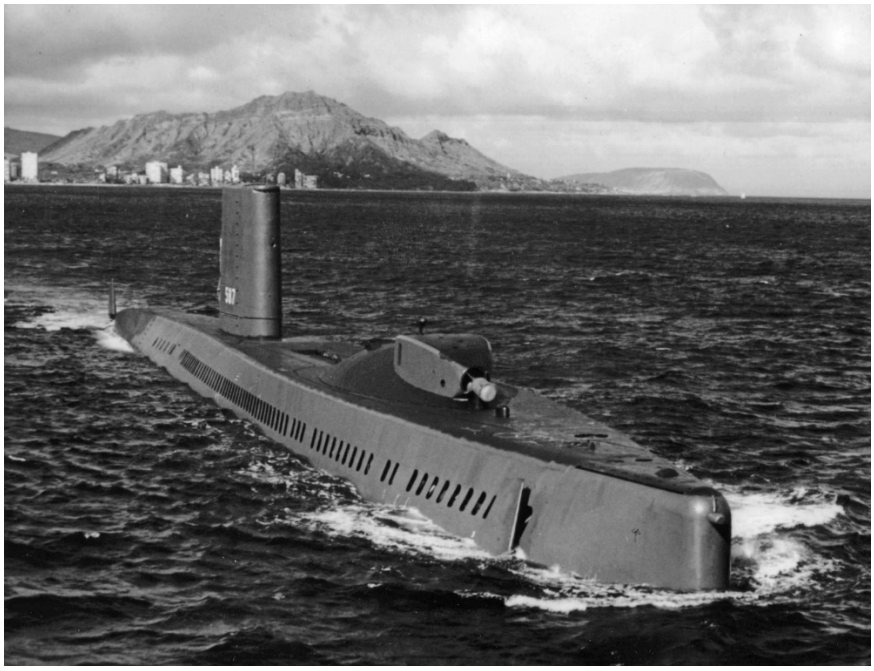
Finalmente, foi um único, mas grande lapso, na "disciplina de rádio" alemã que criou uma abertura para se fazer a engenharia reversa dos sistemas de criptografia alemães, apesar de nunca se ter se visto um pessoalmente.[44] Até mesmo os sistemas mais sofisticados eram vulneráveis a erros de usuário, e um adversário vigilante poderia explorá-los.

Ao quebrar o Enigma e o Lorenz, a Grã-Bretanha teve acesso a algumas das comunicações mais confidenciais da Alemanha. Winston Churchill acreditava que a inteligência tinha sido uma razão fundamental para a Grã-Bretanha ter vencido a guerra, e Dwight D. Eisenhower, ao que consta, chamou-a de "decisiva".[45] O historiador oficial da inteligência britânica, *Sir* Francis Harry Hinsely, argumenta que esses sucessos "encurtaram a guerra em no mínimo dois anos e, provavelmente, por quatro anos", solapando o Marechal-de-Campo Erwin Rommel na África, invertendo drasticamente as perdas marítimas aliadas para os submarinos alemães e permitindo os desembarques na Normandia.[46] Também permitiram à Grã-Bretanha identificar praticamente todos os espiões alemães que entraram no país e, muitas vezes, os convertendo ou usando para repassar informações errôneas. O chefe do programa observou que a inteligência britânica "operava e controlava ativamente o sistema alemão de espionagem naquele país".[47] Poucos países já tiveram um conhecimento tão aprofundado de outro durante um período de guerra.

Reunidos, os êxitos dos esforços da Grã-Bretanha contra a Alemanha, o monitoramento em tempos de paz das comunicações alemãs pela Polônia e a sua decisão de partilhar seu progresso

com a Grã-Bretanha trazem lições aplicáveis hoje para as grandes potências que estão conduzam o reconhecimento cibernético entre si. Em termos mais gerais, aqueles que sugerem que a criptografia atenua os problemas que seriam causados pelo acesso de um adversário a uma determinada rede de telecomunicações podem estar cometendo um erro que não é diferente daquele que a própria Alemanha cometeu no passado: excesso de fé na tecnologia e atenção limitada à possibilidade sempre presente de erro humano.

6. Operação Ivy Bells: as profundezas da busca da informação



O USS Halibut, que supostamente estava envolvido em uma missão para desviar uma linha telefônica subaquática soviética.

Fonte: Marinha dos EUA/Wikimedia Commons[48]

A União Soviética era muito mais cuidadosa com sua criptografia que os nazistas, contando com sua própria versão de Enigma – conhecida como Fialka –, que era substancialmente mais complexa.[49] Por isso, os vastos tesouros de inteligência de nível estratégico produzidos na Segunda Guerra Mundial após a quebra dos códigos alemães não tinham análogo conhecido publicamente na Guerra Fria. Diante desses desafios, outros métodos de penetração nas telecomunicações adversárias foram pioneiros. Um dos mais audaciosos desses esforços ocorreu em relação aos cabos subaquáticos.

O início dos cabos subaquáticos no século XIX tinha levado a esforços para cortá-los e ocasionalmente desviá-los, muitas vezes para águas mais rasas ou em terra, onde tais tarefas eram mais fáceis de se conduzir. Em contraste, a execução dessas operações em águas profundas controladas por um adversário era considerada praticamente impossível, especialmente se fosse feita secretamente. A partir do século XX, os britânicos e, em seguida, as grandes potências em sequência tinham chegado a uma determinação sobre a segurança de cabos subaquáticos: se os locais de colocação fossem seguros e os cabos não atravessassem países neutros ou hostis, então os cabos, em geral, estariam seguros contra interceptação e, muitas vezes, protegidos de cortes, especialmente em tempo de paz.[50]

No entanto, durante a Guerra Fria, esse cálculo mudou. O advento dos submarinos nucleares abriu a possibilidade de se colocar cabos subaquáticos em águas mais profundas. No entanto, a tarefa de enviar mergulhadores para acessar cabos no fundo do mar era considerada mais

semelhante à exploração espacial do que às tentativas mais costumeiras de manipulação de cabos realizadas anteriormente. Criar um cabeamento que pudesse ser instalado nessas condições também era tecnicamente desafiador.

Quando os Estados Unidos suspeitaram que um cabo subaquático soviético poderia existir da sede naval em Vladivostok até uma base submarina na península de Kamchatka, o país procurou superar esses obstáculos, demonstrando o valor da interceptação de sinais de comunicação.[51] Acreditava-se que um emaranhado de fios de cinco polegadas forneceria informações essenciais sobre as forças nucleares soviéticas.[52] Embora os soviéticos criptografassem todo o tráfego enviado pelo ar, os Estados Unidos esperavam que União Soviética considerasse que o tráfego por meio do cabo subaquático protegido fosse praticamente impossível de acessar e, portanto, não o criptografassem. Além disso, "os almirantes e os generais soviéticos seriam demasiado arrogantes e impacientes para aguentar um oceano de criptógrafos já assolados pelo volume gigantesco do seu trabalho atual", o que os levava a insistir em comunicações de voz desprotegidas.[53] Por isso que um grampo daria acesso a um tesouro raro de informações, e a Marinha norte-americana lançou a Operação Ivy Bells para estabelecê-lo.

Muito sobre o grampo e as informações coletadas a partir dele permanecem sob sigilo, mas as fontes abertas fornecem alguns detalhes sobre a operação exclusiva e inovadora. Os Estados Unidos despacharam um submarino nuclear, o *USS Halibut*, para passar silenciosamente pela Marinha soviética e encontrar o cabo subaquático em uma área que abrange quase um milhão de quilômetros quadrados.[54] Foi criada uma tecnologia inovadora para garantir que os mergulhadores pudessem trabalhar sob grandes pressões e em temperaturas extremamente baixas por várias horas. Da mesma forma, foram desenvolvidos novos métodos para instalar um grampo nesse ambiente desafiador.[55] Tudo tinha que ser feito sem que a União Soviética detectasse ou sequer suspeitasse de alguma coisa. Se o submarino fosse detectado, os soviéticos poderiam invadi-lo ou destruí-lo.

No fim, a operação foi um sucesso e, durante a década de 1970, a Marinha dos EUA interceptou e registrou mensagens desprotegidas pelo grampo nesses cabos. A cada poucos meses, os submarinos norte-americanos mergulhavam silenciosamente em águas soviéticas, fugiam de submarinos de ataque, despachavam mergulhadores para as linhas de cabo grampeadas e coletavam fitas de comunicações soviéticas, produzindo um conjunto de informações extremamente valiosas e raras. Embora os Estados Unidos tivessem expandido uma "rede de satélites, aviões, estações de escuta e submarinos espiões" para reunir informações interceptadas de sinais de comunicação, o país não conseguia "penetrar uma linha telefônica direta" dentro do território de um adversário. Esse esforço ilustrou a mudança evolutiva das telecomunicações, ou seja, que os dados e sinais transmitidos por qualquer suporte e por qualquer meio poderiam ser acessados por quem tivesse as ferramentas certas. Ainda que, no fim, o grampo acabou sendo comprometido por causa de um vazamento, as interceptações de telecomunicações resultantes forneceram inestimáveis informações militares e políticas aos Estados Unidos e aliados.[56]

Concorrência moderna nas telecomunicações - uma perspectiva histórica

No final da Guerra Fria, os Estados Unidos tinham claramente substituído a Grã-Bretanha como o poder hegemônico da informação. Os Estados Unidos mantiveram uma posição nodal na Internet global, em recursos de espaço robustos, no domínio da maioria das tecnologias de Internet e, de acordo com as divulgações públicas, em habilidades sofisticadas para interceptar comunicações de adversários ou, possivelmente, negar o serviço a eles.

Essas vantagens norte-americanas estão agora sendo testadas, como ocorreu com a Grã-Bretanha há mais de um século. A Rússia, e especialmente a China, agora desafiam o domínio dos EUA. Embora os Estados Unidos tenham uma posição nodal em muitos fluxos de dados, outras potências procuram cada vez mais reduzir sua dependência das redes norte-americanas. Ao mesmo tempo, a posição nodal norte-americana atual é menos necessária para a interceptação que a da Grã-Bretanha há um século. A Internet possibilita a invasão sem que seja necessário controlar a infraestrutura física. Smartphones e redes de computadores podem ser invadidos, e, se as comunicações confidenciais forem comprometidas por causa de grampos físicos feitos anteriormente ou por invasões virtuais da era moderna, o resultado final é o mesmo. Dessa forma, estar conectado provavelmente cria uma vulnerabilidade maior agora do que na era do telégrafo ou do rádio sem fio.

A Rússia tem liderado a exploração dessa vulnerabilidade. Em 2007, a Rússia lançou uma onda de ataques cibernéticos contra as instituições estonianas, principalmente ataques de negação de serviços distribuídos.[57] Em 2008, realizou ataques cibernéticos na Guerra Russo-Georgiana, que envolveram não apenas ataques de negação de serviço direcionados, mas também esforços para redirecionar sites governamentais, assumir servidores do governo georgiano e redirecionar o tráfego da Internet georgiano por meio de servidores controlados pela Rússia, com alguns dos ataques tendo sido realizados antes do conflito para coincidir com a ação militar russa.[58] Em 2014, quando a Rússia invadiu a Crimeia, ela conjugou ataques cibernéticos ao controle físico de redes de telecomunicações. Os soldados russos tomaram instalações de telecomunicações ucranianas, utilizando-as para interromper a comunicação na Crimeia e até para realizar ataques cibernéticos e disrupções em outras partes da Ucrânia.[59] Em 2015, a Rússia iniciou uma onda de ataques cibernéticos à infraestrutura ucraniana, derrubando a energia elétrica de centenas de milhares de ucranianos em dois grandes momentos. Ao longo dos anos seguintes, continuou com o lançamento de uma onda de ataques sem precedentes na Ucrânia, abrangendo "mídia, finanças, transportes, forças armadas, política e energia" (praticamente todos os segmentos da sociedade ucraniana), no que alguns acreditavam ser parcialmente um esforço de treinamento para uma campanha semelhante contra os Estados Unidos.[60] Ao mesmo tempo, o país seguiu fazendo uma série de ataques em todo o Báltico e, excepcionalmente, procurou moldar a eleição dos EUA em 2016 e 2020 com campanhas de desinformação, bem como em outros países.[61] Em 2021, o governo dos EUA acusou formalmente a Rússia de hackear a empresa de TI SolarWinds, um ataque sofisticado que envolveu grande parte do governo federal e várias grandes empresas dos EUA.[62]

A China é a outra grande potência que investe muito na concorrência em telecomunicações, embora, ao contrário da Rússia, os esforços da China não só buscam explorar a infraestrutura existente da Internet, mas também construir redes e infraestruturas que o país possa influenciar e até mesmo controlar. Como a Rússia, a China tem sido adepta da exploração de vulnerabilidades existentes na Internet. No início dos anos 2000, a China lançou uma onda de ataques às redes do Departamento de Defesa dos EUA, no que ficou conhecido por esse departamento como a Operação Titan Rain.[63] Governos em todo o mundo, como dos Estados Unidos, Reino Unido, França, Alemanha, Canadá, Austrália, Japão, Coreia do Sul, Taiwan, Índia e mais de uma dezena de outros, queixaram-se da invasão chinesa em suas redes governamentais. O Procurador-Geral dos EUA, William Barr, confirmou que alguns dos maiores ataques cibernéticos da última década foram perpetrados por agentes chineses, incluindo roubo de registros do Departamento de Gestão de Pessoal dos EUA (registros de 21 milhões de pessoas), hotéis da rede Marriott (400 milhões), seguro-saúde Anthem (80 milhões) e Equifax (147 milhões), entre outros.[64]

Ao mesmo tempo, a China também está lançando os fundamentos para futuras infraestruturas de Internet e, à luz dos seus esforços anteriores, é pouco provável que esse esforço tenha uma natureza comercial agora ou permaneça puramente comercial no futuro. Os investimentos da China são mais proeminentes nas redes 5G, que devem formar a base para uma economia conectada e mais inteligente, ligando inúmeros dispositivos e sensores. Ávida por construir essas redes em todo o mundo, a China subsidiou suas empresas e projetos campeões de 5G em todo o mundo como parte de uma iniciativa da Nova Rota da Seda Digital. Com preços competitivos, empresas como a Huawei conseguiram superar outros grandes fornecedores de 5G e comandar uma parcela significativa do mercado global, tornando a China o país líder na construção dessas redes. E, além do 5G, o governo da China tem subsidiado esforços para construir infraestruturas de Internet ou de comunicações em praticamente todos os continentes. Todos esses esforços são complementados por uma campanha para moldar os padrões globais, uma prioridade política essencial para a China, conforme estabelecida em documentos de planejamento de alto nível. Como na rivalidade anglo-alemã sobre o rádio, há um século, essa campanha poderia dar nova forma ao futuro das telecomunicações de maneiras que beneficiam a China. Para isso, a China recentemente revelou uma nova iniciativa de segurança de dados.[65]

Alguns temem que as atividades da China deixem em aberto a possibilidade de Pequim ter um controle *de facto* sobre essas redes, seja para interceptar tráfego ou negar acesso. Poucas informações públicas estão disponíveis sobre os esforços da China para obter esse controle, mas o governo dos EUA revelou, em fevereiro de 2020, que a Huawei tinha *backdoors* em seus equipamentos de rede, não os tinha revelado às empresas relevantes com as quais ela havia fechado contrato e que os *backdoors* foram além daqueles às vezes solicitados pelos governos anfitriões como parte de interceptações legais.[66] Além disso, os relatórios públicos revelaram que a Huawei ajudou governos, como os da Uganda e da Zâmbia, a revelar as identidades de dissidentes.[67] Além do caso da Huawei, uma empresa de segurança cibernética recentemente descobriu *backdoors* em um software fiscal obrigatório que o governo chinês exige que empresas estrangeiras instalem.[68] Independentemente de esses casos sugerirem que a Huawei explorou sua posição nessas redes, o comportamento da empresa e o histórico da China com ataques cibernéticos e espionagem são motivos de preocupação.

O outro grande motivo de preocupação vem do histórico e do comportamento de grandes potências, mesmo as liberais, que em geral, são mais limitadas pelo Estado de direito. Na verdade, a história sugere fortemente que o tipo de poder e influência que uma empresa como a Huawei exercerá provavelmente serão explorados pelo governo chinês, tal como outras grandes potências têm frequentemente explorado a posição de suas empresas ou capacidades em telecomunicações.

A partir dessa perspectiva histórica mais ampla, as evidências que podem levar muitos observadores a se decidir pela prudência é justificada pelo papel da Huawei nas redes de telecomunicações, mesmo que os motivos da empresa sejam real e puramente comerciais, mesmo que suas promessas de "sem backdoors e sem espionagem" sejam convincentes e mesmo que Pequim seja sincera na sua promessa de honrar esses compromissos.

Em termos mais gerais, como mostra este relatório, muitas das características da concorrência entre grandes potências no setor das telecomunicações que hoje são consideradas inovadoras têm raízes no passado. Ao longo da história, vários temas se repetiram:

- *Poder:* o controle sobre as redes de telecomunicações tem sido uma forma de poder político desde a criação dessas redes, há mais de 150 anos. A Grã-Bretanha explorou seu papel nas telecomunicações e no rádio, os Estados Unidos provavelmente fizeram-no na era moderna da Internet, e há razões para se preocupar com o fato de a China tentar fazê-lo hoje.

- *Negligência*: longos períodos de paz e prosperidade levaram à negligência quanto aos riscos nas telecomunicações. No século XIX, grandes potências ficavam satisfeitas em contar com empresas estrangeiras e redes operadas no exterior, assim como os países atuais estão dispostos a aceitar equipamentos e operações de telecomunicações chinesas. Mas, no fim das contas, a dependência de potenciais concorrentes ou adversários provou ser desastrosa para países como a Alemanha e reformulou a política mundial.

- *Exploração:* novas tecnologias na área de telecomunicações sempre surgiram simultaneamente a novos esforços para interceptar, negar ou explorar tais tecnologias. Apesar da esperança de que a criptografia possa complicar os esforços da China de interceptar as comunicações modernas, os períodos passados, caracterizados por uma grande confiança em criptografia, foram interrompidos por erros de usuários e os determinados esforços de países rivais para quebrá-la, como se deu conta a Alemanha quando a Grã-Bretanha desvendou seus códigos supostamente "inquebráveis". A humildade deve acompanhar cada onda de tecnologias supostamente seguras.

- *Empresas campeãs:* os países geralmente buscam ter suas próprias campeãs em telecomunicações, especialmente à medida que as tensões entre as grandes potências aumentam. O governo da China tem orgulho das realizações da Huawei e a defende em todo o mundo, chegando ao ponto de ameaçar países que recusam sua tecnologia. Não seria comum uma empresa tão próxima a seu governo de origem ficar imune à pressão do Estado quando tantas outras campeãs de telecomunicações ao longo da história não conseguiram esse distanciamento.

- *Padrões*: os padrões de telecomunicações podem determinar quem detém o poder nas redes. Veja, por exemplo, quando a Alemanha usou um órgão normativo para quebrar o domínio da Grã-Bretanha na área do rádio sem fio. Hoje, essa competição está acontecendo em órgãos como a União Internacional de Telecomunicações, e o papel da Huawei neles sugere que se faz necessário considerar se seus padrões permitirão à China remodelar as telecomunicações.

- *Negação de serviço:* a segurança de rede não se restringe apenas à interceptação e à segurança de dados. Ela tem a ver também com a negação de toda a operação da rede ou do acesso a redes externas. No passado, a Grã-Bretanha interrompeu o acesso da Alemanha a redes de telégrafos em todo o mundo, e o papel da Huawei nas redes pode capacitar a gigante chinesa a derrubar as redes em países onde ela está operando equipamentos, mesmo que não seja possível acessar facilmente os dados.

- *Determinação:* muitos países acabam ignorando os esforços extraordinários que um adversário pode envidar para comprometer suas redes e depois precisam lidar com a surpresa desagradável quando isso acontece. A capacidade de a Grã-Bretanha quebrar códigos alemães na Segunda Guerra Mundial por meio de esforços em escala industrial e a capacidade dos EUA de grampear cabos subaquáticos internos soviéticos que supostamente eram invioláveis demonstra até onde as grandes potências estão dispostas a ir para interceptar de sinais de comunicação essencial. A China provavelmente realizará esses esforços máximos e, mesmo que a Huawei ache difícil usar como arma sua posição nas redes modernas, subestimar a engenhosidade e as motivações de um concorrente determinado como a China é um assunto recorrente na concorrência em telecomunicações.

Como demonstrado neste relatório, muitas das características do jogo entre as grandes potências sobre as telecomunicações permanecem as mesmas, mesmo que os jogadores possam ser diferentes.

Sobre os autores

Rush Doshi foi Diretor da Brookings China Strategy Initiative e membro da área de Política Externa da Brookings. Também foi membro do Paul Tsai China Center da Yale Law School e participou da aula inaugural do grupo Wilson China Fellows. Sua pesquisa se concentra na grande estratégia chinesa principal, bem como nos problemas de segurança na região do Indo-Pacífico. Doshi é autor da obra *The Long Game: China's Grand Strategy to Displace American Order*, a ser publicada pela Oxford University Press. Atualmente, ele está atuando no governo de Biden.

Kevin McGuiness trabalhou recentemente com a Brookings como consultor externo do Programa Skillbridge do Departamento de Defesa, no qual contribuiu para vários projetos no Centro de Estudos Políticos do Leste Asiático. É veterano da Força Aérea e recentemente terminou seu período de serviço como docente na Academia da Força Aérea dos Estados Unidos, dirigindo cursos na área de Relações Internacionais e Política Asiática. Recentemente, trabalhou como assistente de pesquisa no Centro Nacional de Estudos Estratégicos para Estudo de Assuntos Militares Chineses, onde se concentrou na modernização e segurança do Exército Popular de Libertação (PLA) da China na região do Indo-Pacífico.

Agradecimentos

Os autores agradecem aos ex-estagiários Isabella Lu, Zijin Zhou e Gaoqi Zhang por sua assistência na pesquisa deste projeto, a vários revisores anônimos, a Claire Harrison e Ted Reinert por editar o relatório, e a Chris Krupinski e Rachel Slattery pelo layout e webdesign. A Brookings agradece o Departamento de Estado dos EUA e ao Institute for War and Peace Reporting por financiar esta pesquisa.

Este relatório foi concluído antes de Rush Doshi começar a atuar na esfera governamental e envolve apenas fontes abertas, não refletindo necessariamente a política ou posição oficial de qualquer órgão governamental dos EUA.

[1] Steven Chase, Robert Fife, and Barrie McKenna, "Trudeau Refuses to Let 'politics Slip into' Decision on Huawei," The Globe and Mail, 15 de outubro de 2018, https://www.theglobeandmail.com/politics/article-trudeau-refuses-to-let-politics-slip-into-decision-on-huawei/; Greg Quinn and Josh Wingrove, "Trudeau Says Politics Won't Factor Into Huawei 5G Decision," Time, 19 de dezembro de 2018, https://time.com/5485141/justin-trudeau-huawei-5g-decision-politics/.

[2] Daniel R. Headrick, The Invisible Weapon: Telecommunications and International Politics, 1851-1945 (Oxford, U.K.: Oxford University Press, 1991), capítulo 1.
[3] Ibid. , esta observação é de Headrick.
[4] Ibid.
[5] Ibid.
[6] Ibid. , esta observação é de Headrick.
[7] Heidi Tworek, News from Germany: The Competition to Control World Communications, 1900-1945 (New York: Harvard Historical Studies, 2019).
[8] Daniel R. Headrick. *The Invisible Weapon*.Headrick, *The Invisible Weapon*.
[9] "NH 79949 – Operação de Corte de Cabos em Cienfuegos, 11 de maio de 1898", Biblioteca Online do Centro Histórico Naval , https://www.history.navy.mil/content/history/nhhc/our-collections/photography/us-people/b/baker-benjamin-f/nh-79949.html.
[10] Ibid., chapter 5. Ibid., capítulo 5.
[11] Jonathan Winkler, "Information Warfare in World War I," The Journal of Military History 73, no. 3 (2009): 845–67, https://doi.org/10.1353/jmh.0.0324.
[12] Cameron McR. Winslow, "Cable-Cutting at Cienfuegos," The Century Illustrated Monthly Magazine 57 (1899): 708-717, https://books.google.com/books?id=Y7fPAAAAMAAJ&pg=PA708#v=onepage&q&f=false.
[13] Jonathan Winkler, "Silencing the Enemy: Cable-Cutting in the Spanish–American War," War on the Rocks, 6 de novembro de 2015, https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/; Rebecca Raines, "Manifesting Its Destiny: The U.S. Army Signal Corps in the Spanish-American War," Army History 46 (1998): 14–21, https://www.jstor.org/stable/26304991.
[14] Jonathan Winkler, "Silencing the Enemy."
[15] "Spanish American War: Telegraphy and Cable Cutting, Introductory Essay". Naval History and Heritage Command. https://www.history.navy.mil/research/publications/documentary-histories/united-states-navy-s/telegraphy-and-cable.html.
[16] Jonathan Winkler, "Silencing the Enemy."
[17] Biblioteca do Congresso, Coleção George Grantham Bain, https://www.loc.gov/pictures/item/2014683102/.
[18] Embora, como observa Heidi Tworek, seu papel seja com frequência exagerado no desenvolvimento dessa tecnologia. *Heidi Tworek, News from Germany.*
[19] Marc Raboy, "The First Company That Wanted to 'Connect the World' Wasn't Google or Facebook," Media@LSE, August 24, 2016, https://blogs.lse.ac.uk/medialse/2016/08/24/the-first-company-that-wanted-to-connect-the-world-wasnt-google-or-facebook/.
[20] Heidi Tworek, News from Germany, 12–13.
[21] Michael Friedewald, "Telefunken vs. Marconi, or the Race for Wireless Telegraphy at Sea, 1896-1914," SSRN (9 de janeiro de 2014): https://doi.org/10.2139/ssrn.2375755.
[22] Ibid.
[23] Marc Raboy, Marconi: The Man Who Networked the World (Oxford, U.K.: Oxford University Press, 2016), 226–28.
[24] Por exemplo, a Telefunken aturou mesmo em áreas onde a Alemanha não tinha uma grande presença colonial, como a América Latina.
[25] George Johnson, ed., *The All Red Line: The Annals and Aims of the Pacific Cable Project* (Ottawa: James Hope and Sons, 1903), 10, no Internet Archive, https://archive.org/details/allredlineannals00johnuoft/page/n11/mode/2up.
[26] Gordon Corera, "How Britain Pioneered Cable-Cutting in World War One," BBC News, 15 de dezembro de 2017, https://www.bbc.com/news/world-europe-42367551.
[27] Jonathan Winkler, "Information Warfare in World War I," 847.
[28] P. M. Kennedy, "Imperial Cable Communications and Strategy, 1870-1914," The English Historical Review 86, no. 341 (1971): 728–52, https://www.jstor.org/stable/563928.
[29] Jonathan Winkler, "Information Warfare in World War I," 849.
[30] Ibid., 851.
[31] Gordon Corera, "Why Was the Zimmermann Telegram so Important?," BBC News, 17 de janeiro de 2017, https://www.bbc.com/news/uk-38581861; Patrick Beesly, Room 40: British Naval Intelligence 1914-18 (San Diego: Harcourt Brace Jovanovich, 1982).

[32] C. O. Nordensvan e Valdemar Langlet. *Det stora världskriget* [A Grande Guerra Mundial] (1915), em Wikimedia Commons: https://commons.wikimedia.org/wiki/File:German_WW_I_field_telegraph_002.jpg.
[33] Jonathan Winkler, "Information Warfare in World War I."
[34] Wilhelm Flicke, "The Beginnings of Radio Intercept in World War I: A Brief History by a German Intelligence Officer," NSA Cryptologic Spectrum Articles 8, no. 2 (1978): 21, https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/.
[35] Bruce Norman, Secret Warfare: The Battle of Codes and Ciphers (Newton Abbot, U.K.: David & Charles Ltd, 1973); Prit Buttar, Collision of Empires: The War on the Eastern Front in 1914 (Oxford, U.K.: Osprey Publishing, 2014).
[36] Matt Crypto. "The rotors of a Lorenz SZ42 cipher machine on display at Bletchley Park museum", na Wikimedia Commons: https://commons.wikimedia.org/wiki/File:SZ42-6-wheels.jpg.
[37] George I. Beck, "Military Communication - The Advent of Electrical Signaling," Britannica, https://www.britannica.com/technology/military-communication.
[38] Harry Hinsley, "The Influence of ULTRA in the Second World War" (lecture, Cambridge, U.K., October 19, 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.
[39] 1×10^{170} configurações possíveis.
[40] "Bletchley Park Remembers Polish Code Breakers," BBC News, 14 de julho de 2011, https://www.bbc.com/news/uk-england-beds-bucks-herts-14141406.
[41] Gordon Welchman, The Hut Six Story: Breaking the Enigma Codes (Cleobury Mortimer, U.K.: Classic Crypto Books, 1997).
[42] Harry Hinsley, "The Influence of ULTRA."
[43] Ibid.
[44] Jerry Roberts, Lorenz: Breaking Hitler's Top Secret Code at Bletchley Park (Cheltenham, U.K.: History Press, 2017).
[45] F. W. Winterbotham, The Ultra Secret (New York: Harper & Row, 1974), 154, 191.
[46] Harry Hinsley, "The Influence of ULTRA."
[47] Calder Walton, "The Spies Who Came In From the Continent," Foreign Policy, 27 de abril 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.
[48] U.S. Navy, em Wikimedia Commons, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.
[49] Anna Borshchevskaya, "The Soviets' Unbreakable Code," Foreign Policy, 27 de abril de 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.
[50] Daniel R. Headrick, The Invisible Weapon, capítulo 4.
[51] Sherry Sontag, Christopher Drew, and Annette Lawrence Drew, Blind Man's Bluff: The Untold Story of American Submarine Espionage (New York: Public Affairs, 1998), 222.
[52] Ibid.
[53] Ibid., 223.
[54] Ibid.
[55] Matt Blitz, "Navy Divers and Their Daredevil Mission to Spy on the Soviet Union at the Bottom of the Sea," Popular Mechanics, 30 de março, 2017, https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping/.
[56] Michael J. Sulick, American Spies: Espionage Against the United States from the Cold War to the Present (Washington, DC: Georgetown University Press, 2013), 109–14; Matt Blitz, "Navy Divers."
[57] Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC News,27 de abril de 2017, https://www.bbc.com/news/39655415; Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare Perspective," (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008), https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.
[58] David Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, 6 de janeiro de 2011, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008; Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war," Security Dialogue 43, no. 1 (2012): 3–24, https://journals.sagepub.com/doi/10.1177/0967010611431079.

[59] Pavel Polityuk and Jim Finkle, “Ukraine Says Communications Hit, MPs Phones Blocked,” Reuters, 4 de março de 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304; Sergey Sukhankin, “Russian Electronic Warfare in Ukraine: Between Real and Imaginable,” Jamestown Foundation, 24 de maio de 2017, https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/.

[60] Andy Greenberg, “How an Entire Nation Became Russia’s Test Lab for Cyberwar,” Wired, 20 de junho de 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” U.S. Department of Justice, October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[61] Constanze Stelzenmüller, “The impact of Russian interference on Germany’s 2017 elections,” (congressional testimony, 8 de junho de 2017), https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

[62] Maggie Miller. "US intel agencies blame Russia for massive SolarWinds hack". *The Hill,* 5 de janeiro de 2021: https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack.

[63] “Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain,” Council on Foreign Relations, https://www.cfr.org/cyber-operations/titan-rain.

[64] Garrett Graff, “China’s Hacking Spree Will Have a Decades-Long Fallout,” *Wired*, February 11, 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/. Garrett Graff. "China’s Hacking Spree Will Have a Decades-Long Fallout". *Wired*, 11 de fevereiro de 2020: https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

[65] Chun Han Wong. "China Launches Initiative to Set Global Data-Security Roles". *The Wall Street Journal,* 8 de setembro de 2020: https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

[66] Bojan Pancevski, “U.S. Officials Say Huawei Can Covertly Access Telecom Networks,” The Wall Street Journal, 12 de fevereiro de 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

[67] Joe Parkinson, Nicholas Bariyo, and Josh Chin, “Huawei Technicians Helped African Governments Spy on Political Opponents,” The Wall Street Journal, 15 de agosto de 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[68] William Turton, “Hidden Back Door Embedded in Chinese Tax Software, Firm Says,” Bloomberg, 25 de junho de 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.