Huawei đương đầu với lịch sử: Các cường quốc và rủi ro về viễn thông, 1840-2021

Rush Doshi và Kevin McGuess

Brookings Institution, tháng 3 năm 2021

Tóm tắt chung

Vào cuối năm 2018, trước những lo ngại của người Mỹ về việc liệu Canada có chào đón Huawei vào mạng lưới viễn thông của mình hay không, Thủ tướng Canada Justin Trudeau đã đưa ra một loạt các tuyên bố về quan điểm chung của nhiều nước trên thế giới. Vào thời điểm đó, ông tuyên bố: "Đó không phải là một quyết định có tính chính trị" và Canada sẽ không "để chính trị can thiệp vào quyết định" về vai trò của Huawei trong mạng lưới của mình.[1]

Khái niệm về chính trị quyền lực có thể nằm ngoài những vấn đề viễn thông không chỉ lạc quan mà còn không tuân theo lịch sử ngành viễn thông. Báo cáo này khám phá lịch sử đó và cho biết quyền lực và viễn thông gần như luôn liên kết chặt chẽ với nhau như thế nào. Khi các quốc gia bỏ qua những mối liên kết đó và ung dung trước sự an toàn của mạng lưới của chính các quốc gia đó, hậu quả gây ra là bất lợi và đôi khi còn là thảm họa.

Báo cáo này nghiên cứu một số trường hợp chính về sự cạnh tranh giữa các cường quốc trong các hoạt động viễn thông kể từ thời điểm sơ khai của ngành viễn thông điện trong những năm 1840. Các trường hợp này cho thấy nhiều vấn đề mà các nhà hoạch định chính sách phải đối mặt thời nay rất tương tự với những vấn đề trong quá khứ. Mặc dù cuộc tranh luận hiện tại về an ninh mạng và cơ sở hạ tầng 5G dường như là mới mẻ nhưng thực tế là lặp lại những tranh chấp bị quên lãng từ thời sơ khai của ngành viễn thông điện cách đây khoảng 150 năm. Hơn nữa, nhiều yếu tố quen thuộc trong cuộc cạnh tranh viễn thông ngày nay, chẳng hạn như việc sử dụng các cơ quan thiết lập tiêu chuẩn, trợ cấp của chính quyền, các dây cáp, chiến tranh thông tin, thị trường ở các nước đang phát triển, và mã hóa để đạt được lợi thế, được phát triển cách đây hơn một thế kỷ, cho thấy những bài học quan trọng cho cuộc tranh luận hiện tại.

Sau đây là danh sách các bài học then chốt:

1. **Kiểm soát mạng viễn thông toàn cầu là một hình thức quyền lực chính trị.** Các mạng 5G được kỳ vọng hình thành nên nền tảng của nền kinh tế thông minh hơn, có tính kết nối liên kết với vô số thiết bị và cảm biến với nhau. Với mong muốn xây dựng những mạng lưới này trên toàn thế giới, Trung Quốc đã trợ cấp cho các công ty và dự án lớn về 5G trên toàn thế giới, là một phần của sáng kiến "Con đường tơ lụa kỹ thuật số". Nỗ lực đó tương tự như việc theo đuổi sự thống lĩnh về mạng lưới của Anh vào lúc sơ khai của hệ thống điện tín. Nước Anh đã xây dựng lợi thế của mình trong hơn sáu thập kỷ bằng cách gia tăng đều sự lệ thuộc của các quốc gia khác vào mạng lưới của minh, thậm chí là bỏ cả chi phí và lợi ích kinh tế để lôi kéo họ chạy cáp thông qua nước Anh, đồng thời giảm sự phụ thuộc của Anh vào mạng lưới nước ngoài. Cuối cùng, hệ thống này đã kiểm soát hơn một nửa lưu lượng cáp trên thế giới, mạng lưới bộ đàm lớn nhất và đội tàu đặt cáp lớn nhất. "Quyền quản lý thông tin" của Anh cho phép nước này loại bỏ nước Đức khỏi hầu hết tất cả các hoạt động viễn thông toàn cầu trong Thế chiến I và buộc Berlin định tuyến lưu lượng về những đường dây thuộc sở hữu của Anh do người Anh giám sát, sau này chứng minh là yếu tố quyết định về sự thất bại của nước Đức trong cuộc xung đột.

2. **Thời gian dài yên ổn và thịnh vượng thường dẫn đến tự mãn về những rủi ro trong viễn thông.** Trong 30 năm qua, cùng với quá trình toàn cầu hóa kinh tế và hòa bình sau chiến tranh lạnh là sự tiến bộ nhanh chóng của các ngành viễn thông, khiến các quốc gia ưu tiên những lợi ích thương mại mang tính cách mạng hơn so với rủi ro chính trị và bảo mật, bao gồm cả quyền sở hữu nước ngoài hoặc vận hành mạng. Một diễn biến tương tự lúc sơ khai của các hoạt động viễn thông vào những năm 1840, cũng trùng với thời kỳ tương đối yên ổn và quá trình toàn cầu hóa kéo dài cho đến Thế chiến I. Trong phần lớn thời kỳ đó, mong muốn nắm bắt tiềm năng thương mại kỳ diệu của công nghệ liên lạc mới này đã làm mờ đi những vấn đề liên quan đến việc phụ thuộc vào mạng hoặc công ty nước ngoài. Nước Anh được hưởng lợi từ sự tự mãn của những nước khác bằng cách xây dựng, sau đó khai thác vị trí đầu mối không thể phủ nhận trong mạng lưới toàn cầu, với hầu hết các cường quốc khác phụ thuộc vào mạng lưới của họ.

3. **Khi các quốc gia tự mãn về hệ thống bảo mật viễn thông của mình thì có thể dẫn đến tai họa và định hình lại nền chính trị thế giới.** Nhiều thập kỷ tự mãn của Đức về sự phụ thuộc của nước này vào các tuyến viễn thông của Anh nghĩa là vào lúc Berlin hồi tỉnh với nguy cơ của sự phụ thuộc đó thì đã quá muộn để có thể thay đổi được tình hình. Khi Thế chiến I bùng nổ, nước Anh cắt đứt tất cả các dây cáp của Đức và buộc Berlin phải truyền dữ liệu qua các mạng của Anh bất chấp nguy cơ bị nghe lén, dẫn đến việc tiết lộ "bức điện tín Zimmerman", giúp đưa Hoa Kỳ vào tham chiến. Tương tự, hành động vô kỷ luật của người Nga trong những lần truyền phát vô tuyến không dây trong Thế chiến I giúp người Đức nghe lén những lần trao đổi, "nhìn thấy" sự di chuyển của quân đội Nga theo thời gian thực, và đánh bại Nga trong trận quyết định tại Trận chiến Tannenberg. Sau đó, trong Thế chiến II, Đức quốc xã quá tin tưởng vào mật mã của mình nên ít khi cập nhật mật mã, giúp nước Anh giải các mật mã và thu thập thông tin tình báo được cho là giúp rút ngắn cuộc chiến này từ hai đến bốn năm. Với sức mạnh của thông tin, ngay cả những lần đôi khi vô kỷ luật hoặc tự mãn về tín hiệu truyền cũng có thể làm thay đổi lịch sử.

4. **Công nghệ mới luôn tạo ra những nỗ lực mới nhằm chặn đứng nó.** Sự nổi lên của cáp ngầm dưới biển làm dấy lên nỗ lực cắt và nghe lén những đường dây này ngay từ thời Chiến tranh Tây Ban Nha-Hoa Kỳ; đường truyền sóng vô tuyến khiến đối thủ càng nỗ lực thu thập các nút mạng và nghe lén việc truyền tin; và sự nổi lên của các mã phức tạp để mã hóa làm dấy lên nỗ lực theo quy mô ngành nhằm giải các mã này. Trong mỗi kỷ nguyên, một số người cho rằng bước tiến bộ mới trong lĩnh vực liên lạc có thể ít bị tấn công hơn so với trước đó. Tuy nhiên, chu kỳ đổi mới và khai thác vẫn tiếp tục sau mỗi lần như vậy.

5. **Mạng viễn thông chưa bao giờ trung lập về mặt chính trị, đặc biệt là vào thời điểm căng thẳng.** Vào năm 2019, các giám đốc điều hành của Huawei cam kết "không cửa sau, không gián điệp" và hứa rằng công ty của họ sẽ không dính líu đến các hoạt động chính trị và chính phủ Trung Quốc cam kết tôn trọng điều này. Nhưng thậm chí hơn một thế kỷ trước, các công ty viễn thông và chính phủ ở nước họ đã công khai đưa ra những lời hứa tương tự nhưng lại bí mật phá vỡ lời hứa đó và cùng nhau hợp tác trong cả thời bình và thời chiến. Ví dụ, sự thống lĩnh của nước Anh trong cáp dưới biển dẫn đến việc người Pháp, Đức và người Mỹ ủng hộ việc giữ đường dây này trung lập, ngay cả trong lúc chiến tranh. Các công ty Anh công khai tuyên bố sự trung lập của họ nhưng thực tế lại phục vụ cho các lợi ích chính trị của Anh, đặc biệt là vào những thời điểm diễn ra căng thẳng lớn, và từ bỏ hoàn toàn thái độ trung lập trong suốt thời kỳ chiến tranh. Nói chung, quyền lực bắt nguồn từ việc phá vỡ hoặc nghe lén luồng thông tin của đối thủ quá hấp dẫn nên khó có thể giữ vững tuyên bố trung lập.

6. **Các quốc gia thường tìm kiếm những công ty viễn thông lớn của riêng mình sau khi họ nhận ra khả năng dễ bị tấn công do phải phụ thuộc vào đối thủ cạnh tranh hoặc công ty của đối thủ cạnh tranh.** Hoa Kỳ hiện đang thiếu công ty sản xuất lớn về trạm cơ sở 5G, từ đó dấy lên cuộc tranh luận về việc họ có nên đầu tư vào công ty của mình hay không hay dựa vào các công ty liên kết. Việc này cũng thúc đẩy bất đồng về mức độ Huawei thực tế là công ty lớn của chính phủ. Những cuộc tranh luận này có một vài tiền lệ. Vào đầu thế kỷ 20, nhiều quốc gia dựa vào các nước khác về thiết bị hoặc mạng viễn thông bắt đầu xây dựng hệ thống của riêng mình. Ví dụ, Đức đã thúc đẩy hai công ty Đức cạnh tranh với nhau để phát triển vô tuyến là Siemens & Halske và AEG để thiết lập giải pháp thay thế của nước Đức thay cho vị thế thống trị của người Anh trong lĩnh vực vô tuyến. Nhiều công ty được lớn khác được chính phủ chống lưng liền với các chính phủ hỗ trợ họ, mặc dù bề ngoài là công ty tư nhân.

7. **Cuộc đấu tranh cho các tiêu chuẩn viễn thông có thể xác định quốc gia nào sẽ có quyền lực mạng và điều này thường yêu cầu giành được các đồng minh và đối tác tham gia.** Các quốc gia nơi công nghệ trở thành tiêu chuẩn chi phối có thể tận dụng ảnh hưởng đó lên các nước khác. Theo cách này, cuộc cạnh tranh hiện tại về các tiêu chuẩn công nghệ truyền thông thông tin cũng tương tự như cuộc cạnh tranh của người Anh-Đức về mạng vô tuyến. Nước Anh, thông qua Công ty Marconi mà Anh hỗ trợ, chiếm ảnh hưởng chi phối trong lĩnh vực vô tuyến không dây đến nỗi tất cả các cường quốc khác đều phải truyền tin qua mạng không dây của Anh, mạng này cũng từ chối liên kết với bất kỳ trạm không dây nào khác. Cuối cùng, nước Đức đã thành công trong việc phá vỡ sự thống trị đó với một cơ quan thiết lập tiêu chuẩn nghiêm cấm chính sách "không liên lạc với nhau" này với sự giúp đỡ của các quốc gia khác, bao gồm Hoa Kỳ và Pháp - một minh chứng cho thấy các quốc gia theo chủ nghĩa tự do thời nay có thể sử dụng các phương pháp liên minh tương tự như thế nào để thiết lập hoặc giữ lại các tiêu chuẩn công nghệ thông tin và truyền thông (ICT) có lợi nếu họ phối hợp cùng nhau.

8. **Các quốc gia chuyển sang sử dụng mã hóa khi việc liên lạc của họ dễ bị nghe lén hơn nhưng mã hóa thường có giới hạn do lỗi người dùng hoặc do đối thủ cố tình xâm phạm.** Một số quốc gia tranh luận rằng cần bớt lo lắng hơn về vai trò của Huawei trong mạng hoặc về lỗ hổng chung của các thiết bị kết nối với Internet bằng mã hóa hiện đại. Những cuộc tranh luận kiểu như thế đã xảy ra nhiều trong lịch sử. Vào lúc sơ khai của ngành viễn thông cách đây một thế kỷ, khả năng các thông điệp bằng điện tín có thể bị những người khác kiểm soát các nút mạng đọc được hoặc vô tuyến có thể bị nghe lén bởi thiết bị nghe thụ động, giúp thúc đẩy những tiến bộ lớn về mã hóa, thường xuyên làm nảy sinh sự tự tin quá mức. Các máy tạo mật mã phức tạp có rotor của Đức được cho là không thể xâm phạm nhưng lỗi người dùng và những nỗ lực ở quy mô lớn của Anh cho phép nước Anh xâm nhập được mã của người Đức. Các bản cập nhật chi phí thấp cho thiết bị và mật mã của người Đức có thể đã chấm dứt lợi thế của nước Anh nhưng sự tự tin quá mức của Berlin trong việc mã hóa đã đón đầu cho những thay đổi này, từ đó xuất hiện tin tức tình báo bị nghe lén đã định hình lại cục diện của cuộc chiến. Khả năng mã hóa từ đầu đến cuối tiến bộ đáng kể so với những nỗ lực trước đây trong việc mã hóa nhưng lịch sử cho thấy cần phải có một chút khiêm tốn.

9. **Nhiều chính phủ giảm xuống mức độ đối thủ có thể nỗ lực hết sức để xâm phạm mạng lưới của họ.** Trong những cuộc tranh luận về viễn thông hiện đại, điều đáng lưu ý là các quốc gia ưu tiên sự thuận tiện hoặc thương mại, do đó họ thực hiện lối tắt bảo mật, điều này thường gây bất ngờ khó chịu cho đối thủ quyết tâm xâm phạm đến mạng của họ. Trong Thế chiến I, Đức ngạc nhiên bởi tốc độ và sự nhẫn tâm khi Anh đã cắt tất cả các dây cáp Đức dùng để tiếp cận thế giới bên ngoài; tương tự, các nhà lãnh đạo Nga cũng ngạc nhiên khi hành động vô kỷ luật về vô tuyến của họ dẫn đến một thất bại thảm hoạ ở Tannenberg. Trong Thế chiến II, Đức không nghĩ là Anh xây dựng một hoạt động phá mã quy mô lớn và tập trung có thể khai thác các lỗi trong liên lạc của người Đức, dù là không đáng kể hay thoáng qua, để giải các mã của Đức. Và trong thời gian Chiến tranh lạnh, chính quyền Xô Viết chưa bao giờ mã hóa một đường dây điện thoại dưới nước nội bộ mà họ tin là nằm ngoài tầm với của Hoa Kỳ nhưng Washington cũng tìm ra cách để nghe lén qua kênh này, lấy được nguồn thông tin vô giá.

10. **Bảo mật mạng không chỉ là về việc nghe lén, mà còn là từ chối hòa mạng.** Một số cuộc tranh luận về vai trò của Huawei trong mạng lưới nhấn mạnh vấn đề bảo mật dữ liệu nhưng có thể được lợi ích từ việc cân nhắc nhiều hơn khi từ chối hòa mạng, vốn là một phần quan trọng trong cuộc cạnh tranh viễn thông của các cường quốc. Vào thời sơ khai của điện tín, có những cường quốc tìm cách cắt dây cáp và từ chối các cuộc liên lạc, dẫn đến việc nước Anh thực hiện hoạt động chưa từng có tiền lệ và đã được lên kế hoạch tốt là cắt tất cả các dây cáp trên toàn thế giới có thể kết nối Đức với bên ngoài. Đôi khi, một quốc gia có thể tự gây tổn hại khi theo đuổi các chiến lược từ chối hòa mạng và cũng sẽ tiếp tục chiến lược này nếu nước đó tin rằng đối thủ sẽ chịu thiệt hại lớn hơn.

Các cường quốc và ngành viễn thông

Lịch sử của ngành viễn thông ghi lại "Những đế chế lớn đã cố gắng hết sức để tăng tốc độ luồng thông tin". "Người La Mã xây đường, người Ba Tư và người Mông Cổ thiết lập các kíp ngựa, người Anh trợ cấp cho các tàu thư".[2] Mặc dù các quốc gia đều khao khát thông tin, luồng thông tin vẫn bị hạn chế cho đến lúc khởi đầu ngành điện tín hiện đại. Quá trình điện hóa luồng thông tin đã tạo ra ngành viễn thông hiện đại và cùng với đó là các kiểu hình cạnh tranh quen thuộc của các cường quốc về quá trình này.

Những thập kỷ đầu tiên của viễn thông hiện đại, kéo dài từ năm 1840 đến Thế chiến I, có cùng những đặc điểm quan trọng với thời điểm hiện tại. Thời kỳ đó, giống như thời kỳ sau Chiến tranh lạnh hiện tại, là thời kỳ yên bình tương đối của các cường quốc làm cho các quốc gia đứng đầu "ít nhạy cảm hơn" với các vấn đề về chính trị và bảo mật trong mạng viễn thông.[3] Khi những cường quốc xây dựng các mạng quốc gia và quốc tế trong thế kỷ 19, ban đầu nhiều nước sẵn lòng rời khỏi ngành mình kiểm soát, bỏ qua quốc tịch của các công ty tư nhân và đánh giá thấp rủi ro của việc kiểm soát mạng viễn thông của đối thủ. Lợi ích của những thay đổi mang tính cách mạng trong ngành viễn thông, một số thứ tại thời điểm được gọi là "sự hủy diệt thời gian và không gian"[4], rất rõ ràng và áp đảo đến mức "quyền sở hữu cáp được xem là một vấn đề nhỏ".[5] Ở thời kỳ đó, điện tín có tính kinh doanh nhiều hơn là chính trị, một nhà nghiên cứu lịch sử ghi lại trong một nhận xét rằng có thể dễ dàng có được thái độ phấn khích ban đầu về công nghệ thông tin hiện đại và hiện thân mới nhất của nó: 5G.[6]

Thời kỳ tự mãn của các cường quốc tương đối không kéo dài. Các quốc gia như Peru vào năm 1879, rồi Mỹ vào năm 1898, là một số trong những quốc gia đầu tiên cắt mạng viễn thông của đối thủ cạnh tranh. Khi căng thẳng giữa các cường quốc ngày càng gia tăng, các quốc gia trên khắp thế giới tỉnh ra rằng một số nước, cụ thể là Anh, đã quản lý tốt nền hòa bình lâu dài, và thông qua các công ty tư nhân của họ, đã kiểm soát chặt chẽ lĩnh vực truyền thông quốc tế.

Do ngày càng lo sợ về sự phụ thuộc vào mạng lưới cáp ngầm của Anh, các quốc gia như Pháp và Đức đã trợ cấp rất nhiều cho việc phát triển mạng riêng của họ trong một diễn tiến không khác với sự trợ cấp và bảo vệ của riêng Trung Quốc đối với những công ty lớn về công nghệ thông tin như Alibaba, Baidu, Tencent và Huawei. Như nhà nghiên cứu lịch sử Heidi Tworek đã ghi lại, các đối thủ của Anh cũng đã đặt nhiều kỳ vọng hơn vào thế hệ tiếp theo của lĩnh vực công nghệ viễn thông - "điện tín không dây", được biết đến với tên phổ biến hơn là vô tuyến - với hy vọng giảm phụ thuộc vào các dây điện tín ngầm thuộc sở hữu của người Anh.[7] Trong khi người Anh dẫn đầu về lĩnh vực này thì Đức lại từ chối dựa vào mạng lưới của Anh. Nước này đã xây dựng mạng lưới riêng của mình với các công ty lớn được sự hỗ trợ của chính phủ tập trung vào những nơi ít được kết nối hơn của thế giới như Châu Mỹ La Tinh, Châu Phi, Châu Á, những nơi mà hiện có thể phản ánh sự mở rộng của các công ty công nghệ Trung Quốc vào thế giới đang phát triển và quyết tâm của Bắc Kinh để đặt nền móng cho mạng 5G.

Trong suốt thời gian này, nhiều yếu tố của cuộc tranh viễn thông giữa các cường quốc đôi khi bị quên lãng thời nay thường được các quốc gia ở thời kỳ đó xem xét một cách nghiêm túc. Đức, nản lòng vì vị thế chi phối của Anh trong mạng lưới vô tuyến, đã sử dụng một cơ quan thiết lập tiêu chuẩn để phá vỡ vị thế chi phối của Anh, một chiến thuật chứng tỏ rằng những cơ quan này không kém phần quan trọng trong thời kỳ đó so với hiện nay. Và khi lĩnh vực viễn thông bắt đầu chuyển sang không dây và trở nên dễ nghe lén hơn nữa, các cường quốc đặt niềm tin của họ vào mã hóa, đôi khi bỏ qua hoạt động mạng có kỷ luật với giả định "mật mã" đó, các bước chi tiết để mã hóa hoặc giải mã thông điệp, sẽ giải quyết được vấn đề, điều hầu như luôn luôn được chứng minh là có sai sót do lỗi của người dùng. Quan điểm đó tồn tại song song nổi bật với các giả định hiện đại về tính không an toàn chung của mạng viễn thông và sự tin tưởng rõ ràng trong những cuộc tranh luận về Huawei rằng mã hóa sẽ làm vô hiệu hóa phần lớn nguy cơ Trung Quốc tiếp cận mạng viễn thông của một nước.

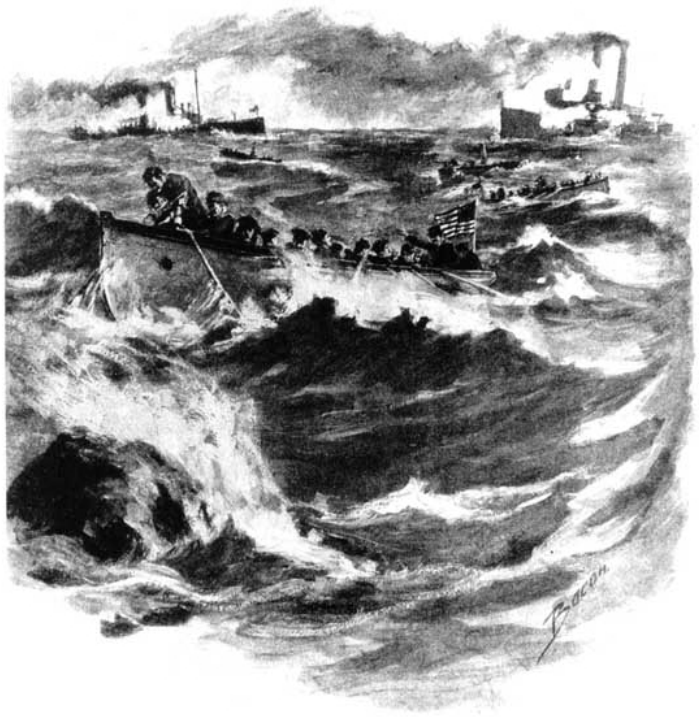
Khi nền hòa bình của các cường quốc kết thúc và chiến tranh bùng nổ, tầm quan trọng có tính chính trị của các hoạt động viễn thông, không phải lúc nào cũng rõ ràng trong thời gian hòa bình, đột nhiên hiển thị rõ. Thành công của người Đức trong việc nghe lén tín hiệu của người Nga trong Thế chiến I đã mang lại chiến thắng vang dội trong trận chiến Tannenberg làm thay đổi cục diện chiến tranh và giúp dồn nước Nga thoát khỏi cuộc xung đột. Vị thế chi phối của nước Anh về dây cáp dưới biển trong Thế chiến II áp đảo đến nỗi là nước này bỏ Đức khỏi hệ thống viễn thông toàn cầu, định tuyến cho lưu lượng cáp của người Đức qua mạng riêng của họ, sau đó là khám phá ra bức điện tín Zimmerman, giúp đưa nước Mỹ vào cuộc xung đột. Trong Thế chiến II, nước Anh đã đạt được một thành công khác về tin tức tình báo bằng cách phá mã của người Đức được cho là không thể xâm phạm, mang lại thông tin tình báo vô cùng quý giá giúp nước Anh rút ngắn lịch sử chính thức vì nhiều năm chiến tranh ở châu Âu. Những trường hợp này chứng minh rằng bảo mật viễn thông không chỉ đơn thuần là vấn đề chiến thuật trên chiến trường mà còn là cuộc cạnh tranh về chính trị, điều có thể quyết định số phận của các cường quốc và tình trạng lịch sử thế giới.

Khi thế giới chuyển sang cuộc Chiến tranh lạnh giữa Hoa Kỳ và Xô Viết, những lợi thế của người Anh không những bị suy yếu bởi cường quốc Hoa Kỳ mà còn do sự chuyển dịch công nghệ làm cho các mạng lưới cũ kỹ trở nên ít phù hợp hơn, cho thấy tầm quan trọng của các cường quốc để duy trì vị trí hàng đầu trong lĩnh vực công nghệ. Trong kỷ nguyên mới này, cuộc cạnh tranh về lĩnh vực viễn thông vẫn theo những lối quen thuộc. Ví dụ, Hoa Kỳ đã đi tiên phong với cách thức mới để nghe lén được những cáp ngầm chôn rất sâu và được xem là bảo mật đến nỗi những thông điệp truyền qua cáp này thường không được mã hóa. Sự cạnh tranh cũng tồn tại trong các lĩnh vực khác, chẳng hạn như vệ tinh và cơ sở hạ tầng internet, mặc dù phần lớn lịch sử của lĩnh vực này vẫn đang được viết lại, trong hầu hết các trường hợp, vẫn được xem là thông tin mật.

Như sê-ri tóm tắt về các trường hợp cho thấy, viễn thông luôn có tính chính trị. Việc khai thác những công nghệ và khả năng này thường phát triển cùng với sự phát triển của chúng. Ngay sau khi xuất hiện những phương thức giao tiếp mới, các cường quốc thường tìm cách chặn hoặc cản trở chúng. "Giao tiếp điện tử thường được mô tả như một trong những thành tựu lớn lao của nhân loại", một nhà nghiên cứu lịch sử ngành viễn thông ghi lại, "nhưng khi chúng ta nhìn lĩnh vực này từ quan điểm bảo mật, chúng ta thấy một bức tranh hoàn toàn khác biệt, vì bảo mật không phải là đặc điểm kỹ thuật mà là đặc điểm xã hội và chính trị". Và "vì chính trị chưa được cải thiện", ông ghi lại, "viễn thông cũng có mặt tối của nó".[8]

Bây giờ, chúng ta chuyển sang phần tóm tắt các chủ đề chính trong gần hai thế kỷ về cuộc cạnh tranh viễn thông.

1. Cuộc chiến Tây Ban Nha-Hoa Kỳ: Các giới hạn về tính trung lập của cáp



Mô tả về hành trình cắt cáp của Hoa Kỳ tại Cienfuegos được công bố vào năm 1907. Hoạt động này cho thấy rằng cáp điện tín dưới biển sẽ không được coi là trung lập trong cuộc xung đột vũ trang, ngay cả khi có một cường quốc vốn từng ủng hộ tính trung lập của cáp.

Nguồn: Thư viện Trực tuyến của Trung tâm Lịch sử Hải quân[9]

Khi dây cáp ngầm bắt đầu kéo chồng lên nhau khắp thế giới vào thế kỷ 19, một số cường quốc, bao gồm Pháp, Đức và Hoa Kỳ, kêu gọi tách biệt họ khỏi chính trị quốc tế. Năm 1858, trong một trong những cáp xuyên Đại Tây Dương đầu tiên được gửi đi, Tổng thống Hoa Kỳ James Buchanan đã kêu gọi Nữ hoàng Victoria đảm bảo rằng các đường dây điện tín mới của thế giới được giữ "mãi trung lập… kể cả khi có chiến sự".[10]

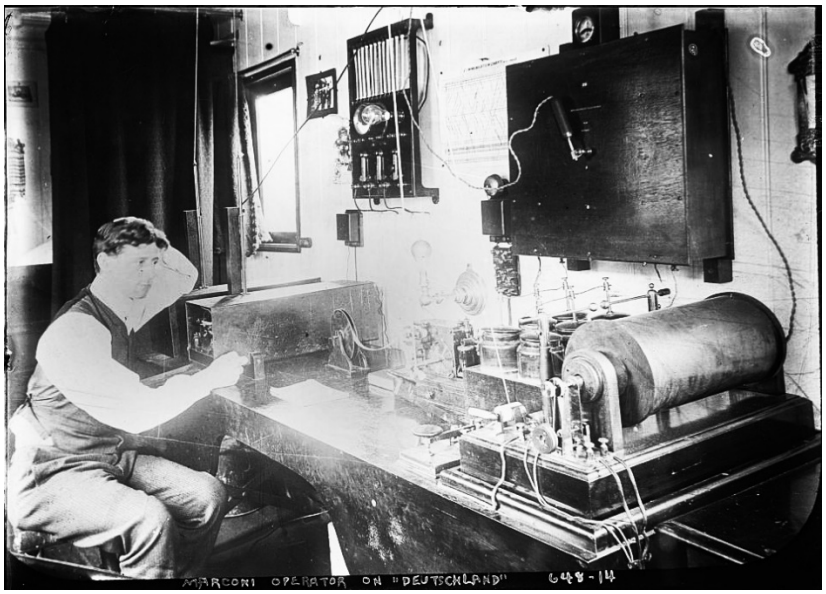
Tuy nhiên, sau khi chiến sự nổ ra, các nguyên tắc trung lập cao cả đã bị bỏ qua. Hai thập kỷ sau thông điệp của Buchanan, Peru cắt các đường dây cáp của Chile chạy vào vùng lãnh thổ đang tranh chấp.[11] Cuộc tranh chấp đó ít được chú ý, nhưng khi Hoa Kỳ, xưa kia là quốc gia đi đầu về cáp trung lập, cắt cáp cả ở Đại Tây Dương và Thái Bình Dương trong chiến tranh Tây Ban Nha-Mỹ, thế giới mới bắt đầu chú ý đến.

Hoạt động cắt cáp của Hoa Kỳ được lên kế hoạch trước khi xảy ra xung đột. Ở chiến trường Đại Tây Dương, Hoa Kỳ hy vọng loại bỏ Tây Ban Nha khỏi lực lượng của nước này ở Cuba. "Hẳn nhiên việc cô lập Havana có tầm quan trọng hàng đầu", một bài tường thuật trên tạp chí ở Hoa Kỳ tại thời điểm đó bình luận và yêu cầu Hoa Kỳ "tách Havana khỏi tất cả các phương thức liên lạc bằng điện tín với thế giới bên ngoài".[12] Hoa Kỳ bắt đầu bằng việc cắt giảm lưu lượng của Tây Ban Nha đi qua lãnh thổ Hoa Kỳ ở Florida. Sau đó, nước này đã gửi đi một đội quân nhỏ của Mỹ để phá hủy một nút viễn thông quan trọng ở Cienfuegos, cắt bỏ thành phố Havana và phần lớn miền tây Cuba khỏi Tây Ban Nha. Sau đó, Hoa Kỳ thực hiện tấn công vào nhiều dây cáp ở đông Cuba cũng như cáp vùng Caribbean nối Puerto Rico với Tây Ban Nha.[13] Từ đây, việc cắt cáp đã giảm đáng kể khả năng chỉ đạo và điều khiển lực lượng của Tây Ban Nha tại Cuba.[14]

Ở khu vực Thái bình Dương, Hoa Kỳ đã cắt cáp tàu ngầm duy nhất giữa Manila và Hồng Kông, tách Philippines khỏi Tây Ban Nha một cách hiệu quả.[15] Quyết định cũng gây tổn hại cho thông tin liên lạc của Hoa Kỳ, nhưng được cho là gây ra mức chi phí lớn hơn đối với Tây Ban Nha, và Hoa Kỳ có thể bù đắp bằng cách điều một tàu thường xuyên tới Hồng Kông để đánh điện tín về Washington.[16] Lực lượng Hoa Kỳ cũng cắt cáp ngầm dưới biển tại Philippines, càng làm giảm khả năng của Tây Ban Nha trong việc chỉ huy lực lượng.

Cuộc chiến Tây Ban Nha-Hoa Kỳ có lẽ là xung đột toàn cầu đầu tiên ở nhiều chiến trường, trong đó lĩnh vực viễn thông điện có tầm quan trọng lớn. Đây cũng là mốc đầu tiên mà một cường quốc tìm cách từ chối một cách tiếp cận khác với dây cáp dưới biển. Trước khi xảy ra xung đột, điện tín vẫn được xem là một lĩnh vực chủ yếu là thương mại và nhiều người hy vọng rằng dây cáp sẽ được tách biệt khỏi cuộc cạnh tranh chính trị và quân đội. Xung đột đã chứng minh được giới hạn của những quan điểm như vậy và cho thấy khả năng kiểm soát cơ sở hạ tầng viễn thông và khả năng phủ nhận những lợi thế đó trước các đối thủ địa chính trị luôn có tầm quan trọng lớn về mặt chính trị.

2. Sự đối đầu của Anh-Đức: Xây dựng mạng lưới và thiết lập tiêu chuẩn



Người vận hành vô tuyến của công ty Marconi trong "Phòng Marconi" của công ty tàu biển của Đức SS Deutschland. Ảnh hưởng của Công ty Marconi lớn đến mức nhân viên của họ hoạt động trong phòng vô tuyến của Đức mặc dù Đức có lo ngại về nguy cơ bị nghe lén và từ chối.

Nguồn: Thư viện Quốc Hội, Bộ sưu tập George Grantham Bain[17]

Thiết lập tiêu chuẩn công nghệ và hiệu ứng mạng kèm theo của công ty là phạm vi lâu đời và nhạy cảm có sự cạnh tranh giữa các cường quốc. Các quốc gia nơi công nghệ trở thành tiêu chuẩn chi phối có thể tận dụng lợi thế đó trước những đối thủ khác - một điều không bị mất đi trước những quốc gia mới nổi, thường nỗ lực giảm thiểu khả năng bị tấn công bằng cách tạo ra các hệ thống song song. Thực vậy, cuộc cạnh tranh giữa Trung-Mỹ hiện tại về lĩnh vực CNTT phản chiếu cuộc cạnh tranh kéo dài một thế kỷ giữa Đức và Anh để chiếm vai trò chi phối về cơ sở hạ tầng CNTT&TT ở kỷ nguyên đó, với những điểm tương đồng lạ kỳ và bài học quan trọng cho hiện tại.

Vào cuối thế kỷ 19, kỹ sư người ý Guglielmo Marconi được Hải quân Hoàng gia Anh Quốc hỗ trợ đã tạo ra hệ thống điện tín không dây.[18] Phát minh này có tính cách mạng. Mặc dù trước đây các cường quốc đã cắt cáp của nhau và trong khi giao tiếp từ tàu này sang tàu khác và giao tiếp từ tàu tới bờ trước đây rất khó khăn, nhưng hệ thống của Marconi đã giải quyết được những vấn đề này và ít bị gây nhiễu hơn.[19] Cuối cùng, Marconi hợp tác với Anh, giúp nước này chiếm vị thế độc quyền về truyền phát vô tuyến. Khi kết hợp với 60% thị phần thế giới về mạng lưới cáp ngầm dưới biển của Anh, nước Anh đã chi phối đường truyền quốc tế. Lợi thế của người Anh là mối lo của người Đức, nhưng cuộc cạnh tranh về công nghệ không dây cũng "mang đến cơ hội cho Đức thực hiện quyền kiểm soát cơ sở hạ tầng quốc tế mới" và "né tránh các dây cáp của Anh;" địa vị đứng đầu của cường quốc gắn liền với kết quả.[20]

Cảm thấy dễ bị tấn công, Hoàng đế Kaiser Wilhelm II đã phê duyệt hỗ trợ trực tiếp của chính phủ cho các nhà khoa học và kỹ sư Đức khi họ sao chép thành công thiết kế của Marconi, đã được cấp bằng sáng chế trong nước Đức, và xây dựng mạng lưới vô tuyến riêng của họ được hỗ trợ tài chính bằng các hợp đồng với quân đội Đức.[21] Thậm chí, lợi thế của người đi đầu và vô tuyến phạm vi dài hơn của Marconi cũng đã hình thành nên công ty có sự hỗ trợ của nước Anh làm tiêu chuẩn toàn cầu, và Marconi đã tận dụng hiệu ứng mạng này để theo đuổi chính sách "không liên lạc với nhau" với những công ty vận hành vô tuyến không phải của Marconi. Các doanh nghiệp và công ty tàu biển không muốn bị loại bỏ khỏi hệ thống liên lạc toàn cầu, nên họ ưu tiên hệ thống được nước Anh hỗ trợ hơn so với hệ thống nước Đức.

Hoàng đế Kaiser Wilhelm II đã tăng cường chính sách ở quy mô lớn của Đức để cạnh tranh với tiêu chuẩn của Anh. Ngài đã nhanh chóng ra lệnh cho hai công ty điện lực lớn của Đức đang cạnh tranh về mảng vô tuyến là Siemens & Halske và AEG, cùng nhau để thiết lập giải pháp thay thế tốt nhất của người Đức là Telefunken. "Cuộc cạnh tranh [nội địa] trong lĩnh vực điện tín không dây làm suy yếu tính cạnh tranh của Đức", Kaiser giải thích, "và cho Công ty Marconi cơ hội để đạt được vị thế độc quyền toàn cầu", "không thuộc mối quan tâm của Đức".[22] Dưới thời Hoàng đế Kaiser Wilhelm II, Đức đã tiếp tục chủ nghĩa bảo hộ bằng cách cấm các hệ thống Marconi trong một số trường hợp. Họ theo đuổi các thị trường mới nổi bằng cách bán công nghệ của mình cho Nam Mỹ và châu Phi để thiết lập tiêu chuẩn ở những khu vực đó và đảm bảo doanh thu.

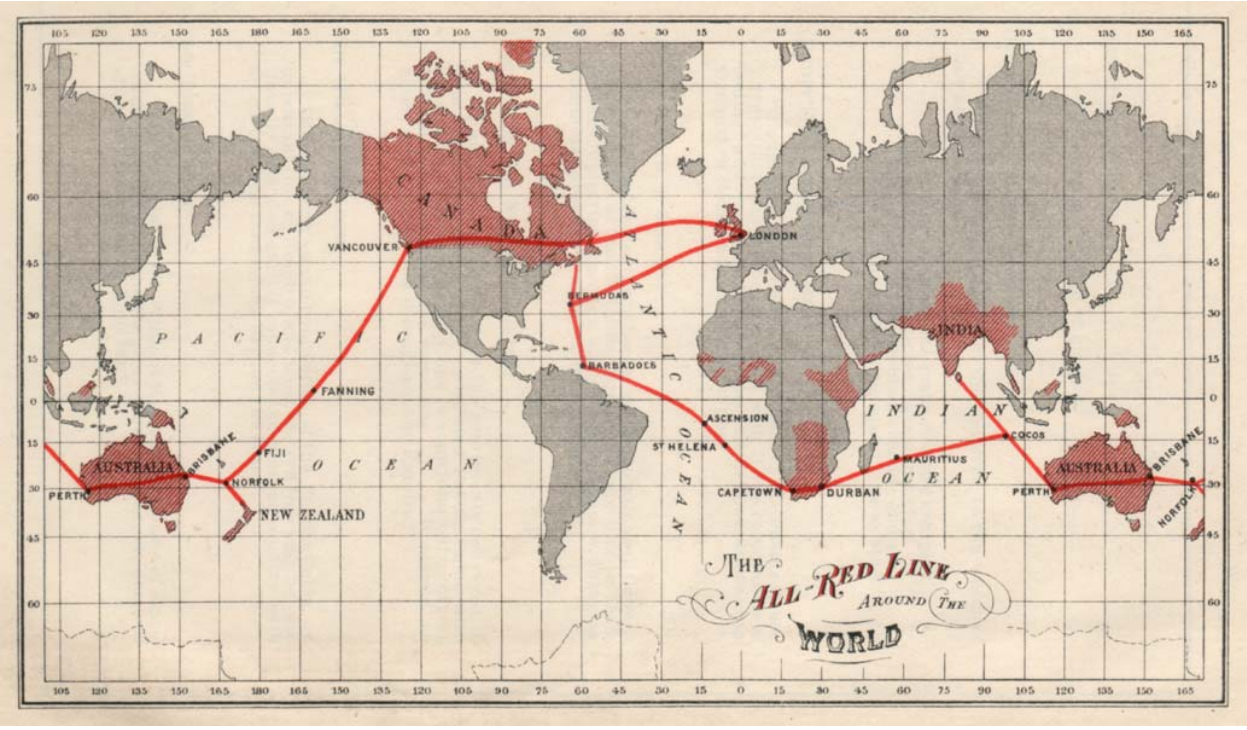
Khi những nỗ lực đó cho thấy là chưa đầy đủ, Đức đã thành công với các cơ quan thiết lập tiêu chuẩn đa phương. Năm 1906, Đức đã tập hợp những cường quốc trong Hội nghị Điện tín Vô tuyến Quốc tế đầu tiên, một hội nghị về các tiêu chuẩn vô tuyến. Ở đó, các thành viên này cùng cấm chính sách "không liên lạc với nhau" của Marconi, phá vỡ thế độc quyền của người Anh và thành lập chế độ độc quyền lưỡng cực Anh-Đức.[23]

Cuộc cạnh tranh Anh-Đức cho thấy các cơ quan thiết lập tiêu chuẩn có ý nghĩa chiến lược lớn. Ngày nay, Trung Quốc sử dụng nhiều kỹ thuật mà Đức đã sử dụng cách đây một thế kỷ - chính sách quy mô lớn đứng đầu là nhà nước, chính sách bảo hộ của nhà nước, vô số hợp đồng của nhà nước, hợp nhất quân sự dân sự, cấm các sản phẩm của đối thủ, sáp nhập cưỡng bức, theo đuổi thị trường mới nổi và thậm chí là các hiệp ước quốc tế để đặt ra các tiêu chuẩn của mình - tất cả những điều này đã giúp các công ty công nghệ Trung Quốc như Alibaba và Tencent, chủ sở hữu của WeChat và Alipay, trở thành những công ty hàng đầu của quốc gia. Kể từ đó, các công ty này đã mở rộng quy mô ra nước ngoài, thường không chỉ nhắm đến thị trường Hoa Kỳ, như công ty Telefunken của Đức trước đó, mà còn là những thị trường mới nổi có lợi nhuận thấp hơn và cạnh tranh ít hơn.[24]

Trung Quốc cũng đang đối mặt với các tiêu chuẩn cạnh tranh về cơ sở hạ tầng bắt buộc đối với kết nối internet. Chính phủ của họ đang đầu tư hàng tỷ đô la để các nhà sản xuất chip Trung Quốc có thể đánh bại các đối thủ Mỹ trong cuộc đua theo tiêu chuẩn internet di động 5G. Tương tự, các công ty Trung Quốc như Huawei và ZTE nhận được khoản cho vay từ chính phủ để xây dựng cơ sở hạ tầng bắt buộc về khả năng kết nối internet ở khắp các quốc gia đang phát triển. Như ví dụ của Anh cho thấy những nỗ lực này không chỉ khiến cho công nghệ Trung Quốc trở thành tiêu chuẩn mà còn mang đến cơ hội giám sát. Trong khi đó, Sáng kiến Vành đai và Con đường tạo ra khả năng cho Trung Quốc có thể thiết lập tiêu chuẩn cho "cơ sở hạ tầng thông minh" trên toàn châu Á, đặc biệt là các cảm biến và phần mềm liên quan và có thể từ chối khả năng tương tác với nhau của các công ty khác, từ đó không cho họ tham gia vào lĩnh vực phương tiện tự lái và các lĩnh vực khác.

Cuộc đối đầu của Anh-Đức trong lĩnh vực điện tín cho thấy Washington cần xem xét nghiêm túc thách thức từ Trung Quốc về các tiêu chuẩn. Điều này cũng mang đến một bước phát triển. Tương tự như vậy, Đức sử dụng các hội nghị quốc tế để phá vỡ thế độc quyền của Anh về điện tín, Hoa Kỳ có thể thiết lập hoặc giữ lại các tiêu chuẩn CNTT có lợi thông qua các thỏa thuận đa phương. Thực hiện được như vậy có thể giúp Trung Quốc tránh được việc thiết lập tiêu chuẩn đơn phương thông qua thỏa thuận thương mại tự do, các công ty lớn của nhà nước hoặc các dự án cơ sở hạ tầng.

3. Nước Anh trong Thế chiến I: Triển khai quyền độc chiếm thông tin



"All Red Line", một mạng lưới đường dây cáp dưới biển đắt đỏ của nước Anh được xây dựng rất nhiều và được bố trí sao cho không có bộ phận nào đi qua lãnh thổ của đối thủ. Khoản đầu tư không đủ của Đức vào mạng lưới viễn thông sôi động trên toàn cầu giúp nước Anh loại bỏ nước này khỏi hoạt động liên lạc trên toàn cầu trong khi nhìn chung Anh vẫn không bị ảnh hưởng.

Nguồn: George Johnson, hiệu đính, All Red Line: Biên niên sử và mục đích của dự án cáp Thái Bình Dương / Internet Archive[25]

Những nỗ lực của nước Đức nhằm phá vỡ vị thế chi phối của nước Anh trong lĩnh vực viễn thông vào đầu thế kỷ 20 không phải ra đời do hoang tưởng. Sau khi Thế chiến I nổ ra, nước Anh đã thành công trong việc tạo ra ảnh hưởng đáng kể lên mạng lưới viễn thông để định hình lại cục diện chiến tranh. Hệ thống này cắt dây cáp của nước Đức, theo dõi đường truyền tin của Đức và buộc lưu lượng của Đức đi vào các mạng do Anh điều khiển, giúp phát hiện bức điện tín Zimmerman giúp đưa nước Mỹ vào cùng tham chiến.[26]

Nước Anh không phải là cường quốc đầu tiên cắt hoặc điều khiển mạng viễn thông: Peru đã cắt đường dây liên kết Chile-Bolivia, Hoa Kỳ đã cắt cáp Tây Ban Nha, và nước Anh đã loại những người Phi gốc Hà Lan khỏi những người ủng hộ ở châu Âu trong một cuộc khủng hoảng và điều khiển lưu lượng cáp sang Pháp theo cách khác.[27] Nhưng những nỗ lực này lên đến đỉnh điểm trong Thế chiến I.

Nước Anh là nước đầu tiên cắt toàn bộ một nước khỏi mạng lưới viễn thông toàn cầu, triển khai một kế hoạch được lập tỉ mỉ trong thời gian hòa bình vào ngày đầu tiên của cuộc chiến.[28] Trong vòng một năm, nước Anh đã phá hủy các dây cáp của Đức trên toàn thế giới: Ở Eo biển Anh, Biển Bắc, Bắc Đại Tây Dương, Nam Mỹ, phần lớn châu Phi, Viễn Đông và thậm chí ở những quốc gia trung lập có cơ sở hạ tầng của nước Đức.[29]

Để bù đắp điều này, nước Đức đã cố mở rộng mạng lưới vô tuyến mà công ty Telefunken đã xây dựng một thập kỷ trước đó ở Mỹ La Tinh và "Phía Nam Bán cầu" để họ có thể bao phủ toàn thế giới. Trong một nỗ lực tương tự hiện đại trong Con đường tơ lụa kỹ thuật số của Trung Quốc, Berlin đã cho vay và đầu tư vào các chính phủ quan tâm đến "lợi ích phát triển của vô tuyến" để họ có thể quản lý các nút giao tiếp của Đức. Đáp lại, Anh Quốc đã thuyết phục hoặc xui khiến hầu hết các nước này từ bỏ ủng hộ cho các nút vô tuyến của Đức hay tích cực phá hoại chúng.[30]

Không có mạng lưới riêng, Berlin không có lựa chọn nào khác ngoài việc dựa vào mạng lưới của Anh trong suốt cuộc chiến. Ngay từ đầu, người Anh bắt đầu bí mật theo dõi tất cả các lưu lượng đi qua cáp của họ và sử dụng lợi thế để tiến hành cuộc chiến thông tin chống lại Đức, tiết lộ một cách có chọn lọc lượng thông tin rối loạn của người Đức nhằm gây tổn hại mối quan hệ của nước này với các quốc gia trung lập. Khi Đức gửi điện tín đề xuất liên minh quân sự với Mexico chống lại Hoa Kỳ, là bức điện tín Zimmerman tai tiếng, thông điệp này đã đi qua mạng của nước Anh và bị người Anh nghe lén và giải mã, sau đó chia sẻ thông tin này với chính phủ Hoa Kỳ, sau đó chính phủ lại chia sẻ với công chúng.[31] Sự cố đó đã đưa Hoa Kỳ tham chiến, định hình lịch sử thế giới, cuối cùng dẫn đến thất bại của người Đức.

Cuộc chiến thông tin của người Anh chống lại người Đức cho thấy những nguy hiểm của việc cho nước đối thủ có khả năng giám sát lưu lượng thông tin hoặc tách bỏ hoạt động tiếp cận thông tin viễn thông của một nước. Nó cũng cho thấy những mạng lưới mà các cường quốc không coi trọng trong thời bình thường bị chối bỏ trong thời chiến và cuộc chiến đấu giành lấy các nút liên lạc chắc chắn sẽ liên quan đến các bên thứ ba và các quốc gia trung lập.

4. Chiến thắng Đức tại Tannenberg: Sự nguy hiểm của việc nghe lén

Một trạm điện tín trường không dây của Đức trong Thế chiến I. Nga không thể mã hóa đầy đủ các thông tin liên lạc tại các trạm trường đã dẫn đến một thất bại thảm hại làm định hình lại cục diện chiến tranh.

Nguồn: C. O. Nordensvan và Valdemar Langlet, Det stora världskriget *[Thế chiến]*[32]

Đức không hoàn toàn thiếu khả năng trong cuộc chiến tranh thông tin. Nước này đã cắt bỏ các dây cáp trên mặt đất và dưới biển của Nga kết nối Nga với các đồng minh phương Tây, cũng như một số cáp vượt Đại Tây Đại mà người Anh sử dụng, đi tiên phong trong việc sử dụng tàu ngầm cho những công việc này.[33] Với vô số mạng lưới của Anh, những nỗ lực này cuối cùng cũng ít diễn ra hơn so với những người Đức đã hy vọng. Điều đã chứng minh có kết quả hơn nhiều là việc Đức sử dụng thông tin tình báo vô tuyến chống lại Nga trong Trận chiến Tannenberg vào tháng 8 năm 1914, tháng đầu tiên của chiến tranh, dẫn đến thất bại thảm họa cho người Nga. Một nhân viên tình báo người Đức vào thời điểm đó gọi sự cố đó là "sự kiện đầu tiên trong lịch sử loài người mà việc nghe lén lưu lượng vô tuyến của kẻ thù đã đóng vai trò quyết định".[34]

Trận chiến diễn ra trong bối cảnh Nga chiếm ưu thế ở mặt trận phía Đông. Khi Nga tiến sâu hơn vào Đông Prussia, quân đội của họ gặp phải một thách thức liên lạc đáng kể khiến giai đoạn này trở thành thất bại thảm họa. Quân Đức rút lui đã cắt đường dây điện tín của họ, và quân Nga tiến công thiếu nhân lực đủ trình độ chuyên môn để thiết lập liên lạc có dây xuyên suốt quá trình tấn công. Truyền vô tuyến là phương án thay thế nhưng trong khi người Nga áp dụng các công nghệ vô tuyến mới cho chức năng kiểm soát và chỉ huy quân sự, họ đã không bảo mật các công nghệ này đầy đủ. Các nhóm khác nhau đã được gán các mật mã khác nhau; hầu hết các nhóm đều không được đào tạo các tín hiệu mã hóa và giải mã; một số mã được người Anh biết đã bị phá mật mã; và sách mã hóa bị giới hạn hoặc không thể hiểu được đối với nhiều lính không biết chữ.[35] Kết quả là các vị lãnh đạo Nga cảm thấy họ phải chấp nhận rủi ro sử dụng các thông điệp vô tuyến không mã hóa và hy vọng người Đức không theo dõi họ một cách sát sao.

Tuy nhiên, người Đức đã theo dõi các tín hiệu này vô cùng sát sao. Sau khi quan sát thấy hành động vô kỷ luật về vô tuyến của người Nga trong cuộc chiến chống lại người Nhật, họ biết rằng những lần truyền tin không được mã hóa của Nga không phải là một phần của chiến dịch lừa đảo. Sau đó, họ sử dụng kiến thức của mình về liên lạc theo thời gian thực của Nga để nâng tầm "sương mù chiến tranh" và đánh bại một lượng lớn đội quân trong trận quyết định. Nước Nga mất toàn bộ quân đội, với hơn 100.000 người bị thương vong và 92.000 tù nhân so với 13.000 thương vong của Đức.

5. Nước Anh trong Thế chiến II: Giới hạn của mã hóa

Những rotor cơ học của máy mã hóa Lorenz được xem như không thể xâm phạm một cách hiệu quả trong Thế chiến II. Những nỗ lực của người Anh nhằm giải mật mã đã giúp các quan chức tiếp cận với những lần liên lạc của quan chức cấp cao Đức.

Nguồn: Matt Crypto / Wikimedia Commons[36]

Các phát minh của điện tín và vô tuyến không dây mang đến sự thuận tiện hơn, so với cáp vật lý, nhưng có nguy cơ bị nghe lén nhiều hơn. Trong Thế giới I và II, các cường quốc đã tồn tại trong thế giới mà ở đó hệ thống liên lạc bằng sóng vô tuyến được cho là có thể tiếp cận các quốc gia khác. Và trong một thế giới như vậy, không khác với giả định hiện tại về lỗ hổng của hệ thống viễn thông và máy tính hiện đại, mã hóa được xem là rất quan trọng đối với tính bảo mật. Như một nhà nghiên cứu lịch sử quân sự Mỹ đã nói rằng, kết quả là một "cuộc chiến giữa máy tạo mật mã và người phân tích mật mã".[37] Khi các cường quốc ở sai vị trí trong cuộc đấu tranh đó, kết quả gây ra có thể là thảm họa.

Để ngăn chặn kết quả như vậy, các tổ chức sẽ sử dụng mật mã để giảm rủi ro việc nghe lén sẽ ảnh hưởng đến tính bảo mật. Họ cũng áp dụng "kỷ luật vô tuyến" để ngăn kẻ thù thu thập thông tin chuyên sâu về mô hình sử dụng thông qua việc phân tích lưu lượng vô tuyến.

Hầu hết các cường quốc đầu tư thực sự lớn để nghiên cứu lưu lượng của đối thủ và, nếu có thể, giải các mật mã của đối thủ. Nước Anh chú trọng rất nhiều vào phân tích mật mã của đối thủ hơn so với Đức, với các phòng ban chức năng ở khắp các cơ quan. Và cũng giống như người Anh thành công trong thông tin tình báo và phân tích mật mã các tín hiệu đã định hình cục diện của Thế chiến I, họ cũng định hình cục diện của Thế chiến II khi nước Anh tại Bletchley Park thực hiện phá mật mã của máy Enigma và Lorenz của Đức.

Các hệ thống tạo mật mã của Enigma và Lorenz đã sử dụng máy tạo mã phức tạp đặc biệt có rotor để mã hóa thông điệp mà Đức cho rằng "sẽ không thể xâm nhập được".[38] Mỗi lần nhấn phím sẽ thay thế một ký tự bằng một ký tự khác dựa trên các cài đặt riêng cho máy và những cài đặt này, đối với hệ thống Lorenz, vượt quá tổng số nguyên tử trong vũ trụ, cần được người gửi và người nhận chia sẻ để đọc tin nhắn.[39] Enigma được quân đội, Mật vụ của Đức và các nhà ngoại giao sử dụng; Lorenz, thậm chí còn phức tạp hơn, được Adolf Hitler và các nhà lãnh đạo Đức quốc xã và quan chức cao cấp trong quân đội sử dụng để giao tiếp với nhau.

Sự thành công của người Anh với máy Enigma và Lorenz giải mã là sản phẩm của một số sự phát triển. Đầu tiên, đó là sản phẩm của sự hợp tác thông tin tình báo với Ba Lan, khai thác một số lỗi của người Đức để giải mã một số máy Enigma đơn giản hơn.[40] Như một nhà phân tích mật mã của Anh thời kỳ đó đã nói, nỗ lực của họ "sẽ không bao giờ thành công" nếu không có sự đóng góp của Ba Lan.[41]

Thứ hai, đó là sản phẩm của sự tự tin quá mức của người Đức, vì người Đức không bao giờ nghi ngờ những mật mã này sẽ bị giải mã, do đó không thực hiện những sửa đổi khá dễ dàng để buộc nước Anh phải bắt đầu lại từ đầu.[42] Thậm chí, một quan chức cao cấp của Bletchley Park kể lại, niềm tin của nước Đức về tình trạng không dễ bị xâm phạm của máy móc của họ "gần như luôn đúng".[43]

Cuối cùng, đó là sản phẩm của một sai sót duy nhất nhưng vô cùng lớn trong "kỷ luật vô tuyến" của nước Đức tạo ra một lỗ hổng để đảo ngược hệ thống tạo mật mã của kỹ sư Đức mặc dù chưa bao giờ trực tiếp thấy hệ thống nào.[44] Ngay cả những hệ thống phức tạp nhất cũng dễ bị tấn công do lỗi của người dùng và đối thủ cảnh giác cũng có thể lợi dụng hệ thống này.

Bằng cách giải mã các máy Enigma và Lorenz, người Anh có thể tiếp cận với một số thông tin liên lạc nhạy cảm nhất của người Đức. Mọi người cho rằng Thủ tướng Winston Churchill đã công nhận thông tin tình báo là lý do chính mà Anh Quốc đã giành chiến thắng trong trận chiến và Dwight D. Eisenhower đã gọi thông tin đó là thông tin "quyết định".[45] Nhà nghiên cứu lịch sử chính thức của Anh về thông tin tình báo của Anh, ông Francis Harry Hinsely, lập luận rằng những thành công này "rút ngắn cuộc chiến còn không quá hai năm và có lẽ là khoảng bốn năm", đánh bại Thống chế Erwin Rommel ở Châu Phi, thay đổi hoàn toàn những tổn thất về vận chuyển của đồng minh với các tàu ngầm quân sự của Đức, giúp đổ bộ vào Normandy.[46] Những thành công này cũng cho phép nước Anh xác định hầu như tất cả các gián điệp của nước Đức vào quốc gia này và thường biến họ hoặc sử dụng họ để gửi lại thông tin tình báo sai sót và người đứng đầu chương trình này lưu ý rằng thông tin tình báo của Anh "chủ động điều hành và kiểm soát hệ thống gián điệp của Đức tại quốc gia này".[47] Một vài quốc gia đã từng có sự hiểu biết sâu sắc về một quốc gia khác trong thời chiến.

Tóm lại, những thành công trong nỗ lực chống lại nước Đức của người Anh, với sự giám sát thời kỳ hòa bình của Ba Lan đối với hệ thống liên lạc của người Đức và quyết định chia sẻ thông tin đột phá của mình với Anh Quốc, mang lại những bài học có thể áp dụng cho ngày nay khi các cường quốc tiến hành dò thám mạng của nhau. Nói rộng hơn, những nước đưa ra đề nghị mã hóa sẽ giảm thiểu các vấn đề về khả năng truy cập mạng viễn thông của bên đối thủ có thể mắc lỗi không khác với lỗi mà chính người Đức từng mắc phải: sự tin tưởng quá mức vào công nghệ và ít chú ý đến khả năng hiện hữu về lỗi của con người.

6. Operation Ivy Bells: Chiều sâu của việc theo đuổi thông tin

USS Halibut, được cho rằng từng cố gắng nghe lén đường dây điện thoại dưới biển của Xô Viết.

Nguồn: Hải quân Hoa Kỳ / Wikimedia Commons[48]

Liên minh Xô Viết đã cẩn thận hơn nhiều với việc mã hóa so với Đức quốc xã, dựa trên phiên bản máy Enigma của họ, được gọi là Fialka, vốn phức tạp hơn rất nhiều.[49] Vì lý do đó, hàng loạt thông tin tình báo có tầm chiến lược thu thập được trong Thế chiến II sau khi những máy tạo mật mã của người Đức bị phá vỡ chưa từng có tiền lệ được biết đến công khai trong thời Chiến tranh lạnh. Với những thách thức này, các phương pháp thâm nhập hệ thống viễn thông của đối thủ khác đã được mở ra. Một trong những nỗ lực táo bạo nhất xảy ra liên quan đến dây cáp ngầm.

Thời điểm sơ khai của cáp dưới biển trong thế kỷ 19, cuối cùng dẫn đến những nỗ lực cắt và thỉnh thoảng là nghe lén những dây cáp này, thường ở vùng nước nông hơn hoặc trên đất liền nơi dễ thực hiện những nhiệm vụ này hơn. Ngược lại, việc thực hiện những hoạt động này trong vùng nước sâu được kiểm soát bởi kẻ thù được cho là không thể thực hiện được, đặc biệt là nếu phải thực hiện một cách bí mật. Đầu từ thế kỷ 20, người Anh và sau đó các cường quốc tiếp theo đi đến quyết định về bảo mật dây cáp dưới biển: nếu các vị trí đặt được bảo vệ và dây cáp không đi qua các quốc gia trung lập hoặc không thân thiện thì thông thường sẽ an toàn để không bị nghe lén và thường an toàn để không bị cắt, đặc biệt là trong thời bình.[50]

Tuy nhiên, trong thời kỳ Chiến tranh lạnh, phép tính đó đã thay đổi. Sự ra đời của tàu ngầm hạt nhân mở ra khả năng nghe lén các dây cáp dưới biển ở vùng nước sâu hơn. Nhưng nhiệm vụ đưa các thợ lặn để tiếp cận dây cáp ở đáy sâu được cho là giống với việc khám phá không gian hơn là những nỗ lực quen thuộc trong việc thực hiện xử lý cáp ở các thời đại trước. Việc cài đặt nghe lén có thể thực hiện được trong những điều kiện như vậy cũng rất khó khăn về mặt kỹ thuật.

Khi Hoa Kỳ nghi ngờ rằng cáp dưới biển của Liên Xô có thể chạy từ trụ sở hải quân ở Vladivostok đến một cơ sở trên tàu ngầm trên bán đảo Kamchatka, nước này tìm cách vượt qua những chướng ngại này, cho thấy giá trị của thông tin tình báo tín hiệu.[51] Họ cho rằng khi nghe lén với một cụm dây dẫn dài 5 inch sẽ cung cấp thông tin quan trọng về các lực lượng hạt nhân của Xô Viết.[52] Trong khi Xô Viết mã hóa tất cả các lượng thông tin được gửi qua vô tuyến, Hoa Kỳ kỳ vọng Xô Viết cho rằng lưu lượng thông tin mà cáp được bảo vệ dưới biển là thông tin gần như không thể truy cập và do đó sẽ không mã hóa. Hơn nữa, "các đô đốc và tướng quân của Xô Viết sẽ quá độc đoán và mất kiên nhẫn khi phải đối mặt với hàng loạt máy tạo mật mã vốn đã bị quá tải bởi hàng đống công việc" và đòi hỏi phải liên lạc bằng giọng nói không bảo mật.[53] Khi đó, việc nghe lén sẽ cung cấp một kho thông tin tình báo quý hiếm, và Hải quân Hoa Kỳ đã thực hiện chiến dịch Operation Ivy Bells để thực hiện điều này.

Phần lớn thông tin về việc nghe lén và thông tin tình báo được thu thập từ đó vẫn được giữ bí mật nhưng các nguồn mở cung cấp một số thông tin chi tiết về hoạt động độc đáo và sáng tạo. Hoa Kỳ đã phái một tàu ngầm hạt nhân, USS Halibut, để bí mật vượt qua hải quân Xô Viết và tìm cáp ngầm trong khu vực trải dài 600.000 dặm vuông.[54] Công nghệ cải tiến được tạo ra nhằm đảm bảo các thợ lặn có thể làm việc dưới áp suất tuyệt vời và trong nhiệt độ cực lạnh trong khoảng thời gian dài vài giờ. Tương tự, một số phương pháp mới được lập ra để thực hiện nghe lén trong môi trường đầy thách thức này.[55] Tất cả những việc này phải được thực hiện mà không bị quân Xô Viết phát hiện hay nghi ngờ. Nếu phát hiện thấy tàu thì quân Xô Viết có thể tấn công hoặc phá hủy nó.

Cuối cùng, hoạt động này đã được chứng minh là thành công và trong suốt những năm 1970, Hải quân Hoa Kỳ đã nghe lén và ghi lại các thông điệp không được bảo mật trên toàn bộ cáp. Cứ vài tháng một lần, các tàu ngầm Mỹ sẽ bí mật lẻn vào vùng nước của Xô Viết, tránh các tàu thủy tấn công, đưa thợ lặn xuống đường cáp nghe lén và truy xuất các băng liên lạc của quân Xô Viết, tạo ra lượng thông tin tình báo cực kỳ quý giá và hiếm có. Trong khi Hoa Kỳ mở rộng "mạng lưới vệ tinh, máy bay, trạm nghe lén và tàu ngầm gián điệp" để thu thập thông tin tình báo tín hiệu, nhưng nước này "lại không thể xâm nhập vào đường dây điện thoại có dây" trong lãnh thổ của đối thủ. Nỗ lực này cho thấy sự thay đổi tiến hóa trong lĩnh vực viễn thông, cụ thể là dữ liệu và tín hiệu được truyền qua bất kỳ phương tiện nào và bằng bất kỳ phương tiện nào cũng có thể được truy cập bởi một đối thủ quyết tâm với các công cụ thích hợp. Trong khi việc nghe lén này cuối cùng cũng được xử lý do sự rò rỉ thì những hình thức nghe lén qua phương tiện viễn thông mang lại đã cung cấp thông tin tình báo chính trị và quân sự vô giá cho Hoa Kỳ và các đồng minh của nước này.[56]

Cuộc cạnh tranh viễn thông hiện đại theo khía cạnh lịch sử

Khi kết thúc thời kỳ Chiến tranh lạnh, rõ ràng là Hoa Kỳ đã thay thế Vương quốc Anh với vai trò hàng đầu về thông tin. Hoa Kỳ vẫn duy trì vị trí nút thắt trên mạng lưới internet toàn cầu, khả năng không gian mạnh mẽ, vai trò thống lĩnh trong hầu hết công nghệ internet và khả năng tối tân để nghe lén hoặc có thể từ chối các thông tin liên lạc của đối thủ theo các công bố công khai.

Những lợi thế của người Mỹ hiện đang được kiểm tra, như nước Anh hơn một thế kỷ trước. Nga, đặc biệt là Trung Quốc, hiện đang thách thức vai trò thống lĩnh của Hoa Kỳ. Mặc dù Hoa Kỳ có vị trí nút thắt trong nhiều luồng dữ liệu, nhưng các cường quốc khác đang ngày càng tìm cách giảm sự phụ thuộc của họ vào mạng lưới Hoa Kỳ. Cùng lúc đó, vị trí nút thắt của người Mỹ ít cần thiết phải nghe lén hơn so với vị trí của Anh Quốc cách đây một thế kỷ. Internet có thể thực hiện xâm nhập mà không cần kiểm soát cơ sở hạ tầng vật lý. Điện thoại thông minh và mạng máy tính có thể bị tấn công, và liệu thông tin liên lạc nhạy cảm của một nước nào đó có bị xâm phạm do việc nghe lén vật lý của thời đại trước hay do xâm nhập trực tuyến của thời hiện đại hay không thì kết quả cuối cùng cũng vậy. Kết nối theo cách này có khả năng gây ra lỗ hổng lớn hơn so với thời đại của điện tín hoặc bộ đàm không dây.

Nga là quốc gia dẫn đầu trong việc khai thác lỗ hổng này. Vào năm 2007, Nga đã tung ra một làn sóng các cuộc tấn công mạng chống lại các tổ chức của người Estonia, chủ yếu là từ chối phân bổ các cuộc tấn công từ chối dịch vụ.[57] Vào năm 2008, nước này đã bắt đầu cuộc tấn công mạng trong cuộc chiến Nga-Georgia. Những hoạt động có liên quan này không chỉ nhằm vào việc từ chối các cuộc tấn công dịch vụ, mà còn là nỗ lực chuyển hướng các trang web của chính phủ, chiếm quyền máy chủ của chính phủ Georgia, và định tuyến lưu lượng truy cập internet của Georgia thông qua các máy chủ do người Nga kiểm soát, với một số cuộc tấn công diễn ra trước xung đột trùng với hành động quân sự của Nga.[58] Vào năm 2014, khi Nga xâm lược Crimea, họ kết hợp các cuộc tấn công mạng với kiểm soát mạng viễn thông vật lý. Lính Nga thu giữ các cơ sở viễn thông của Ukraina, sử dụng các cơ sở này để cắt đứt liên lạc tại Crimea và thậm chí là thực hiện các cuộc tấn công mạng và phá hủy các khu vực khác của Ukraina.[59] Năm 2015, Nga bắt đầu một đợt tấn công mạng cơ sở hạ tầng Ukraina, phá bỏ sức mạnh của hàng trăm ngàn người Ukraina trong hai thời điểm chính. Trong vài năm tới, nước này tiếp tục tung ra một làn sóng tấn công chưa từng có trên khắp Ukraina, bao gồm "truyền thông, tài chính, vận tải, quân sự, chính trị và năng lượng", hầu như là mọi phân khúc của xã hội Ukraina, ở nơi mà một số người tin rằng một phần đang nỗ lực đào tạo cho một chiến dịch tương tự chống lại Hoa Kỳ.[60] Đồng thời, họ tiếp tục tiếp tục hàng loạt các cuộc tấn công khắp các nước Baltic và nổi bật là tìm cách định hình cuộc bầu cử ở Hoa Kỳ vào năm 2016 và 2020 với các chiến dịch đánh lạc hướng đối phương, cũng như ở các quốc gia khác.[61] Vào năm 2021, chính phủ Hoa Kỳ đã chính thức cáo buộc Nga về cuộc tấn công của công ty CNTT SolarWinds, một cuộc tấn công tối tân đã gây tổn hại cho phần lớn chính phủ liên bang và một số công ty lớn của Hoa Kỳ.[62]

Trung Quốc là một cường quốc khác đầu tư đáng kể vào cạnh tranh viễn thông nhưng không giống như Nga, Trung Quốc không chỉ nỗ lực tìm cách khai thác cơ sở hạ tầng internet hiện có mà còn xây dựng mạng lưới và cơ sở hạ tầng có thể gây ảnh hưởng và thậm chí là kiểm soát được. Giống như Nga, Trung Quốc thông thạo trong việc khai thác lỗ hổng internet hiện có. Đầu những năm 2000, nước này đã thực hiện một làn sóng các cuộc tấn công vào mạng lưới của Bộ Quốc phòng Hoa Kỳ trong nội dung mà cơ quan này gọi là Operation Titan Rain.[63] Các chính phủ trên toàn thế giới, gồm Hoa Kỳ, Vương quốc Anh, Pháp, Đức, Canada, Úc, Nhật Bản, Hàn Quốc, Đài Loan, Ấn Độ và nhiều nước khác, đã lên tiếng về sự xâm nhập của Trung Quốc vào mạng lưới chính phủ của họ. Một số vụ tấn công mạng lớn nhất trong thập kỷ qua được Bộ Tư pháp Hoa Kỳ William Barr xác nhận là do các điệp viên Trung Quốc gây ra, bao gồm trộm cắp hồ sơ từ Văn phòng Quản lý Nhân sự Hoa Kỳ (hồ sơ cho 21 triệu người), khách sạn Marriott (400 triệu người), cơ quan bảo hiểm y tế Anthem (80 triệu người) và Equifax (147 triệu người) trong số hàng loạt các vụ khác.[64]

Đồng thời, Trung Quốc cũng đang đặt nền tảng cho cơ sở hạ tầng internet trong tương lai và theo những nỗ lực trước đây, có thể nỗ lực này hiện không mang tính thương mại hoặc sẽ vẫn mang tính thương mại thuần túy trong thời gian tới. Các khoản đầu tư của Trung Quốc được tuyên bố nhiều nhất trong các mạng 5G dự kiến sẽ hình thành nền tảng cho nền kinh tế thông minh hơn, được kết nối liên kết vô số thiết bị và cảm biến với nhau. Với mong muốn xây dựng những mạng lưới này trên toàn thế giới, Trung Quốc đã trợ cấp cho các công ty và dự án lớn về 5G trên toàn thế giới, là một phần của sáng kiến Con đường tơ lụa kỹ thuật số. Với giá cả cạnh tranh, những công ty như Huawei có thể đánh bại các nhà cung cấp 5G lớn khác và giành quyền điều hành thị phần đáng kể trên toàn cầu, khiến Trung Quốc trở thành công ty hàng đầu trong việc xây dựng những mạng lưới này. Ngoài 5G, chính phủ Trung Quốc đã trợ cấp cho những đơn vị nỗ lực xây dựng cơ sở hạ tầng internet hoặc liên lạc trên hầu hết mọi lục địa. Tất cả những nỗ lực này đều được bổ sung bằng một chiến dịch nhằm định hình các tiêu chuẩn toàn cầu, một ưu tiên cho chính sách then chốt dành cho Trung Quốc được ghi nhận trong các tài liệu hoạch định cấp cao, cũng như trong mối quan hệ đối đầu giữa Anh-Đức về vô tuyến cách đây một thế kỷ, có thể định hình tương lai của viễn thông theo những cách thức có lợi cho Trung Quốc. Vì vậy, gần đây Trung Quốc công bố một sáng kiến bảo mật dữ liệu mới.[65]

Một số người lo ngại rằng các hoạt động của Trung Quốc sẽ mở ra cơ hội cho Bắc Kinh có quyền kiểm soát thực tế đối với các mạng này, cho dù chặn lưu lượng hay từ chối truy cập. Có ít thông tin cung cấp công khai về nỗ lực của Trung Quốc trong việc giành được quyền kiểm soát đó nhưng vào tháng 2 năm 2020, chính phủ Hoa Kỳ tiết lộ rằng Huawei có cửa sau cho các thiết bị mạng của mình, không tiết lộ những đơn vị này cho các công ty liên quan ký hợp đồng với họ, và những công ty cửa sau đã vượt xa những điều mà chính phủ sở tại thường yêu cầu như là một phần của việc ngăn chặn hợp pháp.[66] Ngoài ra, báo cáo công khai đã tiết lộ rằng Huawei đã hỗ trợ cho các chính phủ như Uganda và Zambia dàn xếp danh tính của những kẻ chống đối.[67] Ngay cả ngoài trường hợp Huawei, một công ty an ninh mạng gần đây đã phát hiện ra các cửa sau trong phần mềm thuế bắt buộc mà chính phủ Trung Quốc yêu cầu các công ty nước ngoài phải cài đặt.[68] Cho dù những trường hợp này có cho thấy Huawei đã tự khai thác vị trí của mình trong các mạng này hay không, hành vi của công ty và hồ sơ theo dõi của Trung Quốc với các cuộc tấn công mạng và hoạt động gián điệp, là những lý do gây lo ngại.

Lý do chính khác về mối lo ngại đến từ lịch sử và hành vi của những cường quốc theo chủ nghĩa tự do bị hạn chế nghiêm ngặt hơn bởi quy tắc pháp luật. Thực vậy, các trường hợp trước đây trong lịch sử cho thấy rõ ràng loại quyền lực và ảnh hưởng của một công ty như Huawei có khả năng bị chính phủ Trung Quốc khai thác, giống như các cường quốc khác thường xuyên khai thác vị trí của công ty hoặc năng lực của họ trong lĩnh vực viễn thông.

Từ quan điểm lịch sử bao quát hơn đó, bằng chứng có thể khiến nhiều người quan sát kết luận rằng cần thận trọng về vai trò của Huawei trong mạng lưới viễn thông, ngay cả khi động cơ của công ty thực sự chỉ mang tính thương mại, lời hứa của công ty về "không có cửa sau và không có hoạt động gián điệp" có thể đáng tin và Bắc Kinh thực sự muốn tôn trọng những cam kết đó.

Nhìn chung, như báo cáo này cho thấy, nhiều đặc điểm của cuộc cạnh tranh giữa các cường quốc lớn được xem là mới lạ ngày nay đều có nguồn gốc từ quá khứ. Trong suốt lịch sử, một số chủ đề đã tái diễn:

- *Quyền lực:* Quyền kiểm soát mạng viễn thông là một hình thức về quyền lực chính trị kể từ khi hình thành hơn 150 năm trước. Nước Anh đã khai thác vai trò của mình trong lĩnh vực viễn thông và vô tuyến, Hoa Kỳ có thể đã làm như vậy trong thời kỳ internet hiện đại, và có lý do để lo ngại rằng Trung Quốc có thể cố gắng làm như vậy vào thời nay.

- *Tự mãn*: Hòa bình và thịnh vượng trong thời gian dài dẫn đến sự tự mãn về rủi ro trong lĩnh vực viễn thông. Trong thế kỷ 19, các cường quốc hài lòng với việc dựa vào các công ty nước ngoài và mạng lưới do nước ngoài vận hành, cũng như hiện nay các quốc gia sẵn sàng chấp nhận hoạt động và sử dụng thiết bị viễn thông của Trung Quốc. Nhưng cuối cùng, sự phụ thuộc vào các đối thủ cạnh tranh tiềm năng hoặc kẻ thù đã chứng minh là điều thảm họa cho những quốc gia như Đức và tái định hình chính trị thế giới.

- *Khai thác:* Công nghệ viễn thông mới luôn dẫn đến những nỗ lực mới nhằm chặn, từ chối hoặc khai thác công nghệ này. Mặc dù hy vọng mã hóa có thể làm phức tạp nỗi lực của Trung Quốc trong việc ngăn chặn giao tiếp hiện đại nhưng khoảng thời gian nhiều hy vọng trong quá khứ về mã hóa đều bị phá vỡ do sai lầm của người dùng và nỗ lực quyết tâm của các quốc gia đối thủ để phá chúng, như khi nước Đức phát hiện khi người Anh đã giải những mật mã tưởng chừng "không thể phá vỡ". Sự khiêm tốn nên đi kèm với từng làn sóng được xem là công nghệ bảo mật.

- *Công ty lớn:* Các quốc gia thường tìm kiếm những công ty viễn thông lớn của chính mình, đặc biệt là khi căng thẳng giữa các cường quốc gia tăng. Chính phủ Trung Quốc tự hào về những thành tựu của Huawei và biến nó thành công ty lớn trên khắp thế giới, thậm chí còn đe dọa những quốc gia từ chối công nghệ của họ. Sẽ là bất thường nếu một công ty thân chính phủ không bị ảnh hưởng từ áp lực của quốc gia khi nhiều công ty viễn thông khác trong lịch sử chưa từng như vậy.

- *Các tiêu chuẩn*: Các tiêu chuẩn viễn thông có thể xác định ai sẽ có sức mạnh mạng, khi Đức sử dụng một cơ quan thiết lập tiêu chuẩn để phá vỡ vị thế chi phối của Anh trong lĩnh vực vô tuyến không dây. Ngày nay, sự cạnh tranh đó đang diễn ra ở những cơ quan như Liên minh Viễn thông Quốc tế và vai trò của Huawei trong Liên minh này cho thấy cần phải cân nhắc xem tiêu chuẩn của cơ quan này có cho phép Trung Quốc định hình lại hoạt động viễn thông hay không.

- *Từ chối:* Bảo mật mạng không chỉ là về việc chặn và bảo mật dữ liệu, mà còn về việc từ chối toàn bộ hoạt động của mạng hoặc truy cập vào mạng bên ngoài. Nước Anh đã loại bỏ Đức khỏi mạng lưới điện tín của thế giới và vai trò của Huawei trong các mạng lưới này có thể giúp công ty này đóng mạng ở các quốc gia nơi công ty đang vận hành thiết bị ngay cả khi không thể truy cập dữ liệu một cách dễ dàng.

- *Quyết tâm:* Nhiều chính phủ giảm xuống mức độ đối thủ có thể nỗ lực hết sức để xâm phạm mạng lưới của họ và sau đó đối mặt với sự bất ngờ đầy phiền toái khi xảy ra xâm phạm. Khả năng của nước Anh giải những mật mã của Đức trong Thế chiến II thông qua những nỗ lực quy mô lớn và khả năng của nước Mỹ nghe lén cáp tàu ngầm nội bộ của Liên Xô từng được xem là không thể nghe lén cho thấy mức độ mà những cường quốc sẽ nỗ lực để truy cập thông tin tình báo tín hiệu quan trọng. Trung Quốc cũng có khả năng sẽ thực hiện tối đa những nỗ lực như vậy, và ngay cả khi Huawei sẽ thấy khó có thể vũ khí hóa vị trí của mình trong các mạng hiện đại thì việc đánh giá thấp mức độ linh hoạt và động cơ của một đối thủ cạnh tranh quyết tâm như Trung Quốc là một môtip tái diễn về sự cạnh tranh trong lĩnh vực viễn thông.

Như báo cáo này cho thấy, nhiều đặc điểm của cuộc chơi giữa các cường quốc trong lĩnh vực viễn thông vẫn không đổi, ngay cả khi đối tượng tham gia có thể khác nhau.

Giới thiệu về tác giả

Rush Doshi là giám đốc của Brookings China Strategy Initiative (Sáng kiến Chiến lược Trung Quốc của Brookings) và là thành viên của Brookings Foreign Policy (Chính sách Đối ngoại Brookings). Ông cũng là thành viên tại Trung tâm Trung Quốc Paul Tsai thuộc Trường Luật Yale và là một nghiên cứu sinh trong lớp khai giảng chương trình Wilson China. Nghiên cứu của ông tập trung vào đại chiến lược của Trung Quốc cũng như các vấn đề an ninh tại Ấn Độ-Thái Bình Dương. Doshi là tác giả của *The Long Game: China's Grand Strategy to Displace American Order*, sắp xuất bản từ Oxford University Press. Ông hiện đang phục vụ trong chính quyền Biden.

Kevin McGuiness vừa làm việc với Brookings với vai trò chuyên gia bên ngoài của Chương trình Skillbridge của Bộ Quốc phòng, nơi ông đã đóng góp vào nhiều dự án khác nhau trong Trung tâm Nghiên cứu Chính sách Đông Á. Ông là cựu binh của Lực lượng Không quân và gần đây đã hoàn thành một loạt nhiệm vụ của mình với tư cách là giảng viên tại Học viện Không lực Hoa Kỳ, hướng dẫn các khóa học trong quan hệ quốc tế và chính trị châu Á. Gần đây, ông còn làm trợ lý nghiên cứu tại Trung tâm của Viện Nghiên cứu Chiến lược Quốc gia về Nghiên cứu Quân sự Trung Quốc, nơi ông tập trung vào việc hiện đại hóa và bảo mật PLA tại Đông Dương-Thái Bình Dương.

Lời cảm ơn

Các tác giả chân thành cảm ơn cựu thực tập sinh Isabella Lu, Zijin Zhou và Gaoqi Zhang đã hỗ trợ nghiên cứu dự án này, một số nhà đánh giá giấu tên, Claire Harrison và Ted Reinerte đã chỉnh sửa báo cáo và Chris Krupinski và Rachel Slattery vì đã giúp tạo bố cục và thiết kế web. Brookings xin cảm ơn Bộ Ngoại giao Hoa Kỳ và Viện Báo cáo Chiến tranh và Hòa bình đã tài trợ cho nghiên cứu này.

Báo cáo này được hoàn thành trước khi Rush Doshi phục vụ trong chính phủ, chỉ liên quan đến các nguồn tin mở và không nhất thiết phản ánh chính sách chính thức hoặc vị thế của bất kỳ cơ quan nào trong chính phủ Hoa Kỳ.

[1] Steven Chase, Robert Fife và Barrie McKenna, "Trudeau từ chối để chính trị "can thiệp vào quyết định về Huawei", Globe and Mail, ngày 15 tháng 10 năm 2018, https://www.theglobeandmail.com/politics/article-trudeau-refuses-to-let-politics-slip-into-decision-on-huawei/; Greg Quinn và Josh Wingrove, "Trudeau cho biết chính trị sẽ không ảnh hưởng đến quyết định về 5G của Huawei", Time, ngày 19 tháng 12 năm 2018, https://time.com/5485141/justin-trudeau-huawei-5g-decision-politics/.

[2] Daniel R. Headrick, Vũ khí Vô hình: Viễn thông và Chính trị Quốc tế, 1851-1945 (Oxford, Vương quốc Anh: Oxford University Press, năm 1991), chương 1.
[3] Ibid., nhận xét này của Headrick.
[4] Ibid.
[5] Ibid.
[6] Ibid., nhận xét này của Headrick.
[7] Heidi Tworek, Tin tức từ Đức: Cuộc cạnh tranh kiểm soát lĩnh vực truyền thông thế giới, 1900-1945 (New York: Các nghiên cứu về lịch sử của Harvard, 2019).
[8] Daniel R. Headrick, *Vũ khí Vô hình.*
[9] "NH 79949 Hoạt động cắt cáp tại Cienfuegos, ngày 11 tháng 5 năm 1898", Thư viện Trực tuyến của Trung tâm Lịch sử Hải quân, https://www.history.navy.mil/content/history/nhhc/our-collections/photography/us-people/b/baker-benjamin-f/nh-79949.html.
[10] Ibid., chương 5.
[11] Jonathan Winkler, "Xung đột Thông tin trong Thế chiến I", Tạp chí Lịch sử Quân sự 73, số 3 (năm 2009): 845–67, https://doi.org/10.1353/jmh.0.0324.
[12] Cameron McR. Winslow, "Hành động cắt cáp tại Cienfuegos", Tạp chí tháng số 57 của The Century Illustrated (năm 1899): 708-717, https://books.google.com/books?id=Y7fPAAAAMAAJ&pg=PA708#v=onepage&q&f=false.
[13] Jonathan Winkler, "Làm kẻ thù câm lặng: Cắt cáp trong chiến tranh Tây Ban Nha-Hoa Kỳ", Chiến tranh bên bờ vực suy tàn, ngày 6 tháng 11 năm 2015 https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/; Rebecca Raines, "Hiện thân số phận: Binh chủng Thông tin của Quân đội Hoa Kỳ", *Lịch sử Quân đội* số 46 (năm 1998): 14–21, https://www.jstor.org/stable/26304991.
[14] Jonathan Winkler, "Làm kẻ thù câm lặng".
[15] "Cuộc chiến Tây Ban Nha-Hoa Kỳ: Điện tín và cắt cáp, Bài luận giới thiệu," Bộ Tư lệnh Di sản và Lịch sử Hải quân, https://www.history.navy.mil/research/publications/documentary-histories/united-states-navy-s/telegraphy-and-cable.html.
[16] Jonathan Winkler, "Làm kẻ thù câm lặng".
[17] Thư viện Quốc hội, Bộ sưu tập George Grantham Bain, https://www.loc.gov/pictures/item/2014683102/.
[18] Mặc dù Heidi Tworek đã lưu ý, vai trò của chính ông thường được nhấn mạnh trong quá trình phát triển công nghệ này. Heidi Tworek, *Tin tức từ Đức.*
[19] Marc Raboy, "Công ty đầu tiên muốn "kết nối thế giới" không phải là Google hay Facebook", Media@LSE, ngày 24 tháng 8 năm 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, *Tin tức từ Đức, trang 12–13.*
[21] Michael Friedewald, "Telefunken so với Marconi, hoặc Cuộc đua điện tín không dây trên biển, 1896-1914," SSRN (ngày 9 tháng 1 năm 2014): https://doi.org/10.2139/ssrn.2375755.
[22] Ibid.
[23] Marc Raboy, Marconi: Người kết nối thế giới (Oxford, Vương quốc Anh: Oxford University Press, năm 2016), 226–28.
[24] Ví dụ, Telefunken hoạt động ngay cả ở các khu vực không có các thuộc địa lớn của Đức như Châu Mỹ La Tinh.
[25] George Johnson, hiệu đính, *All Red Line: Biên niên sử và mục đích của dự án cáp Thái Bình Dương (Ottawa:* James Hope và Sons, năm 1903), 10, tại Internet Archive, https://archive.org/details/allredlineannals00johnuoft/page/n11/mode/2up.
[26] Gordon Corera, "Nước Anh đã đi tiên phong như thế nào trong việc cắt cáp ở Thế chiến I", BBC News, ngày 15 tháng 12 năm 2017, https://www.bbc.com/news/world-europe-42367551.
[27] Jonathan Winkler, "Xung đột thông tin trong Thế chiến I", 847.
[28] P. M. Kennedy, "Chiến lược và Hệ thống liên lạc cáp dài, 1870-1914", English Historical Review 86, số 341 (năm 1971): 728–52, https://www.jstor.org/stable/563928.
[29] Jonathan Winkler, "Xung đột thông tin trong Thế chiến I", 849.
[30] Ibid., 851.
[31] Gordon Corera, "Tại sao bức điện tín Zimmermann lại quan trọng như vậy?", BBC News, ngày 17 tháng 1 năm 2017, https://www.bbc.com/news/uk-38581861; Patrick Beesly, Room 40: Tình báo Hải quân Anh 1914-18 (San Diego: Harcourt Brace Jovanovich, 1982).

[32] C. O. Nordensvan và Valdemar Langlet, *Det stora världskriget* [Thế chiến] (1915), tại Wikimedia Commons, https://commons.wikimedia.org/wiki/File:German_WW_I_field_telegraph_002.jpg.
[33] Jonathan Winkler, "Xung đột thông tin trong Thế chiến I".
[34] Wilhelm Flicke, "Khởi đầu của việc nghe lén qua vô tuyến trong Thế chiến I: Tóm lược Lịch sử của một Nhân viên tình báo của Đức", Bài viết trên NSA Cryptologic Spectrum 8, số 2 (1978): 21, https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/.
[35] Bruce Norman, Cuộc chiến bí mật: Cuộc chiến về mã hóa và mật mã (Newton Abbot, Vương quốc Anh: David & Charles Ltd, năm 1973); Prit Butar, Sự xung đột của các đế chế: Cuộc chiến ở mặt trận phía Đông vào năm 1914 (Oxford, Vương quốc Anh: Osprey Publishing, năm 2014).
[36] Matt Crypto, "Các rotor của máy tạo mật mã Lorenz SZ42 được trưng bày tại Bảo tàng Bletchley Park", tại Wikimedia Commons, https://commons.wikimedia.org/wiki/File:SZ42-6-wheels.jpg.
[37] George I. Beck, "Liên lạc quân sự - Sự xuất hiện của tín hiệu điện", Britannica, https://www.britannica.com/technology/military-communication.
[38] Harry Hinsley, "Ảnh hưởng của ULTRA trong Thế chiến Thứ Hai" (bài giảng, Cambridge, Vương quốc Anh, ngày 19 tháng 10 năm 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.
[39] Các cài đặt khả thi $1x10^{170}$.
[40] "Bletchley Park nhớ về những máy giải mật mã của Ba Lan," BBC News, ngày 14 tháng 7 năm 2011, https://www.bbc.com/news/uk-england-beds-bucks-herts-14141406.
[41] Gordon Welchman, Câu chuyện về Hut Six: Giải mã Enigma (Cleobury Mortimer, Vương quốc Anh: Classic Crypto Books, năm 1997).
[42] Harry Hinsley, "Ảnh hưởng của ULTRA".
[43] Ibid.
[44] Ví dụ, vui lòng tham khảo Jerry Roberts, *Lorenz: Giải mã bí mật hàng đầu của Hitler ở Bletchley Park* (Cheltenham, Vương quốc Anh: History Press, 2017).
[45] F. Winterbotham, Siêu bí mật (New York: Harper & Row, 1974), 154, 191.
[46] Harry Hinsley, "Ảnh hưởng của ULTRA".
[47] Calder Walton, "Gián điệp, người đến từ lục địa", Chính sách đối ngoại, ngày 27 tháng 4 năm 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.
[48] Hải quân Hoa Kỳ, tại Wikimedia Commons, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.
[49] Anna Borshchevskaya, "Mật mã không thể giải của Xô Viết, Chính sách đối ngoại, ngày 27 tháng 4 năm 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.
[50] Daniel R. Headrick, *Vũ khí vô hình*, chương 4.
[51] Sherry Sontag, Christopher Drew và Annette Lawrence Drew, *Thông tin lừa bịp của kẻ mù: Câu chuyện chưa kể về hoạt động gián điệp trên tàu ngầm của Hoa Kỳ* (New York: Public Affairs, 1998), 222.
[52] Ibid.
[53] Ibid., 223.
[54] Ibid.
[55] Matt Blitz, "Những thợ lặn hải quân và sứ mệnh liều lĩnh để do thám Liên Xô dưới đáy biển", *Popular Mechanics*, ngày 30 tháng 3 năm 2017, https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping/.
[56] Michael J. Sulick, C*ác gián điệp Hoa Kỳ: Hoạt động gián điệp chống lại Hoa Kỳ từ thời Chiến tranh lạnh tới thời điểm hiện tại* (Washington, DC: Georgetown University Press, năm 2013), 109–14; Matt Blitz, "Thợ lặn hải quân"
[57] Damien McGuinness, "Cuộc tấn công mạng đã chuyển đổi Estonia như thế nào", BBC News, ngày 27 tháng 4 năm 2017, https://www.bbc.com/news/39655415; Rain Otis, "Phân tích về cuộc tấn công mạng năm 2007 chống lại Estonia từ góc độ chiến tranh thông tin," (Tallinn: Trung tâm chuyên trách về hợp tác phòng thủ không gian mạng của NATO, năm 2008), https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.
[58] David Hollis, "Nghiên cứu tình huống chiến tranh mạng: Georgia năm 2008", Tạp chí Small Wars, ngày 6 tháng 1 năm 2011, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008; Ronald J. Deeibert, Rafal Rohozinski và Masashi Crete-Nishihata, "Lốc xoáy trong không gian mạng: Sự hình thành và phủ nhận thông tin trong cuộc chiến tranh Nga–Georgia năm 2008", *Cuộc đối thoại về an ninh* 43, số 1 (2012): 3–24, https://journals.sagepub.com/doi/10.1177/0967010611431079.

[59] Pavel Polityuk và Jim Finkle, "Ukraine tuyên bố các hoạt động tấn công liên lạc, điện thoại của các nghị viên bị chặn", Reuters, ngày 4 tháng 3 năm 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304; Sergey Sukhankin, "Cuộc chiến điện tử của Nga ở Ukraina: Giữa thực tế và tưởng tượng", Jamestown Foundation, ngày 24 tháng 5 năm 2017, https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/.

[60] Andy Greenberg, "Làm thế nào toàn bộ quốc gia trở thành phòng thí nghiệm của Nga trong cuộc chiến mạng", *Wired*, ngày 20 tháng 6 năm 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; "Sáu nhân viên của Tổ chức GRU của Nga bị buộc tội liên quan đến việc triển khai toàn cầu phần mềm độc hại phá hoại và các hành động phá hoại khác trong không gian mạng", Bộ Tư pháp Hoa Kỳ, ngày 19 tháng 10 năm 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[61] Constanze Stelzenmüller, "Tác động của việc can thiệp của Nga đối với cuộc bầu cử năm 2017 của Đức", (Chứng nhận của quốc hội, ngày 28 tháng 6 năm 2017), https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

[62] Maggie Miller, "Các cơ quan tình báo của Hoa Kỳ cáo buộc Nga về cuộc tấn công mạng hàng loạt của SolarWinds", *The Hill,* ngày 5 tháng 1 năm 2021, https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack.

[63] "Kết nối các điểm trên sự cố mạng do nhà nước tài trợ - Titan Rain", Hội đồng Đối ngoại, https://www.cfr.org/cyber-operations/titan-rain.

[64] Garrett Graff, "Thời gian tấn công của Trung Quốc sẽ tạo ra hậu quả Kéo dài hàng thế kỷ", *Wired*, ngày 11 tháng 2 năm 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

[65] Chun Han Wong, "Trung Quốc triển khai sáng kiến thiết lập vai trò bảo mật dữ liệu toàn cầu"*, Tạp chí Wall Street,* ngày 8 tháng 9 năm 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

[66] Bojan Pancevski, "Các quan chức Hoa Kỳ cho biết Huawei có thể bí mật tiếp cận các mạng viễn thông", *Tạp chí Wall Street*, ngày 12 tháng 2 năm 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

[67] Joe Parkinson, Nicholas Bariyo và Josh Chin, "Kỹ thuật viên Huawei hỗ trợ các chính phủ Châu Phi thực hiện hoạt động gián điệp trước các đối thủ chính trị", *Tạp chí Wall Street*, ngày 15 tháng 8 năm 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[68] William Turton, "Một công ty cho biết có đơn vị cửa sau được nhúng vào phần mềm thuế Trung Quốc", Bloomberg, ngày 25 tháng 6 năm 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.