Huawei à la rencontre de l'histoire : grandes puissances et risques liés aux télécommunications, 1840-2021

Rush Doshi et Kevin McGuiness

Brookings Institution, mars 2021

Résumé analytique

Fin 2018, alors que les Américains s'inquiétaient de savoir si le Canada accueillerait Huawei dans ses réseaux de télécommunications, le Premier ministre canadien Justin Trudeau a tenu une série de déclarations faisant écho à la sagesse populaire dans la majeure partie du monde. « Cela ne devrait pas être une décision politique », a-t-il déclaré à l'époque, et le Canada ne « laissera pas la politique se glisser dans les décisions » concernant le rôle de Huawei dans son réseau.[1]

L'idée que la politique de pouvoir puisse être éliminée des questions relatives aux télécommunications se voulait non seulement optimiste, mais également en décalage avec l'histoire des télécommunications. Ce rapport retrace cette histoire et montre comment le pouvoir et les télécommunications ont presque toujours été étroitement liés. Lorsque les États ont ignoré ces liens et se sont montrés désinvoltes quant à la sécurité de leurs propres réseaux, les résultats ont été désavantageux et parfois même désastreux.

Ce rapport examine plusieurs cas marquants de concurrence entre grandes puissances dans le domaine des télécommunications, depuis les balbutiements des télécommunications dans les années 1840. Ces cas démontrent que de nombreuses questions auxquelles les décideurs politiques sont confrontés aujourd'hui présentent de nombreuses similitudes avec le passé. Si le débat actuel sur la sécurité des réseaux et l'infrastructure 5G peut sembler nouveau, il fait en fait écho à des différends oubliés qui remontent à l'aube des télécommunications, il y a environ 150 ans. En outre, bon nombre des éléments familiers de la concurrence dans le secteur des télécommunications aujourd'hui (tels que l'utilisation d'organismes de normalisation, les subventions publiques, les écoutes téléphoniques, la guerre de l'information, les marchés des pays en développement et le cryptage pour obtenir des avantages) prennent leur source il y a plus d'un siècle, et permettent de tirer des leçons importantes pour les débats actuels.

Une liste de ces leçons essentielles est présentée ci-dessous :

1. **Le contrôle des réseaux mondiaux de télécommunications est une forme de pouvoir politique.** Les réseaux 5G sont appelés à constituer le fondement d'une économie plus intelligente et connectée, reliant entre eux d'innombrables appareils et capteurs. Désireuse de développer ces réseaux dans le monde entier, la Chine a subventionné ses entreprises championnes de la 5G et ses projets dans le monde entier dans le cadre d'une initiative de « Route de la soie numérique ». Cet effort rappelle la quête de la Grande-Bretagne pour dominer les réseaux à l'aube de la télégraphie électrique. La Grande-Bretagne a forgé son avantage durant six décennies en augmentant régulièrement la dépendance d'autres États

à l'égard de ses réseaux, allant jusqu'à renoncer à des redevances et à des avantages économiques pour les inciter à faire passer des câbles par son territoire, tout en réduisant sa dépendance à l'égard des réseaux étrangers. Elle a fini par contrôler plus de la moitié du trafic mondial de câbles, le plus grand réseau radio et la plus grande flotte de câbliers. L'« hégémonie de l'information » de la Grande-Bretagne lui a permis de priver l'Allemagne de la quasi-totalité des télécommunications mondiales pendant la Première Guerre mondiale et a contraint Berlin à acheminer le trafic sur des lignes britanniques et susceptibles d'être surveillées par la Grande-Bretagne. Cette manœuvre se révélera décisive dans la défaite de l'Allemagne lors de ce conflit.

2. **Les longues périodes de paix et de prospérité conduisent généralement à une certaine insouciance à l'égard des risques liés aux télécommunications.** Au cours des 30 dernières années, la paix et la mondialisation économique de l'après-guerre froide ont coïncidé avec des progrès rapides dans le domaine des télécommunications qui ont conduit les États à privilégier les avantages commerciaux révolutionnaires par rapport aux risques politiques et sécuritaires, y compris la propriété ou l'exploitation étrangère des réseaux. Un phénomène similaire s'est produit à l'aube des télécommunications dans les années 1840, qui coïncide également avec une période de paix relative et de mondialisation qui s'est poursuivie jusqu'à la Première Guerre mondiale. Durant la majeure partie de cette époque, le désir de saisir le potentiel commercial, apparemment miraculeux, des nouvelles technologies de communication a occulté les questions liées à la dépendance à l'égard de réseaux ou d'entreprises étrangères. La Grande-Bretagne a bénéficié de la passivité des autres en établissant puis en exploitant une position nodale inattaquable dans les réseaux mondiaux, la plupart des autres grandes puissances dépendant de ses réseaux.

3. **Lorsque les États se montrent trop confiants quant à la sécurité de leurs télécommunications, les résultats peuvent être désastreux et remodeler la politique mondiale.** Des décennies de désinvolture allemande envers sa dépendance à l'égard des lignes de télécommunications britanniques ont révélé, lorsque Berlin a pris conscience des risques liés à cette dépendance, qu'il était trop tard pour y remédier. Quand la Première Guerre mondiale a éclaté, la Grande-Bretagne a coupé tous les câbles de l'Allemagne et a forcé Berlin à faire passer son trafic par les réseaux britanniques malgré le risque d'interception. C'est ainsi que le « télégramme Zimmerman » a été découvert, provoquant l'entrée en guerre des États-Unis. De même, l'indiscipline russe en matière de transmissions radio sans fil pendant la Première Guerre mondiale a permis aux Allemands d'intercepter les communications, de « voir » le mouvement des troupes russes en temps réel et de leur infliger une défaite décisive lors de la bataille de Tannenberg. Puis, lors de la Seconde Guerre mondiale, la confiance excessive des nazis dans leurs codes secrets s'est traduite par des efforts minimes pour les mettre à jour. La Grande-Bretagne a ainsi pu déchiffrer ces codes et obtenir des renseignements qui ont, semble-t-il, raccourci la guerre de deux à quatre ans. Compte tenu du pouvoir de l'information, même des épisodes occasionnels d'indiscipline ou de négligence en matière de signaux peuvent modifier le cours de l'histoire.

4. **Les nouvelles technologies entraînent toujours de nouveaux efforts pour les intercepter.** L'apparition des câbles sous-marins a incité à couper et à mettre sur écoute ces lignes dès la guerre hispano-américaine ; la transmission radio a donné lieu à des efforts de la part de rivaux pour capturer les nœuds du réseau et intercepter les transmissions ; et l'émergence de codes sophistiqués pour le cryptage a engendré des efforts à l'échelle industrielle pour les déchiffrer. À chaque époque, certains ont cru qu'un nouveau bond en avant dans les communications présenterait moins de risques que les précédents. Pourtant, à chaque fois, le cycle de l'innovation et de l'exploitation s'est poursuivi.

5. **Les réseaux de télécommunications n'ont jamais été politiquement neutres, surtout en période de tension.** En 2019, les dirigeants de Huawei se sont engagés à « ne pas laisser de porte dérobée, ne pas espionner » et ont promis que leur entreprise se tiendrait à l'écart de la politique, le gouvernement chinois s'engageant à respecter cette promesse. Mais il y a plus d'un siècle, les entreprises de télécommunications et les gouvernements qui les accueillaient faisaient publiquement des promesses similaires, tout en les rompant en privé et en travaillant ensemble en temps de paix comme en temps de guerre. Par exemple, la domination britannique sur les câbles sous-marins a conduit les Français, les Allemands et les Américains à prôner le maintien de la neutralité des lignes, même en temps de guerre. Les entreprises britanniques ont publiquement déclaré leur neutralité. En réalité, elles se sont conformées aux intérêts politiques de la Grande-Bretagne, en particulier dans les moments de grande tension, et ont renoncé à toute neutralité pendant les périodes de guerre. Le pouvoir qui découle de la perturbation ou de l'interception des flux d'informations rivaux s'est généralement avéré trop alléchant pour que les revendications de neutralité, même sincères, puissent perdurer.

6. **Les États cherchent souvent à se doter de leurs propres champions des télécommunications lorsqu'ils reconnaissent la vulnérabilité liée au fait de s'appuyer sur les entreprises d'un concurrent ou d'un adversaire.** À ce jour, les États-Unis ne disposent pas d'un grand fabricant de stations de base 5G, ce qui a suscité des débats sur la question de savoir s'ils devaient investir dans leurs propres entreprises ou s'appuyer sur des entreprises alliées. Cela a également suscité des désaccords quant à la mesure dans laquelle Huawei est elle-même une championne d'État de fait. Ces débats ne sont pas sans précédent. Au début du XXe siècle, de nombreux États qui dépendaient de tiers pour leurs équipements ou réseaux de télécommunications ont commencé à développer leurs propres systèmes. Par exemple, l'Allemagne a poussé deux entreprises allemandes ayant des activités radio concurrentes, Siemens & Halske et AEG, à collaborer pour créer une alternative allemande à la domination britannique dans le domaine de la radio. De nombreux autres grands États ont soutenu des entreprises qui, bien que prétendument privées, étaient liées aux États qui les soutenaient.

7. **La lutte pour les normes de télécommunications peut déterminer quels États exerceront le pouvoir sur les réseaux. Elle nécessite souvent la mobilisation d'alliés et de partenaires.** Les États dont la technologie devient la norme dominante peuvent exercer une pression sur les autres. La compétition actuelle sur les normes des technologies de l'information et de la communication est, en ce sens, similaire à la

compétition anglo-allemande pour les réseaux radio. La domination de la Grande-Bretagne, par l'intermédiaire de la compagnie Marconi qu'elle soutenait, était si écrasante dans le domaine de la radio sans fil que toutes les autres grandes puissances devaient faire passer leurs messages par le réseau sans fil britannique, qui refusait de s'engager avec d'autres stations sans fil. L'Allemagne a finalement réussi à briser cette domination au sein d'un organisme de normalisation qui a interdit cette politique de « non-intercommunication » avec l'aide d'autres puissances, dont les États-Unis et la France, une démonstration de la manière dont des approches coalisées similaires pourraient aujourd'hui être utilisées par les États libéraux pour établir ou préserver des normes favorables en matière de technologies de l'information et des communications (TIC) s'ils travaillent ensemble.

8. **Les États se tournent vers le cryptage lorsque leurs communications deviennent plus faciles à intercepter, mais le cryptage présente souvent des limites dues à des adversaires déterminés ou à des erreurs humaines.** Certains affirment que les inquiétudes concernant le rôle de Huawei dans les réseaux ou sur la vulnérabilité générale des appareils connectés à Internet sont atténuées par le cryptage moderne. Ce genre de débat ne date pas d'hier. À l'aube des télécommunications, il y a un siècle, la possibilité que les messages télégraphiques puissent être lus par d'autres personnes contrôlant les nœuds du réseau, ou que la radio puisse être interceptée par un équipement d'écoute passif, a suscité des avancées majeures en matière de cryptage qui ont parfois entraîné un excès de confiance. Les machines de chiffrement à rotor complexes de l'Allemagne étaient réputées inviolables, mais les erreurs humaines et les efforts à l'échelle industrielle déployés par les Britanniques ont permis à ces derniers de percer les codes allemands. Des mises à jour peu coûteuses de l'équipement et des codes allemands auraient pu mettre fin à l'avantage de la Grande-Bretagne. Mais la confiance excessive de Berlin dans son système de cryptage a fait obstacle à ces modifications, ce qui s'est traduit par l'interception de renseignements qui a altéré le cours de la guerre. Le cryptage de bout en bout est nettement plus évolué que les efforts précédents dans ce domaine, mais l'histoire montre qu'une certaine humilité est nécessaire.

9. **De nombreux États minimisent le niveau d'efforts extraordinaires qu'un adversaire peut déployer pour compromettre leurs réseaux.** Dans le cadre des débats sur les télécommunications modernes, il convient de noter que les États qui ont donné la priorité à la commodité ou au commerce, et qui ont donc accepté des compromis en matière de sécurité, ont souvent été désagréablement surpris par les efforts déployés par un adversaire déterminé pour porter atteinte à leurs réseaux. Lors de la Première Guerre mondiale, l'Allemagne a été surprise par la rapidité et le caractère impitoyable avec lesquels la Grande-Bretagne a coupé tous les câbles qu'elle utilisait pour accéder au monde extérieur. De même, les commandants russes ont été surpris lorsque leur indiscipline dans le domaine de la radio a abouti à une défaite désastreuse à Tannenberg. Pendant la Seconde Guerre mondiale, l'Allemagne ne s'attendait pas à ce que les Britanniques élaborent une opération de décryptage hautement centralisée et à l'échelle industrielle, capable d'exploiter les erreurs de communication allemandes (aussi insignifiantes ou fugaces soient-elles) pour déchiffrer les codes allemands. Et pendant la guerre froide, les Soviétiques n'ont jamais pris la peine de crypter une ligne téléphonique

sous-marine interne qu'ils croyaient hors de portée des États-Unis. Washington a néanmoins trouvé le moyen de la mettre sur écoute, obtenant ainsi une source inestimable de renseignements.

10. **La sécurité des réseaux n’est pas seulement une affaire d'interception, mais aussi de déni.** Une partie du débat sur le rôle de Huawei dans les réseaux met l'accent sur les questions de sécurité des données, mais pourrait gagner à prendre davantage en considération le déni de réseau, un aspect important de la concurrence entre grandes puissances en matière de télécommunications. À l'aube de la télégraphie, les grandes puissances ont cherché à couper les câbles et à empêcher les communications, avec pour point culminant l'opération sans précédent et bien planifiée de la Grande-Bretagne visant à couper tous les câbles du monde susceptibles de relier l'Allemagne à l'extérieur. Parfois, un État peut se faire du tort en appliquant des stratégies de déni de réseau, mais il persistera néanmoins s'il estime que le préjudice est plus important pour son adversaire.

Les grandes puissances et les télécommunications

« Les grands empires ont fait beaucoup pour accélérer la circulation de l'information », souligne une histoire des télécommunications. « Les Romains ont construit des routes, les Perses et les Mongols ont établi des relais de chevaux, les Britanniques ont subventionné les navires postaux. »[2] Mais même si les États étaient avides d'informations, les flux de celles-ci sont restés limités jusqu'à l'apparition du télégraphe moderne. L'électrification des flux d'information a donné naissance aux télécommunications modernes et, avec elles, aux modèles familiers de rivalité entre grandes puissances.

Ces premières décennies des télécommunications modernes, qui courent de 1840 à la Première Guerre mondiale, partagent de grandes ressemblances avec le temps présent. Cette période, comme l'ère actuelle de l'après-guerre froide, a été marquée par une paix relative entre grandes puissances qui a rendu les principaux États « moins sensibles » aux questions de politique et de sécurité dans les réseaux de télécommunications.[3] Alors que les grandes puissances ont mis sur pieds des réseaux nationaux et internationaux au XIXe siècle, nombre d'entre elles se sont d'abord contentées de laisser l'industrie aux commandes, d'ignorer la nationalité des entreprises privées et de minimiser les risques liés au contrôle des réseaux de télécommunications par un adversaire. Les avantages des changements révolutionnaires dans les télécommunications, ce que certains à l'époque appelaient « l'annihilation du temps et de l'espace »[4], étaient si évidents et écrasants que « la propriété des câbles était considérée comme un problème mineur ».[5] À cette époque, la télégraphie était plus une affaire commerciale que politique, note un historien dans une observation qui aurait pu tout aussi bien s'appliquer à une partie de l'enthousiasme initial suscité par la technologie moderne de l'information et sa dernière incarnation : la 5G.[6]

La période de relative complaisance des grandes puissances ne devait pas durer. Des États comme le Pérou en 1879, puis les États-Unis en 1898, ont été parmi les premiers à couper les réseaux de télécommunications de leurs rivaux. Alors que les tensions entre les grandes puissances s'intensifiaient, les États du monde entier se sont rendu compte que certains, à savoir la Grande-Bretagne, avaient bien su gérer la longue paix et que, grâce à leurs entreprises privées, ils avaient fait main basse sur les communications internationales.

Craignant de plus en plus de dépendre des réseaux de câbles sous-marins britanniques, des États comme la France et l'Allemagne ont fortement subventionné le développement de leurs propres réseaux, ce qui n'est pas sans rappeler les subventions et la protection accordées par la Chine à ses champions des technologies de l'information comme Alibaba, Baidu, Tencent et Huawei. Et comme le montre l'historienne Heidi Tworek, les rivaux de la Grande-Bretagne ont également misé sur la nouvelle génération de technologies de télécommunications (la « télégraphie sans fil », mieux connue sous le nom de radio) dans l'espoir de réduire la dépendance à l'égard des câbles télégraphiques sous-marins appartenant à la Grande-Bretagne.[7] Alors que les Britanniques étaient leaders dans ce domaine, l'Allemagne refusait alors de dépendre de leurs réseaux. Elle a mis en place son propre réseau avec des champions soutenus par l'État qui ont investi des régions du monde moins bien connectées (Amérique latine, Afrique, Asie) dans ce qui pourrait aujourd'hui refléter l'expansion des entreprises technologiques chinoises dans le monde en développement et la détermination de Pékin à jeter les bases des réseaux 5G.

Tout au long de cette période, bon nombre des aspects de la concurrence entre grandes puissances en matière de télécommunications, parfois négligés aujourd'hui, étaient souvent pris très au sérieux par les États de l'époque. L'Allemagne, frustrée par la domination britannique sur les réseaux radio, a utilisé un organisme de normalisation pour briser cette domination, une tactique qui démontre que ces organismes n'étaient pas moins importants à cette époque qu'ils ne le sont aujourd'hui. Et comme les télécommunications sont devenues sans fil et encore plus faciles à intercepter, les grandes puissances ont misé sur le cryptage, renonçant parfois à une exploitation disciplinée de leurs réseaux en supposant que les « codes », c'est-à-dire les étapes détaillées du cryptage ou du décryptage des messages, résoudraient le problème. Cette croyance s'est presque toujours avérée erronée en raison d'erreurs humaines. Ce point de vue présente des parallèles frappants avec les hypothèses modernes sur l'insécurité générale des réseaux de télécommunications, et la conviction exprimée par certains dans les débats sur Huawei selon laquelle le cryptage neutraliserait largement le risque d'accès de la Chine à son réseau de télécommunications.

Lorsque la paix entre les grandes puissances a pris fin et que la guerre a éclaté, l'importance politique des télécommunications, parfois floue en temps de paix, est soudain apparue évidente. La capacité des Allemands à intercepter les transmissions russes pendant la Première Guerre mondiale a conduit à une victoire si écrasante lors de la bataille de Tannenberg qu'elle a changé le cours de la guerre et contribué à précipiter la sortie de la Russie du conflit. La domination britannique sur les câbles sous-marins pendant la Première Guerre mondiale était si totale qu'elle a coupé l'Allemagne du système mondial de télécommunications, a acheminé le trafic de câbles allemands par ses propres réseaux et a finalement découvert le télégramme Zimmerman, qui a amené les États-Unis à entrer dans le conflit. Au cours de la Seconde Guerre mondiale, la Grande-Bretagne a remporté une autre victoire dans le domaine du renseignement en perçant le cryptage allemand présumé inviolable. Elle a ainsi obtenu des renseignements exceptionnels qui, selon l'histoire officielle britannique, ont permis d'écourter la guerre en Europe de plusieurs années. Ces cas démontrent que la sécurité des télécommunications n'est pas simplement une question de tactique de combat mais aussi de confrontation politique, qui peut dicter le destin des grandes puissances et façonner l'histoire du monde.

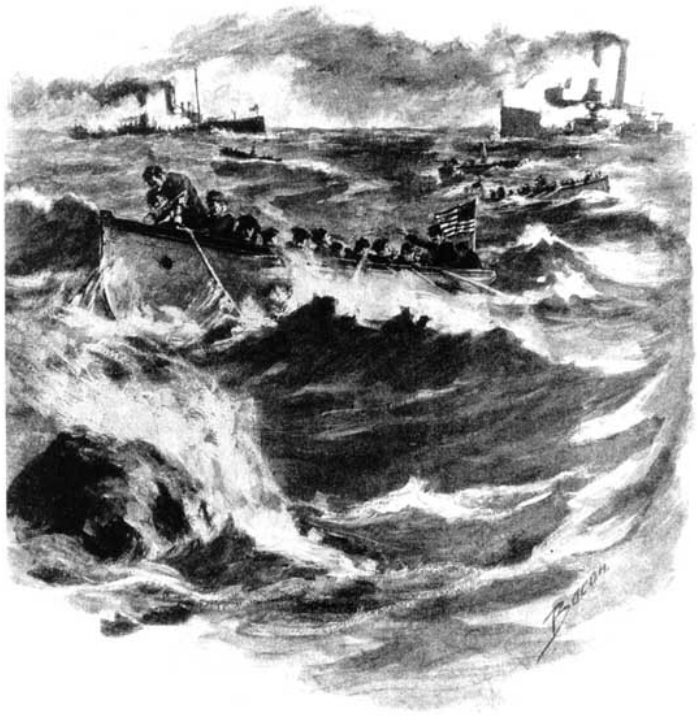
Alors que le monde entrait dans une guerre froide américano-soviétique, les avantages britanniques furent évincés non seulement par la puissance américaine, mais aussi par l'évolution de la technologie, qui rendait les réseaux plus anciens moins pertinents, démontrant ainsi l'importance pour les grandes puissances de rester à la pointe de la technologie. Dans cette nouvelle ère, la concurrence dans le domaine des télécommunications s'est poursuivie selon des schémas familiers. Par exemple, les États-Unis ont mis au point de nouveaux moyens de mettre sur écoute des câbles sous-marins enfouis si profondément et considérés comme si sûrs que les messages qui les traversaient n'étaient souvent pas cryptés. La concurrence s'est également déplacée dans d'autres domaines, tels que les satellites et les infrastructures Internet, bien qu'une grande partie de cette histoire soit encore en cours d'écriture et reste, dans la plupart des cas, classée secrète.

Les télécommunications, comme le montre cette brève série de cas, ont toujours revêtu un caractère politique. L'exploitation de ces technologies et capacités a généralement évolué parallèlement à leur développement. Dès l'arrivée de nouvelles méthodes de communication, les

grandes puissances ont généralement cherché des moyens de les intercepter ou de les interrompre. « Les communications électroniques ont souvent été décrites comme l'une des grandes réalisations de l'humanité », note un historien des télécommunications, « mais lorsque nous les examinons du point de vue de la sécurité, nous voyons un tableau totalement différent. En effet, la sécurité n'est pas une caractéristique technique mais sociale et politique. » Et « puisque la politique ne s'est pas améliorée », remarque-t-il, « les télécommunications ont un côté sombre ».[8]

Nous allons maintenant passer à un résumé des thèmes clés de près de deux siècles de concurrence dans le domaine des télécommunications.

1. La guerre hispano-américaine : les limites de la neutralité du câble



Une représentation de l'expédition américaine de coupe de câble à Cienfuegos publiée en 1907. L'opération a démontré que les câbles télégraphiques sous-marins ne seraient pas traités comme neutres pendant les conflits armés, même par une grande puissance qui avait autrefois prôné la neutralité du câble.

Source : Naval Historical Center Online Library[9]

Lorsque les câbles sous-marins ont commencé à quadriller le monde au XIXe siècle, plusieurs grandes puissances (dont la France, l'Allemagne et les États-Unis) ont demandé qu'ils soient dissociés de la politique internationale. En 1858, dans l'un des premiers télégrammes transatlantiques jamais envoyés, le président américain James Buchanan exhorte la reine Victoria à veiller à ce que les nouvelles lignes télégraphiques du monde restent « à jamais neutres… même au milieu des hostilités ».[10]

Or, lorsque les hostilités ont éclaté, les grands principes de neutralité ont été abandonnés. Deux décennies après le message de Buchanan, le Pérou a coupé les lignes de câble chiliennes en territoire contesté.[11] Ce conflit a peu attiré l'attention, mais lorsque les États-Unis, autrefois chantres de la neutralité des câbles, ont coupé les câbles dans l'Atlantique et le Pacifique lors de la guerre hispano-américaine, le monde l'a remarqué.

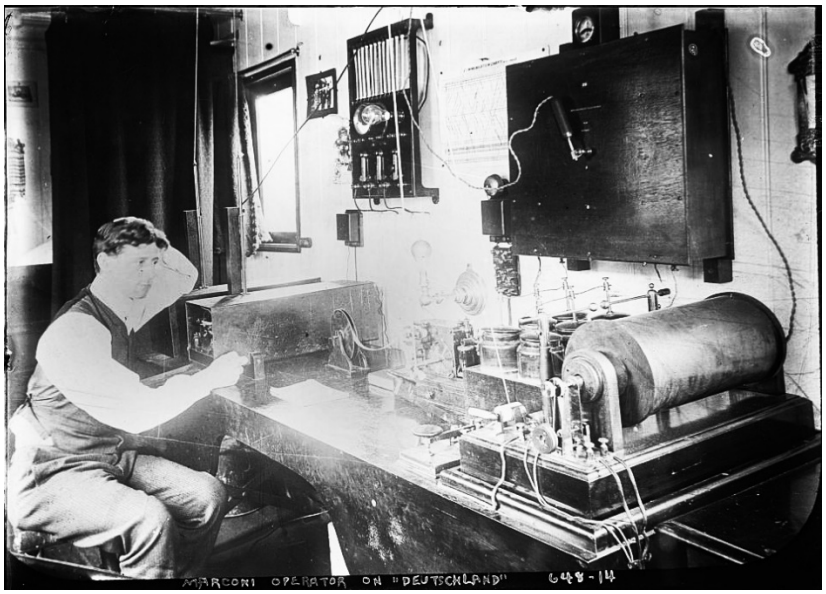
Les États-Unis avaient prévu la coupe des câbles en amont du conflit. Sur le front atlantique, les États-Unis comptaient couper l'Espagne de ses forces à Cuba. « L'isolement de La Havane était, bien sûr, de première importance », note le compte-rendu d'un magazine américain à l'époque. Et cela exigeait que les États-Unis « coupent La Havane de toute communication télégraphique

avec le monde extérieur ».[12] Les États-Unis ont commencé par couper le trafic espagnol qui traversait le territoire américain en Floride. Ensuite, ils ont dépêché une petite équipe pour détruire un nœud de télécommunication clé à Cienfuegos, coupant ainsi la ville de La Havane et une grande partie de l'ouest de Cuba de l'Espagne. Par la suite, les États-Unis ont attaqué divers câbles dans l'est de Cuba ainsi que des câbles dans les Caraïbes qui reliaient Porto Rico à l'Espagne.[13] Au total, la coupe des câbles a considérablement affaibli la capacité de l'Espagne à diriger et à commander ses forces à Cuba.[14]

Dans le Pacifique, les États-Unis ont coupé le seul câble sous-marin entre Manille et Hong Kong, coupant ainsi les Philippines de l'Espagne.[15] Cette décision a également nui aux communications américaines, mais il était présumé qu'elle imposerait un coût encore plus important aux Espagnols, et les États-Unis ont pu compenser en envoyant régulièrement un navire à Hong Kong pour transmettre les messages à Washington.[16] Les forces américaines ont également coupé des câbles sous-marins dans les Philippines, dégradant davantage la capacité de l'Espagne à commander ses forces.

La guerre hispano-américaine a peut-être été le premier conflit mondial à s'étendre sur plusieurs théâtres où les télécommunications électroniques comptaient. C'est aussi la première fois qu'une grande puissance a cherché à interdire à une autre l'accès aux câbles sous-marins. Avant le conflit, la télégraphie était encore considérée comme un domaine essentiellement commercial, et beaucoup espéraient que les câbles resteraient à l'abri de la concurrence politique et militaire. Le conflit a montré les limites de ces perspectives et a révélé que le contrôle des infrastructures de télécommunications, ainsi que la capacité de priver les rivaux géopolitiques de ces avantages ont toujours revêtu une importance politique cruciale.

2. La rivalité anglo-allemande : création de réseaux et établissement de normes



Opérateur radio de la compagnie Marconi dans la « Marconi Room » du paquebot allemand SS Deutschland. L'influence de la compagnie Marconi était si grande que ses employés opéraient dans les salles de radio allemandes, même si l'Allemagne s'inquiétait des risques d'interception et de déni.

Source : Library of Congress, George Grantham Bain Collection[17]

L'établissement de normes technologiques, et les effets de réseau qui en découlent, est depuis longtemps une arène subtile de la concurrence entre grandes puissances. Les États dont la technologie devient la norme dominante peuvent exercer une pression sur les autres. Ce point n'échappe pas aux puissances émergentes, qui s'efforcent souvent de réduire leur vulnérabilité en créant des systèmes parallèles. En effet, l'actuelle lutte sino-américaine pour les TIC est le reflet d'une lutte opposant l'Allemagne et la Grande-Bretagne il y a un siècle pour la domination de l'infrastructure des TIC de l'époque, avec des parallèles troublants et des leçons essentielles pour le présent.

À la fin du XIXe siècle, l'ingénieur italien Guglielmo Marconi, soutenu par la British Royal Navy, a inventé la télégraphie sans fil.[18] Ce fut une invention révolutionnaire. Alors que les grandes puissances coupaient les câbles de leurs concurrents par le passé et que les communications navire-navire et navire-terre étaient auparavant difficiles, le système de Marconi résolvait ces problèmes et présentait moins de risques d'interférences.[19] Marconi s'est finalement associé à la Grande-Bretagne, donnant au pays le monopole des transmissions radio. Si l'on ajoute à cela la part de 60 % de la Grande-Bretagne dans le réseau mondial de câbles sous-marins, celle-ci a dominé les transmissions internationales. L'avantage britannique était troublant pour l'Allemagne, mais la concurrence sur les technologies sans fil « offrait également à l'Allemagne l'occasion d'exercer un contrôle sur une nouvelle infrastructure internationale » et de « contourner les câbles britanniques ». La primauté des grandes puissances était liée au résultat.[20]

Se sentant vulnérable, l'empereur Guillaume II a autorisé l'aide directe de l'État aux scientifiques et ingénieurs allemands, lesquels ont réussi à copier les modèles de Marconi, à les faire breveter en Allemagne et à établir leurs propres réseaux radio financés par des contrats avec l'armée allemande.[21] Malgré cela, la radio à plus longue portée de Marconi et son avantage de pionnier ont imposé sa société, appuyée par la Grande-Bretagne, comme la norme mondiale, et Marconi a tiré parti de ces effets de réseau pour poursuivre une politique de « non-intercommunication » avec les opérateurs radio non Marconi. Les entreprises et les paquebots allemands ne voulant pas être coupés des communications internationales, ils préférèrent le système britannique aux systèmes allemands.

Guillaume II a intensifié la politique industrielle allemande pour contester la norme britannique. Il a rapidement décrété que deux grandes entreprises électriques allemandes, Siemens & Halske et AEG, dont les efforts en matière de radio étaient concurrents, devaient unir leurs forces pour produire l'alternative allemande définitive, Telefunken. « La rivalité [nationale] dans le domaine de la télégraphie sans fil affaiblit la compétitivité de l'Allemagne », expliquait le kaiser, « et donne à la compagnie Marconi la possibilité de parvenir à un monopole mondial » qui n'était « pas dans l'intérêt de l'Allemagne ».[22] Sous Guillaume II, l'Allemagne a poursuivi dans la voie du protectionnisme en interdisant, dans certains cas, les systèmes Marconi. Elle s'est engagée sur les marchés émergents en vendant sa technologie en Amérique du Sud et en Afrique afin d'établir la norme dans ces régions et s'assurer des revenus.

Lorsque ces efforts se sont révélés insuffisants, l'Allemagne a renoué avec le succès dans les organismes multilatéraux de normalisation. En 1906, elle a réuni les grandes puissances dans le cadre de la première Convention radiotélégraphique internationale, une conférence sur les normes radio. Les membres y ont conjointement interdit la politique de « non-intercommunication » de Marconi, brisant le monopole britannique et établissant un duopole anglo-allemand efficace.[23]

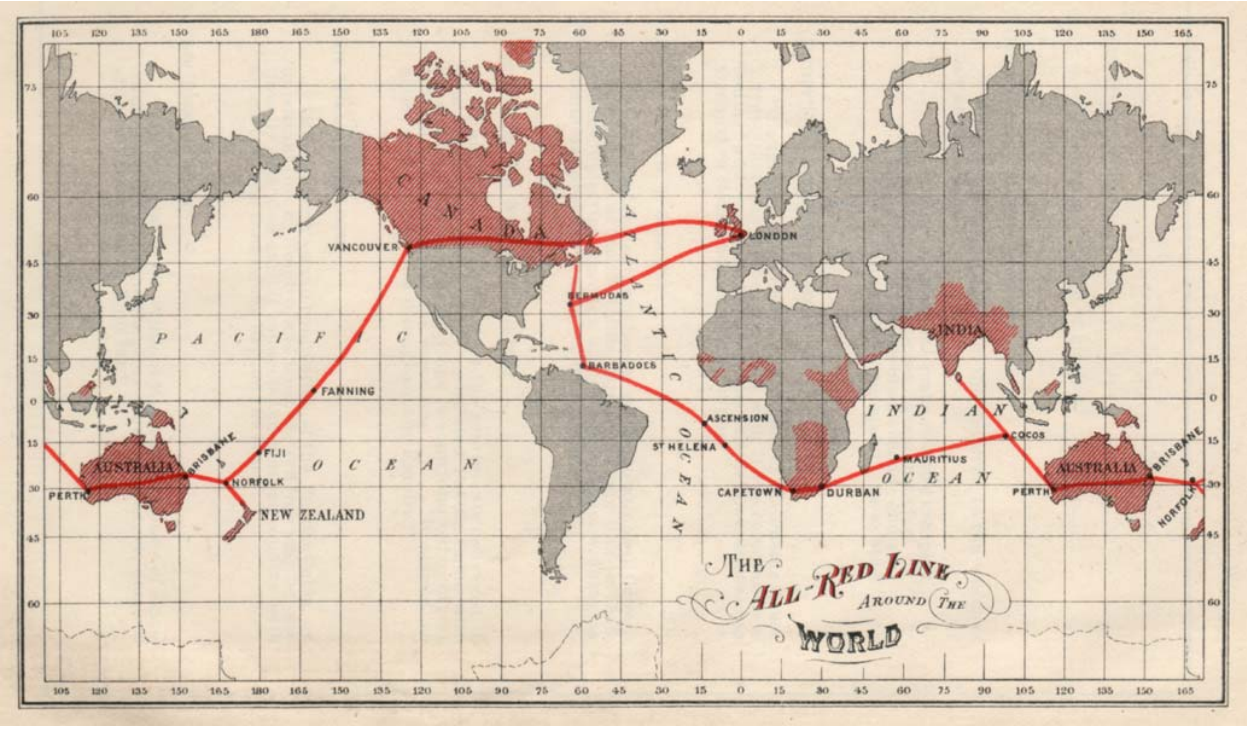
La concurrence anglo-allemande révèle que les organismes de normalisation ont d'énormes implications stratégiques. La Chine emploie aujourd'hui de nombreuses techniques utilisées par l'Allemagne il y a un siècle : politique industrielle dirigée par l'État, protection de l'État, généreux contrats de l'État, intégration civilo-militaire, interdiction des produits rivaux, fusions forcées, poursuite des marchés émergents et même traités internationaux pour fixer ses normes. Tous ces éléments ont aidé des entreprises technologiques chinoises comme Alibaba et Tencent, propriétaires de WeChat et Alipay, à devenir des champions locaux. Ces sociétés se sont depuis développées à l'étranger, ciblant souvent non pas le marché américain, mais (comme Telefunken en Allemagne avant eux) des marchés émergents avec des bénéfices plus faibles et une concurrence réduite.[24]

La Chine conteste également les normes dans l'infrastructure matérielle de la connectivité Internet. Son gouvernement investit des milliards pour que les fabricants de puces chinois puissent battre leurs rivaux américains dans la course aux normes Internet mobile 5G. De même, des entreprises chinoises comme Huawei et ZTE reçoivent des prêts publics pour construire l'infrastructure matérielle de la connectivité Internet dans les pays en développement. Comme le démontre l'exemple britannique, ces efforts font non seulement de la technologie chinoise la norme, mais ils offrent également des possibilités de surveillance. Dans le même temps, la

Nouvelle route de la soie soulève la possibilité que les normes relatives aux « infrastructures intelligentes » à travers l'Asie, en particulier les capteurs et les logiciels pertinents, puissent être établies par la Chine et puissent priver d'autres entreprises de l'interopérabilité, les fermant ainsi aux véhicules autonomes et autres industries.

La rivalité anglo-allemande dans le domaine de la télégraphie montre que Washington doit prendre au sérieux le défi lancé par l'État chinois en matière de normes. Elle présente également une voie à suivre. Tout comme l'Allemagne a utilisé les conférences internationales pour briser le monopole britannique dans le domaine de la télégraphie, les États-Unis pourraient établir ou préserver des normes favorables en matière de TIC par le biais d'accords multilatéraux. Cela pourrait empêcher la Chine d'établir des normes unilatérales par le biais d'accords de libre-échange, de champions de l'État ou de projets d'infrastructure.

3. La Grande-Bretagne dans la Première Guerre mondiale : le déploiement de l'hégémonie des informations



La « All red line », un réseau coûteux de lignes de câble sous-marines britanniques, construit avec d'énormes redondances et disposé de sorte qu'aucune partie ne passe par le territoire d'un rival. L'investissement insuffisant de l'Allemagne dans son propre réseau mondial de télécommunications résilient a permis à la Grande-Bretagne de la couper des communications mondiales, tandis que cette dernière restait généralement non affectée.

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

Les efforts déployés par l'Allemagne pour briser la domination britannique dans le domaine des télécommunications au début du XXe siècle ne relevaient pas de la paranoïa. Lorsque la Première Guerre mondiale a éclaté, la Grande-Bretagne a réussi à exercer son influence considérable sur les réseaux de télécommunications pour influencer le cours de la guerre. Elle a coupé les câbles allemands, surveillé les transmissions allemandes et forcé le trafic allemand sur les réseaux contrôlés par les Britanniques, découvrant ainsi le télégramme Zimmerman, qui a contribué à faire entrer l'Amérique dans la guerre.[26]

La Grande-Bretagne n'a pas été la première grande puissance à couper ou à manipuler les réseaux de télécommunications : le Pérou avait coupé une liaison entre le Chili et la Bolivie, les États-Unis avaient coupé les câbles espagnols, et la Grande-Bretagne avait coupé les Boers de leurs partisans européens lors d'une crise et manipulé le trafic par câble vers la France lors d'une autre.[27] Mais ces efforts ont été poussés à l'extrême lors de la Première Guerre mondiale

La Grande-Bretagne a été la première à couper un pays entier des principaux réseaux mondiaux de télécommunications, en déployant le premier jour de la guerre un plan soigneusement élaboré

en temps de paix.[28] En un an, la Grande-Bretagne a détruit les câbles allemands dans le monde entier : dans la Manche, la mer du Nord, l'Atlantique Nord, l'Amérique du Sud, une grande partie de l'Afrique, l'Extrême-Orient, et même dans les pays neutres qui hébergeaient les infrastructures allemandes.[29]

Pour compenser, l'Allemagne a tenté d'étendre le réseau radio construit par Telefunken une décennie plus tôt en Amérique latine et dans le « Sud », afin qu'il couvre le monde entier. Dans le cadre d'une initiative dont le parallèle moderne est la Route de la soie numérique de la Chine, Berlin a proposé des prêts et des investissements aux gouvernements intéressés par les « avantages de la radio pour le développement » afin qu'ils hébergent des nœuds de communication allemands. En réponse, la Grande-Bretagne a persuadé ou incité la plupart de ces pays à renoncer à soutenir les nœuds radio allemands ou à les saboter activement.[30]

Sans ses propres réseaux, Berlin n'a pas eu d'autre choix que de s'appuyer sur le réseau britannique pendant la guerre. Dès le début, les Britanniques ont commencé à surveiller discrètement tout le trafic qui passait par leurs câbles et ont utilisé cet avantage pour mener une guerre de l'information contre l'Allemagne, en divulguant de manière sélective le trafic allemand compromettant pour nuire à ses relations avec les pays neutres. Lorsque l'Allemagne a envoyé un télégramme proposant une alliance militaire avec le Mexique contre les États-Unis (le funeste télégramme Zimmerman), le message est passé par un réseau britannique et a été intercepté puis décrypté par la Grande-Bretagne, qui l'a ensuite partagé avec le gouvernement des États-Unis, qui l'a à son tour divulgué au public américain.[31] Cet incident a conduit à l'entrée des États-Unis dans la guerre, façonnant l'histoire mondiale et scellant la défaite de l'Allemagne.

La guerre de l'information entre la Grande-Bretagne et l'Allemagne souligne qu'il est dangereux de donner à une puissance rivale la possibilité de surveiller son trafic ou de couper son accès aux télécommunications. Elle révèle également que les réseaux que les grandes puissances considèrent comme acquis en temps de paix sont souvent déniés en temps de guerre, et que la lutte pour les nœuds de communication impliquera inévitablement des tiers et des pays neutres.

4. Victoire allemande à Tannenberg : les dangers de l'interception

Une station de télégraphe allemande sans fil pendant la Première Guerre mondiale. L'incapacité de la Russie à crypter correctement ses communications au niveau de ses stations de campagne a entraîné une défaite désastreuse qui a redéfini le cours de la guerre.

Source : C. O. Nordensvan and Valdemar Langlet, Det stora världskriget *[The Great World War]*[32]

L'Allemagne n'était pas entièrement dépourvue de compétences dans le domaine de la guerre de l'information. Elle a coupé les câbles terrestres et sous-marins russes qui la reliaient à ses alliés occidentaux, ainsi que plusieurs câbles transatlantiques dont dépendaient les Britanniques, introduisant ainsi l'utilisation de sous-marins pour ces tâches.[33] Compte tenu de la redondance des réseaux britanniques, ces efforts se sont en réalité révélés moins handicapants que ne l'espéraient les Allemands. En revanche, l'utilisation par l'Allemagne de renseignements radio contre la Russie lors de la bataille de Tannenberg en août 1914, le premier mois de la guerre, a eu des conséquences bien plus importantes et a abouti à une défaite désastreuse pour les Russes. Un agent des renseignements allemands de l'époque a qualifié l'incident de « premier dans l'histoire de l'humanité dans lequel l'interception du trafic radio ennemi a joué un rôle décisif ».[34]

La bataille a eu lieu alors que les Russes gagnaient du terrain sur le front oriental. Alors que la Russie s'enfonçait plus profondément dans la Prusse orientale, son armée s'est heurtée à un important problème de communication qui a ouvert la voie à une défaite désastreuse. Les Allemands en retraite avaient coupé leurs propres lignes télégraphiques, et les Russes qui avançaient manquaient de personnes formées pour établir des communications câblées sur l'ensemble de leur formation tentaculaire. La transmission radio offrait une alternative, mais si les Russes avaient adopté les nouvelles technologies radio pour leur commandement et leur contrôle militaires, ils ne les avaient pas suffisamment sécurisées. Différents groupes se sont vu attribuer des codes différents ; la plupart n'avaient reçu qu'une formation limitée en matière de codage et de décodage des signaux ; on sait que certains codes ont été déchiffrés par les Britanniques ; et les livres de codes étaient limités ou illisibles pour de nombreux conscrits

analphabètes.[35] En conséquence, les commandants russes ont estimé qu'ils devaient prendre le risque d'utiliser des messages radio non codés, avec l'espoir que les Allemands ne les surveilleraient pas attentivement.

Or, les Allemands surveillaient de près les signaux. Ayant constaté l'indiscipline de la radio russe dans la guerre contre les Japonais, ils savaient que les transmissions non codées russes ne faisaient pas partie d'une campagne de tromperie. Ils ont ensuite utilisé leur connaissance des communications russes en temps réel pour lever le « brouillard de la guerre » et vaincre définitivement la force supérieure. La Russie a perdu toute une armée, avec plus de 100 000 victimes et 92 000 prisonniers contre seulement 13 000 pertes allemandes.

5. La Grande-Bretagne pendant la Seconde Guerre mondiale : les limites du cryptage

Les rotors mécaniques de la machine de chiffrement de Lorenz considérée comme véritablement indéchiffrable pendant la Seconde Guerre mondiale. Les efforts britanniques pour percer le cryptage ont permis aux officiers d'accéder aux communications allemandes de haut niveau.

Source : Matt Crypto / Wikimedia Commons[36]

Les inventions de la télégraphie sans fil et de la radio ont apporté de plus grands avantages par rapport aux câbles physiques, mais comportaient un plus grand risque d'interception. Au cours des deux Guerres mondiales, les grandes puissances évoluaient dans un monde où les communications radio étaient présumées accessibles aux autres. Et dans un tel monde, pas si éloigné des hypothèses actuelles sur la vulnérabilité des systèmes informatiques et de télécommunication modernes, le cryptage était jugé essentiel à la sécurité. Le résultat, comme le décrit un historien militaire américain, était une « lutte entre le cryptographe et le cryptanalyste ».[37] Lorsque les grandes puissances se trouvaient du mauvais côté de cette lutte, les résultats pouvaient être catastrophiques.

Pour éviter de pareils résultats, les organisations utilisaient des codes secrets pour réduire le risque qu'une interception ne compromette la sécurité. Elles ont également imposé une « discipline radio » pour empêcher les adversaires de glaner des informations sur les schémas d'utilisation par l'analyse du trafic radio.

La plupart des grandes puissances ont investi dans un effort vraiment industriel pour étudier le trafic des adversaires et, si possible, pour percer leurs codes. La Grande-Bretagne centralisait

beaucoup plus ses analyses des codes ennemis que l'Allemagne, qui répartissait ces fonctions entre plusieurs agences. Et tout comme les succès britanniques dans le domaine du renseignement électromagnétique et de la cryptanalyse ont influencé le cours de la Première Guerre mondiale, ils ont également façonné le cours de la Seconde Guerre mondiale lorsque l'opération britannique de Bletchley Park a permis de déchiffrer les codes allemands Enigma et Lorenz.

Les systèmes de cryptage Enigma et Lorenz utilisaient des machines à rotor extraordinairement complexes pour coder des messages qui, selon l'Allemagne, « resteraient invulnérables ».[38] Chaque frappe remplaçait un caractère par un autre, selon des paramètres uniques à la machine, et ces paramètres (qui, pour le système de Lorenz, dépassaient le nombre total d'atomes dans l'univers) devaient être partagés par l'émetteur et le receveur pour lire le message.[39] Enigma était utilisé par l'armée, la Gestapo et les diplomates ; Lorenz, qui était encore plus complexe, était utilisé par Adolf Hitler et les hauts responsables et militaires nazis pour communiquer entre eux.

Les exploits britanniques dans le décryptage d'Enigma et de Lorenz sont le fruit de plusieurs développements. Tout d'abord, ils sont le fruit de la coopération des services de renseignement alliés avec la Pologne, qui avait exploité certaines erreurs allemandes pour percer des machines Enigma plus simples.[40] Comme l'a déclaré un cryptanalyste britannique de l'époque, leur effort « n'aurait jamais pu aboutir » sans les contributions de la Pologne.[41]

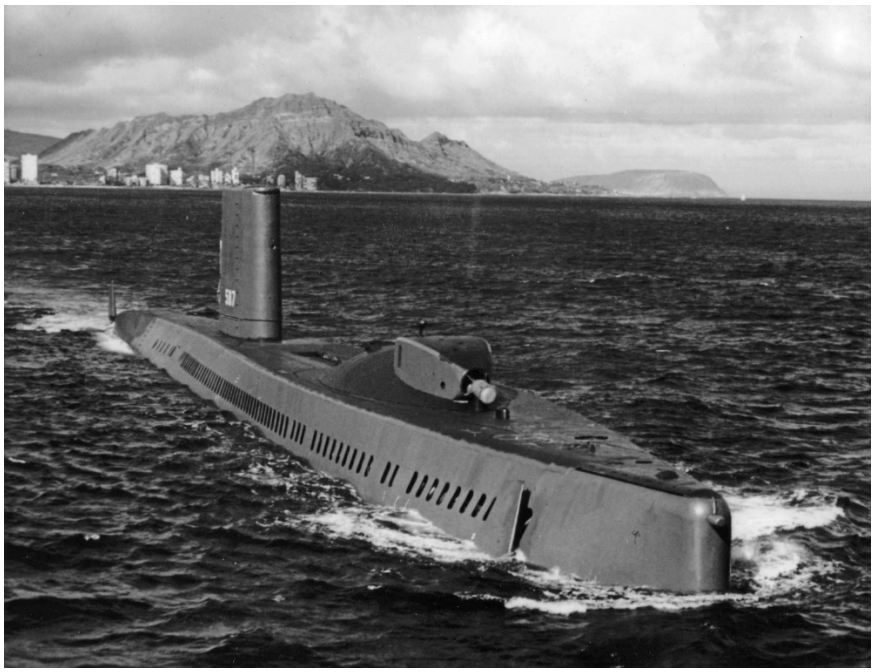
Ensuite, il sont le fruit d'un excès de confiance de la part de l'Allemagne, qui n'a jamais imaginé que les codes puissent être déchiffrés et qui a donc renoncé à des modifications, relativement simples, par lesquelles la Grande-Bretagne aurait été contrainte de tout recommencer.[42] Malgré tout, la foi allemande dans l'invulnérabilité de ses machines « était presque justifiée », témoigne un haut gradé de Bletchley Park.[43]

Et enfin, ils sont le fruit d'une défaillance unique, mais majeure, de la « discipline radio » allemande, qui a permis de rétroconcevoir les systèmes de cryptage allemands sans jamais en avoir vu un en personne.[44] Même les systèmes les plus sophistiqués étaient vulnérables aux erreurs humaines, et un adversaire vigilant pouvait les exploiter.

En brisant le cryptage d'Enigma et de Lorenz, la Grande-Bretagne avait accès à certaines des communications les plus confidentielles de l'Allemagne. Winston Churchill aurait déclaré que ces renseignements étaient l'une des principales raisons pour lesquelles la Grande-Bretagne a gagné la guerre, et Dwight D. Eisenhower les aurait qualifiés de « décisifs ».[45] L'historien officiel du renseignement britannique, Sir Francis Harry Hinsely, soutient que ces succès « ont écourté la guerre d'au moins deux ans et probablement de quatre ans », en sapant le maréchal Erwin Rommel en Afrique, en inversant fortement les pertes maritimes alliées dues aux sous-marins allemands et en permettant le débarquement en Normandie.[46] Ils ont également permis à la Grande-Bretagne d'identifier presque tous les espions allemands qui entraient dans le pays et de les retourner ou de les utiliser pour transmettre des renseignements erronés, le chef du programme faisant remarquer que les services secrets britanniques « dirigeaient et contrôlaient activement le système d'espionnage allemand dans ce pays ».[47] Rares sont les pays qui ont eu une connaissance aussi intime d'un autre pays en temps de guerre.

Pris en bloc, les efforts fructueux de la Grande-Bretagne contre l'Allemagne, la surveillance des communications allemandes par la Pologne en temps de paix et sa décision de partager sa découverte avec la Grande-Bretagne, recèlent des leçons valables aujourd'hui, lorsque les grandes puissances mènent une cyberreconnaissance les unes contre les autres. Plus généralement, ceux qui suggèrent que le cryptage atténue les problèmes liés à l'accès d'un adversaire à un réseau de télécommunications commettent peut-être une erreur semblable à celle que l'Allemagne a elle-même commise autrefois : une confiance excessive dans la technologie et une attention trop limitée à la possibilité toujours présente de l'erreur humaine.

6. Opération Ivy Bells : les profondeurs de la quête d'informations



L'USS Halibut, qui aurait été impliqué dans une tentative de mise sur écoute d'une ligne téléphonique soviétique sous-marine.

Source : U.S. Navy / Wikimedia Commons[48]

L'Union soviétique s'est montrée beaucoup plus prudente que les nazis concernant le cryptage, utilisant sa propre version d'Enigma, appelée Fialka, qui était nettement plus complexe.[49] C'est la raison pour laquelle les vastes quantités de renseignements de niveau stratégique produites pendant la Seconde Guerre mondiale après le décryptage des codes allemands n'avaient aucun équivalent connu du public pendant la guerre froide. Compte tenu de ces difficultés, d'autres méthodes de pénétration des télécommunications des adversaires ont été mises au point. L'un des efforts les plus audacieux portait sur les câbles sous-marins.

L'apparition des câbles sous-marins au XIXe siècle a suscité des actions visant à les couper et parfois à les exploiter, souvent dans des eaux peu profondes ou sur la terre ferme, où ces tâches sont plus faciles à réaliser. En revanche, mener ces opérations dans des eaux profondes contrôlées par un adversaire était considéré comme pratiquement impossible, surtout si cela devait être fait secrètement. Au début du XXe siècle, les Britanniques, puis les grandes puissances qui se sont succédé, ont pris une décision concernant la sécurité des câbles sous-marins : si les sites de pose étaient sécurisés et que les câbles ne traversaient pas de pays neutres ou non amicaux, ils étaient généralement à l'abri des interceptions et ne risquaient pas d'être coupés, en particulier en temps de paix.[50]

Or, pendant la guerre froide, ce calcul a changé. L'avènement des sous-marins nucléaires a ouvert la possibilité de mettre sur écoute des câbles sous-marins dans des eaux plus profondes.

Mais la tâche consistant à envoyer des plongeurs pour accéder aux câbles dans les grands fonds marins était considérée comme plus proche de l'exploration spatiale que les tentatives habituelles de manipulation de câbles des époques précédentes. La mise en place d'une mise sur écoute dans de telles conditions constituait également un défi technique.

Lorsque les États-Unis ont soupçonné qu'un câble sous-marin soviétique pouvait relier le quartier général de la marine à Vladivostok à une base sous-marine sur la péninsule du Kamchatka, ils ont cherché à contourner ces obstacles, démontrant ainsi la valeur du renseignement électromagnétique.[51] On pensait que l'écoute de ce faisceau de câbles de cinq pouces fournirait des informations cruciales sur les forces nucléaires soviétiques.[52] Alors que les Soviétiques cryptaient tout le trafic transmis par voie aérienne, les États-Unis comptaient sur le fait que ceux-ci partiraient du principe qu'il était pratiquement impossible d'accéder au trafic passant par les câbles sous-marins protégés et qu'ils ne le crypteraient donc pas. En outre, « les amiraux et généraux soviétiques seraient bien trop impérieux et impatients pour accepter un océan de cryptographes déjà dépassés par la masse de leur travail » et insisteraient pour avoir des communications vocales non sécurisées.[53] Une mise sur écoute fournirait alors une rare mine d'informations, et la marine américaine a lancé l'opération Ivy Bells pour la mettre en place.

Une grande partie de l'écoute et des renseignements recueillis reste confidentielle, mais des sources ouvertes donnent quelques détails sur cette opération unique et novatrice. Les États-Unis ont envoyé un sous-marin nucléaire, l'USS Halibut, pour se fondre discrètement dans la marine soviétique et trouver le câble sous-marin dans une zone de près de 1 000 000 de mètres carrés.[54] Une technologie innovante a été mise au point pour permettre aux plongeurs de travailler sous de grandes pressions et à des températures extrêmement froides pendant plusieurs heures. De même, de nouvelles méthodes pour installer des mises sur écoute dans cet environnement difficile ont été élaborées.[55] Tout cela devait être réalisé sans être détecté par les soviétiques, ni éveilleur leurs soupçons. Si le vaisseau avait été détecté, les Soviétiques l'auraient abordé ou détruit.

L'opération a finalement été couronnée de succès et, tout au long des années 1970, la marine américaine a exploité et enregistré des messages non sécurisés depuis ce câble. À quelques mois d'intervalle, les sous-marins américains se glissaient discrètement dans les eaux soviétiques, évitaient les sous-marins d'attaque, déployaient des plongeurs vers les câbles mis sur écoute et récupéraient les enregistrements des communications soviétiques, ce qui leur permettait d'obtenir des renseignements extrêmement précieux et rares. Si les États-Unis avaient développé un « réseau de satellites, d'avions, de stations d'écoute et de sous-marins espions » pour recueillir des renseignements sur les transmissions, ils « ne pouvaient pas pénétrer une ligne téléphonique câblée » sur le territoire d'un adversaire. Cet effort illustre le changement évolutif des télécommunications, à savoir que les données et les signaux transmis par n'importe quel support et par n'importe quel moyen peuvent être accessibles à un acteur déterminé disposant des bons outils. Si cette écoute a finalement été victime d'une fuite, les interceptions de télécommunications qui en ont résulté ont fourni des renseignements militaires et politiques inestimables aux États-Unis et à leurs alliés.[56]

La concurrence moderne dans le domaine des télécommunications dans une perspective historique

À la fin de la guerre froide, les États-Unis avaient clairement supplanté la Grande-Bretagne en tant que maîtres de l'information. Les États-Unis ont maintenu une position nodale sur l'Internet mondial, de solides capacités spatiales, une domination dans la plupart des technologies Internet et, selon les informations publiques, des capacités sophistiquées pour intercepter voire bloquer les communications de leurs adversaires.

Ces avantages américains sont aujourd'hui mis à l'épreuve, comme ceux de la Grande-Bretagne il y a plus d'un siècle. La Russie, et surtout la Chine, défient désormais la domination américaine. Si les États-Unis jouissent d'une position nodale dans de nombreux flux de données, d'autres puissances cherchent de plus en plus à réduire leur dépendance vis-à-vis des réseaux américains. Dans le même temps, la position nodale de l'Amérique est moins essentielle pour l'interception que celle de la Grande-Bretagne il y a un siècle. Internet rend possibles les intrusions sans contrôle de l'infrastructure physique. Les smartphones et les réseaux informatiques peuvent être piratés, et si les communications sensibles sont compromises par les écoutes physiques d'une époque antérieure ou par les intrusions virtuelles de l'époque moderne, le résultat final reste le même. Ce type de connexion crée probablement une plus grande vulnérabilité aujourd'hui qu'à l'époque du télégraphe ou de la radio sans fil.

La Russie a été l'un des principaux États à exploiter cette vulnérabilité. En 2007, la Russie a lancé une vague de cyberattaques contre les institutions estoniennes, principalement des attaques par déni de service.[57] En 2008, elle a lancé des cyberattaques lors de la guerre russo-géorgienne. Il s'agissait non seulement d'attaques par déni de service, mais également d'efforts visant à rediriger les sites Web du gouvernement, à prendre le contrôle des serveurs du gouvernement géorgien et à rediriger le trafic Internet géorgien via des serveurs contrôlés par la Russie (certaines des attaques mises en place avant le conflit coïncidant avec l'action militaire russe).[58] En 2014, lorsque la Russie a envahi la Crimée, elle a associé cyberattaques et contrôle physique des réseaux de télécommunications. Les soldats russes se sont emparés des installations de télécommunications ukrainiennes, les utilisant pour couper les communications en Crimée ainsi que pour procéder à des cyberattaques et à des perturbations dans d'autres régions d'Ukraine.[59] En 2015, la Russie a entamé une vague de cyberattaques contre les infrastructures ukrainiennes, privant d'électricité des centaines de milliers d'Ukrainiens dans le cadre de deux épisodes majeurs. Au cours des années suivantes, elle a lancé une vague d'attaques sans précédent dans toute l'Ukraine, touchant « les médias, la finance, les transports, l'armée, la politique et l'énergie », soit pratiquement tous les segments de la société ukrainienne, dans ce que certains considèrent comme faisant partie d'un exercice d'entraînement pour une campagne similaire contre les États-Unis.[60] Dans le même temps, elle a poursuivi toute une série d'attaques dans les pays baltes et a notoirement cherché à influencer les élections américaines de 2016 et 2020 par des campagnes de désinformation, ainsi que dans d'autres pays.[61] En 2021, le gouvernement américain a formellement accusé la Russie du piratage de la société informatique SolarWinds, une attaque sophistiquée qui a mis en péril une grande partie du gouvernement fédéral et plusieurs grandes entreprises américaines.[62]

La Chine est l'autre grande puissance qui investit de manière significative dans la concurrence en matière de télécommunications. Toutefois, contrairement à la Russie, les efforts de la Chine ne visent pas seulement à exploiter les infrastructures internet existantes, mais aussi à mettre en place des réseaux et des infrastructures qu'elle peut influencer, voire contrôler. Comme la Russie, la Chine a su exploiter les vulnérabilités existantes de l'Internet. Au début des années 2000, elle a lancé une vague d'attaques contre les réseaux du département américain de la Défense, dans ce que le département a appelé Opération Titan Rain.[63] Les gouvernements du monde entier (États-Unis, Royaume-Uni, France, Allemagne, Canada, Australie, Japon, Corée du Sud, Taïwan, Inde, et plus d'une douzaine d'autres) se sont plaints de l'intrusion chinoise dans leurs réseaux gouvernementaux. Certaines des cyberattaques les plus importantes de la dernière décennie ont été confirmées par le procureur général des États-Unis William Barr comme ayant été perpétrées par des agents chinois, notamment des vols de dossiers de l'U.S. Office of Personnel Management (dossiers de 21 millions de personnes), des hôtels Marriott (400 millions), de l'assurance santé Anthem (80 millions) et d'Equifax (147 millions), entre autres.[64]

Dans le même temps, la Chine pose également les bases d'une future infrastructure Internet et, à la lumière de ses efforts précédents, il est peu probable que cet effort soit commercial aujourd'hui ou reste purement commercial dans la période à venir. Les investissements de la Chine sont les plus notables dans les réseaux 5G qui devraient constituer les bases d'une économie plus intelligente et connectée reliant entre eux d'innombrables appareils et capteurs. Désireuse de développer ces réseaux dans le monde entier, la Chine a subventionné ses entreprises championnes de la 5G et ses projets dans le monde entier dans le cadre d'une initiative de Route de la soie numérique. Grâce à des prix compétitifs, des entreprises comme Huawei ont pu surpasser les autres grands opérateurs de la 5G et conquérir une part de marché mondial importante, faisant de la Chine un leader dans la mise en place de ces réseaux. Et en dehors de la 5G, le gouvernement chinois a subventionné les efforts de création d'infrastructures internet ou de communication sur pratiquement tous les continents. Tous ces efforts sont complétés par une campagne visant à façonner les normes mondiales, une priorité politique essentielle pour la Chine, inscrite dans des documents de planification de haut niveau qui, comme dans la rivalité anglo-allemande sur la radio il y a un siècle, pourrait façonner l'avenir des télécommunications dans un sens favorable à la Chine. À cette fin, la Chine a récemment dévoilé une nouvelle initiative en matière de sécurité des données.[65]

Certains craignent que les activités de la Chine ne laissent entrevoir la possibilité que Pékin exerce un contrôle de facto sur ces réseaux, que ce soit pour intercepter le trafic ou pour en empêcher l'accès. Peu d'informations publiques sont disponibles sur les efforts de la Chine pour acquérir ce contrôle, mais le gouvernement américain a révélé en février 2020 que Huawei disposait de portes dérobées dans ses équipements réseau, qu'elle ne les avait pas divulguées aux entreprises concernées avec lesquelles elle avait passé des contrats, et que ces portes dérobées allaient au-delà de celles parfois demandées par les gouvernements hôtes dans le cadre d'interceptions légales.[66] En outre, les rapports publics ont révélé que Huawei a aidé des gouvernements comme l'Ouganda et la Zambie à obtenir l'identité de dissidents.[67] Au-delà même de l'affaire Huawei, une entreprise de cybersécurité a récemment découvert des portes dérobées dans un logiciel fiscal obligatoire dont l'installation est imposée par le gouvernement chinois aux entreprises étrangères.[68] Que ces cas suggèrent ou non que Huawei a elle-même profité de sa

position dans ces réseaux, le comportement de l'entreprise et les antécédents de la Chine en matière de cyberattaques et d'espionnage restent une source d'inquiétude.

L'autre grand motif de préoccupation provient de l'histoire et du comportement des grandes puissances, même libérales, qui sont davantage contraintes par l'État de droit. En effet, les cas historiques précédents suggèrent fortement que le type de pouvoir et d'influence qu'une entreprise comme Huawei exercera est susceptible d'être exploité par le gouvernement chinois, tout comme d'autres grandes puissances ont souvent exploité la position de leurs entreprises ou leurs capacités dans le domaine des télécommunications.

Dans cette perspective historique élargie, les faits peuvent amener de nombreux observateurs à conclure que la prudence est de mise quant au rôle de Huawei dans les réseaux de télécommunications, même si les motivations de la société sont en effet purement commerciales, ses promesses de « pas de portes dérobées et pas d'espionnage » crédibles, et Pékin sincère dans son engagement à honorer ces promesses.

Plus généralement, comme le montre ce rapport, de nombreuses caractéristiques de la concurrence entre grandes puissances dans le domaine des télécommunications, considérées comme nouvelles aujourd'hui, ont leurs racines dans le passé. Au fil de l'histoire, plusieurs thèmes se répètent :

- *Pouvoir :* le contrôle des réseaux de télécommunications est une forme de pouvoir politique depuis leur création il y a plus de 150 ans. La Grande-Bretagne a profité de son rôle dans les télécommunications et la radio, les États-Unis l'ont probablement fait à l'ère de l'Internet moderne, et il y a lieu de s'inquiéter de ce que la Chine puisse tenter de le faire aujourd'hui.

- *Négligence* : de longues périodes de paix et de prospérité ont conduit à une certaine insouciance à l'égard des risques liés aux télécommunications. Au XIXe siècle, les grandes puissances se contentaient de faire confiance aux entreprises étrangères et aux réseaux exploités par des étrangers, tout comme les États d'aujourd'hui sont disposés à accepter les équipements et l'exploitation des télécommunications chinois. Mais finalement, le recours à des concurrents ou à des adversaires potentiels s'est avéré désastreux pour des pays comme l'Allemagne et a redéfini la politique internationale.

- *Exploitation :* les nouvelles technologies de télécommunications ont toujours donné lieu à de nouveaux efforts pour les intercepter, les bloquer ou les exploiter. Malgré l'espoir que le cryptage puisse compliquer les efforts de la Chine pour intercepter les communications modernes, les périodes passées de grands espoirs dans le cryptage ont été anéantis par des erreurs humaines et les efforts déterminés de pays rivaux pour les percer, comme l'Allemagne l'a découvert lorsque la Grande-Bretagne a percé ses cryptages supposés « incassables ». L'humilité doit être de rigueur à chaque vague de technologies prétendument sûres.

- *Champions :* les États recherchent souvent leurs propres champions en matière de télécommunications, en particulier lorsque les tensions entre grandes puissances montent. Le gouvernement chinois est fier des réalisations de Huawei et en assure la promotion dans le monde entier, menaçant même les États qui refusent sa technologie. Il serait surprenant qu'une entreprise aussi proche de son gouvernement d'origine soit à l'abri des pressions de l'État, alors que tant d'autres champions des télécommunications à travers l'histoire ne l'ont pas été.

- *Normes* : les normes de télécommunications peuvent déterminer qui détient le pouvoir sur le réseau. L'Allemagne a utilisé un organisme de normalisation pour briser la domination de la Grande-Bretagne dans le domaine de la radio sans fil. Aujourd'hui, cette concurrence est présente au sein d'organismes tels que l'Union internationale des télécommunications, et le rôle de Huawei dans cette lutte montre qu'il est nécessaire de se demander si ses normes permettront à la Chine de remodeler les télécommunications.

- *Déni :* la sécurité des réseaux ne se limite pas à l'interception et à la sécurité des données, mais concerne également le déni d'exploitation de l'ensemble du réseau ou de l'accès aux réseaux extérieurs. La Grande-Bretagne a coupé l'Allemagne des réseaux télégraphiques mondiaux ; le rôle de Huawei dans les réseaux pourrait lui permettre de fermer les réseaux dans les pays où elle exploite des équipements, même si elle est incapable d'accéder facilement aux données.

- *Détermination :* de nombreux États minimisent le niveau d'efforts extraordinaires qu'un adversaire peut déployer pour compromettre leurs réseaux, et sont ensuite désagréablement surpris lorsque cela se produit. La capacité de la Grande-Bretagne à décrypter les codes allemands pendant la Seconde Guerre mondiale grâce à des efforts à l'échelle industrielle et la capacité des États-Unis à exploiter les câbles sous-marins soviétiques internes, censés être inaccessibles, montrent jusqu'où les grandes puissances sont prêtes à aller pour accéder à des renseignements critiques dans le domaine des transmissions. La Chine, elle aussi, est susceptible d'entreprendre de tels efforts considérables, et même si Huawei aura du mal à tirer parti de sa position dans les réseaux modernes, sous-estimer l'ingéniosité et la détermination d'un concurrent déterminé comme la Chine est un thème récurrent dans la lutte pour les télécommunications.

Comme le démontre ce rapport, de nombreuses caractéristiques du jeu des grandes puissances en matière de télécommunications restent les mêmes, même si les acteurs sont différents.

À propos des auteurs

Rush Doshi a été directeur de la Brookings China Strategy Initiative et membre de la Brookings Foreign Policy. Il a également été membre du Paul Tsai China Center de l'école de droit de Yale et membre de la première promotion des Wilson China Fellows. Ses recherches se sont concentrées sur la grande stratégie chinoise et sur les questions de sécurité indo-pacifiques. Rush Doshi est l'auteur de *The Long Game: China's Grand Strategy to Displace American Order*, à paraître chez Oxford University Press. Il est actuellement au service de l'administration Biden.

Kevin McGuiness a récemment travaillé avec Brookings en tant qu'intervenant externe auprès du Department of Defense Skillbridge Program, où il a contribué à divers projets au sein du Center for East Asia Policy Studies. Vétéran de l'armée de l'air, il a récemment terminé son mandat de professeur à la United States Air Force Academy, où il dirigeait des cours de relations internationales et de politique asiatique. Récemment, il a également exercé les fonctions d'assistant de recherche au Center for the Study of Chinese Military Affairs de l'Institute for National Strategic Studies, où il s'est consacré à la modernisation de l'APL et à la sécurité dans la région indo-pacifique.

Remerciements

Les auteurs souhaitent remercier les anciens stagiaires Isabella lu, Zijin Zhou et Gaoqi Zhang pour leur aide à la recherche sur ce projet, plusieurs examinateurs anonymes, Claire Harrison et Ted Reinert pour l'édition du rapport, ainsi que Chris Krupinski et Rachel Slattery pour la mise en page et la conception Web. Brookings remercie le Département d'État américain et l'Institute for War and Peace Reporting d'avoir financé ces recherches.

Ce rapport a été élaboré avant l'entrée au service gouvernemental de Rush Doshi, concerne uniquement des sources ouvertes et ne reflète pas nécessairement la politique ou la position officielle d'un organisme du gouvernement américain.

La Brookings Institution est une organisation à but non lucratif qui se consacre à la recherche et aux solutions politiques indépendantes. Sa mission est de mener des recherches indépendantes de haute qualité et, sur la base de ces recherches, de formuler des recommandations pratiques et novatrices à l'intention des responsables politiques et du public. Les conclusions et les recommandations de toute publication de Brookings sont uniquement celles de son ou de ses auteurs et ne reflètent pas l'opinion de l'institution, de sa direction ou de ses autres chercheurs.

---

[1] Steven Chase, Robert Fife, et Barrie McKenna, « Trudeau Refuses to Let 'politics Slip into' Decision on Huawei, » The Globe and Mail, 15 octobre 2018, https://www.theglobeandmail.com/politics/article-trudeau-refuses-to-let-politics-slip-into-decision-on-huawei/ ; Greg Quinn et Josh Wingrove, « Trudeau Says Politics Won't Factor Into Huawei 5G Decision, » Time, 19 décembre 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), chapitre 1.

[3] Ibid., cette observation est celle d'Headrick.

[4] Ibid.

[5] Ibid.
[6] Ibid., cette observation est celle d'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.
[9] « NH 79949 Cienfuegos Cable-Cutting Operation, 11 May 1898, » Naval Historical Center Online Library, https://www.history.navy.mil/content/history/nhhc/our-collections/photography/us-people/b/baker-benjamin-f/nh-79949.html.
[10] Ibid., chapitre 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 novembre 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] Library of Congress, George Grantham Bain Collection, https://www.loc.gov/pictures/item/2014683102/.
[18] Bien que, comme le remarque Heidi Tworek, son propre rôle ait souvent été exagéré dans le développement de cette technologie. Heidi Tworek, *News from Germany.*
[19] Marc Raboy, « The First Company That Wanted to 'Connect the World' Wasn't Google or Facebook, » Media@LSE, 24 août 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 janvier 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] Par exemple, Telefunken était actif même dans les régions où l'Allemagne n'avait pas une présence coloniale importante, comme l'Amérique latine.
[25] George Johnson, ed., *The All Red Line: The Annals and Aims of the Pacific Cable Project* (Ottawa : James Hope and Sons, 1903), 10, at 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 décembre 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 janvier 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 and Valdemar Langlet, *Det stora världskriget* [The Great World War] (1915), at 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, » 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., 19 octobre 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.
[39] 1 x 10^{170} réglages possibles.
[40] « Bletchley Park Remembers Polish Code Breakers, » BBC News, 14 juillet 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] Voir, par exemple, 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 avril 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.
[48] U.S. Navy, Wikimedia Commons, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.
[49] Anna Borshchevskaya, « The Soviets' Unbreakable Code, » Foreign Policy, 27 avril 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.
[50] Daniel R. Headrick, The Invisible Weapon, chapitre 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 mars 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 avril 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 janvier 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 mars 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 mai 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 juin 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, 19 octobre 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, 28 juin 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 janvier 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, 11 février 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 septembre 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 février 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 août 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 juin 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.