화웨이와 역사의 만남: 강대국과 통신 위험, 1840년~2021년

Rush Doshi 및 Kevin McGuiness

Brookings Institution, 2021년 3월

요약

2018년 말 캐나다가 화웨이를 통신 네트워크로 허용할지 여부에 대해 미국이 우려하는 가운데 Justin Trudeau 캐나다 총리는 세계 각지의 전통적인 지혜를 포착한 일련의 성명을 발표했습니다. 캐나다 총리는 당시 "이것은 정치적 결정이 아니어야 한다"고 말하며 캐나다는 자국 네트워크에서 화웨이의 역할에 대해 "정치적 결정을 내리지" 않을 것이라고 선언했습니다.[1]

통신 관련 문제에서 패권 정치가 배제될 수 있다는 생각은 낙관적일 뿐만 아니라 통신의 역사와도 맞지 않는 것입니다. 이 보고서는 이러한 역사를 탐구하며, 패권과 통신이 거의 항상 긴밀하게 연결되어 있음을 보여줍니다. 국가들이 그러한 연결 고리를 무시하고 자국의 네트워크 보안에 무신경했을 때, 그 결과는 불이익이었고 때로는 재앙이었습니다.

이 보고서에서는 1840년대 전기 통신 초창기 시대로 거슬러 올라가 통신 분야에서 강대국 간 경쟁의 몇 가지 주요 사례를 검토합니다. 이러한 사례는 오늘날 정책 입안자들이 직면한 많은 문제들이 과거와 밀접한 유사점을 가지고 있음을 보여줍니다. 네트워크 보안과 5G 인프라에 대한 현재의 논쟁은 새로운 느낌을 줄 수 있지만, 실제로 150년 전 전기 통신의 여명기로 거슬러 올라가면 잊혀진 논쟁들을 반영하는 것입니다. 더욱이, 경쟁 우위를 확보하기 위해 이용하는 표준 설정 기구, 국가 보조금, 케이블 탭핑, 정보 전쟁, 개발도상국 시장 등 오늘날의 통신 분야 경쟁의 많은 익숙한 요소가 1세기 이상 전에 개발되었으며, 현재 논쟁에 중요한 교훈을 줍니다.

이러한 주요 교훈의 목록은 아래와 같습니다.

1. **글로벌 통신 네트워크에 대한 통제는 정치적 패권의 한 형태입니다.** 5G 네트워크는 수많은 기기와 센서를 연결하는 보다 스마트한 연결된 경제의 기반을 형성할 것으로 기대됩니다. 전 세계에 이러한 네트워크를 구축하고자 하는 중국은 "디지털 실크 로드" 이니셔티브의 일환으로 전 세계적으로 5G Champion 기업 및 프로젝트에 자금을 지원하고 있습니다. 이러한 노력은 전신 개발 초창기에 네트워크 지배권을 추구한 영국의 노력에 비유할 수 있습니다. 영국은 심지어 케이블이 영국을 통과하도록 유도하기 위해 수수료 및 경제적 혜택을 포기하는 등 다른 국가들의 네트워크 의존도를 꾸준히 높이는 한편 영국의 해외 네트워크에 대한 의존도를 줄임으로써 60년 이상 그 이점을 누릴 수 있었습니다. 결과적으로 영국은 세계 케이블 트래픽의 절반 이상, 최대 무선 네트워크, 최대 규모의 케이블 선박을 통제했습니다. 영국의 "정보 헤게모니"는 제1차 세계대전에서 거의 모든 세계 통신으로부터 독일을 단절시키고 독일에게 영국이 감시하기 쉬운 영국 소유 통신선을 경유하도록 강요했는데, 이는 후일 독일 패배의 결정적 요인으로 판명되었습니다.

2. **장기간의 평화와 번영은 일반적으로 통신 위험을 경시하게 됩니다.** 지난 30년 동안 탈냉전 시대 평화와 경제적 세계화는 통신 분야의 급속한 발전과 일치했으며, 이로 인해 각국은 외국이 소유 또는 운영하는 네트워크를 비롯해 정치 및 안보 위험보다 혁신적인 상업적 혜택에 우선 순위를 두었습니다. 1840년대 통신 여명기에도 비슷한 전개가 발생했고, 이는 또한 제1차 세계대전이 발발할 때까지 지속된 비교적 평화로운 세계화 시대와 일치합니다. 그 기간 동안 대부분은 겉으로 보기에는 기적 같은 새로운 통신 기술의 상업적 잠재력을 포착하고자 하는 열망에 외국 네트워크 또는 회사에 대한 의존과 관련된 의문은 모호해졌습니다. 영국은 다른 국가들의 안주로 혜택을 누렸습니다. 글로벌 네트워크에서는 공격받을 수 없는 접속점 위치를 구축하고 이용함으로써, 다른 강대국 대부분은 영국의 네트워크에 의존하게 되었습니다.

3. **국가가 통신 안보에 대해 안주하면 그 결과는 재앙이 될 수 있고 세계 정치의 판도를 바꿀 수 있습니다.** 독일 정부가 수십 년 동안 영국 통신선에 안이하게 의존하다가 그러한 의존성의 위험을 깨달았을 때는 상황을 바꾸기에 이미 너무 늦었습니다. 제1차 세계대전이 발발했을 때, 영국이 독일의 모든 케이블을 절단하여 독일은 감청의 위험에도 불구하고 영국 네트워크를 경유할 수 밖에 없었는데, 이 덕분에 미국을 전쟁으로 내몬 "치머만 전보"가 발견되었습니다. 마찬가지로, 제1차 세계대전에서 러시아군의 규율 없는 무선 통신 덕분에 독일군은 통신을 도청하여 타넨베르크 전투에서 러시아군의 이동을 실시간으로 "확인"하면서 결정적인 패배를 안길 수 있었습니다. 또한 제2차 세계대전에서는 나치가 암호에 대한 지나친 자신감으로 암호를 업데이트하는 노력을 소홀히 하는 바람에 영국은 암호를 해독하여 전쟁을 2~4년 단축시킨 것으로 믿어지는 정보를 얻을 수 있었습니다. 정보의 힘을 감안하면 신호가 간헐적으로 증가하는 경우에도 무규율 또는 안주로 역사가 바뀔 수 있습니다.

4. **새로운 기술은 항상 감청에 대한 새로운 노력을 촉발합니다.** 해저 케이블의 등장은 미국-스페인 전쟁 초기에 이러한 케이블을 절단하고 탭핑하기 위한 노력으로 이어졌습니다. 무선 전송은 네트워크 노드를 캡처하고 통신을 감청하기 위한 경쟁국들의 노력을 증가시켰고, 암호화를 위한 정교한 암호의 출현은 이를 해독하기 위한 산업 차원의 노력을 촉발했습니다. 각 시대마다, 통신 기술의 새로운 도약이 이전 기술보다 덜 취약할 것이라고 믿는 사람들이 있었습니다. 그러나 매번 혁신과 악용의 주기는 계속되었습니다.

5. **통신 네트워크는 특히 긴장의 시기에 정치적 중립이 된 적이 없습니다.** 2019년 화웨이 경영진은 "백도어 및 스파이 행위 없음" 서약을 하고 회사가 정치적 중립을 유지할 것을 약속하고 중국 정부도 이 서약을 존중하겠다고 확인했습니다. 그러나 1세기 전에, 통신 회사 및 해당 정부는 공개적으로 그와 비슷한 약속을 해놓고는 평화 시와 전시 모두에서 비밀리에 협력하며 약속을 깼습니다. 예를 들어 영국은 해저 케이블 지배력 덕분에 프랑스, 독일, 미국이 전시에도 통신선을 중립적으로 유지할 것을 지지하도록 이끌었습니다. 영국 기업들은 공개적으로 중립을 선언했지만 실제로는, 특히 긴장이 고조되는 순간에, 영국의 정치적 이해를 따랐고, 전쟁 기간 중에는 중립성을 완전히 포기했습니다. 경쟁국의 정보 흐름을 방해하거나 감청해 확보할 수 있는 힘은 일반적으로 진지한 중립 표명을 지키기에는 너무 매력적이었습니다.

6. **국가들은 흔히 경쟁국 또는 적대국 기업에 의존하는 데 따른 취약성을 인지하면 종종 자국의 통신 분야 챔피언을 찾습니다.** 미국은 현재 5G 기지국의 주요 제조업체가 없으며, 이는 자국 기업에 투자해야 하는지 아니면 동맹국 기업에 의존해야 하는지에 대한 논쟁을 촉발하고 있습니다. 또한 화웨이가 사실상 국가 챔피언이 되는 정도에 대한 의견 차이를 더욱 첨예하게 만들었습니다. 이러한 논쟁은 몇몇 선례가 있습니다. 20세기 초, 통신 장비 또는 네트워크를 다른 국가에 의존하는 많은 국가들이 자체 시스템을 구축하기 시작했습니다. 예를 들어, 독일은 무선 분야에서 경쟁하는 두 독일 기업 Siemens & Halske 및 AEG가 공동으로 영국의 무선 통신 지배력에 대항할 독일 기업을 설립하도록 종용했습니다. 다른 많은 주요 국가들은 겉으로는 민간 기업으로 보이지만 지원 국가와 서로 얽혀 있는 기업들을 지지했습니다.

7. **통신 표준을 위한 투쟁은 어떤 국가가 네트워크 권력을 휘두르는지 결정할 수 있으며, 동맹국과 협력국들을 나열해야 하는 경우가 많습니다.** 보유 기술이 지배적 표준이 된 국가는 다른 국가보다 더 큰 영향력을 발휘할 수 있습니다. 현재 정보통신 기술 표준을 놓고 경쟁하는 것은, 이런 면에서, 무선 네트워크에 대한 영국과 독일 간 경쟁과 비슷합니다. 영국은 지원하는 Marconi사를 통해 무선에서 매우 지배적인 위치에 있었고, 다른 모든 강대국들은 다른 모든 무선 기지국과의 연결을 거부한 영국의 무선 네트워크를 통해 메시지를 전달해야 했습니다. 독일은 결국 미국, 프랑스 등 다른 강대국의 도움을 받아 이 "비 상호 통신" 정책을 금지한 표준 설정 기구에서의 주도권을 무너뜨리는 데 성공을 거두었습니다. 이는 자유주의 국가들이 함께 협력할 경우 어떻게 이와 유사한 동맹 접근 방식을 사용하여 유리한 정보 통신 기술(ICT) 표준을 설정하거나 유지할 수 있는지 잘 보여줍니다.

8. **국가들은 통신 감청이 용이해짐에 따라 암호화로 전환했지만, 완강한 적대국 또는 사용자 실수로 인해 암호화가 한계를 갖는 경우가 많습니다.** 일각에서는 화웨이의 네트워크 역할 또는 인터넷에 연결된 기기의 일반적인 취약성을 우려할 경우 최신 암호화를 통해 문제를 개선할 수 있다고 주장합니다. 이러한 주장은 오랜 역사를 가지고 있습니다. 1세기 전 통신 기술의 여명기에, 네트워크 노드를 제어하는 다른 사람이 전보 메시지를 읽을 수 있거나 수동형 수신 장치로 무선 시스템을 감청할 수 있는 가능성 때문에 암호화 기술이 크게 발전하면서 때로는 지나친 자신감이 생겼습니다. 독일의 복잡한 회전자 암호기는 해독이 불가능한 것으로 여겨졌지만, 사용자 오류와 영국의 산업 차원의 노력 덕분에 영국이 독일 암호를 해독할 수 있었습니다. 독일의 장비 및 암호를 저렴한 비용으로 업데이트했다면 영국의 우위를 막을 수 있었을 것입니다. 그러나 암호화에 대한 독일의 지나친 자신감이 이러한 변화를 미리 차단하는 바람에 정보 누설로 전쟁 판도가 재편되었습니다. 종단간 암호화는 이전의 암호화 방식보다 훨씬 더 발전했지만 역사는 약간의 겸손이 필요하다고 경고합니다.

9. **많은 국가가 적대국이 그들의 네트워크를 손상시키기 위해 엄청난 노력을 할 수 있는 정도를 평가 절하합니다.** 현대 통신에 대한 논쟁 속에서 편의성 또는 상업성에 우선순위를 두고 따라서 안보에서는 지름길을 택한 국가들은 완강한 적대국이 그들의 네트워크를 손상시키는 노력에 종종 경악하게 되었다는 것을 주목할 필요가 있습니다. 제1차 세계대전에서 독일은 독일이 외부 세계에 액세스하는 데 사용한 모든 케이블을 영국이 잘라내는 속도와 무자비함에 경악했습니다. 마찬가지로 러시아 지휘관들은 규율 없는 무선 통신으로 타넨베르크에서 재앙 수준의 패배를 당했을 때 경악했습니다. 제2차 세계대전 당시 독일은 영국이 아무리 사소하고 일시적이더라도 독일의 통신 실수를 이용할 수 있는 고도로 중앙화된 산업 차원의 암호 해독 작업을 구축할 것으로 예상하지 못했습니다. 그리고 냉전 기간 동안 소련은 미국이 접근할 수 없을 것이라고 믿었던 해저 전화선을 암호화한 적이 없었지만, 미국은 그것을 탭핑할 방법을 발견했고 귀중한 정보 소스를 얻게 되었습니다.

10. **네트워크 보안은 감청뿐 아니라 거부와도 관련됩니다.** 화웨이의 네트워크 역할에 대한 논쟁의 일부는 데이터 보안에 대한 의문을 강조하고 있지만, 강대국 통신 경쟁의 중요한 부분인 네트워크 거부를 더 많이 고려하면 도움이 될 수 있습니다. 전신의 여명기에는 독일이 외부와 연결할 수 있는 전 세계의 모든 케이블을 절단하는 영국의 전례 없는 치밀한 작전에서 강대국들이 케이블을 절단하고 통신을 거부하는 노력이 절정에 달했습니다. 경우에 따라 네트워크 거부 전략을 추진하는 국가가 피해를 입을 수 있지만 상대국 피해가 더 클 것으로 판단하면 강행할 수 있습니다.

강대국과 통신

"대제국들은 정보의 흐름을 가속하기 위해 많은 노력을 기울였다"고 통신 역사는 말합니다. "로마인은 도로를 건설했고 페르시아인과 몽골인은 말을 사육했고 영국인은 우편 증기선을 지원했습니다."[2] 각국이 정보를 갈망했지만 현대의 전신 기술이 등장할 때까지는 그 흐름이 제한적이었습니다. 정보 흐름의 전기화가 현대 통신을 창조했고, 현대 통신에 대한 익숙한 패턴의 강대국 경쟁이 촉발되었습니다.

1840년부터 제1차 세계대전에 이르기까지 현대 통신 초기의 몇십 년은 현재 순간과 중요한 특성을 공유하고 있습니다. 이 시기는 현재의 탈냉전 시대와 마찬가지로 통신 네트워크의 정치 및 안보에 대한 질문에 주요국들이 "덜 민감하게" 반응하는 상대적인 강대국 평화 중 하나였습니다.[3] 19세기에 강대국들이 국가 및 국제 네트워크를 확장하면서, 많은 국가가 처음에는 산업에 일임하고, 민간 기업의 국적을 무시하고, 적대국이 통신 네트워크를 통제하는 위험을 평가 절하했습니다. 당시 일부 사람들은 "시간과 공간의 소멸"이라 불렀던 통신 분야의 혁신적인 변화의 이점은[4] 너무나 분명하고 압도적이어서 "케이블 소유권은 사소한 문제로 인식되었습니다."[5] 한 역사가는 당시에는 전신이 정치보다는 비즈니스에서 더 큰 의미를 가졌다고 언급했는데, 이는 현대 정보 기술과 최근의 재현인 5G에 대한 초기의 흥분에도 쉽게 적용될 것입니다.[6]

상대적 강대국 안주 시기는 지속되지 않았습니다. 1879년의 페루와 1898년의 미국과 같은 국가들이 최초로 경쟁국의 통신 네트워크를 단절했습니다. 강대국 간 긴장이 고조되자, 세계 각국은 영국이라는 국가가 어떻게 긴 평화를 잘 관리했는지, 그들의 민간 회사를 통해 국제 통신에서 교두보를 확보했는지 깨달았습니다.

영국 해저 케이블 네트워크에 대한 의존도가 점차 높아짐에 따라 프랑스와 독일 같은 국가에서는 자체 네트워크 개발 과정에서 상당한 개발 보조금을 지급했습니다. 이는 중국이 알리바바, 바이두, 텐센트, 화웨이와 같은 정보 기술 챔피언을 보호하고 지원하는 것과 다르지 않습니다. 역사가 Heidi Tworek는 영국의 경쟁국들 또한 영국 소유의 해저 텔레그래프 케이블에 대한 의존도를 줄이기 위해 차세대 통신 기술인 "무선 전신"에 막대한 투자를 했다고 기록하고 있습니다.[7] 영국이 이 분야를 주도했지만 독일은 영국의 네트워크에 의존하기를 거부했습니다. 독일은 국가 지원 챔피언들이 세계의 저연결 지역(라틴 아메리카, 아프리카, 아시아)에 진출하는 등 자체 네트워크를 구축했습니다. 이는 중국 기술 기업의 개발도상국 진출과 중국의 5G 네트워크 구축 의지와 닮은꼴입니다.

이 기간 동안, 오늘날 때때로 무시되고 있는 강대국 통신 경쟁의 많은 요소들을 그 시대의 국가들은 상당히 심각하게 받아들인 경우가 많았습니다. 영국의 무선 네트워크 주도권에 좌절한 독일은 영국의 주도권을 무너뜨리는데 표준 설정 기구를 사용했습니다. 이 전술은 당시 그러한 기구가 지금보다 덜 중요한 것이 아니었음을 잘 보여줍니다. 그리고 통신이 무선으로 전환되고 감청이 더욱 쉬워지면서 강대국은 암호화에 대한 믿음을 갖게 되었습니다. "암호화"(메시지 암호화 또는 해독을 위한 세부 단계)가 문제를 해결할 것이라는 가정 하에 때때로 규율이 엄격한 네트워크 운영을 믿게 되었습니다. 이는 사용자 실수 때문에 거의 항상 잘못된 믿음으로 판명되었습니다. 이러한 견해는 통신 네트워크의 전반적인 불안정성에 대한 현대적 가정, 그리고 화웨이에 대한 논쟁에서 암호화가 중국의 통신 네트워크 액세스 위험을 크게 상쇄할 것이라는 일각의 믿음과 놀라울 정도로 유사합니다.

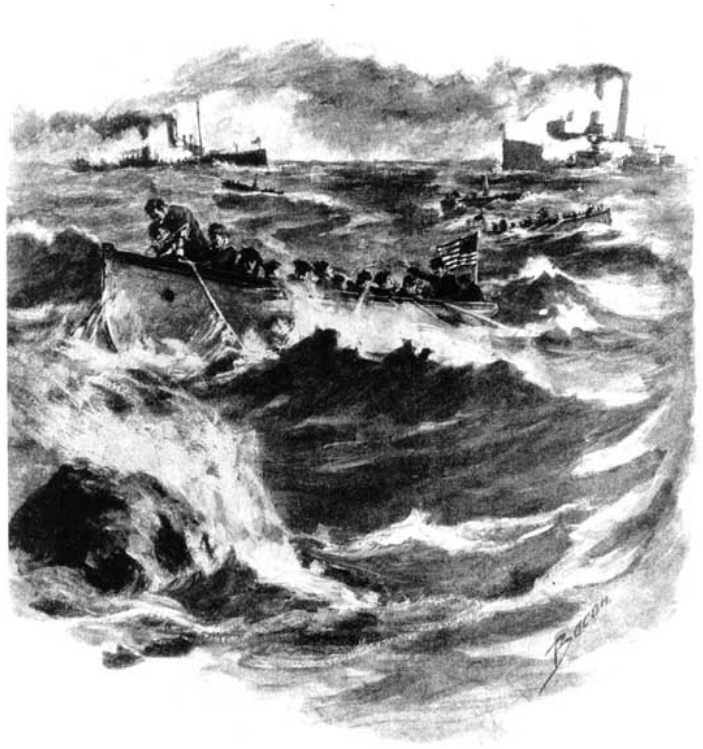
강대국 평화가 끝나고 전쟁이 발발했을 때, 평화 시에는 늘 분명하지는 않았던 통신의 정치적 중요성이 갑자기 분명해졌습니다 제1차 세계대전에서 러시아의 무선 통신을 감청하는 데 성공한 독일은 타넨베르크 전투에서 완벽하게 승리함으로써 전쟁의 판도를 변화시켰으며 러시아가 분쟁에서 빠져나올 수 있도록 도왔습니다. 제1차 세계대전 당시 영국은 해저 케이블을 완벽하게 지배함으로써 독일을 전 세계 통신 시스템으로부터 단절시키고, 독일 케이블 트래픽을 영국 네트워크를 통해 전달하고, 결국 미국이 참전하는 계기가 된 치머만 전보를 발견했습니다. 제2차 세계대전에서 영국은 해독 불가능한 것으로 여겨지던 독일 암호를 해독함으로써 다시 한 번 정보전에서 성공을 거두었습니다. 그 결과 영국의 공식 역사들이 유럽에서 전쟁을 몇 년이나 단축했다고 주장하는 귀중한 정보들이 유출되었습니다. 이 사례들은 통신 안보가 단순히 전장 전술의 문제가 아니라, 강대국의 운명이나 세계사의 판도를 좌우할 수 있는 정치적 경쟁이라는 것을 보여줍니다.

세계가 미소 냉전으로 옮겨가고 있을 때 영국의 강점은 미국의 힘에 의해서 뿐만 아니라 기술 변화에 따라 구식 네트워크의 중요성 감소에 의해서도 제지되었으며, 이는 강대국이 기술의 최전선에 위치해야 하는 중요성을 잘 보여줍니다. 이 새로운 시대에도 통신 경쟁은 익숙한 노선을 따라 계속되었습니다. 예를 들어, 미국은 흔히 메시지가 암호화되지 않는 해저 케이블 통신을 탭핑하는 새로운 방법을 개척했습니다. 경쟁은 위성 및 인터넷 인프라 등 다른 분야로도 옮겨갔습니다. 하지만 이에 대한 역사는 여전히 기록 중이며 대부분의 경우 기밀 사항입니다.

이 일련의 간략한 사례에서 볼 수 있듯이, 통신은 항상 정치적 존재였습니다. 이러한 기술 및 역량의 악용은 일반적으로 그 개발과 함께 진화하고 있습니다. 새로운 통신 방법이 개발되자마자, 강대국은 그러한 통신을 감청하거나 방해하는 방법을 찾았습니다. "전기 통신은 종종 인류의 위대한 업적 중 하나로 묘사되어 왔습니다."라고 한 통신 역사가는 말합니다. "하지만 안보 측면에서 보면 완전히 다른 모습을 볼 수 있습니다. 안보는 기술적인 특성이 아니라 사회적, 정치적 특성이기 때문입니다." 그리고 "정치도 개선되지 않았기 때문에 통신에는 어두운 면이 있습니다."라고 그는 지적합니다.[8]

이제 거의 두 세기에 걸친 통신 경쟁의 주요 주제를 요약으로 돌아봅니다.

1. 미국-스페인 전쟁: 케이블 중립성의 한계



1907년에 출판된 시엔푸에고스의 미국 케이블 절단 작전에 대한 묘사. 이 작전은 해저 전신 케이블은 무장 충돌 중에 중립적인 것으로 취급되지 않을 것이며, 이는 한때 케이블 중립성을 옹호했던 강대국조차 마찬가지라는 점을 여실히 보여줍니다.

출처: 미국 해군 역사 센터 온라인 도서관[9]

19세기에 해저 케이블이 전 세계를 연결하기 시작하면서 프랑스, 독일, 미국 등 몇몇 강대국은 이러한 케이블을 국제 정치에서 배제할 것을 요구했습니다. 1858년, 최초의 대서양 횡단 전신문 중 하나에서 James Buchanan 미국 대통령은 빅토리아 여왕에게 세계의 새로운 전신 케이블이 교전 중에도 "영원히 중립"을 유지하도록 해달라고 촉구했습니다.[10]

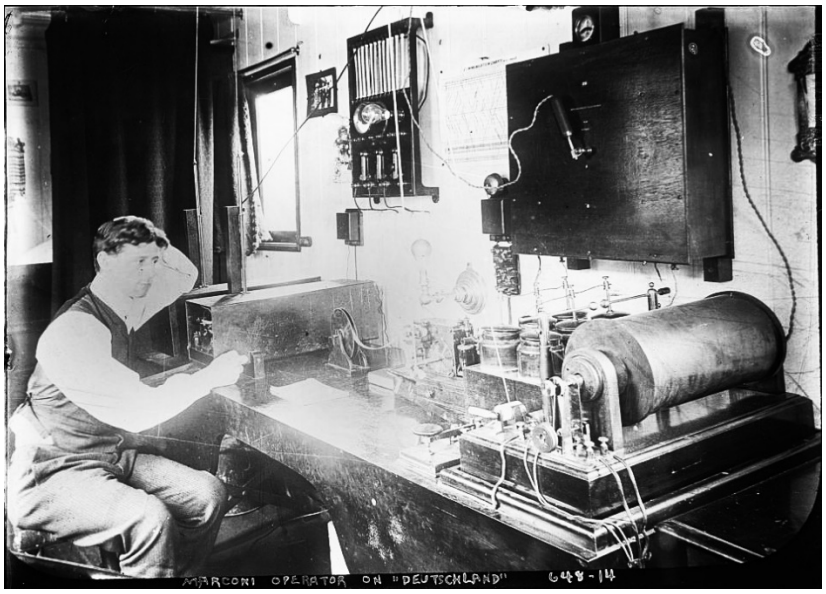
그러나 적대 행위가 발발하면 숭고한 중립성 원칙은 버려졌습니다. Buchanan의 메시지가 나온 지 20년 후 페루는 분쟁 지역을 통과하는 칠레의 케이블 라인을 절단했습니다.[11] 이 분쟁은 거의 주목을 받지 못했으나, 케이블 중립성을 옹호한 미국이 스페인과의 전쟁에서 대서양 및 태평양 모두에서 케이블을 절단했을 때는 세계가 주목했습니다.

미국에 의한 케이블 절단은 분쟁에 앞서 계획되었습니다. 대서양에서 미국은 스페인을 쿠바 주둔군과 단절시키기를 원했습니다. 당시 미국의 한 잡지 기사는 “아바나 고립은 물론 가장 중요했다”고 지적하며, 미국이 “아바나를 외부 세계와 통신하는 모든 전신 통신에서 차단해야 한다”고 촉구했습니다.[12] 미국은 플로리다 주에서 미국 영토를 횡단하는 스페인 트래픽을 단절하는 것부터 시작했습니다. 그 후, 미국은 소규모 작전 팀을 파견하여 시엔푸에고스의 주요 통신 노드를 파괴하고, 아바나 시 및 쿠바 서부 지역 대부분을 스페인과 단절시켰습니다. 이후 미국은 푸에르토리코와 스페인을 연결하는 카리브해 케이블뿐만 아니라 쿠바 동부의 다양한 케이블도 공격했습니다.[13] 결과적으로 케이블 절단으로 인해 스페인이 쿠바 주둔군을 직접 지휘할 수 있는 능력이 크게 저하되었습니다.[14]

태평양에서 미국은 마닐라와 홍콩을 연결하는 유일한 해저 케이블을 절단하여 효과적으로 필리핀을 스페인과 단절시켰습니다.[15] 이 결정으로 미국 통신도 큰 피해를 입었지만 스페인에 훨씬 많은 피해를 입힌 것으로 추정되었으며, 미국은 정기적으로 선박 한 척을 홍콩에 파견하는 것으로 보상할 수 있었습니다.[16] 미군은 또한 필리핀 내의 해저 케이블을 절단함으로써 스페인군 지휘 능력을 더욱 저하시켰습니다.

미국-스페인 전쟁은 아마도 여러 지역에 걸쳐 전기 통신이 중요했던 최초의 글로벌 분쟁이었을 것입니다. 또한 한 강대국이 다른 강대국의 해저 케이블 액세스를 거부했던 최초의 사례였습니다. 분쟁 전에 전신은 여전히 상업적 영역으로 간주되었고 많은 사람들은 케이블이 정치 및 군사 경쟁에서 벗어나 있을 것으로 기대했습니다. 이 분쟁은 이러한 관점의 한계를 입증했고, 통신 인프라에 대한 통제와 지정학적 경쟁국들에게 그 장점을 거부하는 능력이 항상 중요한 정치적 의미를 지닌다는 것을 시사했습니다.

2. 영국-독일 경쟁: 네트워크 구축 및 표준 설정



독일 원양 여객선 SS Deutschland의 "마르코니 룸"에 있는 Marconi사 무선 통신 작업자. Marconi사의 영향력은 매우 커서 독일이 감청 및 거부의 위험에 대해 염려했음에도 그 직원들이 독일 무선실에서 작업했습니다.

출처: 미국 의회 도서관, George Grantham Bain 컬렉션[17]

기술 표준 설정 및 부수 네트워크 효과는 강대국이 오랜 기간 경쟁하는 미묘한 분야입니다. 지배적 표준이 된 기술을 보유한 국가는 다른 국가보다 큰 영향력을 행사할 수 있습니다. 이는 흔히 병렬 시스템을 구축하여 취약성을 줄이기 위해 노력함으로써 신흥 강대국이 빼기지 않는 요점 중 하나입니다. 사실, ICT를 놓고 현재 진행 중인 중미 경쟁은 100년 전 독일과 영국 사이의 ICT 인프라 주도권 다툼과 놀랍도록 유사하며 현재에도 중요한 교훈을 줍니다.

19세기 말 이탈리아 엔지니어 Guglielmo Marconi는 영국 해군의 지원을 받아 무선 전신을 개발했습니다.[18] 이 발명은 혁명적이었습니다. 과거에는 강대국이 서로의 케이블을 절단했고, 선박 간 통신과 선박과 육상 간 통신이 어려웠지만, Marconi의 시스템은 이러한 문제를 해결했고 간섭에 덜 취약했습니다.[19] Marconi는 궁극적으로 영국과 제휴하여 무선 전송 독점권을 영국에 제공했습니다. 세계 해저 케이블 네트워크의 60%와 결합되어 영국은 국제 전송을 지배했습니다. 영국의 강점은 독일을 불안하게 했지만, 무선 기술에 대한 경쟁은 "독일이 새로운 국제 인프라를 장악"하고 "영국 케이블을 회피"할 수 있는 기회를 제공했습니다. 강대국 우위가 성과로 연결된 것입니다.[20]

취약함을 느낀 Wilhelm 2세 황제가 독일 과학자 및 엔지니어에 대한 직접적인 국가 지원을 승인함으로써 이들은 Marconi의 디자인을 성공적으로 복제하고, 독일에서 특허를 취득하고, 독일군과의 계약으로 재정을 조달하여 자체 무선 네트워크를 구축하는데 성공했습니다.[21] 그러나 Marconi의 우월한 장거리 무선 통신 및 최초 개발자 이점으로 인해 그의 영국 기반 회사가 글로벌 표준으로 자리잡게 되었고, Marconi는 이러한 네트워크 효과를 활용하여 Marconi 이외의 무선 사업자와의 "비 상호 통신" 정책을 추구했습니다. 독일 기업 및 원양 여객선은 글로벌 통신에서 단절되는 것을 원하지 않았기 때문에 영국이 지원하는 시스템을 독일 시스템보다 선호했습니다.

Wilhelm 2세 황제는 독일 산업 정책을 강화해서 영국 표준에 대항했습니다. 그는 신속하게 칙령을 제정하여 Siemens & Halske 및 AEG라는 두 대형 독일 전기 회사가 합작하여 독일의 결정적인 대안인 Telefunken을 설립하도록 했습니다. 황제는 "무선 전신 분야에서 [국내] 경쟁은 독일의 경쟁력을 약화시킨다"고 설명했습니다. "그리고 Marconi사에게 세계 독점을 달성할 수 있는 기회를 주며" 이는 "독일에게 이익이 되지 않는다"고 설명했습니다.[22] 빌헬름 2세 황제 치하의 독일은 일부의 경우에는 Marconi 시스템을 금지함으로써 보호주의를 추구했습니다. 독일은 신흥 시장을 공략해 남미 및 아프리카에 기술을 판매하여 해당 지역의 표준을 정립하고 매출을 확보했습니다.

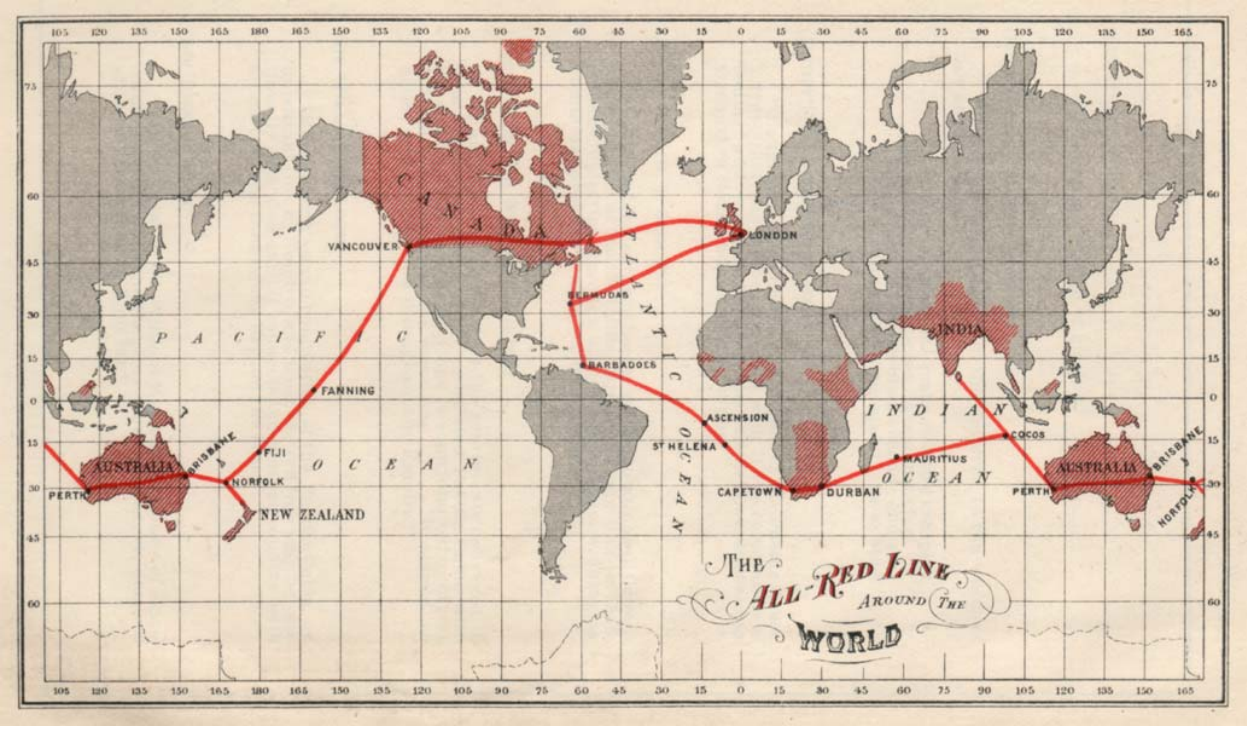
이러한 노력이 불충분한 것으로 판명되었을 때 독일은 다자간 표준 설정 기구에서 성공을 거두었습니다. 1906년, 독일은 무선 표준에 관한 회의인 제1차 국제 무선 전신 협약에 여러 강대국을 끌어들였습니다. 이 과정에서 회원국들은 Marconi의 "비 상호 통신" 정책을 공동으로 금지함으로써 영국의 독점 체제를 무너뜨리고 유효하게 영독 과점 체제를 확립했습니다.[23]

영독 경쟁은 표준 설정 기구가 엄청난 전략적 의미를 가지고 있음을 보여줍니다. 중국은 현재 독일이 100년 전에 사용한 기법들을 답습하고 있습니다. 국가 주도 산업 정책, 국가 보호, 관대한 관급 계약, 군민 통합, 경쟁 제품 금지, 강제 합병, 신흥 시장 개척, 심지어 표준 설정을 위한 국제 조약, 이 모든 것이 WeChat 및 AliPay의 소유주인 알리바바, 텐센트와 같은 중국 기술 기업들이 현지 챔피언이 될 수 있도록 도와주었습니다. 이러한 기업은 이후 해외로 사업을 확장하면서 독일의 Telefunken처럼 미국 시장이 아니라 수익은 낮지만 경쟁이 덜한 신흥 시장을 대상으로 삼는 경우가 흔했습니다.[24]

중국 역시 인터넷 연결의 하드 인프라에 대한 표준에서 경쟁하고 있습니다. 중국 정부는 5G 모바일 인터넷 표준 경쟁에서 중국 칩 제조업체들이 미국 경쟁업체들을 따돌릴 수 있도록 수십억 달러를 투자하고 있습니다. 마찬가지로, 화웨이, ZTE 같은 중국 기업은 정부 대출을 받아 개발도상국 전체에 인터넷 연결 인프라를 구축합니다. 영국의 예에서 알 수 있는 것처럼, 이러한 노력은 중국 기술을 표준으로 만들 뿐만 아니라 감시를 위한 기회도 제공합니다. 한편, 벨트 로드 이니셔티브는 아시아 전역의 "스마트 인프라", 특히 관련 센서 및 소프트웨어에 대한 표준이 중국에 의해 설정될 수 있으며 타사와의 상호 운용성을 거부함으로써 자율 차량 및 기타 산업에서 타사를 배제할 수 있는 가능성을 제기합니다.

전신 분야에서의 영독 경쟁은 미국이 중국의 국가적 도전을 심각하게 받아들여야 한다는 것을 보여줍니다. 또한 앞으로 나아갈 길을 제시합니다. 독일이 국제회의를 통해 영국의 전신 독점을 무너뜨린 것과 마찬가지로 미국은 다자간 협정을 통해 우호적인 ICT 표준을 설정하거나 유지할 수 있습니다. 이를 통해 중국이 자유 무역 협정, 국가 챔피언 또는 인프라 프로젝트를 통해 일방적으로 표준을 설정하는 것을 막을 수 있습니다.

3. 제1차 세계대전의 영국: 정보 헤게모니 구축



"All Red Line"은 영국이 거액을 들여 엄청난 중복성으로 구축한 해저 케이블 네트워크로서, 어떤 부분도 경쟁국 영토를 통과하지 않도록 배치되었습니다. 독일의 복원력이 뛰어난 자체 글로벌 통신 네트워크에 대한 투자가 부실하여 영국은 독일 네트워크를 글로벌 통신과 차단했지만 자국은 전반적으로 영향을 받지 않을 수 있었습니다.

출처: George Johnson, ed., The All Red Line: The Annals and Aims of the Pacific Cable Project / 인터넷 아카이브[25]

20세기 초 통신 분야에서 영국의 지배력을 무너뜨리려는 독일의 노력은 편집증에서 비롯한 것이 아닙니다. 제1차 세계대전이 발발하자 영국은 통신 네트워크에 상당한 영향력을 행사해 전쟁의 판도를 바꾸었습니다. 독일의 케이블을 절단하고, 독일 통신을 감시하고, 독일 트래픽이 영국에서 통제하는 네트워크를 경유할 수 밖에 없도록 했으며, 결과적으로 치머만 전보를 발견하여 미국이 참전하는 데 기여했습니다.[26]

영국이 통신망을 차단하거나 조작한 첫 번째 강대국은 아닙니다. 페루는 칠레-볼리비아 링크를 단절했고, 미국은 스페인의 케이블들을 절단했으며, 영국은 한 분쟁에서는 보어인을 그들의 유럽 지지자들로부터 고립시켰고, 다른 분쟁에서는 프랑스로 향하는 케이블 트래픽을 조작했습니다.[27] 그러나 이러한 노력은 제1차 세계대전에서 극단으로 치달았습니다.

평화 시에 신중하게 수립한 계획을 전쟁 첫날부터 실행하여 한 국가를 글로벌 통신 네트워크로부터 완전히 단절한 것은 영국이 처음이었습니다.[28] 1년 내에 영국은 영국 해협, 북해, 북대서양, 남아메리카, 아프리카의 많은 지역, 극동, 심지어 독일 인프라를 호스트하는 중립 국가를 포함해 전 세계에서 독일 케이블을 파괴했습니다.[29]

이를 만회하기 위해 독일은 Telefunken이 라틴 아메리카에서 10년 전 구축한 무선 네트워크와 "Global South"를 확장해 전 세계를 커버하려 했습니다. 중국의 디지털 실크로드와 유사한 노력으로, 독일은 독일 통신 노드를 호스트할 수 있도록 "무선 개발 혜택"에 관심이 있는 정부에 대출 및 투자를 제공했습니다. 이에 대응하여 영국은 이러한 국가 대부분이 독일 무선 노드를 지지하지 않도록 설득 또는 유도하거나 적극적으로 방해했습니다.[30]

독일은 자체 네트워크가 없는 상태에서 전쟁 중에 영국의 네트워크에 의존할 수밖에 없었습니다. 처음부터 영국은 자국 케이블을 통과하는 모든 트래픽을 은밀히 감시하기 시작했고, 독일과 중립국 간의 관계를 손상시키기 위해 선택적으로 독일 트래픽을 누출하며 독일과 정보전을 벌였습니다. 독일이 미국에 군사동맹을 제안하는 전보(유명한 치머만 전보)를 보냈을 때 이 메시지가 영국 네트워크를 통과했고 영국이 이 메시지를 감청하고 해독했습니다. 영국은 이를 미국 정부와 공유했고, 미국 정부는 이를 자국민에게 공개했습니다.[31] 이 사건은 미국이 전쟁에 참가하여 결국 독일이 패배하는 세계 역사를 만드는 데 일조했습니다.

영국이 독일을 상대로 벌인 정보전을 통해 적대국이 통신을 감청하거나 통신 액세스를 차단할 능력을 보유할 경우의 위험을 알 수 있습니다. 또한 평화 시에는 당연하게 여기는 네트워크가 전시에는 자주 거부되고 있으며, 통신 노드에 대한 투쟁은 필연적으로 제3자와 중립국을 수반할 것이라는 점도 드러납니다.

4. 타넨베르크에서 독일의 승리: 감청의 위험

제1차 세계대전 중 독일의 야전 무선 전신국. 러시아가 야전에서 통신 내용을 적절히 암호화하지 못해 참담하게 패배함으로써 전쟁이 재편되었습니다.

출처: C. O. Nordensvan 및 Valdemar Langlet, Det stora världskriget*[세계대전]*[32]

독일이 정보전에서 독자적 능력이 전혀 없는 것은 아니었습니다. 독일은 러시아와 서방 동맹국을 연결하는 육상 및 해저 케이블뿐만 아니라 영국이 사용하는 몇몇 대서양 횡단 케이블들을 절단했는데, 처음으로 이 임무에 잠수함을 사용했습니다.[33] 영국 네트워크의 중복성을 고려했을 때, 이러한 노력은 독일이 기대했던 것보다 효과가 약했습니다. 전쟁이 발발한 첫 달인 1914년 8월, 타넨베르크 전투에서 독일이 러시아에 대해 무선 감청을 사용한 것이 훨씬 더 큰 효과가 있음이 입증되었습니다. 러시아가 참담하게 패배한 것입니다. 당시 한 독일 정보 요원은 이 사건을 "인류 역사에서 적대국 무선 통신 감청이 결정적인 역할을 한 첫 번째 사례"라고 했습니다.[34]

이 전투는 러시아가 동부 전선에서 득세하는 가운데 벌어졌습니다. 러시아가 프러시아 동부로 더 깊숙이 진입하면서, 러시아군은 재앙적인 패배의 무대가 된 중요한 통신 문제에 직면했습니다. 후퇴하는 독일군은 자체 전신망을 절단했고, 진격하는 러시아군은 넓은 전선에서 유선 통신망을 설치하는 데 충분한 훈련을 받은 인력이 부족했습니다. 무선 전송이 대안을 제공했지만 러시아군은 군사 명령 및 통제를 위해 새로운 무선 기술을 채택하면서 적절히 보호하지 못했습니다. 부대마다 다른 암호가 할당되었고 신호를 암호화 및 해독하는 훈련을 받은 인력이 거의 없었습니다. 일부 암호는 영국에서 해독한 것으로 알려졌으며, 암호서는 많은 문맹 징집병에게 이해하기 어렵거나 불가능한 것으로 알려졌습니다.[35] 그 결과 러시아 지휘관들은 위험을 감수하고 암호화되지 않은 무선 통신을 사용할 수 밖에 없다고 느꼈으며 독일군이 이를 주의 깊게 감시하지 않기만을 바랬습니다.

그러나 독일군은 신호를 면밀히 감시하고 있었습니다. 일본과의 전쟁에서 러시아의 규율 없는 무선 통신을 목격한 그들은 러시아의 암호화되지 않은 통신이 속임수가 아니라는 것을 알았습니다. 그래서 실시간으로 확보되는 러시아 통신 내용을 활용하여 “전운”을 걷어 올리고 우월한 전력에 결정적 패배를 안겼습니다. 독일군 사상자 1만 3,000명에 비해 러시아군은 10만 명 이상의 사상자를 냈으며 9만 2,000명이 포로로 잡혔으며 전체 육군이 패배했습니다.

5. 제2차 세계대전의 영국: 암호화의 제한

제2차 세계대전 동안 사실상 해독 불가능한 것으로 여겨지던 Lorenz 암호기의 기계식 회전자. 영국 정부는 암호문을 해독하여 고급 독일 통신에 액세스할 수 있었습니다.

출처: Matt Crypto/위키미디어 공용[36]

무선 전신 및 무선 통신의 발명은 물리적 케이블에 비해 더 편리했지만 감청 위험이 더 큽니다. 제1차 및 제2차 세계대전에서 강대국들은 다른 사람이 무선 통신에 액세스할 수 있다고 가정했습니다. 현대 컴퓨터 및 통신 시스템의 취약성에 대한 가정과 그다지 다르지 않은 이러한 가정에서는 암호화가 보안에 중요하다고 여겨졌습니다. 그 결과는, 한 미국 군사 역사가가 말한 것처럼, "암호화 전문가와 암호 해독 전문가 사이의 투쟁"이었습니다.[37] 강대국이 이 투쟁의 잘못된 편에 섰을 때 결과는 재앙이 될 수 있습니다.

이러한 결과를 방지하기 위해 조직에서는 암호를 사용하여 감청으로 보안이 침해될 위험을 줄일 수 있습니다. 또한 공격자가 무선 트래픽 분석을 통해 사용 패턴에 대한 통찰력을 확보하지 못하도록 "무선 규율"을 시행했습니다.

대부분의 강대국들은 적대국의 트래픽 상황을 연구하고 가능한 한 적대국의 암호를 해독하기 위해 진정한 산업적 노력을 경주했습니다. 영국은 적대국 암호를 분석하는 데 있어 독일보다 훨씬 더 중앙 집중식이었습니다. 독일은 이 기능을 여러 첩보원에게 분산했습니다. 그리고 영국이 신호 인텔리전스 및 암호 해독에 성공하여 제1차 세계대전의 판도를 바꾼 것과 마찬가지로, 영국은 제2차 세계대전에서도 블레츨리 파크에서의 작전으로 독일의 Enigma 및 Lorenz 암호를 해독하여 전쟁의 양상을 바꿨습니다.

Enigma 및 Lorenz 암호화 시스템은 매우 복잡한 회전자 장치를 사용하여 메시지를 암호화했는데, 독일은 이 암호가 "훼손 불가능"할 것으로 믿었습니다.[38] 키를 입력할 때마다 암호기 고유 설정에 따라 한 문자가 다른 문자로 대체되며, Lorenz 시스템의 경우 메시지를 읽기 위해 발신자와 수신자가 우주에 존재하는 모든 원자의 수보다 많은 이러한 설정을 공유해야 합니다.[39] Enigma 암호기는 군, 게슈타포, 외교관이 사용했고, Adolf Hitler와 나치 및 고위 군부 인사가 통신할 때는 훨씬 더 복잡한 Lorenz 암호기를 사용했습니다.

영국은 몇 가지 전개의 산물로 Enigma 및 Lorenz 암호를 해독하는 데 성공했습니다. 첫째, 폴란드와 정보 동맹의 산물로 독일의 실수를 이용하여 훨씬 단순한 Enigma 암호기를 해독했습니다.[40] 당시 영국의 한 암호 해독 전문가가 말했던 것처럼, 그들의 노력은 폴란드의 기여 없이는 "결코 얻을 수 없었을" 것입니다.[41]

둘째, 독일의 자만심의 산물이었습니다. 독일은 그 암호들이 해독될 것이라고 의심하지 않았기 때문에 간단한 수정조차 하지 않았습니다. 그랬다면 영국은 처음부터 다시 시작할 수 밖에 없었을 것입니다.[42] 하지만 블레츨리 파크의 한 고위 관리는 "시스템 훼손은 불가능하다는 독일인의 믿음이 거의 옳았다"고 말했습니다.[43]

마지막으로, 독일 "무선 규율"에서 단 하나의 중대한 실수의 산물이었습니다. 이를 통해 한 번도 직접 본적이 없었던 독일 암호 시스템을 리버스 엔지니어링할 수 있는 문이 열렸습니다.[44] 아무리 정교한 시스템이라도 사용자 실수에 취약했고, 기회를 노리는 적대국은 이를 악용할 수 있습니다.

영국에서는 Enigma 및 Lorenz 암호를 해독하면서 독일에서 가장 중요한 통신에 액세스할 수 있었습니다. Winston Churchill은 정보가 영국이 전쟁에서 승리한 주요 이유 중 하나라고 믿었고 Dwight D. Eisenhower는 정보를 "결정적"이라고 말한 것으로 알려졌습니다.[45] 영국 정보 기관의 공식 역사가인 Francis Harry Hinsely 경은 이러한 성공이 "2년에서 4년 정도 전쟁"을 단축시킨 것이라고 주장합니다. 이 성공으로 아프리카의 Erwin Rommel 야전사령관을 약화시키고, 독일 U 보트에 의한 연합국 운송 피해를 급반전시키고, 노르망디 상륙을 감행할 수 있었습니다.[46] 또한 영국으로 잠입하는 모든 독일 스파이를 실제로 식별하고 종종 전향시키거나 잘못된 정보를 보내는 데 이용할 수 있었습니다. 이 프로그램의 책임자는 "영국 정보 기관이 국내에서 독일 스파이 시스템을 적극적으로 운영하고 통제했다"고 언급했습니다.[47] 전시에 다른 국가에 대해 그와 같은 밀접한 지식을 가진 국가는 거의 없었습니다.

종합해 볼 때, 영국이 독일에 기울인 노력의 성공, 폴란드가 평화 시부터 수행한 독일 통신에 대한 감시, 그리고 성과를 영국과 공유하기로 한 결정은 강대국들이 서로 사이버 정찰 활동을 하는 오늘날에도 적용 가능한 교훈을 가지고 있습니다. 보다 광범위하게는, 암호화가 적대국의 통신 네트워크에 대한 액세스 문제를 완화시킬 수 있다고 주장하는 사람은 한때 독일이 저지른 것과는 전혀 다른 실수를 범하는 것일 수 있습니다. 즉, 기술에 대한 지나친 믿음과 끊임없이 존재하는 인간의 실수 가능성에 대한 제한된 관심 말입니다.

6. 아이비 벨 작전: 정보 추구의 깊이

소련 해저 전화선을 탭핑하기 위해 동원된 것으로 알려진 USS Halibut.

출처: 미국 해군/위키미디어 공용[48]

소련은 Enigma 암호기보다 훨씬 더 복잡한 Fialka로 알려진 자체 버전을 사용하며 나치보다 암호화를 훨씬 더 조심했습니다.[49] 이러한 이유 때문에 제2차 세계대전에서 독일 암호 해독 이후 방대한 양의 전략적 수준 정보들이 쏟아진 것과 달리 냉전 시대에는 그렇지 않았습니다. 이러한 점을 고려해 적대국의 통신을 침투하는 다른 방법이 개척되었습니다. 이 가운데 가장 대담한 노력 중 하나는 해저 케이블과 관련된 것입니다.

19세기 해저 케이블이 등장한 후 종국에는 케이블 절단 또는 탭핑으로 이어졌습니다. 육상 또는 천해에서는 그러한 작업을 수행하기가 수월했습니다. 반면, 적대국이 통제하는 심해에서 이러한 작업을 수행하는 것은 사실상 불가능하다고 생각되었습니다. 특히 은밀한 수행이 필요한 경우에는 더욱 그랬습니다. 20세기에 들어서면서 영국을 비롯한 강대국들은 해저 케이블 보안에 대한 결심을 하게 되었습니다. 육상 연결 사이트가 보호되고 케이블이 중립 또는 적대 국가를 통과하지 않는다면, 일반적으로 감청으로부터 안전하고, 특히 평화 시에는 절단으로부터 안전할 것입니다.[50]

그러나 냉전 기간 동안 그 계산은 달라졌습니다. 핵잠수함의 출현으로 더 깊은 수심에 설치된 해저 케이블을 탭핑할 수 있는 가능성이 열렸습니다. 그러나 깊은 해저의 케이블에 접근하기 위해 다이버를 파견하는 일은 이전 시대에 시도했던 익숙한 케이블 조작 시도에 비하면 우주 탐사와 더 비슷한 것으로 여겨졌습니다. 이러한 조건에서 설치할 수 있는 탭을 만드는 것도 기술적으로 어려운 일입니다.

미국은 소련 해저 케이블이 블라디보스토크의 해군 본부에서 캄차카 반도의 잠수함 기지로 연결된다는 것을 의심했고, 이러한 장애물을 극복해 신호 정보의 가치를 입증했습니다.[51] 5인치 통신선 묶음을 탭핑하면 소련군 핵 전력에 대한 중요한 정보를 얻을 것으로 믿어졌습니다.[52] 소련은 공중으로 전송되는 모든 트래픽을 암호화했지만 미국이 보호되는 해저 케이블을 통한 트래픽에는 액세스할 수 없을 것으로 가정했고 따라서 암호화하지 않았습니다. 게다가 "소련 제독 및 장군들은 이미 엄청난 작업량에 압도되어 있는 암호 해독가들을 기다리기에는 너무 고압적이고 참을성이 없을 것"이고 보안되지 않은 음성 통신을 고집했을 것입니다.[53] 그러므로 일단 탭핑이 성공하면 희귀한 정보를 수집할 수 있을 것이기에 미국 해군은 아이비 벨 작전에 착수했습니다.

탭핑 및 이를 통해 획득한 정보는 여전히 기밀로 유지되지만 오픈 소스는 독특하고 혁신적인 작전에 대한 세부 정보를 제공합니다. 미국은 핵잠수함 USS Halibut을 파견했습니다. 이 잠수함은 소련 해군을 조용히 지나쳐 60만 평방 마일에 달하는 지역에서 해저 케이블을 찾았습니다.[54] 다이버들이 몇 시간 동안 엄청난 수압과 극심한 저온에서 작업할 수 있도록 하기 위해 혁신적인 기술이 개발되었습니다. 마찬가지로, 이 어려운 환경에서 탭을 설치하기 위한 새로운 방법이 고안되었습니다.[55] 이 모든 작업은 소련이 탐지하거나 의심하지 않도록 수행해야 했습니다. 만일 잠수함이 발견된다면, 소련이 잠수함에 승선하거나 잠수함을 파괴할 수도 있습니다.

이 작전은 성공으로 판명되었고 1970년대 내내 미국 해군은 케이블을 통해 보안되지 않은 메시지를 도청 및 녹음했습니다. 몇 달에 한 번씩 미국 잠수함은 소련 해역으로 잠입하고 공격용 잠수함을 피해 탭이 설치된 케이블 라인에 다이버를 파견하여 소련의 통신 내용이 녹음된 테이프를 회수하여 매우 귀중하고 드문 정보를 얻을 수 있었습니다. 미국은 신호 정보를 수집하기 위해 "스파이 위성, 항공기, 감청 스테이션 및 잠수함의 네트워크"를 확장했지만 적대국 지역 내에서 "유선 전화선은 침투할 수 없었습니다". 이 노력은 통신에서의 진화적 변화를 보여줍니다. 즉, 어떤 매체를 통해 전송되든 데이터 및 신호는 올바른 도구를 가진 완강한 행위자에 의해 액세스될 수 있다는 것입니다. 정보가 유출되어 결국 이 탭은 훼손되었지만, 결과적으로 통신 감청은 미국과 그 동맹국에 귀중한 군사 및 정치 정보를 제공했습니다.[56]

역사적인 관점에서 현대의 통신 경쟁

냉전 종식 무렵에 미국은 정보 헤게모니 국가로서 분명히 영국을 대체했습니다. 미국은 글로벌 인터넷의 노드 위치, 강력한 우주 역량, 인터넷 기술에서의 압도적 지배력, 그리고 공개 자료에 따르면 적대국의 통신을 감청하거나 거부할 수 있는 정교한 능력을 갖추고 있습니다.

이러한 미국의 장점은 지금 1세기 전의 영국과 같이 시험을 받고 있습니다. 이제 러시아, 특히 중국이 미국의 지배력에 도전하고 있습니다. 미국은 많은 데이터 흐름에서 노드 위치를 누리고 있지만 다른 강대국들은 미국 네트워크에 대한 의존도를 줄이려고 노력하고 있습니다. 동시에 미국의 노드 위치는 100년 전 영국보다 감청할 필요가 적었습니다. 인터넷은 물리적 인프라에 대한 제어 없이 침입이 가능합니다. 스마트폰과 컴퓨터 네트워크가 해킹될 수 있으며, 중요한 통신이 이전 시대의 물리적 탭을 통해 유출되든 현대의 가상 침입을 통해 유출되든 최종 결과는 동일합니다. 이러한 방식의 연결에서는 전신 또는 무선 통신 시대보다 더 큰 취약점이 발생할 수 있습니다.

러시아는 이 취약점을 악용하는 최고의 국가였습니다. 2007년, 러시아는 에스토니아 기관을 대상으로 파상적인 사이버 공격을 시작했는데, 주로 분산 서비스 거부 공격이었습니다.[57] 2008년에는 러시아-조지아 전쟁에서 사이버 공격을 감행했습니다. 이러한 공격에는 서비스 거부 공격뿐 아니라 정부 웹 사이트를 리디렉션하고, 조지아 정부 서버를 점령하고, 러시아 제어 서버를 통해 조지아 인터넷 트래픽을 재라우팅하는 공격도 포함되었습니다. 일부 공격은 충돌 전에 러시아 군사 행동에 맞춰 준비되었습니다.[58] 2014년, 러시아가 크림 반도를 침공했을 때는 사이버 공격과 통신 네트워크의 물리적 제어가 결합되었습니다. 러시아군은 우크라이나 통신 시설을 장악해 크림 반도에서의 통신을 차단하고, 심지어 우크라이나의 다른 지역에도 사이버 공격 및 중단을 수행했습니다.[59] 2015년, 러시아는 우크라이나 인프라에 대한 파상적인 사이버 공격을 시작하여 두 가지 주요 상황에서 우크라이나인 수십만 명에 대한 전력 공급을 차단했습니다. 향후 몇 년 동안 러시아는 우크라이나에 대한 "미디어, 금융, 운송, 군사, 정치, 에너지"(우크라이나 사회의 거의 모든 부문)에 걸쳐 유례 없는 공격을 지속했습니다. 일각에서는 이를 부분적으로 미국에 대한 유사한 공격을 위한 훈련이라고 믿습니다.[60] 동시에 발트해 전역에서 다양한 공격을 계속했으며, 2016년 및 2020년 허위 정보로 미국 선거를 조작하려 했고 다른 국가에서도 이러한 시도를 한 것은 유명합니다.[61] 2021년, 미국 정부는 러시아가 IT 회사 SolarWinds를 해킹한 것을 공식적으로 비난하였습니다. 이 정교한 공격으로 연방 정부 및 여러 주요 미국 기업이 피해를 입었습니다.[62]

중국은 통신 경쟁에 상당한 투자를 하고 있는 또 하나의 주요 강대국입니다. 하지만, 러시아와 달리 중국은 기존의 인터넷 인프라를 이용하려는 것뿐만 아니라 영향을 미치고 통제할 수 있는 네트워크 및 인프라를 구축하려는 노력을 하고 있습니다. 러시아처럼 중국은 기존의 인터넷 취약성을 악용하는 데 능숙했습니다. 2000년대 초, 중국은 Operation Titan Rain이라는 작전명으로 미 국방부 네트워크에 대한 파상 공격을 시작했습니다.[63] 미국, 영국, 프랑스, 독일, 캐나다, 호주, 일본, 한국, 대만, 인도 등 여러 국가에서 중국 정부의 네트워크 침입을 성토했습니다. 미국 인사 관리국 기록 도난(2,100만 명), Marriott 호텔(4억 명), Anthem 의료 보험(8,000만 명), Equifax(1억 4,700만 명) 등 지난 10년 동안 발생한 최대 규모 사이버 공격 중 일부는 중국 요원들이 저지른 것으로 미국 법무장관 William Barr는 확인했습니다.[64]

동시에, 중국은 미래의 인터넷 인프라를 위한 토대를 마련하고 있으며, 이전의 노력에 비추어 볼 때 이러한 노력이 현재 상업적으로 보이지는 않으며 앞으로도 순전히 상업적으로 유지될 것으로 보이지도 않습니다. 중국의 투자는 5G 네트워크에서 가장 두드러집니다. 5G 네트워크는 수많은 기기와 센서를 하나로 연결하는 보다 스마트한 연결된 경제의 기반을 형성할 것으로 기대됩니다. 전 세계에 이러한 네트워크를 구축하고자 하는 중국은 디지털 실크 로드 이니셔티브의 일환으로 전 세계적으로 5G 챔피언 및 프로젝트에 자금을 지원하고 있습니다. 화웨이와 같은 기업은 경쟁력 있는 가격으로 다른 주요 5G 공급업체를 압도할 수 있었으며, 상당한 글로벌 시장 점유율을 확보하고 있어 중국이 이 네트워크를 구축하는 데 선두 주자가 되었습니다. 5G 외에도 중국 정부는 거의 모든 대륙에서 인터넷 또는 통신 인프라를 구축하기 위한 노력에 보조금을 지급하고 있습니다. 이러한 노력은 모두 중국의 주요 정책 우선순위인 글로벌 표준을 설정하기 위한 캠페인으로 보완됩니다. 이는 100년 전 무선에 대한 영독 경쟁과 마찬가지로 중국에 유리한 방식으로 통신의 미래를 형성할 수 있는 상위 계획에 포함되어 있습니다. 이를 위해 중국은 최근 새로운 데이터 보안 이니셔티브를 발표했습니다.[65]

일각에서는 중국의 활동이 트래픽을 감청하든 액세스를 거부하든 중국 정부가 사실상 이러한 네트워크를 통제할 가능성을 열어 주는 것을 우려하고 있습니다. 중국의 통제 확보 노력에 대한 공개 정보는 거의 없지만, 미국 정부는 2020년 2월에 화웨이가 네트워크 장비에 백도어를 갖추고 있지만 계약을 맺은 관련 회사에 그 사실을 공개하지 않았으며 해당 백도어는 해당 국가가 합법적 감청의 일부로 요구하는 수준을 넘어서는 것이었다고 밝혔습니다.[66] 또한, 언론 보도에서는 화웨이가 우간다, 잠비아 같은 정부들이 반체제 인사들의 자격증명을 훼손하는 것을 지원했다고 폭로했습니다.[67] 화웨이 사례 외에도 최근 한 사이버 보안 기업은 중국 정부가 외국 기업에 설치를 요구하는 필수 세금 소프트웨어에서 백도어를 발견했습니다.[68] 이러한 사례가 화웨이가 해당 네트워크에서 위치를 악용했다는 것을 시사하는지 여부와 관계없이 이 회사의 행동과 중국의 사이버 공격 및 스파이 행위에 대한 기록은 우려의 대상입니다.

우려의 또 다른 중요한 이유는 역사뿐 아니라 자유주의 강대국의 행동이 법치에 의해 더욱 철저히 제한된다는 점에서 비롯됩니다. 사실, 이전의 역사적 사례는 화웨이와 같은 회사가 휘두르는 권력 및 영향력이 중국 정부에 의해 이용될 가능성이 있음을 강력히 시사합니다. 다른 강대국들도 통신 분야의 기업이나 역량을 악용하는 경우가 많기 때문입니다.

보다 광범위한 역사적 관점에서 볼 때, 비록 화웨이의 의도가 순수하게 상업적이고, "백도어 및 스파이 활동 없음"이라는 약속이 믿을 만한 것이고, 중국 정부가 이러한 약속을 충실히 이행한다고 하더라도, 증거에 의해 많은 관찰자들은 통신 네트워크에서 화웨이의 역할에 대해 신중해야 한다는 결론을 내릴 수밖에 없을 것입니다.

이 보고서에서 알 수 있듯이 오늘날 새롭게 인식되고 있는 강대국 통신 경쟁의 많은 특징들이 과거에 뿌리를 두고 있습니다. 역사 전반에 걸쳐 다음과 같은 여러 주제가 반복됩니다.

- *강대국:* 통신 네트워크에 대한 통제가 시작된 지 150년이 넘었습니다. 영국은 통신 및 무선에서 자신의 역할을 이용했고, 미국은 현대 인터넷 시대에 그렇게 했을 가능성이 높으며, 중국이 현재 그렇게 하려고 할지도 모르기 때문에 우려할 만한 이유가 있습니다.

- *안주*: 오랜 평화 및 번영으로 통신 위험을 경시하게 되었습니다. 오늘날 여러 국가가 중국의 통신 장비와 운영을 기꺼이 수용하듯이 19세기에 강대국들은 외국 회사 및 외국 운영 네트워크에 의존하는 데 만족했습니다. 그러나 결국 잠재적인 경쟁국 또는 적대국에 대한 의존은 독일과 같은 국가에게 재앙을 초래하고 세계 정치 판도를 개편했습니다.

- *악용:* 새로운 통신 기술은 항상 이를 감청, 거부, 또는 악용하려는 새로운 노력을 촉발했습니다. 암호화가 중국의 현대 통신 감청 시도를 어렵게 만들 것이라는 희망에도 불구하고, 영국이 "해독 불가능"한 것으로 여겨지던 독일의 암호를 해독했을 때 독일이 발견한 것처럼, 당시 암호화에 대한 희망은 사용자 실수와 경쟁국의 완강한 노력 앞에서는 의미가 없었습니다. 안전한 것으로 여겨지는 기술에는 겸손이 수반되어야 합니다.

- *챔피언:* 특히 강대국 간 긴장이 고조됨에 따라 국가들은 흔히 자국의 통신 분야 챔피언을 찾습니다. 중국 정부는 화웨이의 성과를 자랑스럽게 생각하며, 전 세계에서 이를 옹호하고 있습니다. 심지어 이 회사의 기술을 거부하는 국가들을 위협하기도 합니다. 자국 정부와 그렇게 밀접한 관계를 맺고 있는 기업이 역사상 다른 많은 통신 챔피언과는 달리 정부 압력으로부터 자유롭다면 이례적일 것입니다.

- *표준:* 통신 표준은 누가 네트워크 권력을 휘두를지 결정할 수 있습니다. 독일은 표준 설정 기구를 사용하여 무선 통신에서 영국의 지배력을 무너뜨릴 수 있습니다. 현재, 국제 통신 연합(International Telecommunications Union)과 같은 기구에서 경쟁이 진행 중이며, 이 기구에서 화웨이의 역할은 해당 표준을 통해 중국이 통신 분야를 재편할 수 있을지 고려해야 함을 의미합니다.

- *거부:* 네트워크 보안은 감청 및 데이터 보안에 대한 것뿐만 아니라 전체 네트워크의 운영 또는 외부 네트워크에 대한 액세스 거부와도 관련됩니다. 영국은 전 세계 전신 네트워크에서 독일을 단절했고, 화웨이의 네트워크 역할은 이 회사가 데이터에 쉽게 액세스할 수는 없더라도 장비를 운영하는 국가에서 네트워크를 차단할 수 있는 능력은 가질 수 있습니다.

- *완강함:* 많은 국가가 적대국이 그들의 네트워크를 손상시키기 위해 엄청난 노력을 할 수 있는 정도를 평가 절하하다 나중에 네트워크가 손상되면 비로소 경악합니다. 산업 수준의 노력을 통해 제2차 세계대전에서 독일의 암호를 해독한 영국의 능력과 탭핑이 불가능할 것으로 여겨지던 소련 해저 케이블을 탭핑한 미국의 능력은 강대국들이 중요한 신호 정보에 접근하는 깊이를 보여줍니다. 중국도 이처럼 최대의 노력을 기울일 것으로 보입니다. 그리고 화웨이가 현대 네트워크에서의 입지를 무기화하기는 어려울 것이라고 생각하더라도, 중국과 같은 완강한 경쟁국의 자원과 추진력을 과소 평가하는 것은 통신 경쟁에서 반복되는 모티브입니다.

이 보고서에서 알 수 있듯이, 통신 분야에 대한 강대국 게임의 많은 특징은 플레이어가 다르더라도 그대로 유지됩니다.

저자 소개

Rush Doshi는 Brookings China Strategy Initiative의 책임자였고 Brookings Foreign Policy의 선임연구원이었습니다. 또한 예일대학교 법학대학원의 Paul Tsai China Center의 선임연구원이었고 Wilson China Fellows의 창립 멤버였습니다. 그는 중국 대전략 및 인도 태평양 보안 문제를 중점적으로 연구했습니다. Doshi는 *The Long Game: China's Grand Strategy to Displace American Order*(옥스포드대학출판부 출간 예정)의 저자입니다. 현재 Biden 행정부에서 재직하고 있습니다.

Kevin McGuiness는 최근 Brookings와 함께 미국 국방부 Skillbridge Program의 외래연구원으로 일하면서 Center for East Asia Policy Studies 내의 다양한 프로젝트에 기여했습니다. 그는 공군에서 복무했으며 최근 미국 공군 아카데미에서 교수로 근무하면서 국제 관계 및 아시아 정치 과정을 지도하고 있습니다. 또한 최근 Institute for National Strategic Studies의 Center for the Study of Chinese Military Affairs에서 연구 조수로 일하며 인도 태평양 지역의 PLA 현대화 및 안보를 집중적으로 연구했습니다.

감사의 말

저자들은 이 프로젝트에서 연구 조수로 수고한 전 인턴 Isabella Lu, Zijin Zhou 및 Gaoqi Zhang, 수많은 익명의 검토자, 이 보고서를 편집해 준 Claire Harrison 및 Ted Reinert, 레이아웃 및 웹 디자인을 담당한 Chris Krupinski 및 Rachel Slattery에게 감사를 전합니다. Brookings는 이 연구에 자금을 지원하는 미국 국무부 및 Institute for War and Peace Reporting에 감사를 전합니다.

이 보고서는 Rush Doshi가 정부에 근무하기 전에 작성되었고, 오픈 소스만 포함되었으며, 미국 정부의 공식 정책 또는 입장을 반영하지 않습니다.

Brookings Institution은 독립적인 연구 및 정책 솔루션을 전문으로 하는 비영리 단체입니다. 이 연구소의 사명은 독립적으로 고품질 연구를 수행하고 이러한 연구를 바탕으로 정책 입안자 및 일반 대중에게 혁신적이고 실용적인 권장 사항을 제공하는 것입니다. Brookings 출판물의 결론 및 권장 사항은 전적으로 해당 저자의 결론이며, 본 연구소, 경영진 또는 다른 학자들의 견해를 반영하지 않습니다.

---

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

[3] Ibid., Headrick의 관찰입니다.

[4] Ibid.
[5] Ibid.
[6] Ibid., Headrick의 관찰입니다.
[7] Heidi Tworek, *News from Germany: The Competition to Control World Communications, 1900-1945* (New York: Harvard Historical Studies, 2019).
[8] Daniel R. Headrick, The Invisible Weapon. Headrick, *The Invisible Weapon*.
[9] "NH 79949 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., chapter 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, November 6, 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] 하지만 Heidi Tworek가 지적하듯이, 이 기술의 개발에서 그의 역할은 과장되어 왔습니다. Heidi Tworek, *News from Germany*.
[19] Marc Raboy, "The First Company That Wanted to 'Connect the World' Wasn't Google or Facebook," Media@LSE, August 24, 2016, https://blogs.lse.ac.uk/medialse/2016/08/24/the-first-company-that-wanted-to-connect-the-world-wasnt-google-or-facebook/.
[20] Heidi Tworek, *News from Germany*, 12–13.
[21] Michael Friedewald, "Telefunken vs. Marconi, or the Race for Wireless Telegraphy at Sea, 1896-1914," SSRN (January 9, 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] 예를 들어, Telefunken은 라틴 아메리카와 같이 독일 식민지가 없는 지역에서도 활동했습니다.
[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, December 15, 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, January 17, 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," at Wikimedia Commons, https://commons.wikimedia.org/wiki/File:SZ42-6-wheels.jpg.
[37] George I. Beck, "Military Communication - The Advent of Electrical Signaling," Britannica, https://www.britannica.com/technology/military-communication.
[38] Harry Hinsley, "The Influence of ULTRA in the Second World War" (lecture, Cambridge, U.K., October 19, 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.
[39] $1x10^{170}$개 설정이 가능.
[40] "Bletchley Park Remembers Polish Code Breakers," BBC News, July 14, 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]예를 들어Jerry Roberts, *Lorenz: Breaking Hitler's Top Secret Code at Bletchley Park* (Cheltenham, U.K.: History Press, 2017)를 참조하십시오.
[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*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.
[48] U.S. Navy, at Wikimedia Commons, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.
[49] Anna Borshchevskaya, "The Soviets' Unbreakable Code," *Foreign Policy*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.
[50] Daniel R. Headrick, *The Invisible Weapon*, chapter 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*, 2017년 3월 30일, 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, April 27, 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, January 6, 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, March 4, 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, May 24, 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*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," U.S. Department of Justice, October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[61] Constanze Stelzenmüller, "The impact of Russian interference on Germany's 2017 elections," (congressional testimony, June 28, 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,* January 5, 2021, https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack.

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

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

[65] Chun Han Wong, "China Launches Initiative to Set Global Data-Security Roles," *The Wall Street Journal,* September 8, 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*, February 12, 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*, August 15, 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, June 25, 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.