हुआवे बैठकों का इतिहास: महाशक्तियां और दूरसंचार संबंधी जोखिम, 1840-2021

रश दोशी और केविन मैकगुनेस

ब्रुकिंग्स इंस्टीट्यूशन, मार्च 2021

कार्यकारी सारांश

2018 के उत्तरार्ध में, अमेरिकी चिंताओं के बीच कि क्या कनाडा अपने दूरसंचार नेटवर्क में हुआवे का स्वागत करेगा कि नहीं, कनाडाई प्रधान मंत्री जस्टिन ट्रूडो ने कई बयान दिए, जिन्होंने दुनिया भर में पारंपरिक ज्ञान पर कब्जा कर लिया. उस समय उन्होंने घोषणा की कि "यह कोई राजनीतिक निर्णय नहीं होना चाहिए," और कनाडा अपने नेटवर्क में हुआवे की भूमिका के बारे में "राजनीति को इन निर्णयों में दखल" नहीं देने देगा.[1]

यह धारणा कि दूरसंचार पर सवाल खड़े करके सत्ता की राजनीति का खात्मा किया जा सकता है, न केवल आशावादी था बल्कि दूरसंचार के इतिहास की सोच से अलग भी था. यह रिपोर्ट उसी इतिहास के बारे में और जानकारी देती है और यह बताती है कि किस तरह सत्ता और दूरसंचार हमेशा से ही एक-दूसरे से करीब से जुड़े रहे हैं. जब देशों ने उन संबंधों को अनदेखा किया और वे अपने ही नेटवर्कों की सुरक्षा को लेकर लापरवाह थे, तो इसके परिणाम नुकसानदायक और कभी-कभी विनाशकारी भी थे.

यह रिपोर्ट 1840 के दशक में विद्युत दूरसंचार की शुरुआती स्थापना के समय दूरसंचार से महान शक्ति प्रतिस्पर्धा के कई प्रमुख मामलों की जांच करती है. ये मामले दर्शाते हैं कि आज के नीति-निर्धारक जो सवाल उठाते हैं उनमें से कई सवाल अतीत के करीब हैं. जहां नेटवर्क सुरक्षा और 5G की बुनियादी संरचना पर होने वाला मौजूदा विवाद नया लग सकता है, लेकिन असल में यह लगभग 150 साल पहले बिजली के दूरसंचार की शुरुआत में भुलाए गए विवादों की ही प्रतिध्वनि करते हैं. इतना ही नहीं, आज की दूरसंचार प्रतिस्पर्धा के कई परिचित तत्व– जैसे कि मानक-सेटिंग निकाय, देश की सब्सिडी, केबल टैप, सूचना युद्ध, विकासशील देश के

बाजारों और लाभ प्राप्त करने के लिए एन्क्रिप्शन– एक दशक से भी पहले विकसित किए गए थे, जिनमें मौजूदा विवाद के लिए महत्वपूर्ण सबक शामिल हैं.

इन प्रमुख सबकों की एक सूची नीचे दी गई है:

1. **वैश्विक दूरसंचार नेटवर्क पर नियंत्रण राजनीतिक शक्ति का एक रूप है.** 5G नेटवर्कों से उम्मीद की जाती है कि वे एक स्मार्ट और कनेक्टेड अर्थव्यवस्था की नींव बनाएंगे, जिसमें अनगिनत डिवाइस और सेंसर एक साथ जुड़ेंगे. दुनिया भर में इन नेटवर्क को बनाने के लिए उत्सुक, चीन ने "डिजिटल सिल्क रोड" पहल के हिस्से के रूप में दुनिया भर में अपनी 5G चैंपियन कंपनियों और परियोजनाओं को सब्सिडी दी है. वह कोशिश इलेक्ट्रिकल टेलीग्राफ़ी के आरंभ के समय नेटवर्क प्रभुत्व में ग्रेट ब्रिटेन के प्रयासों के अनुरूप है. ब्रिटेन ने अपने नेटवर्कों पर दूसरे देशों की निर्भरता में लगातार वृद्धि करते हुए छह दशकों में इसका लाभ उठाया है – यहां तक कि ब्रिटेन से होकर केबल बिछाने के लिए भी शुल्क और आर्थिक लाभ लिए गए – साथ ही इससे विदेशी नेटवर्कों पर ब्रिटेन की निर्भरता भी कम हुई है. अंतत: दुनिया के आधे से भी ज़्यादा केबल ट्रैफ़िक, सबसे बड़े रेडियो नेटवर्क और केबल जहाज़ों के सबसे बड़े बेड़े पर उसका नियंत्रण हो गया. ब्रिटेन के "सूचना आधिपत्य" ने उसे जर्मनी को प्रथम विश्व युद्ध में सभी वैश्विक दूरसंचार से आभासी रूप से अलग करने में और बर्लिन को ब्रिटिश-स्वामित्व वाली लाइनों से ब्रिटिश निगरानी में ट्रैफ़िक ले जाने को बाध्य कर दिया, जिससे बाद में इस संघर्ष में जर्मनी की हार में निर्णायक साबित हुआ.

2. **लंबे समय तक शांति और समृद्धि से आम तौर पर दूरसंचार संबंधी जोखिमों में आत्मसंतुष्टि आ जाती है.** पिछले 30 सालों में, शीत युद्ध के बाद शांति और आर्थिक वैश्वीकरण और दूरसंचार के क्षेत्र में त्वरित प्रगति का संयोग बना जिसके चलते देशों ने राजनीतिक और सुरक्षा जोखिमों से ऊपर क्रांतिकारी व्यावसायिक लाभों को प्राथमिकता दी, जिनमें विदेशी स्वामित्व या नेटवर्कों का संचालन तक शामिल था. 1840 के दशक में दूरसंचार के आरंभ के समय इसी तरह का विकास हुआ और उसका संयोग भी प्रथम विश्व युद्ध तक जारी रही सापेक्ष शांति और वैश्वीकरण की अवधि के साथ हुआ. उस युग के लिए, नई संचार तकनीकों की संभावित जादुई व्यावसायिक क्षमता पर कब्ज़ा करने की इच्छा ने विदेशी नेटवर्कों या कंपनियों पर निर्भरता से संबंधित सवालों को अस्पष्ट कर दिया. ग्रेट ब्रिटेन वैश्विक नेटवर्क में एक अनुपलब्ध नोडल स्थिति का निर्माण और

फिर उसका दोहन करके दूसरों की शालीनता से लाभान्वित हुआ, जिसमें अधिकांश अन्य महान शक्तियां उसके नेटवर्क पर निर्भर थीं.

3. **जब देश अपनी दूरसंचार सुरक्षा के बारे में आत्मसंतुष्ट हो जाते हैं, तो इसके परिणाम विनाशकारी हो सकते हैं और दुनिया की राजनीति में फेरबदल कर सकते हैं.** दशकों तक ब्रिटिश दूरसंचार लाइनों पर निर्भरता की दशकों की जर्मन आत्मसंतुष्टि का मतलब था कि जब तक बर्लिन उस आत्मसंतुष्टि के जोखिमों के प्रति सचेत हुआ, तब तक उसे बदलने में बहुत देर हो चुकी थी. जब प्रथम विश्व युद्ध शुरू हो गया, तो ब्रिटेन ने जर्मनी की सारी केबल काट दीं और बर्लिन को मजबूर कर दिया कि वह इंटरसेप्ट होने के जोखिम के बावजूद ब्रिटिश नेटवर्कों के माध्यम से ट्रैफ़िक को रूट करे, जिसके चलते "ज़िमरमैन टेलीग्राम" का खुलासा हुआ जिसकी मदद से अमेरिका इस युद्ध में शामिल हो गया. इसी तरह से, प्रथम विश्व युद्ध में वायरलेस रेडियो ट्रांसमिशन में रूसी अनुशासन के अभाव के चलते जर्मनी संचारों को इंटरसेप्ट कर पाए, वे रूसी सैनिकों की आवाजाही को वास्तविक समय में "देख" पाए और उन्हें टैनेनबर्ग की लड़ाई में निर्णायक मात दे पाए. इसके बाद, दूसरे विश्व युद्ध में, नाज़ी का अपने साइफर्स पर अति-आत्मविश्वास उन्हें अद्यतित करने की कम कोशिशों का कारण बना, जिसके चलते ग्रेट ब्रिटेन ने वे कोड जान लिए और ऐसी गोपनीय जानकारी हासिल की जिसके बारे में माना जाता है कि इसी की वजह से युद्ध की अवधि दो से चार सालों तक कम हो गई. सूचना की शक्ति को देखते हुए, कभी-कभी संकेतों की अनुशासनहीनता या आत्मसंतुष्टि भी इतिहास में बदलाव ला सकती है.

4. **नई तकनीक हमेशा इसे बाधित करने के लिए नए प्रयासों की ओर ले जाती है.** समुद्रतल में केबल बिछाने पर उन्हें काटने और टैप करने की शुरुआत स्पेनिश-अमेरिकी से ही हो चुकी थी, रेडियो ट्रांसमिशनों ने विरोधियों को नेटवर्क नोट पकड़ने और ट्रांसमिशन को इंटरसेप्ट करने के प्रयासों को बढ़ावा दिया; और एन्क्रिप्शन के लिए परिष्कृत साइफर के उभरने से उन्हें तोड़ने के लिए औद्योगिक-स्तर के प्रयासों की शुरुआत हो गई. हर युग में, कुछ लोगों का मानना था कि संचार के क्षेत्र की नई छलांग इससे पहले की तुलना में कम जोखिम भरी हो सकती है. हालांकि, हर बार, नवाचार और शोषण का सिलसिला जारी रहा.

5. **दूरसंचार नेटवर्क कभी भी राजनीतिक रूप से तटस्थ नहीं रहे हैं, खासकर तनाव के समय में.** 2019 में, हुआवे के अधिकारियों ने एक "नो-बैकडोर, नो-स्पाइंग" की शपथ ली और

वादा किया कि उनकी कंपनी राजनीति से बाहर रहेगी, साथ ही, चीन की सरकार ने इस शपथ का सम्मान करने की प्रतिबद्धता जाहिर की. लेकिन एक सदी से भी बहुत पहले, दूरसंचार कंपनियों और उनकी मेजबान सरकारों ने सार्वजनिक रूप से इसी तरह के वादे किए थे जबकि शांतिकाल में और युद्धकाल में भी साथ मिलकर उन्हें निजी रूप से तोड़ा था और उन पर काम किया था. उदाहरण के लिए, समुद्रतल में केबल बिछाने के ब्रिटिश प्रभुत्व से फ़्रांसीसी, जर्मन और अमेरिकियों को युद्ध के समय में भी इन लाइनों तटस्थ बनाए रखने की वकालत करनी पड़ी. ब्रिटिश फ़र्मों ने सार्वजनिक रूप से उनकी तटस्थता की घोषणा की लेकिन वास्तविकता में उन्हें ब्रिटिश राजनीतिक हितों के लिए स्थगित कर दिया, खासकर भीषण तनाव के समय में और युद्ध की अवधि में तो उन्होंने तटस्थता को पूरी तरह से दरकिनार कर दिया. प्रतिद्वंद्वी सूचना प्रवाहों को बाधित करने या इंटरसेप्ट करने से मिलने वाली शक्ति आम तौर पर सहन करने के लिए तटस्थता के ईमानदार दावों के लिए भी बहुत आकर्षक रही है.

6. **किसी प्रतिस्पर्धी या विरोधी की फ़र्मों पर भरोसा करने के जोखिम को मान लेने के बाद सरकारें अक्सर अपने खुद के दूरसंचार चैंपियन चाहती हैं.** संयुक्त राज्य के पास फ़िलहाल 5G बेस स्टेशन बनाने वाला कोई भी प्रमुख निर्माता नहीं है, जिसने इस बारे में बहस छेड़ दी है कि उसे अपनी ही कंपनियों में निवेश करना चाहिए या सहयोगी कंपनियों पर भरोसा करना चाहिए. इससे इस बात पर भी असहमति जताई गई है कि हुआवे खुद किस सीमा तक देश की एक वास्तविक चैंपियन है. इन बहसों की कुछ मिसालें भी मिलती हैं. 20 वीं सदी की शुरुआत में, दूरसंचार उपकरण या नेटवर्कों पर दूसरों के भरोसे रहने वाले कई देशों ने अपने खुद के सिस्टम बनाने शुरू कर दिए थे. उदाहरण के लिए, जर्मनी ने प्रतिस्पर्धी रेडियो प्रयासों वाली दो जर्मन कंपनियों –सीमेंस एंड हाल्स्के और एईजी – को साथ मिलकर आगे बढ़ाया ताकि रेडियो में ब्रिटिश प्रभुत्व के लिए एक जर्मन विकल्प स्थापित किया जा सके. कई अन्य अग्रणी देशों ने ऐसी कंपनियों का समर्थन किया जो, सामान्य रूप से निजी होकर भी, उन देशों से जुड़ी हुई थीं जिन्होंने उनका समर्थन किया था.

7. **दूरसंचार मानकों का संघर्ष यह निर्धारित कर सकता है कि कौन-से देश नेटवर्क शक्ति का फ़ायदा उठाएंगे और इसके लिए अक्सर सहयोगियों और साझेदारों को सूचीबद्ध करने की आवश्यकता होती है.** जिन देशों की प्रौद्योगिकी प्रमुख मानक बन जाती है वे दूसरों के मुकाबले उसका लाभ उठा सकते हैं. सूचना संचार प्रौद्योगिकी मानकों पर हो रही मौजूदा प्रतिस्पर्धा, इस तरह से, रेडियो नेटवर्क पर एंग्लो-जर्मन प्रतिस्पर्धा जैसी है. ब्रिटेन,

अपनी समर्थित कंपनी मार्कोनी कंपनी के माध्यम से, वायरलेस रेडियो में इतना प्रभावी था कि दूसरी सभी महाशक्तियों को ब्रिटेन के वायरलेस नेटवर्क के माध्यम से संदेश भेजने पड़ते थे, जिसने किसी भी अन्य वायरलेस स्टेशन के साथ जुड़ने से इनकार कर दिया था. जर्मनी को आखिरकार एक मानक-सेटिंग निकाय पर उस प्रभुत्व को तोड़ने में सफलता मिली जिसने दूसरी शक्तियों की मदद से इस "गैर-अंतर-संचार" नीति को निषिद्ध कर दिया, जिनमें संयुक्त राज्य अमेरिका और फ़्रांस भी शामिल थे – यह एक प्रमाण है कि आज के मिलते-जुलते गठबंधन दृष्टिकोण का इस्तेमाल उदार राज्यों द्वारा किस तरह अनुकूल सूचना और संचार प्रौद्योगिकी (आईसीटी) मानकों को निर्धारित या संरक्षित करने के लिए किया जा सकता है अगर वे साथ मिलकर काम करें.

8. **देश एन्क्रिप्शन की ओर रुख करते हैं क्योंकि उनके संचार को इंटरसेप्ट करना आसान हो जाता है, लेकिन निर्धारित सलाहकारों या उपयोगकर्ता त्रुटि के कारण एन्क्रिप्शन की अक्सर एक सीमा होती है.** कुछ तर्क देते हैं कि नेटवर्क में हुआवे की भूमिका पर या इंटरनेट से जुड़े उपकरणों के सामान्य जोखिम पर चिंताएं आधुनिक एन्क्रिप्शन द्वारा अमल में लाई जाती हैं. इस तरह के तर्कों का एक लंबा इतिहास रहा है. एक सदी पहले दूरसंचार के आरंभ के समय, यह संभावना कि नेटवर्क नोड नियंत्रित करने वाले दूसरे लोगों द्वारा टेलीग्राफ़ संदेश पढ़े जा सकते हैं या यह कि निष्क्रिय श्रवण उपकरण द्वारा रेडियो को इंटरसेप्ट किया जा सकता है, प्रमुख एन्क्रिप्शन सुधारों का कारण बना जिन्होंने यदा-कदा अति-आत्मविश्वास को बढ़ावा दिया. जर्मनी की जटिल रोटर साइफर मशीनों को अटूट माना जाता था, लेकिन उपयोगकर्ता त्रुटि और ब्रिटिश औद्योगिक-स्तर के प्रयासों के चलते ग्रेट ब्रिटेन को जर्मन कोड से छेड़खानी कर पाया. जर्मन उपकरण और साइफर में कम खर्च वाले अपडेट से ब्रिटेन का लाभ खत्म हो सकता था, लेकिन अपने एन्क्रिप्शन में बर्लिन के अति-आत्मविश्वास ने उन बदलावों को रोक दिया, जिसमें इंटरसेप्ट की गई ऐसी गोपनीय जानकारी थी जिसने युद्ध का तरीका ही बदलकर रख दिया. एंड-टू-एंड एन्क्रिप्शन, एन्क्रिप्शन के पिछले प्रयासों से कहीं अधिक उन्नत है, लेकिन इतिहास बताता है कि कुछ विनम्रता आवश्यक है.

9. **कई देश उस सीमा तक छूट देते हैं जिस पर कोई विरोधी अपने नेटवर्क से समझौता करने के लिए असाधारण प्रयास कर सकता है.** आधुनिक दूरसंचार पर हो रही बहस के बीच, यह उल्लेख करना महत्वपूर्ण है कि जिन देशों ने सुविधा या व्यवसाय को प्राथमिकता दी थी और इसकी वजह से सुरक्षा के छोटे रास्ते चुने थे, उन्हें किसी विरोधी के प्रयासों द्वारा अक्सर ऐसे अप्रिय आश्चर्य हुए हैं जो उनके नेटवर्कों से छेड़खानी करेगा.

प्रथम विश्व युद्ध में, जर्मनी उस गति और क्रूरता से आश्चर्यचकित था जिससे ब्रिटेन ने उन सभी केबलों को काटा था जिनसे जर्मनी बाहरी दुनिया से संपर्क करता था, इसी तरह से, रूसी कमांडर भी आश्चर्यचकित था जब उनकी रेडियो अनुशसानहीनता टैनेनबर्ग में विनाशकारी हार का कारण बन गई. दूसरे विश्व युद्ध में, जर्मनी ने उम्मीद नहीं की थी कि ब्रिटिश एक अत्यधिक-केंद्रीयकृत औद्योगिक-स्तर की कोड तोड़ने वाली प्रणाली बना लेंगे जो जर्मन दूरसंचार की त्रुटियों का गलत लाभ उठा सकती थीं – चाहे वे कितने भी छोटे या क्षणभंगुर क्यों न हो – जिनसे जर्मन कोड तोड़े जा सकते थे. और शीत युद्ध के दौरान, सोवियतों ने कभी भी पानी के नीचे बिछी किसी आंतरिक टेलीफ़ोन लाइन को एन्क्रिप्ट नहीं किया जो उनके हिसाब से संयुक्त राज्य अमेरिका की पहुंच से दूर थी, लेकिन वाशिंगटन ने उसे टैप करने का तरीका ढूंढ ही लिया – जिससे उसे सूचना का एक अमूल्य स्रोत मिल गया.

10. **नेटवर्क सुरक्षा केवल इंटरसेप्शन के बारे में ही नहीं है, बल्कि यह अस्वीकृति के बारे में भी है.** नेटवर्क में हुआवे की भूमिका पर होने वाली कुछ बहस डेटा सुरक्षा के सवालों पर ज़ोर देती है लेकिन उसे नेटवर्क की अस्वीकृति पर बेहतर विचार करने से लाभ हो सकता है, जो महाशक्ति की दूरसंचार प्रतिस्पर्धा का एक महत्वपूर्ण भाग रहा है. टेलीग्राफ़ी के आरंभ ने महान शक्तियों को केबलें काटने और दूरसंचारों को अस्वीकार करते हुए देखा, जिसके चलते ग्रेट ब्रिटेन के अभूतपूर्व और सुव्यवस्थित संचालन की परिणति दुनिया भर के उन सभी केबलों को अलग करने के लिए हुई जो जर्मनी को बाहर से जोड़ सकते थे. कभी-कभी, कोई देश नेटवर्क अस्वीकृति की रणनीतियों में खुद को ही नुकसान पहुंचा सकता है, लेकिन अगर वह मानता है कि यह नुकसान उसके विरोधी के लिए कहीं अधिक होगा तो वह कुछ भी करके आगे बढ़ेगा.

महाशक्तियां और दूरसंचार

दूरसंचार के इतिहास में उल्लेख है कि "सूचना के प्रवाह की गति बढ़ाने के लिए महान साम्राज्यों ने लंबी दूरी तय की है". "रोमन ने सड़कें बनाईं, फ़ारसियों और मंगोलों ने घोड़ों की दौड़ स्थापित की, ब्रिटिश ने मेल स्टीमर्स को सब्सिडी दी."[2] लेकिन भले ही देश सूचना के लिए तरसते रहे हों, आधुनिक टेलीग्राफ़ के आरंभ तक उसका प्रवाह सीमित ही रहा. सूचना प्रवाह के विद्युतीकरण ने आधुनिक दूरसंचार का निर्माण किया और उसी के साथ, उस पर महाशक्ति की प्रतिद्वंद्विता के चिर-परिचित मिसालों का भी निर्माण हुआ.

आधुनिक दूरसंचार के वे पहले दशक, जिनकी अवधि 1840 से प्रथम विश्व युद्ध तक थी, मौजूदा समय के साथ महत्वपूर्ण विशेषताएं साझा करते हैं. शीत युद्ध के बाद के मौजूदा युग की तरह ही, वह अवधि, सापेक्ष महाशक्ति शांति थी जिसने अग्रणी देशों को दूरसंचार नेटवर्कों में राजनीति और सुरक्षा के सवालों को लेकर "कम संवेदनशील" बनाया.[3] जब महाशक्तियों ने 19वीं सदी में राष्ट्रीय और अंतरराष्ट्रीय नेटवर्क बनाए, तो शुरुआत में कईयों ने कॉन्टेंट को उद्योगों के हाथ छोड़ दिया, निजी कंपनियों की राष्ट्रीयता को अनदेखा किया और दूरसंचार नेटवर्कों पर विरोधी के नियंत्रण के जोखिम को कमतर आंका. दूरसंचार में क्रांतिकारी बदलावों के लाभ – जिसे कुछ लोगों ने कभी "समय और स्थान की बर्बादी"[4] कहा था – इतने स्पष्ट और अभिभूत थे कि "केबलों के स्वामित्व को एक छोटी सी समस्या के रूप में देखा गया."[5] एक इतिहासकार ने एक अवलोकन में उल्लेख किया कि उस अवधि में टेलीग्राफ़ी का तात्पर्य राजनीति से कहीं अधिक व्यवसाय से था जिसे शायद उतनी ही आसानी से आधुनिक सूचना प्रौद्योगिकी के शुरुआती उत्साह और उसके नवीनतम अवतार पर भी लागू कर दिया गया: 5G.[6]

संबंधित महाशक्ति की आत्मसंतुष्टि की अवधि लंबी नहीं चली. 1879 में पेरू जैसे देश और फिर 1898 में संयुक्त राज्य अमेरिका ऐसे कुछ पहले देश थे जिन्होंने किसी दुश्मन के दूरसंचार नेटवर्कों को काट दिया था. जब महाशक्ति के तनाव बहुत अधिक बढ़ गए, तो दुनिया भर के देशों को पता चला कि कुछ देश – खासकर ग्रेट ब्रिटेन – ने लंबी शांति को अच्छी तरह से प्रबंधित किया और अपनी निजी फ़र्मों के माध्यम से, अंतरराष्ट्रीय संचारों पर मज़बूत पकड़ बना ली.

ब्रिटिश समुद्रतल में बिछे केबल नेटवर्कों पर निर्भरता से बढ़ती घबराहट के साथ, फ़्रांस और जर्मनी जैसे देशों ने अपने खुद के नेटवर्कों के विकास के लिए ऐसी बेतहाशा सब्सिडी दी जो चीन

की अपनी सब्सिडी और अपने सूचना प्रौद्योगिकी चैंपियनों, जैसे कि अलीबाबा, बायडू, टेंसेंट और हुआवे की सुरक्षा से बहुत अधिक अलग नहीं थी. और जैसा कि इतिहासकार हैदी ट्वोरेक के दस्तावेज़ बताते हैं, ब्रिटेन के विरोधियों ने दूरसंचार प्रौद्योगिकी की अगली पीढ़ी पर भी बड़ा दांव लगाया – "वायरलेस टेलीग्राफ़ी," जिसे रेडियो के नाम से बेहतर जाना जाता है – इस उम्मीद में कि ब्रिटिश-स्वामित्व वाले समुद्रतल की टेलीग्राफ़ केबलों पर निर्भरता कम हो जाएगी.[7] जहां ब्रिटिश ने इस क्षेत्र में अगुवाई की, वहीं जर्मनी ने ब्रिटिश नेटवर्कों पर भरोसा करने से मना कर दिया. उसने सरकारी-समर्थन वाले चैंपियन के साथ अपना खुद का नेटवर्क बनाया और दुनिया के कम कनेक्टेड हिस्सों – लैटिन अमेरिका, अफ़्रीका, एशिया – में अपनी पैठ बनाई जो आज की तारीख में विकासशील देशों में चीनी प्रौद्योगिकी कंपनियों के विस्तार और 5G नेटवर्क की नींव रखने के लिए बीजिंग के दृढ़ संकल्प को प्रदर्शित करता है.

इस पूरी अवधि में, महाशक्ति की दूरसंचार प्रतिस्पर्धा के कई तत्वों को आज अनदेखा किया जाता है जिन्हें उस युग के देशों ने अक्सर बहुत ही गंभीरता से लिया था. रेडियो नेटवर्कों में ब्रिटिश प्रभुत्व से निराश होकर, जर्मनी ने ब्रिटिश प्रभुत्व को खत्म करने के लिए एक मानक-तय करने वाले निकाय का इस्तेमाल किया – एक ऐसी रणनीति जो दर्शाती है कि वे निकाय उस युग में भी कम महत्वपूर्ण नहीं थे जितने कि वे आज हैं. और जैसे-जैसे दूरसंचार वायरलेस होते गए और इंटरसेप्ट करने में और भी आसान हो गए, वैसे-वैसे महान शक्तियों ने एन्क्रिप्शन में अपना भरोसा जताया – कभी-कभी इस धारणा के अंतर्गत उनके नेटवर्कों के पूर्वगामी अनुशासित संचालन कि "साइफर" – संदेशों को एन्क्रिप्ट या डिक्रिप्ट करने के विस्तृत चरण – समस्या को सुलझा लेंगे, एक ऐसी मान्यता जो उपयोगकर्ता त्रुटि के कारण हमेशा ही गलत सिद्ध हुई है. उस दृष्टिकोण में दूरसंचार नेटवर्क की सामान्य असुरक्षा के बारे में आधुनिक धारणाओं के लिए समानताएं हैं और हुआवे पर हुई बहस में कुछ लोगों द्वारा यह मान्यता व्यक्त की गई कि एन्क्रिप्शन से चीन द्वारा किसी के दूरसंचार नेटवर्कों को एक्सेस कर लेने का जोखिम बेअसर हो जाएगा.

जब महाशक्ति शांति खत्म हुई और युद्ध शुरू हो गया, तब दूरसंचार का राजनीतिक महत्व – जो शांतिकाल में हमेशा ही स्पष्ट नहीं रही – अचानक से स्पष्ट हो चुकी थी. प्रथम विश्व युद्ध में रूसी प्रसारण को इंटरसेप्ट करने में जर्मनी की सफलता ने टैनेनबर्ग की लड़ाई में इतनी जीत हासिल की कि इसने युद्ध के तरीके को ही बदल दिया और इस टकराव से रूस को बाहर निकालने में मदद की. प्रथम विश्व युद्ध में समुद्रतल में बिछी केबलों के ब्रिटिश प्रभुत्व इतना पूर्ण था कि इसने जर्मनी को वैश्विक दूरसंचार प्रणाली से अलग कर दिया, जर्मनी के केबल ट्रैफ़िक को अपने खुद के नेटवर्कों से रूट किया और अंतत: ज़िमरमैन टेलीग्राम का खुलासा

किया, जिसकी मदद से संयुक्त राज्य इस टकराव में आ गया. द्वितीय विश्व युद्ध में ब्रिटेन ने जर्मन एन्क्रिप्शन को तोड़कर एक और खूफ़िया सफलता हासिल की जिसे अटूट माना गया था, जिससे ऐसी अद्वितीय खूफ़िया जानकारी मिली जिसे लेकर ब्रिटेन के आधिकारिक इतिहास में तर्क दिया जाता है कि इससे यूरोप में युद्ध की अवधि कई वर्षों तक कम हो गई. ये मामले दर्शाते हैं कि दूरसंचार सुरक्षा सिर्फ़ युद्ध के मैदान की रणनीति का विषय नहीं है, बल्कि राजनीतिक प्रतिस्पर्धा का भी है, जो महाशक्तियों के भाग्य और विश्व इतिहास के आकार को निर्धारित कर सकती है.

जैसे-जैसे विश्व अमेरिकी-सोवियत शीत युद्ध की तरफ़ बढ़ने लगा, ब्रिटिश लाभों को न सिर्फ़ अमेरिकी शक्ति द्वारा बल्कि प्रौद्योगिकी में हुए ऐसे बदलाव द्वारा भी खत्म कर दिया गया जिसने पुराने नेटवर्कों को कम प्रासंगिक बना दिया, जो प्रौद्योगिकी के मामले में सबसे आगे रहने के लिए महाशक्तियों के महत्व को दर्शाता है. उस नए युग में, दूरसंचार प्रतिस्पर्धा चिर-परिचित लाइनों पर जारी रही. उदाहरण के लिए, संयुक्त राज्य ने ऐसी सबमरीन केबलों को टैप करने के नए तरीकों में महारत हासिल कर ली जिन्हें इतनी गहराई में बिछाया गया था और इतना सुरक्षित माना गया था कि उनसे गुज़रने वाले संदेश अक्सर एन्क्रिप्ट किए बिना छोड़ दिए जाते थे. प्रतिस्पर्धा दूसरे डोमेन में भी चली गई – जैसे कि उपग्रह और इंटरनेट की बुनियादी संरचना – हालांकि इसका बहुत सा इतिहास अब भी लिखा जा रहा है, फिर भी ज़्यादातर मामलों में, यह वर्गीकृत ही है.

दूरसंचार, जैसा कि मामलों की इस संक्षिप्त श्रृंखला से पता चलता है, हमेशा से राजनीतिक ही रहा है. इन प्रौद्योगिकियों और क्षमताओं के गलत इस्तेमाल आम तौर पर उनके विकास के साथ-साथ ही विकसित हुआ है. जैसे ही संचार के नए तरीके आए, वैसे ही महाशक्तियों ने उन्हें इंटरसेप्ट या बाधित करने के तरीके खोजने शुरू कर दिए. एक इतिहासकार का कहना है कि "विद्युतीय संचार को अक्सर मानवता की महान उपब्धियों में से एक के रूप में बताया जाता है," "लेकिन जब हम इसे सुरक्षा के दृष्टिकोण से देखते हैं, तो हम एक बिल्कुल अलग ही तस्वीर देखते हैं, क्योंकि सुरक्षा के लिए यह तकनीकी नहीं बल्कि एक सामाजिक और राजनीतिक चारित्रिक विशेषता है." और "चूंकि राजनीति बेहतर नहीं हुई है," इसलिए, "दूरसंचार का एक अंधेरा पहलू भी है."[8]

अब हम लगभग दो सदियों की दूरसंचार प्रतिस्पर्धा के प्रमुख विषयों का सारांश देखते हैं.

1. स्पेनिश-अमेरिकी युद्ध: केबल तटस्थता की सीमाएं

1907 में प्रकाशित सेनफ्यूगॉस में अमेरिका केबल-कटिंग अभियान का चित्रण. इस ऑपरेशन ने दर्शाया कि समुद्रतल में बिछी टेलीग्राफ़ केबलों को सैन्य टकराव के दौरान तटस्थ नहीं माना जाएगा, यहां तक कि उस महाशक्ति द्वारा भी जिसने कभी केबल तटस्थता की वकालत की थी.

स्रोत: नेवल हिस्टॉरिकल सेंटर ऑनलाइन लाइब्रेरी[9]

जब 19वीं सदी में दुनियाभर में सबमरीन केबलें बिछाई जाने लगीं, तो कई अग्रणी शक्तियों – जिनमें फ़्रांस, जर्मनी और संयुक्त राज्य अमेरिका – ने उन्हें अंतरराष्ट्रीय राजनीति से अलग रखने का आह्वान किया. 1858 में, सबसे पहले भेजे गए ट्रांस-अटलांटिक केबलों में से एक में, अमेरिकी राष्ट्रपति जेम्स बुखानन ने महारानी विक्टोरिया से यह सुनिश्चित करने का आग्रह किया कि दुनिया की नई टेलीग्राफ़ लाइनों को शत्रुता के बीच भी "हमेशा तटस्थ... रखा जाएगा."[10]

हालांकि जैसे ही शत्रुता खत्म हुई, वैसे ही तटस्थता के उच्च विचार वाले सिद्धांतों को छोड़ दिया गया. बुकानन के संदेश के दो दशक बाद, पेरू ने विवादित क्षेत्र से गुज़र रही चिली की केबल लाइनें काट दीं.[11] उस विवाद ने थोड़ा सा ध्यान आकर्षित किया, लेकिन जब संयुक्त राज्य

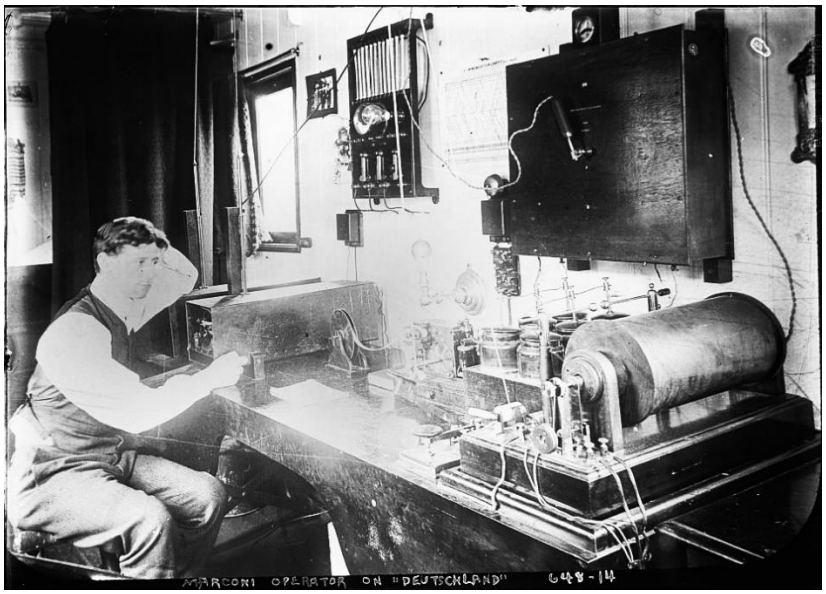
अमेरिका – केबल तटस्थता के एक पूर्व चैंपियन – ने स्पेनिश-अमेरिकी युद्ध में अटलांटिक और पैसिफ़िक, दोनों जगहों में केबलें काटीं, तो इस पर दुनिया की नज़र गई.

अमेरिकी केबल कटिंग की योजना टकराव से पहले ही बना ली गई थी. अटलांटिक थिएटर में, संयुक्त राज्य अमेरिका ने स्पेन को क्यूबा में उसके सैन्य बलों से अलग करने की उम्मीद की थी. उस समय की एक अमेरिकी पत्रिका में बताया गया कि "हवाना का अलगाव बेशक प्रमुख महत्व रखता था," और उसके लिए संयुक्त राज्य अमेरिका को "हवाना को दुनिया से सभी तरह के टेलीग्राफ़िक संचार से हटाना" था.[12] संयुक्त राज्य अमेरिका ने इसकी शुरुआत उस स्पेनिश ट्रैफ़िक को काटते हुए की जो फ़्लोरिडा में अमेरिकी क्षेत्र से गुज़र रही थी. इसके बाद, उसने सेनफ्यूगॉस में एक प्रमुख दूरसंचार नोड को नष्ट करने के लिए एक छोटी अमेरिकी टुकड़ी भेजी, जिसने हवाना शहर और पश्चिमी क्यूबा के ज़्यादातर हिस्से का संपर्क स्पेन से काट दिया. इसके बाद, संयुक्त राज्य अमेरिका ने पूर्वी क्यूबा में कई केबलों के साथ ही कैरेबियाई केबलों पर भी हमला किया जो प्योर्टो रिको को स्पेन से जोड़ते थे.[13] साथ मिलकर, केबल कटिंग की वजह से क्यूबा में सैन्य बलों को निर्देश और आदेश देने की स्पेन की क्षमता काफ़ी हद तक घट गई.[14]

पैसिफ़िक में, संयुक्त राज्य अमेरिका ने सिर्फ़ मनीला और हांगकांग के बीच की सबमरीन केबल को काटा, जिसके असर से फिलीपींस स्पेन से अलग हो गया.[15] इस फ़ैसले से अमेरिकी संचारों को भी नुकसान पहुंचा, लेकिन यह माना गया कि इसकी वजह से स्पेन को कहीं ज़्यादा नुकसान भुगतना पड़ेगा और संयुक्त राज्य अमेरिका हांगकांग को नियमित रूप से एक जहाज भेजता रहा ताकि वह वायर डिस्पैचों को वापस वाशिंगटन भेज सके.[16] अमेरिका सैन्य बलों ने फिलीपींस में समुद्रतल में बिछी केबलें भी काट दीं, जिससे अपने सैन्य बलों को आदेश देने की स्पेन की क्षमता और भी घट गई.

स्पेनिश-अमेरिकी युद्ध शायद पहला वैश्विक टकराव था जिसमें ऐसे एकाधिक थियेटर शामिल हो गए थे जिनके लिए इलेक्ट्रिकल दूरसंचार मायने रखता था. यह भी पहली बार ही हुआ था कि किसी एक महाशक्ति ने दूसरी शक्ति को समुद्रतल में बिछी केबलों का इस्तेमाल करने से रोकना चाहा हो. संघर्ष से पहले, टेलीग्राफी को अभी भी मुख्य रूप से व्यावसायिक दायरे के रूप में देखा जाता था और कईयों ने उम्मीद की थी कि केबलों को राजनीतिक और सैन्य प्रतिस्पर्धा से कोई खतरा नहीं होगा. इस टकराव ने ऐसे दृष्टिकोणों की सीमाएं साबित कर दीं, और उनसे यह संकेत मिला कि दूरसंचार के बुनियादी ढांचें पर नियंत्रण और भू-राजनीतिक विरोधियों को मिलने वाले लाभ को अस्वीकार करने की क्षमता का हमेशा से ही जटिल राजनीतिक महत्व रहा है.

2. एंग्लो-जर्मन प्रतिद्वंद्विता: नेटवर्कों का निर्माण करना और मानक तय करना



जर्मन महासागर लाइनर एसएस डचलैंड के "मार्कोनी रूम" में मार्कोनी कंपनी के रेडियो ऑपरेटर. मार्कोनी कंपनी का प्रभाव इतना ज़्यादा था कि उनके कर्मचारियों ने जर्मन रेडियो रूम्स में भी ऑपरेट किया था भले ही जर्मनी इंटरसेप्शन और अस्वीकृति के जोखिमों के बारे में चिंतित था.

स्रोत: लाइब्रेरी ऑफ़ कांग्रेस, जॉर्ज ग्रांथम बैन कलेक्शन [17]

तकनीकी मानक-सेटिंग और इसके परिचर नेटवर्क प्रभाव, महाशक्ति प्रतिस्पर्धा का एक दीर्घकालिक और सूक्ष्म क्षेत्र है. जिन देशों की प्रौद्योगिकी प्रमुख मानक बन जाती है वे दूसरों के मुकाबले उसका लाभ उठा सकते हैं – एक ऐसा बिंदु जो बढ़ती शक्तियों से परास्त नहीं हुआ, जो अक्सर समानांतर सिस्टम बनाकर अपनी कमज़ोरी को कम करने का काम करते हैं. दरअसल, आईसीटी पर वर्तमान चीन-अमेरिकी प्रतिस्पर्धा जर्मनी और ग्रेट ब्रिटेन के बीच उस युग के आईसीटी के बुनियादी ढांचे में प्रभुत्व के लिए एक सदी पुरानी प्रतिस्पर्धा को दर्शाती है, जिसमें मौजूद समानताएं और वर्तमान सबक महत्वपूर्ण हैं.

19वीं सदी के आखिर में, अंग्रेज़ों की रॉयल नेवी के समर्थन प्राप्त, इतालवी इंजीनियर गुगलिएलमो मार्कोनी ने वायरलेस टेलीग्राफ़ी का निर्माण किया.[18] यह आविष्कार क्रांतिकारी था. अतीत में जहां महाशक्तियों ने एक-दूसरे के केबल काटे थे, और जहां पहले जहाज-से-जहाज और जहाज-से-किनारे का संचार मुश्किल था, मार्कोनी के सिस्टम ने उन समस्याओं को हल किया

और उसमें हस्तक्षेप की संभावना भी कम थी.[19] मार्कोनी ने आखिरकार ग्रेट ब्रिटेन से साझेदारी कर ली, जिससे रेडियो ट्रांसमिशन पर देश का एकाधिकार हो गया. दुनिया के समुद्रतल में बिछे केबल नेटवर्क के 60% हिस्से के साथ संयुक्त रूप से, ब्रिटेन के पास अंतर्राष्ट्रीय ट्रांसमिशन का प्रभुत्व है. ब्रिटेन को हो रहे इस लाभ से जर्मनी परेशान हो रहा था, लेकिन वायरलेस प्रौद्योगिकियों पर प्रतिस्पर्धा ने भी "जर्मनी के लिए एक नए अंतर्राष्ट्रीय बुनियादी ढांचे पर नियंत्रण" और "अंग्रेज़ केबलों को दरकिनार करने" का अवसर दिया; महाक्ति प्रधानता को परिणाम में बांधा गया था.[20]

कमज़ोर महसूस करते हुए, कैसर विल्हेम द्वितीय ने जर्मन वैज्ञानिकों और इंजीनियरों के लिए सरकार के प्रत्यक्ष समर्थन को अधिकृत किया क्योंकि उन्होंने कामयाबी से मार्कोनी के डिज़ाइनों की नकल कर ली थी, उन्हें जर्मनी में ही पेटेंट कराया गया और जर्मन सेना के साथ अनुबंध द्वारा वित्तपोषित करते हुए अपने स्वयं के रेडियो नेटवर्क का निर्माण किया.[21] फिर भी, मार्कोनी के बेहतर लंबी दूरी के रेडियो और पहले-प्रस्तावक लाभ ने उनकी अंग्रेज़ समर्थित कंपनी को वैश्विक मानक के रूप में स्थापित किया और मार्कोनी ने गैर-मार्कोनी रेडियो ऑपरेटरों के साथ "गैर-अंतर-संचार" की नीति को आगे बढ़ाने के लिए इन नेटवर्क प्रभावों का लाभ उठाया. जर्मन व्यवसायी और ओशियल लाइनर वैश्विक संचार से कटना नहीं चाहते थे, इसलिए उन्होंने जर्मन की बजाय अंग्रेज़-समर्थन वाले सिस्टम को प्राथमिकता दी.

काइज़र विलहेम द्वितीय ने अंग्रेज़ों के मानक से प्रतिस्पर्धा करने के लिए जर्मन औद्योगिक नीति को तीव्र कर दिया. उन्होंने तेजी से यह फ़ैसला किया कि प्रतिस्पर्धी रेडियो कोशिशों के साथ दो बड़ी जर्मन इलेक्ट्रिकल कंपनियां, सीमेंस एंड हाल्स्के और एईजी, एक साथ मिलकर निश्चित जर्मन विकल्प, टेलीफ़ुनकेन की स्थापना करें. काइज़र समझाते हैं कि "वायरलेस टेलीग्राफ़ी के क्षेत्र में [घरेलू] शत्रुता ने जर्मनी का प्रतिस्पर्धात्मकता को कमज़ोर कर दिया" "और मार्कोनी कंपनी को दुनियाभर में आधिपत्य पाने का अवसर दिया" जो "जर्मनी के हित में नहीं" था.[22] काइज़र विलहेम द्वितीय के अधीन, जर्मनी ने कुछ मामलों में मार्कोनी सिस्टम पर प्रतिबंध लगाकर संरक्षणवाद का अनुसरण किया. उसने दक्षिण अमेरिका और अफ़्रीका में अपनी प्रौद्योगिकी बेचकर उन क्षेत्रों में मानक तय करने और आय सुरक्षित करने के लिए उभरते बाज़ारों का अनुसरण किया.

जब वे कोशिशें नाकाफ़ी साबित हो गईं, तो जर्मनी ने बहुपक्षीय मानक-सेटिंग निकायों में कामयाबी हासिल की. 1906 में, जर्मनी ने रेडियो मानकों के सम्मेलन, पहले अंतरराष्ट्रीय रेडियोटेलीग्राफ़ कन्वेन्शन के आयोजन में महाशक्तियों को साथ लाया. वहां, सदस्यों ने संयुक्त

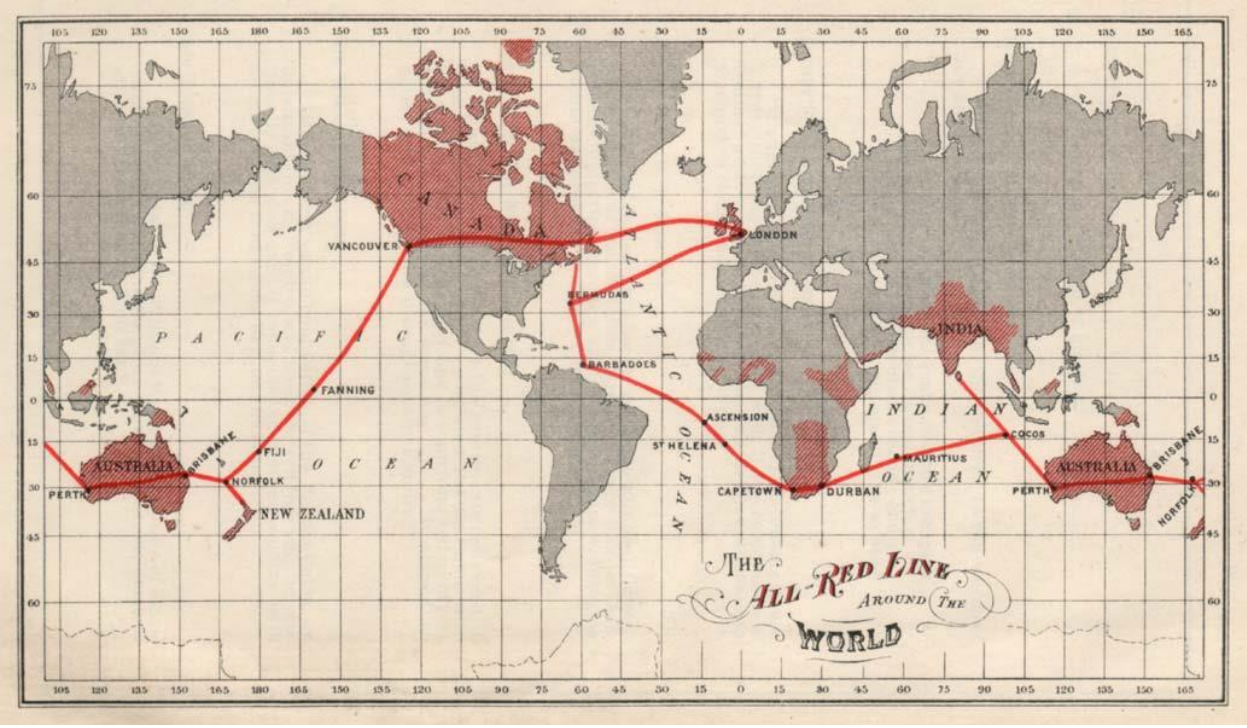
रूप से मार्कोनी की "गैर-अंतर-संचार" नीति को प्रतिबंधित कर दिया, जिससे अंग्रेज़ों का आधिपत्य खंडित हो गया और एक प्रभावी एंग्लो-जर्मन द्वयाधिकार स्थापित हुआ.[23]

एंग्लो-जर्मन प्रतिस्पर्धा से यह खुलासा हुआ कि मानक-सेटिंग निकायों के भारी रणनीतिक प्रभाव हैं. चीन आज ऐसी कई प्रौद्योगोकियों का इस्तेमाल कर रहा है जिन्हें जर्मनी ने एक सदी पहले इस्तेमाल किया था – सरकारी नेतृत्व वाली औद्योगिक नीति, सरकारी-सुरक्षा, उदार सरकारी अनुबंध, नागरिक-सैन्य एकीकरण, प्रतिद्वंद्वी उत्पादों पर प्रतिबंध, मजबूरी में होने वाले विलय, उभरते बाज़ारों की खोज और यहां तक कि इसके मानक तय करने के लिए अंतरराष्ट्रीय संधियां भी – इन सभी ने वीचेट और अलीपे की मालिक अलीबाबा और टेंसेंट जैसी चीनी प्रौद्योगिकी कंपनियों को स्थानीय चैंपियन बनने में मदद की है. तब से, इन कंपनियों ने विदेशों में विस्तार किया है, जिनका लक्ष्य अक्सर अमेरिकी बाज़ार तो नहीं होते हैं – लेकिन जर्मनी के टेलीफ़ुनकेन जैसी कंपनियां होती हैं– जहां उनके लिए कम मुनाफ़े और प्रतिस्पर्धा वाले उभरते बाज़ार हैं.[24]

चीन भी इंटरनेट कनेक्टिविटी के कठिन बुनियादी ढांचे में मानकों से प्रतिस्पर्धा कर रहा है. वहां की सरकार अरबों का निवेश कर रही हैं ताकि चीनी चिपमेकर्स 5G मोबाइल इंटरनेट मानकों की दौड़ में अमेरिकी प्रतिद्वंद्विता को हरा सकें. इसी तरह से, हुआवे और ज़ेडटीई जैसी चीनी फ़र्मों को पूरे विकासशील विश्व में इंटरनेट कनेक्टिविटी के कठोर बुनियादी ढांचे का निर्माण करने के लिए सरकारी लोन मिलते हैं. जैसा कि अंग्रेज़ों का उदाहरण दर्शाता है, ये कोशिशें न सिर्फ़ चीनी प्रौद्योगिकी को मानक बनाती हैं, बल्कि वे निगरानी करने के अवसर भी उपलब्ध कराती हैं. इस बीच, बेल्ट एंड रोड इनीशिएटिव इस बात की संभावना को बल देती है कि पूरे एशिया में "समझदार बुनियादी ढांचे" के मानक, खास तौर पर प्रासंगिक सेंसर और सॉफ़्टवेयर, चीन द्वारा तय किए जा सकते हैं और दूसरी कंपनियों की इंटरऑपरेबिलिटी को नकार सकते हैं, जिससे वे स्वचालित वाहन और अन्य उद्योगों से बाहर हो जाएंगी.

टेलीग्राफ़ी में एंग्लो-जर्मन प्रतिद्वंद्विता से पता चलता है कि वाशिंगटन को मानकों में चीन की सरकार-निर्देशित चुनौती को गंभीरता से लेना होगा. इससे आगे का रास्ता भी मिलता है. जिस तरह जर्मनी ने टेलीग्राफ़ी पर अंग्रेज़ एकाधिकार में सेंध लगाने के लिए अंतरराष्ट्रीय कांफ़्रेंस का सहारा लिया था, लगभग उसी तरह से संयुक्त राज्य अमेरिका भी बहुपक्षीय समझौतों के माध्यम से अनुकूल आईसीटी मानक तय कर सकता है या उनका संरक्षण कर सकता है. ऐसा करने से चीन को उसके मुक्त व्यापार समझौतों, देश की चैंपियन कंपनियों या बुनियादी ढांचे वाली परियोजनाओं के माध्यम से एकतरफा मानक-सेटिंग करने से रोका जा सकता है.

3. प्रथम विश्व युद्ध में ब्रिटेन: सूचना आधिपत्य की तैनाती करना



"ऑल रेड लाइन," समुद्रतल में बिछी अंग्रेज़ों की केबल लाइनों का एक महंगा नेटवर्क जिसे भारी अतिरेक के साथ बनाया गया और इस तरह व्यवस्था की गई कि उसका कोई भी हिस्सा किसी प्रतिद्वंद्वी के क्षेत्र से न गुज़रे. जर्मनी द्वारा अपने ही लचीले वैश्विक दूरसंचार में अपर्याप्त निवेश के चलते ब्रिटेन ने उसे वैश्विक संचारों से अलग कर दिया जबकि ब्रिटेन पर आम तौर पर कोई असर नहीं पड़ा.

स्रोत: जॉर्ज जॉनसन, *ed.,* दि ऑल रेड लाइन: दि एनल्स एंड एम्स ऑफ़ दि पैसिफ़िक केबल प्रोजेक्ट / इंटरनेट आकाईव[25]

20वीं सदी की शुरुआत में दूरसंचार के क्षेत्र में अंग्रेज़ प्रभुत्व में सेंध लगाने की जर्मनी की कोशिशों का जन्म मानसिक उन्माद की वजह से नहीं हुआ था. प्रथम विश्व युद्ध के शुरू होते ही, ब्रिटेन ने युद्ध के तरीके को आकार देने के लिए दूरसंचार नेटवर्कों में कामयाबी से अपना महत्वपूर्ण प्रभाव डाला. उसने जर्मन केबलों को काट दिया, जर्मन ट्रांसमिशनों की निगरानी की और जर्मन ट्रैफ़िक को अंग्रेज़-नियंत्रण वाले नेटवर्कों से गुज़रने पर मजबूर कर दिया – जिसके चलते ज़िमरमैन टेलीग्राम का खुलासा हुआ, जिसकी मदद से अमेरिका उस युद्ध में उतर सका.[26]

ग्रेट ब्रिटेन वह पहली महाशक्ति नहीं थी जिसने दूरसंचार नेटवर्कों को काटा या उनमें हेर-फेर किया था: पेरू ने एक चिली-बोलीविया लिंक को काटा था, संयुक्त राज्य अमेरिका ने स्पेनिश केबलों को काटा था और ब्रिटेन ने एक संकट के समय बोएर्स को उनके यूरोपीय समर्थकों से काट दिया था और दूसरे संकट में फ़्रांस को जाने वाले ट्रैफ़िक में हेर-फेर किया था.[27] लेकिन प्रथम विश्व युद्ध में इन कोशिशों को चरम पर ले जाया गया.

ग्रेट ब्रिटेन किसी पूरे देश को मुख्य धारा के वैश्विक दूरसंचार नेटवर्कों से काटने वाला पहला देश था, जिसने शांतिकाल में सावधानीपूर्वक योजना बनाकर पहले ही दिन इसे नियोजित कर दिया था.[28] एक ही साल के अंदर, ग्रेट ब्रिटेन ने दुनियाभर की जर्मन केबलों को नष्ट कर दिया: इंग्लिश चैनल, नॉर्थ सी, नॉर्थ अटलांटिक, साउथ अमेरिका, ज़्यादातर अफ़्रीका, सुदूर पूर्व, और यहां तक कि जर्मनी के बुनियादी ढांचे को होस्ट करने वाले तटस्थ देशों में भी.[29]

इसकी भरपाई करने के लिए, जर्मनी ने रेडियो नेटवर्क का विस्तार करने की कोशिश की जिसे टेलीफ़ुनकेन ने एक दशक पहले लैटिन अमेरिका में बनाया था और "ग्लोबल साउथ" ताकि वह पूरी दुनिया को कवर कर लेगी. चीन की डिजिटल सिल्क रोड की आधुनिक समानता की कोशिशों में, बर्लिन ने "रेडियो के विकास संबंधी लाभों" में रुचि रखने वाली सरकारों को ऋण और निवेश की पेशकश की, ताकि वे जर्मन संचार नोडों की मेजबानी करेंगे. इसके जवाब में, ग्रेट ब्रिटेन ने जर्मन रेडियो नोड्स के लिए समर्थन छोड़ने या उसमें सक्रिय रूप से तोड़फोड़ करने के लिए इनमें से अधिकांश देशों को राजी या प्रेरित किया.[30]

अपने ही नेटवर्कों से वंचित होकर, बर्लिन के पास युद्ध के दौरान ब्रिटेन के नेटवर्क पर भरोसा करने के अलावा कोई चारा नहीं था. शुरुआत में, अंग्रेज़ों ने अपने केबलों से गुजरने वाले सभी ट्रैफ़िक की चुपचाप निगरानी करने लगे और जर्मनी के खिलाफ़ सूचना युद्ध छेड़ने के लिए इस फ़ायदे का इस्तेमाल किया, इसमें उसने जर्मन ट्रैफ़िक को शर्मनाक तरीके से लीक करते हुए तटस्थ देशों के साथ उसके संबंधों को नुकसान पहुंचाया. जब जर्मनी ने अमेरिका के खिलाफ मेक्सिको के साथ सैन्य गठबंधन का प्रस्ताव देते हुए एक टेलीग्राम – अप्रसिद्ध ज़िमरमैन टेलीग्राम – भेजा, तो वह मैसेज एक अंग्रेज़ नेटवर्क से होकर गुज़रा और तो ग्रेट ब्रिटेन ने उसे इंटरसेप्ट करके डिक्रिप्ट कर लिया और उसे संयुक्त राज्य अमेरिका की सरकार के साथ साझा कर दिया, जिसने इसके बाद उसे अमेरिकी जनता से साझा कर लिया.[31] उस घटना ने संयुक्त राज्य अमेरिका को युद्ध में उतरने, विश्व के इतिहास को आकार देने और आखिर में जर्मनी की हार को अमली जामा पहनाने में मदद की.

जर्मनी के खिलाफ अंग्रेज़ सूचना युद्ध एक प्रतिद्वंद्वी शक्ति को प्रदर्शित करने के खतरों का खुलासा करता है जो किसी के ट्रैफ़िक की निगरानी करने या किसी की दूरसंचार पहुंच को बंद करने की क्षमता रखता है. इससे यह भी पता चलता है कि शांतिकाल में जो महाशक्तियों नेटवर्कों को हल्के में लेती हैं उन्हें अक्सर युद्ध के समय में नकार दिया जाता है, और यह कि संचार नोडों के संघर्ष में अनिवार्य रूप से तीसरे पक्ष और तटस्थ देश शामिल होंगे.

4. टैनेनबर्ग में जर्मनी की जीत: इंटरसेप्शन के खतरे

पहले विश्व युद्ध के दौरान एक जर्मन वायरलेस फ़ील्ड टेलीग्राफ़ स्टेशन. अपने क्षेत्र के स्टेशनों पर अपने संचार को पर्याप्त रूप से एन्क्रिप्ट करने में रूस की अक्षमता एक विनाशकारी हार की वजह बनी जिसने युद्ध का तरीका ही बदलकर रख दिया.

स्रोत: सी. ओ. नॉर्डनस्वान एंड वाल्देमार लैंग्लेट, Det stora världskriget *[दि ग्रेट वर्ल्ड वॉर]*[32]

सूचना युद्ध में जर्मनी पूरी तरह से अपनी क्षमताओं के बिना नहीं था. उसने रूसी ओवरलैंड और समुद्रतल में बिछी केबलें काट दीं जो उसे अपने पश्चिमी सहयोगियों से जोड़ती थीं, साथ ही कई ट्रांसअटलांटिक केबलें भी जिन पर अंग्रेज़ों ने भरोसा किया था। उसने इन कामों के लिए पनडुब्बियों का इस्तेमाल करने में महारत हासिल कर ली थी.[33] अंग्रेज़ों के नेटवर्कों के अतिरेक को देखते हुए, ये कोशिशें आखिर में जर्मन लोगों की उम्मीद से कमतर ही साबित हुईं. जो चीज़ कहीं ज़्यादा परिणामी साबित हुई वह अगस्त 1914 में टैनेनबर्ग की लड़ाई के दौरान रूस के खिलाफ़ जर्मनी की रेडियो इंटेलिजेंस का जर्मनी द्वारा इस्तेमाल करना रही, जो युद्ध के पहले ही महीने में रूसियों के लिए विनाशकारी रही. उस समय के एक जर्मन इंटेलिजेंस ऑफ़िसर ने इस घटना को "मानव इतिहास में पहली घटना, जिसमें दुश्मन के रेडियो ट्रैफ़िक के इंटरसेप्शन ने निर्णायक भूमिका निभाई" बताया.[34]

यह लड़ाई पूर्वी मोर्चे पर रूसी फ़ायदे के बीच हुई. जब रूस इस्ट प्रूशिया में और आगे बढ़ा, तो उसकी सेना के सामने एक महत्वपूर्ण संचार चुनौती खड़ी हो गई जिसने एक विनाशकारी हार का

मंच तैयार कर दिया. पीछे हटने वाले जर्मनों ने अपनी ही टेलीग्राफ़ लाइनों को काट दिया और आगे बढ़ते रूसियों के पास अपनी विशाल बनावट में वायर्ड संचार स्थापित करने के लिए पर्याप्त प्रशिक्षित कर्मियों की कमी थी. रेडियो ट्रांसमिशन ने एक विकल्प उपलब्ध कराया, लेकिन जहां रूसियों ने अपनी सैन्य कमांड और कंट्रोल के लिए नई रेडियो प्रौद्योगिकियां अपनाईं, वहीं उन्होंने उनकी उचित रूप से सुरक्षा नहीं की. अलग-अलग समूहों को अलग-अलग साइफर सौंपे गए; ज़्यादातर के पास संकेतों को एन्कोड या डीकोड करने का बहुत कम प्रशिक्षण था; ऐसा कहा जाता है कि कुछ कोड अंग्रेज़ों द्वारा तोड़े गए थे; और अनपढ़ सनातनियों में से कईयों के लिए कोडबुक्स सीमित या अनजान थीं.[35] नतीजा यह हुआ कि रूसी कमांडरों को लगा कि उन्हें कोड नहीं किए गए रेडियो संदेशों के इस्तेमाल का जोखिम उठाना होगा और उम्मीद करनी होगी जर्मन सावधानी से उनकी निगरानी नहीं कर रहे हों.

हालांकि, जर्मन इन संकेतों की करीब से निगरानी कर रहे थे. जापानियों के खिलाफ़ युद्ध में रूसी रेडियो की अनुशासन में कमी पर नज़र रखने के बाद, वे जानते थे कि रूसी अनकोडेड ट्रांसमिशन किसी धोखे वाले अभियान का हिस्सा नहीं थे. इसके बाद उन्होंने "युद्ध का कोहरे" को हटाने के लिए वास्तविक समय के रूसी संचार के अपने ज्ञान का इस्तेमाल किया और बेहतर सैन्य बल को निर्णायक रूप से मात दे दी. रूस ने एक पूरी सेना गवां दी, जिसमें 100,000 से ज़्यादा हताहत हुए 92,000 को बंदी बना लिया गया जबकि इसकी तुलना में जर्मनी के सिर्फ़ 13,000 सैनिक हताहत हुए थे.

5. दूसरे विश्व युद्ध में ब्रिटेन: एन्क्रिप्शन की सीमाएं

दूसरे विश्व युद्ध के दौरान लोरेंज़ एनसाइफरिंग मशीन के मैकेनिकल रोटर्स को प्रभावी रूप से अटूट माना जाता था. साइफर में सेंध लगाने की अंग्रेज़ों की कोशिशों ने अधिकारियों को उच्च-स्तरीय संचार की पहुंच उपलब्ध करा दी.

स्रोत: मैट क्रिप्टो / वीकिपीडिया कॉमन्स[36]

वायरलेस टेलीग्राफ़ी और रेडियो के आविष्कारों ने भौतिक केबलों के सापेक्ष अधिक सुविधा ला दी थी, लेकिन इंटरसेप्शन का बहुत बड़ा जोखिम था. पहले और दूसरे विश्व युद्ध में, महाशक्तियां एक ऐसी दुनिया में मौजूद थीं जहां रेडियो संचार दूसरों के लिए पहुंच-योग्य माने जाते थे. और एक ऐसी दुनिया में एन्क्रिप्शन को सुरक्षा के लिए महत्वपूर्ण माना जाता था जो – आधुनिक कंप्यूटर और दूरसंचार प्रणालियों की कमज़ोरी से जुड़ी मान्यताओं से उतना अलग नहीं – थी. इसका नतीजा, जैसा कि हमारे एक अमेरिकी सैन्य इतिहासकार बताते हैं, एक "क्रिप्टोग्राफर और क्रिप्टाएनालिस्ट के बीच का संघर्ष" था.[37] जब महाशक्तियां उस संघर्ष के गलत पक्ष पर थीं, तो नतीजे भयावह हो सकते थे.

इस तरह के परिणाम को रोकने के लिए, संगठन उस जोखिम को कम करने के लिए साइफरों का इस्तेमाल करते कि इंटरसेप्शन की वजह से सुरक्षा से छेड़छाड़ की जा सकती है. उन्होंने रेडियो ट्रैफ़िक विश्लेषण के माध्यम से इस्तेमाल के पैटर्न के बारे में जानकारियों को रोकने के लिए "रेडियो अनुशासन" का भी इस्तेमाल किया.

ज़्यादातर महाशक्तियों ने विरोधी ट्रैफ़िक का अध्ययन करने और अगर संभव हो, तो विरोधी साइफरों में सेंध लगाने के लिए, वास्तव में औद्योगिक कोशिश में निवेश किया. जर्मनी के मुकाबले ग्रेट ब्रिटेन विरोधी साइफरों के अपने विश्लेषण में कहीं ज़्यादा केंद्रीयकृत था, जिसने उन कार्यों को कई एजेंसियो के बीच बांट रखा था. और जिस तरह संकेतों और गोपनीय जानकारी में अंग्रेज़ों की कामयाबी ने प्रथम विश्व युद्ध के तरीके को आकार दिया था, उसी तरह उन्होंने दूसरे विश्व युद्ध के तरीके को भी आकार दिया जब ब्लेचली पार्क में अंग्रेज़ ऑपरेशन से जर्मनी के एनिग्मा और लॉरेंज साइफर्स को तोड़ा.

एनिग्मा और लॉरेंज़ साइफर्स सिस्टमों ने असाधारण रूप से जटिल रोटर मशीनों का इस्तेमाल उन संदेशों को एन्क्रिप्ट करने के लिए किया जिन्हें जर्मनी "अजेय बने रहेंगे" मानता था.[38] मशीन की खास सेटिंग के आधार पर हर कीस्ट्रोक एक वर्ण को किसी दूसरे वर्ण से बदल देगा, और वे सेटिंग – जो, लॉरेंज़ सिस्टम के लिए, ब्रह्मांड में परमाणुओं की कुल संख्या से अधिक हो गई थीं – संदेश को पढ़ने के लिए प्रेषक और प्राप्तकर्ता द्वारा साझा करना ज़रूरी था.[39] एनिग्मा का इस्तेमाल सेना द्वारा किया जाता था, गेस्तापो और राजनयिक; लॉरेंज, जो और भी ज़्यादा जटिल था, एडोल्फ़ हिटलर और वरिष्ठ नाज़ी अधिकारियों द्वारा एक-दूसरे से बातचीत करने के लिए इस्तेमाल किया जाता था.

एनिग्मा और लॉरेंज़ को तोड़ लेने की अंग्रेज़ों की कामयाबी कई विकासों का नतीजा थी. सबसे पहले, यह पोलैंड के साथ सहयोगी खूफ़िया सहयोग का नतीजा थी, जिसने ज़्यादा आसान एनिग्मा मशीनों में सेंध लगाने के लिए जर्मनी की कुछ गलतियों का दोहन किया.[40] जैसा कि अपने समय के एक अंग्रेज़ क्रिप्टाएनालिस्ट ने बताया, कि पोलिश योगदानों के बिना उनकी कोशिश "कभी भी कामयाब नहीं हो पाती".[41]

दूसरा यह जर्मनी के अति-आत्मविश्वास का नतीजा था, जब जर्मनी को कभी संदेह नहीं हुआ कि साइफर में सेंध लग चुकी है और इसलिए काफी आसान संशोधन किए जा रहे हैं जिनसे ब्रिटेन को शुरुआत से शुरू करने के लिए मजबूर होना पड़ेगा.[42] इतना ही नहीं, ब्लेचली पार्क के एक

वरिष्ठ अधिकारी कहते हैं कि अपनी मशीनों की कमज़ोरी में जर्मनी का भरोसा "लगभग सही था".[43]

आखिर में, यह जर्मन "रेडियो अनुशासन" की एक ही लेकिन बड़ी चूक का नतीजा था जिसने जर्मन साइफरिंग सिस्टम को रिवर्स इंजीनियर करने का रास्ता खोल दिया, बावजूद इसके कि उसे किसी ने व्यक्तिगत रूप से नहीं देखा था.[44] यहां तक कि सबसे परिष्कृत सिस्टम भी उपयोगकर्ता त्रुटि के लिए कमज़ोर थे और एक चौकस विरोधी इसका दोहन कर सकता था.

एनिग्मा और लॉरेंज में सेंध लगाकर, ग्रेट ब्रिटेन को जर्मनी के कुछ सबसे संवेदनशील संचारों की पहुंच हासिल हो गई. विंस्टन चर्चिल ने कथित रूप से एक खूफ़िया जानकारी को श्रेय दिया जो युद्ध में ग्रेट ब्रिटेन की जीत की एक प्रमुख वजह बना, और ड्वाइट डी. आइज़नहॉवर ने इसे कथित रूप से "निर्णायक" करार दिया.[45] ब्रिटिश खूफ़िया विभाग के आधिकारिक इतिहासकार सर फ़्रांसिस हैरी हिन्स्ली का तर्क है कि इन कामयाबियों ने "युद्ध को दो साल से लेकर शायद चार साल तक कम कर दिया," जिससे अफ़्रीका में फ़ील्ड मार्शल इरविन रोमेल कमज़ोर हो गए और जर्मन यू बोट्स को होने वाला संबद्ध शिपिंग नुकसान काफ़ी तेज़ी से पलटा और जिससे नॉर्मैंडी लैंडिंग सक्षम हो गईं.[46] उन्होंने ब्रिटेन को देश में प्रवेश करने वाले लगभग सभी जर्मन जासूसों की पहचान करने में भी समर्थ बनाया और अक्सर उन्हें बारी-बारी से वापस लाने या उनका इस्तेमाल करने के लिए दोषपूर्ण खूफ़िया जानकारी देने के लिए कहा, इस कार्यक्रम के प्रमुख ने उल्लेख किया कि ब्रिटिश खूफ़िया विभाग ने "इस देश में जर्मन जासूसी प्रणाली को सक्रिय रूप से चलाया और नियंत्रित किया."[47] कुछ देशों को युद्ध के दौरान कभी भी दूसरे की इतनी अंतरंग जानकारी नहीं होती है.

साथ मिलाकर, जर्मनी के खिलाफ़ ब्रिटेन की कोशिशों की कामयाबी, जर्मन संचार के लिए पोलैंड की शांतिकालीन निगरानी और ग्रेट ब्रिटेन के साथ अपनी कामयाबी को साझा करने का उसका फ़ैसला, आज के सबक हैं, जब महाशक्तियां एक दूसरे के खिलाफ़ साइबर-टोही आचरण करती हैं. मोटे तौर पर, जो लोग सुझाव देते हैं कि एन्क्रिप्शन किसी के दूरसंचार नेटवर्क तक एक विरोधी की पहुंच की समस्याओं को कम करता है, वे शायद गलती कर रहे हैं जो उस गलती से ज़्यादा अलग नहीं है जो जर्मनी ने खुद एक बार की थी: प्रौद्योगिकी में बहुत ज़्यादा भरोसा और इंसानी गलती की हमेशा से मौजूद संभावना पर सीमित रूप से ध्यान देना.

6. ऑपरेशन आइवी बेल्स: सूचना की गहराईयों की खोज

यूएसएस हैलिबट, जिसके बारे में कहा गया था कि वह समुद्रतल में बिछी एक टेलीफ़ोन लाइन को टैप करने की कोशिश में शामिल था.

स्रोत: यू.एस. नेवी / वीकिमीडिया कॉमन्स[48]

सोवियत संघ अपने एन्क्रिप्शन को लेकर नाज़ियों से कहीं ज़्यादा सतर्क था और उसने एनिग्मा के अपने ही पर भरोसा किया – जिसका नाम फ़ियाल्का था – जो महत्वपूर्ण रूप से ज़्यादा जटिल था.[49] इसी वजह से, इस कारण से, जर्मन साइफर में सेंध लगने के बाद दूसरे विश्व युद्ध में निर्मित सामरिक स्तर की खुफिया जानकारी के विशाल टुकड़ियों का शीत युद्ध में कोई सार्वजनिक रूप से ज्ञात एनालॉग नहीं था. इन्हीं चुनौतियों को देखते हुए, विरोधी दूरसंचारों में घुसपैठ करने के अन्य तरीकों में महारत हासिल की गई. इन कोशिशों में से सबसे ज़्यादा साहसी कोशिश समुद्रतल में बिछी केबलों के संबंध में की गई.

19 वीं सदी में समुद्रतल में बिछी केबलों की शुरुआत आखिर में उन्हें काटने और समय-समय पर उन्हें टैप करने की कोशिशों तक आ गई, अक्सर उथले पानी में या ज़मीन पर जहां ऐसे कार्यों का संचालन आसान था. इसके विपरीत, किसी विरोधी द्वारा नियंत्रित गहरे पानी में इन कार्यों को निष्पादित करना लगभग असंभव माना जाता था, खासकर अगर यह गुप्त रूप से

किया जाना था. 20वीं सदी की शुरुआत में, अंग्रेज़ और उस समय की कामयाब महाशक्तियां समुद्रतल में बिछी केबल की सुरक्षा को लेकर दृढ संकल्प हो गई थीं: अगर लैंडिंग साइटें सुरक्षित कर ली जातीं और केबलें तटस्थ या दुश्मन देशों से होकर नहीं गुज़रतीं, तो वे आम तौर पर इंटरसेप्शन से सुरक्षित रहेंगी और अक्सर कटने से सुरक्षित रहेंगी, खास तौर पर शांतिकाल में.[50]

हालांकि, शीत युद्ध के दौरान, वह गणना बदल गई. परमाणु पनडुब्बियों के आगमन ने गहरे पानी में समुद्रतल में बिछी केबलों को टैप करने की संभावना खोल दी. लेकिन गहरे समुद्रतल में केबल तक पहुंचने के लिए गोताखोरों को भेजने का काम पिछले युगों में किए गए केबल हेरफेर की चिर-परिचित कोशिशों को अंतरिक्ष अन्वेषण के मुकाबले ज़्यादा महत्वपूर्ण माना जाता था. ऐसे हालातों में इंस्टॉल किए जा सकने वाले किसी टैप का निर्माण करना भी तकनीकी रूप से चुनौती भरा था.

जब संयुक्त राज्य अमेरिका को संदेह हुआ कि समुद्रतल में बिछी एक सोवियत केबल व्लादिवोस्तोक स्थित नौसेना मुख्यालय से कामचतका प्रायद्वीप पर मौजूद एक पनडुब्बी तक जा सकती है, तो उसने सिग्नल की बुद्धिमत्ता की अहमियत का प्रदर्शन करते हुए इन बाधाओं को दूर करने की कोशिश की.[51] पांच इंच वाली वायरों के उस बंडल को टैप करके, यह माना गया कि इससे सोवियत परमाणु बलों की महत्वपूर्ण जानकारी मिलेगी.[52] जहां सोवियत संघ ने हवा के माध्यम से भेजे गए सभी ट्रैफ़िक को एन्क्रिप्ट किया था, संयुक्त राज्य अमेरिका को उम्मीद थी कि सोवियत यह मानेंगे कि समुद्रतल में बिछी सुरक्षित केबल के माध्यम से जाने वाले ट्रैफ़िक को एक्सेस करना लगभग असंभव है, और इसलिए वे उसे एन्क्रिप्ट नहीं करेंगे. इतना ही नहीं, “सोवियत एडमिरल और जनरलों के लिए ऐसे क्रिप्टोग्राफ़रों का सामना करना बहुत ज़्यादा असंगत और अधीर होगा, जो पहले से ही अपने काम की भारी मात्रा से अभिभूत हैं और वे असुरक्षित वॉइस कम्यूनिकेशन पर ज़ोर देंगे.[53] ऐसे में टैप की मदद से दुर्लभ खूफ़िया जानकारी का खजाना हाथ लग जाएगा और अमेरिकी नौसेना ने इसे स्थापित करने के लिए ऑपरेशन आइवी बेल्स लॉन्च कर दिया.

उस टैप और उससे इकट्ठा की गई ज़्यादातर खूफ़िया जानकारी गोपनीय ही रही, लेकिन खुले स्रोतों से इस अद्वितीय और अभिनव ऑपरेशन के बारे में कुछ विवरण मिलता है. संयुक्त राज्य अमेरिका ने सोवियत नौसेना के पास से होकर चुपचाप निकलने और 600,000 वर्ग मील के क्षेत्र में पानी के नीछे बिछी केबल का पता लगाने के लिए एक परमाणु पनडुब्बी, यूएसएस हैलिबट को भेज दिया.[54] यह सुनिश्चित करने के लिए अभिनव प्रौद्योगिकी का निर्माण किया

गया था कि गोताखोर अत्यधिक दबाव में और अत्यंत ठंडे तापमानों में कई-कई घंटों तक काम कर सकें. इसी तरह से, इस चुनौती भरे परिवेश में एक टैप इंस्टॉल करने के नए तरीके तैयार किए गए.[55] यह सब कुछ सोवियत पहचान या संदेह के बिना किया जाना था. अगर जहाज का पता लगा लिया जाता, तो सोवियत शायद उस पर सवार हो जाते या उसे नष्ट कर देते.

ऑपरेशन आखिरकार कामयाब रहा और 1970 के दशक में, अमेरिकी नौसेना ने केबल से गुज़रने वाले असुरक्षित संदेशों को टैप और रिकॉर्ड किया. हर कुछ महीनों में, अमेरिकी पनडुब्बियां सोवियत जल में चली जातीं, हमलावर पनडुब्बियों से बचतीं, टैप की हुई केबल लाइनों में गोताखोर लगातीं और सोवियत संचार के टेप हासिल कर लेतीं – जिससे खूफ़िया जानकारी का बहुत ही कीमती और दुर्लभ हिस्सा हासिल हो जाता था. जहां संयुक्त राज्य अमेरिका ने सिग्नल से खूफ़िया जानकारी इकट्ठा करने के लिए "जासूसी उपग्रहों, विमानों, सुनने के स्टेशनों और उप-नेटवर्कों" का विस्तार कर लिया था, लेकिन वह विरोधी के क्षेत्र में “किसी हार्डवायर्ड फ़ोन लाइन तक नहीं पहुंच सका था”. इस कोशिश ने दूरसंचार में विकासवादी बदलाव को चित्रित किया है, खासकर यह कि किसी भी तरह से और किसी भी तरीके से ट्रांसमिट किए गए डेटा और सिग्नल किसी दृढ़ संकल्प किरदार द्वारा सही टूल के ज़रिए एक्सेस किए जा सकते हैं. हालांकि इस टैप के लिए अंततः एक लीक से छेड़छाड़ की गई थी, लेकिन इसके परिणामस्वरूप मिले दूरसंचार ने संयुक्त राज्य अमेरिका और उसके सहयोगियों को अमूल्य सैन्य और राजनीतिक खूफ़िया जानकारी दे दी.[56]

ऐतिहासिक परिप्रेक्ष्य में आधुनिक दूरसंचार प्रतिस्पर्धा

शीत युद्ध खत्म होने तक, संयुक्त राज्य अमेरिका ने स्पष्ट रूप से सूचना अधिपति के रूप में ग्रेट ब्रिटेन की जगह ले ली थी. संयुक्त राज्य अमेरिका ने वैश्विक इंटरनेट, मज़बूत अंतरिक्ष क्षमताओं, अधिकांश इंटरनेट प्रौद्योगिकी, और – सार्वजनिक प्रकटीकरणों के अनुसार – विरोधी संचारों को इंटरसेप्ट या संभावित रूप से अस्वीकार करने की परिष्कृत क्षमताओं के प्रभुत्व में एक नोडल स्थिति बना ली.

इन अमेरिकी लाभों का अब परीक्षण हो रहा है, जैसा कि एक सदी पहले ग्रेट ब्रिटेन का हुआ था. रूस, और खास तौर पर चीन, अब अमेरिकी प्रभुत्व को चुनौती दे रहा है. जहां संयुक्त राज्य अमेरिका को कई डेटा प्रवाहों में एक नोडल स्थिति हासिल है, वहीं दूसरी शक्तियां अमेरिकी नेटवर्क पर अपनी निर्भरता लगातार कम करने की कोशिश कर रही हैं. उसी समय, एक सदी पहले के ग्रेट ब्रिटेन के मुकाबले आज अमेरिका की नोडल स्थिति की आवश्यकता कम रह गई है. इंटरनेट भौतिक बुनियादी ढांचे पर नियंत्रण के बिना भी घुसपैठ को संभव बना देता है. स्मार्टफ़ोन और कंप्यूटर नेटवर्कों को हैक किया जा सकता है, और चाहे पहले के किसी युग में भौतिक टैप द्वारा किसी के संवेदनशील संचारों से छेड़छाड़ करना हो या आधुनिक युग में आभासी घुसपैठ द्वारा, अंतिम परिणाम समान ही है. इस तरह से कनेक्शन की संभावना टेलीग्राफ़ या वायरलेस रेडियो के युग की तुलना में अब ज़्यादा कमज़ोरी उत्पन्न करती है.

उस कमज़ोरी का दोहन करने में रूस एक अग्रणी देश रहा है. 2007 में, रूस ने एस्टोनियाई संस्थानों के खिलाफ़ साइबर हमलों का सिलसिला शुरू कर दिया था, जिसमें ज़्यादातर सेवा से वंचित करने के हमले थे.[57] 2008 में, उसने रूसो-जॉर्जियन युद्ध में साइबर हमले लॉन्च किए थे. इनमें न सिर्फ़ सेवा से वंचित करने के हमले शामिल थी, लेकिन सरकारी वेबसाइटों को रीडायरेक्ट करने की कोशिशें, जॉर्जियन सरकारी सर्वरों पर कब्ज़ा करना और जॉर्जियन इंटरनेट ट्रैफ़िक को रूसी-नियंत्रण वाले सर्वरों से री-रूट करना भी शामिल था – इनमें से कुछ हमले रूसी सैनिक कार्रवाई के संयोग के साथ टकराव से पहले ही तैयार कर लिए गए थे.[58] 2014 में, जब रूस ने क्रीमिया पर हमला किया, तो उसने साइबर हमलों को दूरसंचार नेटवर्कों पर भौतिक नियंत्रण के साथ संयोजित कर दिया था. रूसी सैनिकों ने यूक्रेनियाई दूरसंचार सुविधाओं पर कब्ज़ा कर लिया, उनका इस्तेमाल क्रीमिया में संचार को काटने के लिए और यहां तक कि यूक्रेन के दूसरे हिस्सों में साइबर हमले और अवरोध पैदा करने के लिए भी किया.[59] 2015 में, रूस ने यूक्रेन के बुनियादी ढांचे पर साइबर हमलों का सिलसिला शुरू कर दिया, जिसमें दो बड़ी घटनाओं

में ही यूक्रेन के सैकड़ों हज़ारों लोगों की बिजली काट दी गई. अगले कुछ सालों में, उसने पूरे यूक्रेन में अभूतपूर्व हमलों का सिलसिला शुरू कर दिया जिसमें "मीडिया, वित्त, परिवहन, सेना, राजनीति, और ऊर्जा" – आभासी रूप से युक्रेनियाई समाज का हर तबका शामिल था – कुछ लोगों ने इसे संयुक्त राज्य अमेरिका के खिलाफ़ एक मिलते-जुलते अभियान के प्रशिक्षण की आंशिक कोशिश माना.[60] इसी समय, उसने पूरे बाल्टिक में हमलों की श्रृंखला जारी रखी, साथ ही, विघटनकारी अभियानों के माध्यम से दूसरे देशों के अलावा 2016 तथा 2020 में अमेरिकी चुनावों को भी आकार देने की कोशिश की.[61] 2021 में, अमेरिकी सरकार ने औपचारिक रूप से आईटी कंपनी सोलर विंड्स को हैक करने के लिए रूस पर आरोप लगाया, जो एक ऐसा परिष्कृत हमला था जिसमें ज़्यादातर संघीय सरकार और कई बड़ी अमेरिकी कंपनियों से छेड़छाड़ की गई थी.[62]

चीन दूरसंचार प्रतिस्पर्धा में महत्वपूर्ण निवेश करने वाली दूसरी प्रमुख शक्ति है, हालांकि रूस के विपरीत, चीन की कोशिशें न सिर्फ़ मौजूदा इंटरनेट बुनियादी ढांचे का दोहन करना है, बल्कि नेटवर्क और बुनियादी ढांचे का निर्माण करना भी है ताकि वह इसे प्रभावित कर सके और यहां तक कि इसे नियंत्रित भी कर सके. रूस की तरह, चीन भी इंटरनेट की मौजूदा कमियों का दोहन करने में माहिर है. 2000 के दशक की शुरुआत में, उसने अमेरिकी रक्षा विभाग के नेटवर्कों पर सिलसिलेवार हमलों की शुरुआत कर दी जिसे विभाग ने ऑपरेशन टाइटन रेन का नाम दिया.[63] दुनिया भर की सरकारों – संयुक्त राज्य अमेरिका, यूनाइटेड किंगडम, फ़्रांस, जर्मनी, कनाडा, ऑस्ट्रेलिया, जापान, दक्षिण कोरिया, ताइवान, भारत, और दर्जन भर से भी ज़्यादा दूसरी सरकारों – ने अपने सरकारी नेटवर्कों में चीनी घुसपैठ के बारे में शिकायत की. अमेरिका के अटॉर्नी जनरल विलियम बार द्वारा पुष्टि किए गए पिछले दशक के कुछ सबसे बड़े साइबर हमलों को चीनी एजेंटों द्वारा बढ़ावा दिया गया था, जिनमें अन्य के साथ ही, अमेरिकी कार्मिक प्रबंधन कार्यालय (21 मिलियन लोगों के दस्तावेज़), मैरियट होटेल्स (400 मिलियन), एंथेम हेल्थ इंश्योरेंस (80 मिलियन), और इक्विफ़ैक्स (147 मिलियन) से दस्तावेज़ों की चोरी शामिल थी.[64]

इसी समय, चीन भविष्य के इंटरनेट बुनियादी ढांचे की नींव भी रख रहा है और उसकी पिछली कोशिशों को ध्यान में रखते हुए, यह संभावना कम ही है कि यह कोशिश अभी व्यावसायिक है या आगे की अवधि में पूरी तरह से व्यावसायिक रहेगी. चीन के निवेश 5G नेटवर्क में सबसे स्पष्ट रूप से जुड़े हुए हैं, जो कई उपकरणों और सेंसरों को एक साथ जोड़ने के लिए एक स्मार्ट, कनेक्टेड अर्थव्यवस्था की नींव बनाने की उम्मीद करते हैं. दुनिया भर में ऐसे नेटवर्क बनाने को आतुर, चीन ने अपनी 5G चैंपियन कंपनियों को और दुनिया भर में डिजिटल सिल्क रोड की पहल के रूप में दुनिया भर में चल रहे प्रोजेक्ट को सब्सिडी दी है. प्रतिस्पर्धी कीमतों के साथ,

हुआवे जैसी कंपनियां दूसरे बड़े 5G वेंडरों को प्रतिस्पर्धा से बाहर कर पाई और बाज़ार में एक महत्वपूर्ण वैश्विक हिस्सेदारी पर कब्ज़ा कर पाई, जिसने चीन को ऐसे नेटवर्क बनाने में अग्रणी बना दिया. और 5G से बाहर, चीन की सरकार ने लगभग हर महाद्वीप पर इंटरनेट या संचार के बुनियादी ढांचे के निर्माण के लिए सब्सिडी की कोशिशों को बढ़ावा दिया है. ये कोशिशें वैश्विक मानकों को आकार देने के एक अभियान की पूरक हैं, जो चीन के लिए एक प्रमुख नीतिगत प्राथमिकता के उच्च-स्तरीय नियोजन दस्तावेजों में निहित है – जैसा एक सदी पहले एंग्लो-जर्मनी विरोध में हुआ था – जो चीन को फ़ायदा पहुंचाने वाले तरीकों में दूरसंचार के भविष्य को आकार दे सकते हैं. उसे खत्म करने के लिए, चीन ने हाल ही में एक नई डेटा सुरक्षा पहल की शुरुआत की है.[65]

कुछ को डर है कि चीन की गतिविधियों से ऐसी संभावना खुल गई है कि बीजिंग का इन नेटवर्कों पर वास्तविक नियंत्रण हो जाएगा, चाहे ट्रैफ़िक इंटरसेप्ट करना हो या पहुंच देने से मना करना हो. वह नियंत्रण हासिल करने की चीन की कोशिशों के बारे में बहुत ही कम सार्वजनिक जानकारी उपलब्ध है, लेकिन अमेरिकी सरकार ने फरवरी 2020 में खुलासा किया था कि हुआवे के पास उसके नेटवर्क उपकरण में पीछे के दरवाज़े हैं, जिनके बारे में उसने उन प्रासंगिक कंपनियों को नहीं बताया है जिनके साथ उसका अनुबंध है, और यह कि पीछे के दरवाज़े कभी-कभी होस्ट सरकारों द्वारा कानूनी इंटरसेप्ट के रूप में अनुरोध किए गए से भी आगे चले गए थे.[66] इसके अलावा, सार्वजनिक रिपोर्टिंग से पता चला है कि हुआवे ने असंतुष्टों की पहचान से छेड़छाड़ करते हुए युगांडा और ज़ाम्बिया जैसी सरकारों की सहायता की है.[67] हुआवे के मामले से भी आगे, एक साइबर सुरक्षा फ़र्म ने हाल ही में उस अनिवार्य टैक्स सॉफ़्टवेयर में पीछे के दरवाज़ों का पता लगाया है जिन्हें चीनी सरकार विदेशी कंपनियों के लिए इंस्टॉल करना आवश्यक बनाती है.[68] चाहे इन मामलों से संकेत मिलता है या नहीं कि हुआवे ने इन नेटवर्कों में अपनी ही स्थिति का दोहन किया है, कंपनी का व्यवहार और साइबर हमले और जासूसी में चीन का ट्रैक रिकॉर्ड चिंता का कारण है.

चिंता की दूसरी प्रमुख वजह इतिहास से है और यहां तक कि उदार महाशक्तियों का व्यवहार भी कानून के शासन से विवश है. वास्तव में, पहले के ऐतिहासिक मामले दृढ़ता से संकेत करते हैं कि हुआवे जैसी कंपनी को जिस तरह की शक्ति और प्रभाव मिलेगा, उसका दोहन चीनी सरकार द्वारा किया जाएगा, जिस तरह दूसरी महाशक्तियों ने अक्सर दूरसंचार में अपनी कंपनियों या क्षमताओं की स्थिति का दोहन किया है

उस व्यापक ऐतिहासिक परिप्रेक्ष्य से, साक्ष्य बहुत से पर्यवेक्षकों को विवेकपूर्ण निष्कर्ष निकालने का रास्ता दिखा सकते हैं, कि दूरसंचार नेटवर्कों में हुआवे की भूमिका के बारे में विवेक से काम लेने की चेतावनी दी जाए – भले ही कंपनी के इरादे वास्तव में विशुद्ध रूप से व्यावसायिक हों, "कोई पीछे का दरवाज़ा नहीं और न ही कोई जासूसी" के उसके वादे भरोसेमंद हैं, और बीजिंग उन प्रतिबद्धताओं को पूरा करने के अपने वादे में ईमानदार है.

मोटे तौर पर, जैसा कि यह रिपोर्ट दर्शाती है, महाशक्ति की दूरसंचार प्रतिस्पर्धा की कई विशेषताएं जिन्हें आज अनोखा माना जाता है उनकी जड़ें अतीत में हैं. पूरे इतिहास में, कई विषयों की पुनरावृत्ति हुई है:

- *शक्ति:* दूरसंचार नेटवर्कों पर नियंत्रण 150 साल से भी पहले इसकी शुरुआत के समय से ही एक तरह की राजनीतिक शक्ति रहा है. ग्रेट ब्रिटेन ने दूरसंचार और रेडियो में अपनी भूमिका का दोहन किया है, संयुक्त राज्य अमेरिका ने शायद आधुनिक इंटरनेट युग में ऐसा किया है, और इस बारे में चिंतित होने की वजह है कि चीन भी आज ऐसा ही कर सकता है.

- *आत्मसंतुष्टि*: लंबे समय तक शांति और समृद्धि से दूरसंचार संबंधी जोखिमों में आत्मसंतुष्टि आ गई है. 19वीं सदी में, महाशक्तियां विदेशी फ़र्मों और विदेशी-संचालन वाले नेटवर्कों पर भरोसा करने को लेकर संतुष्ट थी, उसी तरह आज के देश चीनी दूरसंचार उपकरण और संचालन को स्वीकार करना चाहते हैं. लेकिन आखिर में, संभावित प्रतिस्पर्धियों या विरोधियों पर भरोसा करना जर्मनी जैसे देशों के लिए विनाशकारी साबित हुआ है और इससे दुनिया की राजनीति का आकार बदल चुका है.

- *दोहन:* नई दूरसंचार प्रौद्योगिकियों ने हमेशा से ही इंटरसेप्ट करने, अस्वीकार करने या उसका दोहन करने की नई कोशिशों को जन्म दिया है. इस उम्मीद के बावजूद कि एन्क्रिप्शन आधुनिक संचारों को इंटरसेप्ट करने की चीन की कोशिशों को मुश्किल बना सकता है, एन्क्रिप्शन में बड़ी उम्मीद की पिछली अवधियां उपयोगकर्ता की त्रुटि और उनमें सेंध लगाने की प्रतिद्वंद्वी देशों की दृढ़ संकल्प कोशिशों से धराशायी हो चुकी है, जैसा कि जर्मनी को उस समय पता चला था जब ग्रेट ब्रिटेन ने उसके कथित रूप से "अटूट" साइफर में सेंध लगा दी थी. सुरक्षित मानी जाने वाली प्रौद्योगिकियों के हर सिलसिले के साथ विनम्रता होनी ही चाहिए.

- *चैंपियन:* देशों को अक्सर अपने खुद के दूरसंचार चैंपियनों की तलाश रहती है, खास कर जब महाशक्ति के तनाव बढ़ रहे हैं. चीन की सरकार को हुआवे की उपलब्धियों पर गर्व है, और वह इसे दुनिया भर में भुनाना चाहती है – यहां तक कि वह उसकी प्रौद्योगिकी को नकारने वाले देशों को धमका भी रही है. जो कंपनी अपनी घरेलू सरकार के इतने करीब है उसके लिए सरकारी दबाव से मुक्त होना असामान्य ही होगा जबकि इतिहास में कई अन्य दूरसंचार चैंपियन भी इससे नहीं बच पाए हैं.

- *मानक*: दूरसंचार के मानक यह तय कर सकते हैं कि नेटवर्क की शक्ति कौन संभालेगा, जहां जर्मनी मानक तय करने वाले निकाय का इस्तेमाल वायरलेस रेडियो में ग्रेट ब्रिटेन के प्रभुत्व में सेंध लगाने के लिए कर रहा है. आज, वह प्रतिस्पर्धा अंतरराष्ट्रीय दूरसंचार संघ जैसे निकायों में आ गई है, और उसमें हुआवे की भूमिका इस बारे में विचार करने का संकेत देती है कि उसके मानक कहीं चीन को दूरसंचार का आकार बदलने की काबिलियत तो नहीं दे देंगे.

- *अस्वीकृति:* नेटवर्क सुरक्षा का तात्पर्य केवल इंटरसेप्शन और डेटा सुरक्षा से नहीं है, बल्कि पूरे नेटवर्क के संचालन या नेटवर्कों के बाहर एक्सेस देने की अस्वीकृति से भी है. ग्रेट ब्रिटेन ने जर्मनी को दुनिया के टेलीग्राफ़ नेटवर्कों से काट दिया था और नेटवर्कों में हुआवे की भूमिका उसे उन देशों में नेटवर्कों को बंद करने की ताकत दे सकती है जहां वह उपकरण का संचालन कर रही है भले ही वह आसानी से डेटा एक्सेस नहीं कर सकती हो.

- *दृढ़ संकल्प:* कई देश उस सीमा तक छूट देते हैं जिस पर कोई विरोधी अपने नेटवर्क से समझौता करने की असाधारण कोशिश कर सकता है, और बाद में ऐसा होने पर उसे एक अप्रिय आश्चर्य का सामना करना पड़ता हैं जिस पर कोई विरोधी अपने नेटवर्क से समझौता करने के लिए असाधारण कोशिश कर सकता है. दूसरे विश्व युद्ध में औद्योगिक-स्तर की कोशिशों के ज़रिए जर्मन साइफरों में सेंध लगाने की ब्रिटेन की काबिलियत और कथित रूप से टैप नहीं की जा सकने वाली आंतरिक सोवियत सबमरीन केबल को टैप करने की अमेरिकी काबिलियत ने उन गहराइयों को दर्शाया जिन तक जाकर महाशक्तियां महत्वपूर्ण खूफ़िया संकेतों तक पहुंचेंगी. चीन भी शायद ऐसी ही अधिकतम कोशिशें करने वाला है, और भले ही हुआवे के लिए आधुनिक नेटवर्कों में अपनी स्थिति को हथियार बनाना मुश्किल लगेगा, लेकिन चीन जैसे दृढ़ संकल्प

प्रतिस्पर्धी की साधन-संपन्नता को कमतर आंकना दूरसंचार की प्रतिस्पर्धा में एक पुनरावर्ती मूल भाव है.

जैसा कि यह रिपोर्ट दर्शाती है, दूरसंचारों पर महाशक्ति के खेल की कई विशेषताएं वैसी ही हैं, भले ही खिलाड़ी अलग हो सकते हैं.

लेखकों के बारे में

रश दोशी ब्रूकिंग्स चाइना स्ट्रेटेजी इनिशिएटिव के निदेशक और ब्रूकिंग्स फ़ॉरेन पॉलिसी में साथी रह चुके हैं. वे येल लॉ स्कूल के पॉल त्साई चाइना सेंटर में भी साथी रहे हैं और विल्सन चाइना फ़ेलोज़ की शुरुआती कक्षा का हिस्सा भी रहे हैं. उनके शोध में चीन की भव्य रणनीति के साथ ही भारत-प्रशांत सुरक्षा मामलों पर भी ध्यान केंद्रित किया गया है. दोषी, ऑक्सफ़ोर्ड यूनिवर्सिटी प्रेस से आने वाली *द लॉन्ग गेम: चाइनाज़ ग्रांड स्ट्रेटेजी टू डिस्प्लेस अमेरिका ऑर्डर,* के लेखक हैं. फिलहाल वे बाइडेन प्रशासन में सेवा दे रहे हैं.

केविन मॅकगिनेस ने हाल ही में ब्रूकिंग्स के साथ डिपार्टमेंट ऑफ़ डिफ़ेंस स्किलब्रिज प्रोग्राम से एक एक्स्टर्न के नाते काम किया है, जहां उन्होंने सेंटर फ़ॉर इस्ट एशिया पॉलिसी स्टडीज़ में कई प्रोजेक्ट में योगदान दिया है. वे वायु सेना के एक दिग्गज हैं और उन्होंने हाल ही में यूनाइटेड स्टेट्स एयर फ़ोर्स एकेडमी में फ़ैकल्टी के नाते अपना सफ़र खत्म किया है, जिसमें वे अंतरराष्ट्रीय संबंधों और एशियाई राजनीति में पाठ्यक्रमों का निर्देशन करते थे. उन्होंने हाल ही में स्टडी ऑफ़ चाइनीज़ मिलिटरी अफ़ेयर्स के लिए इंस्टीट्यूट फ़ॉर नेशनल स्ट्रैटेजिक स्टडीज़ के साथ एक शोध सहायक के नाते भी काम किया है, जहां उन्होंने पीएलए के आधुनिकीकरण और भारत-प्रशांत में सुरक्षा पर ध्यान केंद्रित किया है.

स्वीकृतियां

लेखक, पूर्व इंटर्न इसाबेला लू, ज़िजिन झोउ और गाओकी झांग को इस प्रोजेक्ट पर उनकी शोध सहायता के लिए, कई अनाम समीक्षकों, क्लेयर हैरिसन और टेड रिनर्ट को रिपोर्ट का संपादन करने के लिए, और क्रिस क्रुपिन्स्की और रशेल स्लैटरी को लेआउट तथा वेब डिज़ाइन के लिए धन्यवाद देना चाहते हैं. ब्रूकिंग्स इस अनुसंधान के वित्तपोषण के लिए यू.एस. डिपार्टमेंट ऑफ़ स्टेट और इंस्टीट्यूट ऑफ़ वॉर एंड पीस रिपोर्टिंग के प्रति आभारी है.

यह रिपोर्ट रश दोशी की सरकारी सेवा से पहले पूरी की गई थी, जिसमें केवल ओपन सोर्स सम्मिलित हैं और वे आवश्यक रूप से अमेरिकी सरकार की किसी भी एजेंसी की आधिकारिक नीति या स्थिति को नहीं दर्शाते हैं.

ब्रूकिंग्स इंस्टीट्यूशन एक गैर-लाभकारी संगठन है जो स्वतंत्र अनुसंधान और नीति समाधानों के लिए समर्पित है. इसका मिशन उच्च-गुणवत्ता वाला, स्वतंत्र अनुसंधान करना और उस अनुसंधान के आधार पर नीति-निर्माताओं और जनता के लिए नवीन, व्यावहारिक सिफारिशें प्रदान करना है. ब्रूकिंग्स के किसी भी प्रकाशन के निष्कर्ष और सिफ़ारिशें केवल उसके लेखक (लेखकों) के निष्कर्ष हैं और इंस्टीट्यूशन, इसके प्रबंधन या इसके अन्य विद्वानों के विचारों को नहीं दर्शाते हैं.

---

[1] स्टीवन चेज़, रॉबर्ट फ़ाइफ़ और बैरी मॅककेना, "ट्रूडो ने हुआवे के निर्णय में 'राजनीति के दखल' से इंकार किया," द ग्लोब और मेल, 15 अक्टूबर, 2018, https://www.theglobeandmail.com/politics/article-trudeau-refuses-to-let-politics-slip-into-decision-on-huawei/; ग्रेग क्विन और जॉश विनग्रोव, "ट्रूडो ने कहा कि हुआवे के 5G निर्णय में राजनीति दखल नहीं देगी," टाइम, 19 दिसंबर, 2018, https://time.com/5485141/justin-trudeau-huawei-5g-decision-politics/.

[2] डैनियल आर. हेडरिक, द इंविंसिबल वेपन: टेलीकम्यूनिकेशंस एंड इंटरनेशनल पॉलिटिक्स, 1851-1945 (ऑक्सफ़ोर्ड, यू.के.: ऑक्सफ़ोर्ड यूनिवर्सिटी प्रेस, 1991), चैप्टर 1.

[3] उक्त., यह अवलोकन हेड्रिक का है.

[4] उक्त.

[5] उक्त.

[6] उक्त., यह अवलोकन हेड्रिक का है.

[7] हैदी ट्वोरेक, न्यूज़ फ़्रॉम जर्मनी: दि कॉम्पीटिशन टू कंट्रोल वर्ल्ड कम्यूनिकेशंस, 1900-1945 (न्यूयॉर्क: हार्वर्ड हिस्टॉरिकल स्टडीज़, 2019).

[8] डैनियल आर. हेडरिक, द इंविंसिबल वेपन.

[9] "NH 79949 सेन्फ्यूगॉस केबल-कटिंग ऑपरेशन, 11 मई 1898," नेवल हिस्टॉरिकल सेंटर ऑनलाइन लाइब्रेरी, https://www.history.navy.mil/content/history/nhhc/our-collections/photography/us-people/b/baker-benjamin-f/nh-79949.html.

[10] उक्त., चैप्टर 5.

[11] जोनाथन विंक्लर, "इंफ़ॉर्मेशन वॉरफ़ेयर इन वर्ल्ड वॉर वन," द जर्नल ऑफ़ मिलिटरी हिस्ट्री 73, नं. 3 (2009): 845–67, https://doi.org/10.1353/jmh.0.0324.

[12] कैमरॉन मॅक आर. विंस्लो, "केबल-कटिंग एट सेनफ्यूगॉस," द सेंचुरी इलस्ट्रेटेड मंथली मैगज़ीन 57 (1899): 708-717, https://books.google.com/books?id=Y7fPAAAAMAAJ&pg=PA708#v=onepage&q&f=false.

[13] जोनाथन विंक्लर, "साइलेंसिंग दि एनिमी: केबल-कटिंग इन द स्पेनिश–अमेरिकन वॉर," वॉर ऑन दि रॉक्स, 6 नवंबर, 2015, https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/; रेबेका रेन्स, "मैनिफ़ेस्टिंग इट्स डेस्टिनी: दि यू.एस. आर्मी सिग्नल कॉर्प्स इन द स्पेनिश-अमेरिकन वॉर," *आर्मी हिस्ट्री* 46 (1998): 14–21, https://www.jstor.org/stable/26304991.

[14] जोनाथन विंक्लर, "साइलेंसिंग दि एनिमी."

[15] "स्पेनिश अमेरिकन वॉर: टेलीग्राफी एंड केबल कटिंग, इंट्रोडक्टरी एसे," नेवल हिस्ट्री एंड हेरिटेज कमांड, https://www.history.navy.mil/research/publications/documentary-histories/united-states-navy-s/telegraphy-and-cable.html.

[16] जोनाथन विंक्लर, "साइलेंसिंग दि एनिमी."

[17] लाइब्रेरी ऑफ़ कांग्रेस, जॉर्ज ग्रांथम बैन कलेक्शन, https://www.loc.gov/pictures/item/2014683102/.

[18] हालांकि जैसा हैदी ट्वोरेक उल्लेख करते हैं, इस प्रौद्योगिकी के विकास में अक्सर उनकी अपनी भूमिका फलीभूत हुई है. हैदी ट्वोरेक, *न्यूज़ फ़्रॉम जर्मनी.*

[19] मार्क रेबॉय, "द फ़र्स्ट कंपनी दैट वांटेड टू 'कनेक्ट द वर्ल्ड' वॉज़ नॉट गूगल और फ़ेसबुक," Media@LSE, 24 अगस्त, 2016, https://blogs.lse.ac.uk/medialse/2016/08/24/the-first-company-that-wanted-to-connect-the-world-wasnt-google-or-facebook/.

[20] हैदी ट्वोरेक, न्यूज़ फ़्रॉम जर्मनी, 12–13.

[21] मिशेल फ़्रेडवाल्ड, "टेलीफ़ुनकेन वर्सेस मार्कोनी, या द रेस फ़ॉर वायरलेस टेलीग्राफ़ी एट सी, 1896-1914," SSRN (9 जनवरी, 2014): https://doi.org/10.2139/ssrn.2375755.

[22] उक्त.

[23] मार्क रेबॉय, मार्कोनी: दि मैन हू नेटवर्क्ड द वर्ल्ड (ऑक्सफ़ोर्ड, यू.के.: ऑक्सफ़ोर्ड यूनिवर्सिटी प्रेस, 2016), 226–28.

[24] उदाहरण के लिए, टेलीफ़ुनकेन जर्मनी में उन क्षेत्रों में भी सक्रिय थी जहां बड़ी औपनिवेशिक मौजूद नहीं थी, जैसे कि लैटिन अमेरिका.

[25] जॉर्ज जॉनसन, ed., *दि ऑल रेड लाइन: दि एनल्स एंड एम्स ऑफ़ दि पैसिफ़िक केबल प्रोजेक्ट* (ओटावा: जेम्स होप एंड संस, 1903), 10, एट इंटरनेट आर्काइव, https://archive.org/details/allredlineannals00johnuoft/page/n11/mode/2up.

[26] गॉर्डन कोरेरा, "हाउ ब्रिटेन पायनीयर्ड केबल-कटिंग इन वर्ल्ड वॉर वन," बीबीसी न्यूज़, 15 दिसंबर, 2017, https://www.bbc.com/news/world-europe-42367551.

[27] जोनाथन विंक्लर, "इंफ़ोर्मेशन वॉरफ़ेयर इन वर्ल्ड वॉर I," 847.

[28] पी.एम. केनेडी, "इंपीरियल केबल कम्यूनिकेशंस एंड स्ट्रेटेजी, 1870-1914," दि इंग्लिश हिस्टॉरिकल रिव्यू 86, नं. 341 (1971): 728–52, https://www.jstor.org/stable/563928.

[29] जोनाथन विंक्लर, "इंफ़ोर्मेशन वॉरफ़ेयर इन वर्ल्ड वॉर I," 849.

[30] उक्त., 851. उक्त., 851.

[31] गॉर्डन कोरेरा, "व्हाय वॉज़ द ज़िमरमैन टेलीग्राम सो इंपोर्टेंट?," बीबीसी न्यूज़, 17, जनवरी, 2017, https://www.bbc.com/news/uk-38581861; पैट्रिक बीसली, रूम 40: ब्रिटिश नेवल इंटेलिजेंस 1914-18 (सैन डिएगो: हारकोर्ट ब्रेस जोवानोविच, 1982).

[32] सी. ओ. नॉर्डनस्वान एंड वाल्देमार लैंग्लेट, *Det stora världskriget* [दि ग्रेट वर्ल्ड वॉर] (1915), एट वीकिमीडिया कॉमन्स, https://commons.wikimedia.org/wiki/File:German_WW_I_field_telegraph_002.jpg.

[33] जोनाथन विंक्लर, "इंफ़ोर्मेशन वॉरफ़ेयर इन वर्ल्ड वॉर फर्स्ट."Winkler, "Information Warfare in World War I."

[34] विलहेम फ़्लिक, "दि बिगिनर्स ऑफ़ रेडियो इंटरसेप्ट इन वर्ल्ड वॉर फर्स्ट: अ ब्रीफ़ हिस्ट्री बाय अ जर्मन इंटेलिजेंस ऑफ़िसर," एनएसए क्रिप्टोलॉजिक स्पेक्ट्रम आर्टिकल्स 8, नं. 2 (1978): 21, https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/.

[35] ब्रूस नॉर्मन, सीक्रेट वॉरफ़ेयर: दि बैटल ऑफ़ कोड्स एंड साइफर्स (न्यूटन एबॉट, यू.के.: डेविड एंड चार्ल्स लिमिटेड, 1973); प्रिट बुट्टर, कोलिजन ऑफ़ एम्पायर्स: द वॉर ऑन दि इस्टर्न फ़्रंट इन 1914 (ऑक्सफ़ोर्ड, यू.के.: ऑस्प्रे पब्लिशिंग, 2014).

[36] मैट क्रिप्टो, "ब्लेचली पार्क म्यूज़ियम में प्रदर्शनी में रखी गई लॉरेंज़ SZ42 साइफर मशीन के रोटर्स," वीकिमीडिया कॉमंस में, https://commons.wikimedia.org/wiki/File:SZ42-6-wheels.jpg.

[37] जॉर्ज फर्स्ट. बेक, "मिलिटरी कम्यूनिकेशन - दि एड्वेंट ऑफ़ इलेक्ट्रिकल सिग्नलिंग," ब्रिटानिका, https://www.britannica.com/technology/military-communication. "मिलिटरी कम्यूनिकेशन - दि एड्वेंट ऑफ़ इलेक्ट्रिकल सिग्नलिंग," ब्रिटानिका, https://www.britannica.com/technology/military-communication.

[38] हैरी हिन्स्ली, "दि इन्फ़्लूएंस ऑफ़ अल्ट्रा (ULTRA) इन दि सेकंड वर्ल्ड वॉर" (लेक्चर, कैम्ब्रिज, यू.के., 19 अक्टूबर, 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.

[39] $1x10^{170}$ संभावित सेटिंग्स.

[40] "ब्लेचली पार्क रिमेंबर्स पोलिश कोड ब्रेकर्स," बीबीसी न्यूज़, 14 जुलाई, 2011, https://www.bbc.com/news/uk-england-beds-bucks-herts-14141406.

[41] गॉर्डन वेल्चमैन, दि हट सिक्स स्टोरी: ब्रेकिंग दि एनिग्मा कोड्स (क्लिओबरी मोरटाइमर, यू.के.: क्लासिक क्रिप्टो बुक्स, 1997).

[42] हैरी हिन्स्ली, "दि इन्फ़्लूएंस ऑफ़ अल्ट्रा (ULTRA)."

[43] उक्त.

[44] उदाहरण के लिए, देखिए, जेरी रॉबर्ट्स, लॉरेंज: ब्रेकिंग हिटलर्स टॉप सीक्रेट कोड एट ब्लेचली पार्क (चेल्टेनहैम, यू.के.: हिस्ट्री प्रेस, 2017).

[45] एफ़. डबल्यू. विंटरबॉथम, दि अल्ट्रा सीक्रेट (न्यूयॉर्क: हार्पर एंड रो, 1974), 154, 191.

[46] हैरी हिन्स्ली, "दि इन्फ़्लूएंस ऑफ़ अल्ट्रा (ULTRA)."

[47] काल्डर वॉल्टन, "दि स्पाइज़ हू केम इन फ़्रॉम दि कंटिनेंट," फ़ॉरेन पॉलिसी, 27 अप्रैल, 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.

[48] यू.एस. नेवी, वीकिमीडिया कॉमन्स में, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.

[49] ऐना बोर्शखेव्स्काया, "दि सोवियत्स' अनब्रेकेबल कोड," फ़ॉरेन पॉलिसी, 27 अप्रैल, 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.

[50] डैनियल आर. हेडरिक, दि इंविंसिबल वेपन, अध्याय 4.

[51] शेरी सोनटाग, क्रिस्टोफर ड्रयू, और एनेट लॉरेंस ड्रयू, ब्लाइंड मैन्स ब्लफ़: दि अनटोल्ड स्टोरी ऑफ़ अमेरिका सबमरीन एस्पियोनेज (न्यूयॉर्क: पब्लिक अफ़ेयर्स, 1998), 222.

[52] उक्त.

[53] उक्त., 223.

[54] उक्त.

[55] मैट ब्लिट्ज़, "नेवी डाइवर्स एंड देयर डेयरडेविल मिशन टू स्पाय ऑन द सोवियत यूनियन एट द बॉटम ऑफ़ द सी," पॉप्युलर मेकैनिक्स, 30 मार्च, 2017, https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping/.

[56] माइकल जे. सुलिक, अमेरिकी स्पाइज़: एस्पियोनेज अगेंस्ट दि यूनाइटेड स्टेट्स फ़्रॉम दि कोल्ड वॉर टू दि प्रेज़ेंट (वाशिंगटन, डीसी: जॉर्जटाउन यूनिवर्सिटी प्रेस, 2013), 109–14; मैट ब्लिट्ज़, "नेवी डाइवर्स."

[57] डेमियन मॅकगिनेस, "हाउ अ साइबर अटैक ट्रांसफ़ॉर्म्ड एस्टोनिया," बीबीसी न्यूज़, 27 अप्रैल, 2017, https://www.bbc.com/news/39655415; Rain Ottis, "एनालिसिस ऑफ़ दि 2007 साइबर अटैक्स अगेंस्ट इस्टोनिया फ़्रॉम दी इंफ़ोर्मेशन वारफेयर परस्पेक्टिव," (टैलिन: नाटो कोऑपरेटिव साइबर डिफ़ेंस सेंटर ऑफ़ एक्सीलेंस, 2008), https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.

[58] डेविड हॉलिस, "साइबर वॉर केस स्टडी: जॉर्जिया 2008," स्मॉल वॉर्स जर्नल, 6 जनवरी, 2011, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008; रोनाल्ड जे. डाएबर्ट, रूल रोहोज़िंस्की, और मसाशी क्रीट-निशिहाता, "साइक्लोंस इन साइबरस्पेस: इंफ़ोर्मेशन शेपिंग एंड डिनायल इन दि 2008 रशिया–जॉर्जिया वॉर," सिक्योरिटी डायलॉग 43, नं. 1 (2012): 3–24, https://journals.sagepub.com/doi/10.1177/0967010611431079.

[59] पावेल पोलीट्यूक एंड जिम फ़िंकल, "यूक्रेन सेज़ कम्यूनिकेशन हट, एमपीज़ फ़ोंस ब्लॉक्ड," रॉयटर्स, 4 मार्च, 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304; सर्गी सुखानकिन, "रशियन इलेक्ट्रॉनिक वॉरफ़ेयर इन यूक्रेन: बिटवीन रियल एंड इमेजिनेबल," जेम्सटाउन फ़ाउंडेशन, 24 मई, 2017, https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/.

[60] एंडी ग्रीनबर्ग, "हाउ एन एंटायर नेशन बिकेम रशियाज़ टेस्ट लैब फ़ॉर साइबर वॉर," वायर्ड, 20 जून, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; "सिक्स रशियन जीआरयू ऑफ़िसर्स चार्ज्ड इन कनेक्शन विद वर्ल्डवाइड डिप्लॉयमेंट ऑफ़ डिस्ट्रक्टिव मैलवेयर एंड अदर डिसरप्टिव एक्शंस इन साइबरस्पेस," यू.एस. डिपार्टमेंट ऑफ़ जस्टिस, 19 अक्टूबर, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[61] कॉन्स्टांज़ स्टेल्ज़ेम्यूलर, "दि इम्पैक्ट ऑफ़ रशियन इंटरफ़ेस ऑन जर्मनीज़ 2017 इलेक्शंस," (कांग्रेसशनल टेस्टीमोनी, 28 जून, 2017), https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

[62] मैगी मिलर, "यूएस इंटेल एजेंसीज़ ब्लेम रशिया फ़ॉर मैसिव सोलरविंड्स हैक," *द हिल,* 5 जनवरी, 2021, https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack.

[63] "कनेक्ट दि डॉट्स ऑन स्टेट-स्पांसर्ड साइबर इंसीडेंट्स - टाइटन रेन," काउंसिल ऑन फ़ॉरेन रिलेशंस, https://www.cfr.org/cyber-operations/titan-rain.

[64] गैरेट ग्राफ़, "चाइनाज़ हैकिंग स्प्री विल हेव अ डैकेड्स-लांग फ़ॉलआउट," वायर्ड, 11 फरवरी, 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

[65] चुन हान वोंग, "चाइना लॉन्चेस इनिशिएटिव टू सेट ग्लोबल डेटा-सिक्योरिटी रूल्स," *दि वॉल स्ट्रीट जर्नल,* 8 सितंबर, 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

[66] बोजान पानसेव्स्की, "यू.एस. ऑफ़िशियल्स से हुआवे कैन कोवर्टली एक्सेस टेलीकॉम नेटवर्क्स," दि वॉल स्ट्रीट जर्नल, 12 फ़रवरी, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

[67] जो पार्किंसन, निकोलस बैरियो, और जॉश चिन, "हुआवे टेक्निशियंस हेल्प्ड अफ़्रीकन गवर्नमेंट्स स्पाय ऑन पॉलिटिकल ओपोनेंट्स," दि वॉल स्ट्रीट जर्नल, 15 अगस्त, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[68] विलियम टर्टन, "हिडन बैक डोर एम्बेडेड इन चाइनीज़ टैक्स सॉफ़्टवेयर, फ़र्म सेज़," ब्लूमबर्ग, 25 जून, 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.