King's Research Portal

DOI:

[10.1080/01611194.2015.1028686](https://doi.org/10.1080/01611194.2015.1028686)

Document Version

Early version, also known as pre-print

[Link to publication record in King's Research Portal](#)

Citation for published version (APA):

Goodman, M. S., & Dylan, H. (2016). British Intelligence and the Fear of a Soviet Attack on Allied Communications. *CRYPTOLOGIA*, 40(1), 15-32. <https://doi.org/10.1080/01611194.2015.1028686>

Citing this paper

Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

General rights

Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Research Portal

Take down policy

If you believe that this document breaches copyright please contact librarypure@kcl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

British Intelligence and the Fear of a Soviet Attack on Allied Communications

Huw Dylan and Michael Goodman

The release of the Ultra secret in the early 1970s revolutionised the way that the Second World War was understood. Not only did it render a good number of earlier accounts obsolete but, for some, it suggested that intelligence had been the vital element in the Allied victory. For many historians of the Cold War the implications were obvious: if a secret could be held on this scale for a number of decades, might the revelation of a similar intelligence triumph suddenly render our understanding of the Cold War obsolete?¹ It is probably fair to say that the important spies have all been revealed for the Cold War period, even if specific facts remain obscured, but what of the sigint effort undertaken by East and West?

Recent archival releases by the National Security Agency (NSA) arguably offer the most informative and authoritative account of Cold War sigint.² In Britain, Government Communications Headquarters (GCHQ) remains more secretive, but a number of archival releases have shed some light on its post-war activities.³ Far more mysterious is the history of post-war Soviet sigint. A number of attempts have been made to redress this, and the detail they offer is tantalising. General information is known about the scale and size of the Soviet sigint effort in the later Cold War: separate enterprises located within the KGB, GRU and other military components employed over 300,000 personnel; over 500 ground stations; sigint systems in at least 64 countries; at least 60 dedicated sigint vessels; and at least 20 sigint aircraft.⁴ Statistics of course do not tell the whole story, but on numbers alone it can be inferred that this was a substantial effort, sustained over a long period of time. Even less is known about Soviet comint efforts, though a 1967 annual report suggested that the KGB read

¹ Various inferences to this can be found in R.J.Aldrich. *The Hidden Hand: Britain, America and Cold War Secret Intelligence*. (London: John Murray, 2001).

² 'National Security Agency Releases History of Cold War Intelligence Activities', *The National Security Archive*, George Washington University. Available here: <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/> [accessed December 2014]

³ The most detailed account is R.J.Aldrich. *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. (London: HarperPress, 2011). See also a number of recent articles by David Easter: 'GCHQ and British External Policy in the 1960s', *Intelligence and National Security* 23:5 (2008), pp.681-706; 'Code Words, Euphemisms and what they can tell us about Cold War Anglo-American Communications', *Intelligence and National Security* 27:6 (2012), pp.875-95; 'Spying on Nasser: British Signals Intelligence in Middle East Crises and Conflicts, 1956-67', *Intelligence and National Security* 28:6 (2013), pp.824-44; and 'Soviet Bloc and Western Bugging of Opponents' Diplomatic Premises during the Early Cold War', *Intelligence and National Security* 31:1 (2014, forthcoming).

⁴ For more, see D.Ball and R.Windrem, 'Soviet Signals Intelligence (Sigint): Organization and Management', *Intelligence and National Security* 4:4 (1989), pp.621-59.

188,400 cables of 152 systems of 72 capitalist countries.⁵ Again, the numbers are tantalising and reveal the sheer scale of effort involved.⁶ Unsurprisingly, the priority target was the United States and, to a lesser extent, the United Kingdom.

This research note considers Soviet comint from the perspective of British intelligence. Specifically it refers to a 1959 assessment, reproduced below, by Britain's Joint Intelligence Committee (JIC) on 'Soviet interdiction of Allied communications'. The JIC had been created in 1936 for two clear purposes: to remedy the inefficiency and duplication of effort going on in the various military intelligence departments; and to ensure that if and when war came, military planners would have the best possible intelligence available to them. Despite existing on the fringes of the government, the Second World War signaled the JIC's maturity and rise in prestige, standing, and influence. By 1945 it had become an integral component of the intelligence and planning machinery, operating at the interface between the secret and policy worlds. Its views on the vulnerability of allied communications would therefore have carried significant weight, both in Britain and across the Atlantic.

The JIC was (and is) an intelligence assessment organisation. Membership is drawn from those in the intelligence and policy realms. The 1959 Committee included, on the one hand, the heads of SIS (MI6), GCHQ, MI5, the Joint Intelligence Bureau and military intelligence directorates; and, on the other, senior representatives from the Foreign Office, Colonial Office, Commonwealth Relations Office, and Ministry of Defence. Its tasks ranged from the setting of intelligence community priorities to the production of assessments, but it also retained a responsibility for security matters. In 1956 the JIC moved out of the Chiefs of Staff military structure, where it had resided since 1936, into the Cabinet Office. This had two important implications: assessments could be commissioned by a broader array of government departments; and the assessed product could be disseminated to Ministers and other senior officials.

Central to the JIC's work and remit were a number of important aspects. The Committee's assessments were based on consensus; in other words, nothing could be issued

⁵ R.L.Garthoff, 'The KGB Reports to Gorbachev', *Intelligence and National Security* 11 (1996), p.228. In fact, comint more broadly remains an underexplored area of research. See R.J.Aldrich, 'Whitehall Wiring: The Communications-Electronics Security Group and the Struggle for Secure Speech', *Public Policy and Administration* 28:2 (2012), p.179.

⁶ For a fascinating account of what is known, see D.Kahn, 'Soviet Comint in the Cold War', *Cryptologia* 22:1 (1998), pp.1-24.

with the JIC's appellation unless all constituent members agreed to its conclusions and wording. It was here that the mixture of intelligence professionals and officials from policy-making departments was crucial. Related to this disparate membership was the JIC's relationship with allied intelligence communities, and nowhere was this as close as the transatlantic partnership. The effect of working so closely together during the Second World War had a lasting effect after 1945, and the JIC's relationship to its American and Canadian brethren was virtually symbiotic. Assessments were often discussed in the drafting stage, and representatives of American and Canadian intelligence attended specific portions of the JIC's meetings. Therefore, it is no surprise that the JIC document reproduced below should be circulated to the Americans and Canadians; its conclusions carried significant implications for both countries' management of allied communications during periods of crisis, or in the early stages of global war.

In the mid-1950s, amidst a fear of a Soviet attack, elaborate procedures were put into place between the capital cities of all three powers to ensure that London, Ottawa and Washington could instantly warn the others if and when a Soviet strike came.⁷ They required a robust system, but communications channels between them in the 1940s and 1950s were often beset by problems of capacity and reliability. This affected the crucial matter of exchanging Sigint on an almost daily basis in the mid-1950s, as the inadequate cable system and radio frequencies struggled to cope.⁸ It also affected bi-lateral discussions between the British Prime Minister and the President of the United States. These required extremely high security and reliability, but this was only achieved by the early 1960s with the roll out of the 'Pickwick' secure voice system.⁹ Throughout the 1950s the speed and reliability of transatlantic communications, in general and at times of crisis was a matter of the utmost importance. 'Pickwick' was one solution to the problem. By the 1970s Britain and the US's development of powerful communications satellites was another, more comprehensive, answer, though problems persisted.¹⁰

⁷ For more detail on the preceding paragraphs on the JIC see M.S.Goodman. *The Official History of the Joint Intelligence Committee, Volume 1: From the Approach of the Second World War to the Suez Crisis*. (London: Routledge, 2014).

⁸ See Aldrich, *GCHQ*, p.347.

⁹ For more, see Aldrich, 'Whitehall Wiring', pp.185-186.

¹⁰ See Aldrich, *GCHQ*, pp.347-348.

It is not obvious which department of state drafted the report for the JIC. The logical choice would have been the London Communications Security Agency, subsequently a component of GCHQ, but in the late 1950s a separate organisation responsible for communications security.¹¹

Regardless of which organization drafted it, the report was approved and disseminated by the JIC in July 1959, but remained a live document subject to revision and editing until at least 1961. The Soviet Union at this juncture, despite the general thawing of relations following Khrushchev's ascent to power, remained the primary intelligence target. The JIC's view, consistently held, was that all-out war with the Soviet Union was unlikely but that war by miscalculation remained a possibility. Nonetheless, it was assumed that the Russians would do all they could to subvert the West. In this context the JIC set about looking at 'the means available to the USSR for disturbing the flow of traffic on allied telecommunications circuits...particularly trans-Atlantic communications'. The cables and wireless networks criss-crossing the Atlantic offered the UK a vital means for interaction with the US and Canada. But as we have noted above they were not wholly reliable. In war they would have been vital for effective command and control. Assessing their vulnerability to Soviet interference was therefore crucial.¹² Britain could be in no doubt that the Soviets would consider allied communications systems a vital target system. Cables had been targets of war since they were first laid, and remain so in modern conflict. The British cut German cables in the First World War; the US attacked the North's cables during the Korean War; the NSA worked with the US navy to identify and tap Soviet undersea cables throughout the Cold War; in the 1991 Gulf War British special forces were tasked with destroying Iraqi fibre-optic cables.¹³ For a relatively small island it was a problem that required constant consideration.

The JIC's report was split into five parts:

¹¹ On LCSA see Aldrich, 'Whitehall Wiring'.

¹² Cutting cables deliberately to stop communication, or tapping into them to procure intelligence was, of course, not new. Just consider the intelligence supply from the Vienna and Berlin tunnels. See D.Stafford. *Spies Beneath Berlin*. (London: John Murray, 2003).

¹³ For the history of British thinking on cable security and imperial communications see P. M. Kennedy 'Imperial Cable Communications and Strategy, 1870-1914', *The English Historical Review* 86:341 (1971); see also for further examples, *Studies in Intelligence: Journal of the American Intelligence Professional* 57:2 (2013); p.71, Bob Woodward, *Veil: The Secret Wars of the CIA* (Simon and Schuster: London, 1987), p.449; Matthew Aid, 'How the CIA Cut an Undersea Cable and Helped American Signal Collectors During the Korean War', available at <<http://www.matthewaid.com/post/65052358164/how-the-cia-cut-an-undersea-cable-and-helped>>; Aldrich, *GCHQ*, p.468.

Part I – List of Vital Targets in the Atlantic Area

Part II – Assessment of the Threat of Soviet Interdiction of Allied Communications

Part III – Deployment and Use of Soviet Capabilities

Part IV – Assessment of the Likely Effects on Allied Trans-Atlantic Communications

Part V – Recommendations for Counter-Measures

The first three Parts are reproduced below. Unfortunately there is no trace of Parts IV and V in The National Archives in London.

The JIC considered three types of communications system: land lines, sub marine cables, and radio circuits. Each was vulnerable to interference to a greater or lesser extent. Land lines, and associated systems, were relatively easy to locate and were open to sabotage. Sub marine cables, similarly, were relatively easy to locate and were susceptible to damage from trawlers, submarines, or explosions. Radio circuits, depending on the particulars of individual systems, were exposed to two forms of disruption: first, jamming, which the Soviets could do from a variety of locations and through a number of techniques, including high-powered transmitters based in Soviet territory, naval assets positioned near receiving stations, aircraft, and potentially through clandestine operations using low-power, close-range jammers. Second, the Soviets could affect radio propagation through ionospheric disturbance. They could achieve this either by detonating nuclear weapons or by seeding the ionosphere with radioactive materials. A concerted effort could, theoretically, severely compromise Britain's ability to communicate with its allies.

The JIC's assessment as to whether or not the potential threat to allied communications would ever materialise hinged on two factors: Soviet capabilities and Soviet intentions.¹⁴ The Committee had little doubt that the Soviets enjoyed significant capabilities. They were experienced at deep-water trawling; it was highly likely that they were capable of mounting submarine attacks on cables; they had ample stocks of nuclear weapons; they had constructed a network of powerful jamming transmitters in the USSR; they were capable of disrupting focal points through special operations. In short, the RAF's Bomber Command

¹⁴ On this see M.S.Goodman, 'Jones' Paradigm: The How, Why, And Wherefore of Scientific Intelligence', *Intelligence and National Security* 24:2 (2009), pp.236-56.

and USAF's Strategic Air Command's nets could 'almost certainly' be targeted by specialised Soviet aircraft, as could Britain's early warning radar.

The key issue for the JIC's customers was how the Soviets intended to deploy this capability immediately preceding a global war. The JIC judged that disrupting a retaliatory strike would be a key Soviet objective. Some potential techniques were effective but would reveal the Soviet hand too soon: for example, targeting communication terminals with nuclear weapons. Others, such as detonating nuclear weapons below the ionosphere, were deemed to be too disruptive to Soviet systems to be useful. The most viable approaches for the Soviets were presumed to be sabotage and electronic countermeasures. They would, in all likelihood, target 'military networks associated with the alerting and launching of the West's nuclear retaliatory forces'. The JIC noted that 'it should be assumed that the Soviets would attempt to carry out jamming of ionospheric and tropospheric scatter systems', both of which carried transatlantic communications. It was assumed likely that Soviet intelligence was devoting significant resources to identifying these systems. With regards to long range communications, although it was judged unlikely that Soviet action could disrupt all circuits, the probability of an attack was high enough for the JIC to assume they would take place. Should these operations be mounted, the West's ability to mount an effective coordinated response would be seriously diminished, and with it, of course, the potency of its deterrent capability.

Research into British and Allied command and control procedures has revealed that they devoted significant energy to the problem of command and control and the nuclear deterrent during the period in question. This included assessments of Soviet techniques and capabilities. As early as 1953 Britain's Joint Strategic Communications Panel noted that the 'Russians are well versed in the techniques of jamming...'.¹⁵ The creation of a modulating VHF communications system for Britain's Bomber Command to use in communicating with its V-bomber force was based on the ease with which previous systems could be undermined.¹⁶ Nevertheless, it is clear that Britain, in particular, could not assume that it would retain positive communications with its retaliatory forces in the event of war. The solution, and the maintenance of a credible deterrent, was found in delegating authority for

¹⁵ S.Twigge and L.Scott. *Planning Armageddon: Britain, the United States and the Command of Western Nuclear Forces, 1945-1964*. (Amsterdam: Harwood, 2000). pp.214-215.

¹⁶ *Planning Armageddon*. pp.218-219.

retaliation against the USSR to Bomber Command in the event of a communications failure.¹⁷

The intriguing question is to what extent this planning, and the effective relinquishing of political control over British nuclear weapons, was conducted in an information vacuum, both with regards to Soviet capabilities and intentions?¹⁸ The JIC could infer Soviet jamming capability through their relatively consistent jamming of BBC signals, and had also mapped broadcasting and jamming transmitters in the USSR. But the Committee observed little evidence of large scale jamming as part of Soviet military exercises. They judged that it was almost certain that the Soviets had aircraft capable of targeting VHF circuits, that they were well versed in the potential use of submarines to target undersea cables, and that they appreciated the importance of jamming VLF communications with Polaris submarines. Despite these views, the report frustratingly offers few specifics.

The literature on Soviet communications intelligence and military doctrine certainly suggests that the JIC was correct in erring on the side of caution with regards to Soviet capabilities and intentions. Soviet air doctrine emphasised the importance of compromising enemy communications, either by destroying or by jamming, at the outset of war as a key element for successful surprise.¹⁹ The revelations of defectors like Vasili Mitrokhin illustrate that aspects of the Soviet sigint and comint programmes were extremely advanced.²⁰ The KGB's efforts, outlined above, do not tell the whole story. Soviet military intelligence, the GRU, maintained a separate capability targeting military systems and communications. This was managed by the Sixth Directorate; their main target was the US, the second priority was the RAF.²¹ The precise nature of its capability in the late 1950s is currently unclear, as it would have been to the JIC at the time.

The document reminds us that intelligence was central to major aspects of alliance politics and war planning in the Cold War, but also that, unlike during the Second World War, comint could not provide a consistent overview of the adversary's affairs. However, it

¹⁷ *Planning Armageddon*. p. 227.

¹⁸ The only real attempt to look at this, albeit written at a time of very few intelligence record releases, is I.Clark and N.J.Wheeler. *The British Origins of Nuclear Strategy, 1945-1955*. (Oxford: Oxford University Press, 1989).

¹⁹ Colonel L. Kuleszynski, 'Some Problems of Surprise in Warfare' *Military Thought*, Number 5, 1971, in U.S. Air Force, *Selected Readings from Soviet Military Thought, 1963-1973*, Studies in Communist Affairs, Volume 5, Part 2, (Washington: GPO, 1982).

²⁰ C.Andrew and V.Mitrokhin. *The Mitrokhin Archive: The KGB in Europe and the West*. (London: Penguin, 2000).

²¹ Ball and Windrem, 'Soviet signals intelligence', p.633.

also provides a rare perspective on how Western intelligence viewed the capabilities of Soviet comint. If it is ever released, the inside story of Soviet comint will offer us fascinating insights not only into the communist empire's most secretive service, but also into the viability of both the East and West's plans for nuclear war. Until then, declassified contemporaneous assessments offer an intriguing glimpse into the Soviet Union.

**CABINET
JOINT INTELLIGENCE COMMITTEE**

**SOVIET INTERDICTION OF ALLIED COMMUNICATION – PART I –
LIST OF VITAL TARGETS IN THE ATLANTIC AREA**

REPORT BY THE JOINT INTELLIGENCE COMMITTEE

Attached are lists of vital targets in the Atlantic area, as prepared in the United Kingdom. They are set out as follows:-

- (a) Transatlantic Radio Circuits
- (b) Atlantic Submarine Cable Resources
- (c) Transatlantic Cable Circuits

2. Copies of this report have been passed for comment to the American and Canadian Authorities. This report will be revised in the light of these comments and the revised report will be the basis on which Part III of this Study will be prepared.

(Signed) P.H.Dean,

*On behalf of the
Joint Intelligence Committee*

Cabinet Office, SW1

14th July, 1959.

²² TNA: CAB 158/37.

**CABINET
JOINT INTELLIGENCE COMMITTEE**

SOVIET INTERDICTION OF ALLIED COMMUNICATIONS

PART II – ASSESSMENT OF THE THREAT OF SOVIET INTERDICTION

REPORT BY THE JOINT INTELLIGENCE COMMITTEE

A United Kingdom assessment of the threat of Soviet interdiction of Allied communications is at Annex.

2. Copies of the report have been passed for comment to the American and Canadian authorities. This report will be revised in the light of these comments and the revised report, together with Part I (revised as necessary) will be the basis on which Part III of the study will be prepared.

(Signed) P.H.Dean,

On behalf of the Joint Intelligence Committee

Cabinet Office, SW1

12th November, 1959.

SECRET

US/UK/Canadian Eyes Only

ANNEX to JIC(59)54 – Part II

ASSESSMENT OF THE THREAT OF SOVIET INTERDICTION OF ALLIED COMMUNICATIONS

Introduction

In this part of the paper the means available to the USSR for disturbing the flow of traffic on allied telecommunications circuits are reviewed. The main consideration has been given to strategic communications and, as directed, “particularly trans-Atlantic communications”. The forms of telecommunication subject to disruption are three-fold, viz., submarine cables, landlines, and radio circuits of each of which there are various types. The susceptibility of each of these to interference is considered and conclusions on the threat are recorded. The way in which the USSR may deploy their facilities against Western targets will be discussed in Part III of the paper.

Submarine Cables

2. The first reference to the security of submarine cables by an authoritative body has been traced to a report from the Chiefs Signals Officer, United States Army, to the Secretary of War, of which excerpts appear in the November 16th, 1920, issue of *Telegraph and Telephone Age*. These are cited, *inter alia*, in the Imperial Communications Advisory Committee paper No. 1416-A, dated February 28th, 1944.

3. Submarine cables are subject to physical damage which may be breakage by trawling, cutting or underwater explosion. The result may be complete or partial loss of traffic capacity in one or more cables, and for damage to be caused it is necessary that the cables should first be located.

4. The routes of the cable approaches to shore termini are relatively well known from the technical Press and from the publications and advertising matter of the cable operating companies. The cable runs to the termini at Valentia and Porthcurno lie within approximately 2½ degrees of latitude at a distance of some 150 miles from the Irish coast. Up to this distance from the coast the cables lie at depths at which trawling for fish – up to 300 fathoms – is normally practised, and beyond that at practicable trawling depths; but not at depths where edible fish are normally found. The cable runs from Waterville to Weston-Super-Mare and from Porthcurno to North America lie within 2 degrees of latitude at the approaches to St. George’s Channel, and on the sea bottom within normal fishing trawl depth to about 300 miles from Lands End. The other main terminal for trans-Atlantic cables – Oban – is served by the two most modern telephone cables which lie some 10 miles apart and in about 100 fathoms of water at longitude 9 degrees W. The English Channel and the southern North Sea, as well as the south-western approaches to the English Channel, also bear a dense complex of cables of which many are “common-user” cables. Other than in the

area to the south and south-east of Newfoundland, trans-Atlantic cables lie outside the waters regularly fished commercially. These areas could, of course, change with the habits of edible fish.

5. The problem of location of these cables is, therefore, not a serious one and it can be achieved by trawling - and is frequently and inadvertently by fishing vessels - grappling or by electro-potential, magnetic, or electro-magnetic radiation. The various types of cable can be located with varying degrees of facility; but none may be considered undiscoverable.

6. The record of interruption of submarine cables by fishing vessels engaged in normal trawling operations is long, and the incidence of such interruptions is increasingly disturbing cable operating companies. Some 122 cases of damage have been reported off Newfoundland where the waters are of normal fishing depth, viz., about 200 fathoms, over three years 1955-57. The recent case of damage to a number of cables (4) within a short period (26 hours) is not unique; six out of seven cables owned by one company were unserviceable at one time during the three years previously mentioned. These interruptions to cable services have all been due to the fouling of the cables by the otter boards of the trawls of fishing vessels and to the immediate damage, or to the subsequent severance of the cable after hauling on deck to clear the trawling gear. The breakage of the American Telegraph and Telephone Company and Western-Union cables in the last week of February 1959 was almost certainly **due** to fishing operations of a Soviet trawler, the *Novorossisk*. The USSR have conducted trawling operations for scientific purposes at depths of up to 5,000 fathoms.

7. The use of cable-cutting shears and grapnels for the deliberate breakage of cables has been practiced by the German Navy and referred to overtly in at least one published record of personal war experiences. The technique is undoubtedly well known to the USSR who must be credited with the ability to deploy such equipment, possibly by means of nuclear submarines not readily detected. Surface vessels clearly may be similarly used.

8. Underwater explosion is also a practicable means of disturbing submarine cables. Very powerful explosions, either nuclear or high-explosive, are thought to be necessary to achieve any significant degree of damage unless the charge is laid in contact with the cable. Small charges laid in contact with the cable(s) - a readily achieved condition - provide an effective means of disruption.

Landlines, Microwave Links, Terminal Installations

9. The landline, microwave link, and co-axial cable feeders to trunk telecommunications circuits, and the terminal installations - whether traffic centres or transmitting, receiving or relay installations - are possible targets for sabotage. They may serve either cable routes or long-distance point-to-point radio circuits. The future protection of these services depends on the adoption of those counter-sabotage measures which have been recommended. These methods should provide substantial but not complete protection.

Radio Circuits

10. The preponderance of the traffic on British Commonwealth radio communications is passed at High Frequency. One Very High Frequency ionospheric forward-scatter radio circuit has been completed and is operated by the USAF between the United States and the United Kingdom. In addition to direct HF circuits, supplementary and/or alternative circuits

are available for United Kingdom-North American traffic by relay or retransmission via Barbados, Bermuda, Ascension Island, Cape Town, Melbourne, Sydney and Wellington. Part I of this paper defines the most important circuits and the Annual General Report of the Commonwealth Communications Board describes these and all other Commonwealth telecommunications. A considerable number of radio telephone and radio telegraph circuits are also operated by other countries, especially the United States, to give a wide diversity of circuits between Europe and North America. A certain very limited traffic capacity could be made available by utilising VLF, LF, and MF marine services. The basic great-circle paths of the circuits are shown in Figure 3.

Susceptibility of Types of Transmission to Interference

11. VLF and LF transmissions are subject to jamming; HF transmissions are subject to jamming and to disturbance of the ionosphere; VHF scatter transmissions, while less susceptible to ionospheric disturbance than HF transmissions, have proven more vulnerable to jamming than had been claimed by early advocates of the system. Traffic centres, microwave links and landlines to transmission points, as well as installations at these points, are possibly targets for sabotage, as has been discussed in paragraph 9.

Soviet Ability to Interfere with Radio Circuits

12 - (a) *By Jamming*

(i) *From Soviet Bloc Territory.* - Certain circuits, e.g., London-Sydney, are very susceptible to deliberate jamming when they are operated at optimum communications frequencies. Even direct United Kingdom-North American circuits are believed vulnerable to jamming by high-powered transmitters located in the USSR. The USSR command a powerful net of known ground-based broadcast-band jammers which could be supplemented by a large number of high-power broadcast transmitters in the same role. These transmitters are located such that propagation conditions could usually support jamming at United Kingdom and North American receiving stations when the communications circuits were operating at optimum frequency. The seriousness of the interference - which might be mitigated by a number of technical and operational expedients - could be greater if the USSR devoted all their available resources to the task. The considerable use of rhombic aerials is much to our disadvantage. It is unlikely, however, that even were the USSR to abandon internal broadcast and jamming services, they have sufficient transmitters completely to disrupt radio communications traffic between the United Kingdom and North America. Soviet occupation or control of Western Europe and/or North America, and the establishment there of high-power HF transmitters, would appreciably aggravate the situation. The distribution of known jammers and high-power (10kW. and above) broadcast transmitters probably radiating in the HF Band between 3 Mc/s and 30 Mc/s is shown in Figures 4 and 5.

(ii) *From Surface Vessels - Including Surface Submarines.* - The use of surface vessels to jam by ground-wave propagation HF relay points or receiving stations near coasts is possible provided the vessel can approach to within, say, 50 miles of the target. Low radiated power only can be provided by these means and the jammer is relatively vulnerable due to that revelation of its existence and position. Jamming from surface submarines at HF is considered impracticable against high-power circuits, although some success would be

expected against VHF ionospheric scatter circuits. Jamming from submerged vessels is not possible.

- (iii) *From Aircraft* - Airborne jammers would be very effective against VHF ionospheric scatter circuits, though power considerations lead to the conclusion that their use on other frequencies is impracticable.
- (iv) *From Clandestine Low-Power Jammers*. - The use of low-power close-range clandestine jammers against HF receivers or relay stations had been considered and is believed to be ineffectual. At best, such jamming would be of short duration due to the revelation of the existence and position of the transmitter. Against ionospheric scatter circuits such devices might be troublesome.

(b) *By Ionospheric Disturbance*

- (i) *HF Circuits*. - HF circuits have been shown to be susceptible to ionospheric disturbance exulting from the explosion of nuclear weapons with the USSR are capable of deploying. Shock waves from large explosion, whether nuclear or conventional, can also provide conditions of anomalous propagation in the ionosphere by changing the location concentration with consequent effect upon the critical frequency. The physical phenomenon causing the major effect from nuclear explosions is increased absorption due to increased electronic density. A similar effect may be produced by seeding the ionosphere with radio-active material is of appropriate half-life from rockets argued missiles. While it would be practicable to disrupt some of the available circuits for periods of, perhaps, a few days, by powerful (megaton) nuclear explosions, the effect over all the circuits for an appreciable effort is likely to be less than is normally observed during the periodic ionospheric storms due to solar activity. It has been said that 50, 10 megaton nuclear weapons properly placed could kill or injure at least 30 per cent of the population of the United States.²³ It is unlikely that the USSR could be assured that all radio-communications or even any particular radio-communication circuit, had been destroyed by these means.
- (ii) *The VHF Circuit*. - The VHF forward-scarer circuit is unlikely to be affected other than in a minor degree by short-term ionospheric disturbance - it is indeed, designed to minimise the effects of the perturbations of the ionosphere induced by solar activity. This circuit could, nevertheless, be interrupted briefly by the passage of the ionised gas and particular debris from a nuclear explosion across the path of the transmission. It could similarly be enhanced by the provision of, or improvement in, an artificial scattering mechanism in the absence, or deterioration, of the natural phenomena.

Conclusions

13. It is concluded that -

(A) it is possible for the USSR to: -

- (i) locate and cut allied submarine cables by the use of :-

²³ H. A. Kissinger. *Nuclear Weapons and Foreign Policy*. (New York: Harper & Bros., 1957). p.95.

- (a) surface or sub-surface vessels;
 - (b) grapnels, shears, underwater explosion or standard fishing trawl equipment;
 - (ii) jam trans-Atlantic HF radio circuits to an extent dependent upon the number of high-power transmitters devoted to the tasks. Complete interruption of existing circuits is thought to be impracticable with the number of transmitters known to be available to the USSR in the Soviet *Bloc*;
 - (iii) jam with a considerable degree of success, HF circuits crossing USSR territory or other territory contiguous to the USSR;
 - (iv) interrupt temporarily the HF radio circuits conveying traffic between the United Kingdom and North America by powerful (megaton) nuclear explosions in, or immediately below, the ionosphere, or by otherwise increasing the absorption of the D and E ionospheric layers;
- (B) traffic centres, landlines, microwave links, transmitters and receivers auxiliary to submarine cable routes and long-distance radio circuits are susceptible to sabotage.

10th May, 1961

**CABINET
JOINT INTELLIGENCE COMMITTEE**

SOVIET INTERDICTIONS OF ALLIED TELECOMMUNICATIONS

PART III - DEPLOYMENT AND USE OF SOIET CAPABILITIES

REPORT BY THE JOINT INTELLIGENCE COMMITTEE

In our Report at Annex we examine how and with what degree of success the Soviet Union is likely to use its known capabilities to disrupt those Allied telecommunications likely to be in use immediately preceding global war.

Conclusions

2. We conclude that if the Soviet Union exercises her interdiction capabilities:

(a) she is most likely to concentrate on the interdiction of military networks associated with the altering and launching of the West's nuclear retaliatory forces and disrupt those Allied telecommunications likely to be in use links between the United Kingdom and the United States;

(b) selected submarine cables could be cut without the purpose being immediately recognised by the West;

(c) the probability of success of jamming selected links of high strategic importance is sufficiently high to ale it necessary to assume that complete interruption could occur;

(d) it should be assumed that the Soviet Union would attempt to carry out jamming of ionospheric and tropospheric scatter systems;

(e) The Soviet Union almost certainly has aircraft equipped to jam Bomber Command and SAC VHF/UHF circuits;

(f) sabotage of focal points in the cable and radio communications system is a practicable and effective method of interdiction, and the Soviet Union is capable of planning and attempting such selective sabotage.

3. This is this third part of a report in five parts, and is designed to lead up to Part IV, which will be an assessment of the likely effects on Allied Trans-Atlantic Communications, and Part V which will contain recommendations for counter-measures.

4. Because it would be misleading to read this Part III isolated from the other Parts its distribution has been limited to within the intelligence community. Copies have been passed for comment to the American and Canadian authorities.

(Signed) H. S. STEPHENSON,

Chairman on behalf of the

Joint Intelligence Committee

Cabinet Office, S. W. 1,

27th April, 1961.

ANNEX TO JIC (59) 54 - PART III

PART III - DEPLOYMENT AND USE OF SOVIET CAPABILITIES

INTRODUCTION

In this part of the study we assess how, and with what degree of success the Soviet Union is likely to use its known capabilities to disrupt those telecommunications likely to be in use immediately preceding global war and which the Soviet Union considered to be vital to the West. We consider that Soviet interdiction on other occasions would, in general, be restricted to the jamming of news and propaganda broadcasts from the East, and that no attempt will be made to interfere with military and civil telecommunications. However, during periods of tension, *e.g.* over Berlin, and limited wars, the possibility of some Soviet interference with telecommunications cannot be entirely discounted. We believe that any interdiction in the circumstance would probable delimited to that which could be carried out from Soviet and satellite territory and, therefore, as this study covers these methods and the targets against which they could be used, we do not discuss separately possible Soviet action in circumstance short of global war. Further, we reiterate that communications between NATO countries, other than those between the United Kingdom and Canada, continue to be excluded from consideration.

INTERDICTION TARGETS

2. We consider that the most likely Soviet courses of action and, from her point of view, the most profitable, would be to interdict the cable and ration links between the United Kingdom and the United States, the military networks controlling nuclear retaliatory forces of the United Kingdom and the United States, and early-warning reporting links. Successful interdiction of those systems at a crucial time would seriously affect the West's ability to retaliate effectively, and it is likely that the Soviet Union is directing considerable effort to identifying and keeping up to date its target line of these systems.

3. However, the Soviet Union, either to prevent loss of surprise or because the interdiction of all the above systems was assessed to be beyond her capabilities, might choose to concentrate her initial effort on disruption the military systems directly concerned with altering and launching the West's nuclear retaliatory forces and, at the same time, mount relatively

inefficient operations against the remounted of the West's communications system as a whole, hoping that such operations would have at least an overall nuisance value.

4. Both the above courses of action (paragraphs 2 and 3) incorporate interdiction of the military communication network and systems controlling the nuclear retaliatory forces of the United Kingdom and the United States. We consider these systems to be the prime target of any interdiction effort.

METHODS OF INTERDICTION

Against Submarine Cables System

5. There are at present two modern cables in use. These can carry speech and telegraph. In addition there is a decreasing number of older cables which cannot carry speech. Plans have been made for the provision of three more modern cables in the next three years. Thus, it would not require a very large number of breaks to dislocate the system and to force traffic on to alternative (indirect) cable routes of low traffic handling capacity or on to radio links.

6. Against these cables the possible methods of attack are as follows:

- (a) cutting by trawlers;
- (b) cutting by submarines;
- (c) nuclear attacks on shore terminals;
- (d) underwater explosions using nuclear weapons;
- (e) sabotage of focal points in the cable communications system (the definition of these points in in paragraph 8 below).

7. Of these potential methods (a) would be the least difficult to implement. Although a successful operation would call for the co-ordination of activities in different places and for accurate timing and control, it would be a comparatively easy matter to position trawlers near certain selected cables, in readiness to haul up and cut them on receipt of a pre-arranged signal. Crewing of the trawlers by picked men (possibly of the Soviet Navy) would reduce the risk of compromise. In addition, as a result of the repeated accidental cutting of the cables by trawlers which had already occurred, it is possible that the West would not immediately appreciate that the cables had been cut deliberately with the intention of interrupting trans-Atlantic communications.

8. With regard to sabotage, we consider that the Soviet Union could effectively interdict communications by this means at focal points, *i.e.*, points between the cable terminal and the users, where alternative means of communications cannot be provided within the critical period.

9. It is unlikely that submarines and nuclear weapons would be used for cable-cutting, since they would be required for other tasks of higher priority or importance. Another factor against the use of nuclear weapons to destroy terminals is that in order to disrupt effectively strategic cable communications, *i.e.*, to stop trans-Atlantic discussion regarding the launching of the West's nuclear retaliatory forces, nuclear attacks would need to be launched before the main nuclear offensive and would this only serve to alert the West and precipitate retaliation.

Against Radio Communicants System

10. We consider that the main radio communications which the Soviet Union would wish to disrupt are:

- (a) long-range voice, telegraph and teletype radio link operating in the HF band (includes Bomber Command and SAC radio links);
- (b) links using ionospheric forward scatter;
- (c) tropospheric forward scatter circuits;
- (d) UHF/VHF communications (includes early-warning reporting links);
- (e) VLF communications;
- (f) associated landlines and ancillaries.

11. There are essentially four ways of disrupting the above circuits;

- (a) electronic countermeasures (mainly jamming);
- (b) sabotage of focal points in the communications system;
- (c) physical destruction of terminals;
- (d) ionospheric disturbances by nuclear explosions.

12. The arguments against the use of nuclear weapons to destroy terminals and create disturbances in the ionosphere are the same as those in paragraph 9 above. In addition high altitude nuclear explosions would create disturbances which might also cripple certain vital Soviet radio links, and in the case of nuclear weapons being used against terminals, we consider it unlikely that more than the main terminals of a few radio links could be destroyed.

13. The Soviet Union would, therefore, be left with two methods of disturbing the radio communications in paragraph 10 above - the use of electronic countermeasures and selective sabotage (including the sabotage of terminals).

14. *The Jamming of Long-range Communication* .- So far there is no evidence that the Soviet Union had used her considerable jamming resources in any major exercise, as might have been expected if jamming were part of the Soviet War plan. However, it may be, that in the interests of preserving the surprise value, her policy is to restrict operations to the disturbing of news and propaganda broadcasts. This would be sufficient to enable techniques to be tested and control procedure investigated. There is evidence to suggest that the Soviet Union is interested in obtaining wave propagation data, which, together with strict control and co-ordination, is essential to successful jamming. A wholesale jamming barrage by large numbers of transmitters would be disadvantageous to the Soviet Union herself and, therefore, intensive jamming of selected links of high strategic importance would seem to be the most likely Soviet course of action. Although we do not believe that such Soviet action would achieve complete interruption of all such circuits, the probability of this happening is sufficiently high to make it necessary to assume that it could occur.

15. *Jamming of Ionospheric and Tropospheric Scatter Systems* - Ionospheric scatter systems are vulnerable to in-beam and, to a lesser extent, out-of-beam jamming. In-beam jamming of trans-Atlantic links could be carried out from surface vessels or aircraft; out-of-beam

jamming, on the occasions when it is feasible, could be carried out from Soviet or satellite territory. Tropospheric systems are less easily jammed than the ionospheric systems; in particular, out-of-beam jamming is much more difficult. Although we have no evidence of Soviet intentions to jam these systems, we believe that it would be well within Soviet capabilities to do so. Consequently it should be assumed that the Soviet Union would attempt to carry out such jamming.

16. *Jamming of UHF/VHF Communications* - The most effective form of jamming ground-to-air UHF/VHF radio circuits is from aircraft, and it is almost certain that the Soviet Union has aircraft specially equipped for the purpose of jamming Bomber Command and SAC radio circuits operating on these frequencies. Regarding the jamming of ground-to-ground early warning reporting links, we consider that, because the Soviet Union is capable of jamming the EW radar itself, she would concentrate on this form of interference rather than attempt to carry out the more difficult operation of interdicting such links.

17. *Jamming of VLF Communications* - VLF communications are used to control Polaris-carrying submarines and, if required, could be used as an alternative to other forms of transatlantic communications which may have been successfully interdicted. The jamming of this form of communication is technically more difficult. Nevertheless we believe that the Soviet Union, appreciating the importance of VLF communications with Polaris submarines, would almost certainly attempt to interdict them, though with no guarantee of success.

18. *Sabotage of Focal Points* - We consider, as in the case of interdiction of the cables system, that the Soviet Union could effectively interdict radio communications at focal points (such as receiver/transmitter installations, relay points, and links between radio terminals and communications centres) by sabotage. Such selective sabotage could be directed against any of the systems referred to in paragraph 10 above.

CONCLUSIONS

19. We conclude that, if the Soviet Union exercises her interdiction capability:

- (a) she is most likely to concentrate on the interdiction of military networks associated with the alerting and launching of the West's nuclear retaliatory forces and selected cable and radio links between the United Kingdom and the United States.
- (b) selected submarine cable could be cut without the purpose being immediately recognised by the West;
- (c) the probability of success of jamming selected links of high strategic importance is sufficiently high to make it necessary to assume that complete interruption could occur;
- (d) it should be assumed that the Soviet Union would attempt to carry out jamming of ionospheric and tropospheric scatter systems;
- (e) the Soviet Union almost certainly has aircraft equipped to jam Bomber Command and SAC VHF/UHF circuits;
- (f) sabotage of focal points in the cable and radio communications system is a practicable and effective method of interdiction, and the Soviet Union is capable of planning and attempting such selective sabotage.

References

1. Aldrich, R.J., 'Whitehall Wiring: The Communications-Electronics Security Group and the Struggle for Secure Speech', *Public Policy and Administration* 28:2 (2012).
2. Aldrich, R.J., *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. (London: HarperPress, 2011).
3. Aldrich, R.J., *The Hidden Hand: Britain, America and Cold War Secret Intelligence*. (London: John Murray, 2001).
4. Andrew, C. and Mitrokhin, V., *The Mitrokhin Archive: The KGB in Europe and the West*. (London: Penguin, 2000).
5. Ball, D. and Windrem, R., 'Soviet Signals Intelligence (Sigint): Organization and Management', *Intelligence and National Security* 4:4 (1989).
6. Easter, David, 'Soviet Bloc and Western Bugging of Opponents' Diplomatic Premises during the Early Cold War', *Intelligence and National Security* 31:1 (2014, forthcoming).
7. Easter, David, 'Spying on Nasser: British Signals Intelligence in Middle East Crises and Conflicts, 1956-67', *Intelligence and National Security* 28:6 (2013).
8. Easter, David, 'Code Words, Euphemisms and what they can tell us about Cold War Anglo-American Communications', *Intelligence and National Security* 27:6 (2012).
9. Easter, David, 'GCHQ and British External Policy in the 1960s', *Intelligence and National Security* 23:5 (2008).
10. Garthoff, R.L., 'The KGB Reports to Gorbachev', *Intelligence and National Security* 11 (1996).
11. Goodman, M.S., *The Official History of the Joint Intelligence Committee, Volume 1: From the Approach of the Second World War to the Suez Crisis*. (London: Routledge, 2014).
12. Goodman, M.S., 'Jones' Paradigm: The How, Why, And Wherefore of Scientific Intelligence', *Intelligence and National Security* 24:2 (2009).
13. Kahn, D., 'Soviet Comint in the Cold War', *Cryptologia* 22:1 (1998).
14. Clark, I. and Wheeler, N.J., *The British Origins of Nuclear Strategy, 1945-1955*. (Oxford: Oxford University Press, 1989).
15. Stafford, D., *Spies Beneath Berlin*. (London: John Murray, 2003).
16. Twigge, S. and Scott, L., *Planning Armageddon: Britain, the United States and the Command of Western Nuclear Forces, 1945-1964*. (Amsterdam: Harwood, 2000).
17. U.S. Air Force, *Selected Readings from Soviet Military Thought, 1963-1973, Studies in Communist Affairs, Volume 5, Part 2*, (Washington: GPO, 1982).