




## The impact of 'Tempest' on Anglo-American communications security and intelligence, 1943–1970

David Easter 

### ABSTRACT

This article examines the impact of the discovery by Britain and the United States in the late 1940s/early 1950s that cipher machines produced compromising emissions, a phenomenon which became known as Tempest. The British and Americans were forced to develop security measures to protect their encrypted communications but the Soviet Union was still able to exploit Tempest emissions from cipher machines in Western embassies in Moscow and read their diplomatic traffic. At the same time, Tempest became an important new way for the NSA and GCHQ to gather communications intelligence, particularly from developing world states and NATO allies.

In the early years of the Cold War, Britain and the United States accidentally discovered that cipher machines produced electromagnetic and acoustic emissions which could reveal the original plain text of encrypted messages. Suddenly, many high level American and British code machines appeared vulnerable, raising the frightening possibility that the new Soviet enemy might be able to read their most secret diplomatic and military signals. The two allies had to urgently carry out research to determine the scale of the problem, which became known as Tempest, and develop counter-measures to secure their communications. At the same time though, Tempest opened up new ways for the American and British communications intelligence (Comint) agencies, the National Security Agency (NSA) and Government Communications Headquarters (GCHQ), to attack the ciphers of other states.

Tempest has since become an important field in information security.<sup>1</sup> The problem of compromising emissions was found to also affect other, non-classified types of communication and data processing equipment, such as fax machines, computers, keyboards and visual display units, and it was made public by the Dutch researcher Wim van Eck in 1985.<sup>2</sup> But there has been little academic writing on Tempest's early, Cold War history apart from brief sections in books on GCHQ and the NSA by Richard Aldrich and Stephen Budiansky, and an article by Ashley Sweetman on Tempest and Bank of England computers.<sup>3</sup> Official secrecy has been an obstacle to more in depth studies of how Tempest affected Anglo-American communications security (Comsec) and Comint. For a long time the American and British governments sought to keep these aspects of Tempest secret and they withheld relevant historical documents of the NSA, GCHQ and Central Intelligence Agency (CIA).

In recent years, however, there has been some loosening of the secrecy around Tempest's past. The NSA has released more Tempest related material, including the private papers of the eminent cryptologist William Friedman and internal histories of the American army's Comint branch, the Army Security Agency (ASA).<sup>4</sup> Similarly, the Canadian government has declassified documents from its former Comint agency, the Communications Branch of the National Research Council of Canada (CBNRC), which shed light on the American and British response to Tempest.<sup>5</sup>

Drawing on this newly released material and other American, British and Russian sources, this article will assess the impact of Tempest on Anglo-American Comsec and Comint in the first half of the Cold War. It will explain the complicated, piecemeal process by which the Americans and British discovered compromising emissions and examine how they tried, and sometimes failed, to secure their cipher machines from Tempest attack in the 1950s and 1960s. It will also show that Tempest became a central part of Anglo-American Comint operations, helping the NSA and GCHQ to read the encrypted traffic of developing world states, NATO allies, and perhaps the Soviet Union.

## Defining Tempest and compromising emissions

Originally Tempest was just an NSA cover name for studies on suppressing compromising emissions.<sup>6</sup> The emissions themselves were called 'radiation' or 'spurious radiation'. Over time though, through a process of association, the term 'Tempest' took on a broader meaning and was used loosely to describe both the problem of compromising emissions and measures to limit these emissions.<sup>7</sup> In this article 'Tempest' will refer to the problem of compromising emissions. Some authors have claimed that Tempest is an acronym of Transient Electromagnetic Pulse Emanation Standard or the more baroque Telecommunications Electronics Material Protected from Emanating Spurious Transmissions.<sup>8</sup> But these etymologies are incorrect – the word 'Tempest' was simply chosen from a cover name list by an NSA engineer in the early 1950s and did not originate as an acronym.<sup>9</sup>

Compromising emissions are unintentional intelligence bearing signals that can disclose the classified information received, processed and transmitted by communications equipment.<sup>10</sup> As a cipher machine operates, its contacts, switches, relays and other components can produce a range of compromising emissions. An NSA glossary explains that these emissions:

... may be divided into two basic types: electromagnetic and acoustic. Electromagnetic emanations consist of space radiations, stray magnetic fields, conducted signals, and power line modulation. Acoustic emanations consist of sound waves produced by mechanical motions and striking of parts in a functional relationship to the information being processed.<sup>11</sup>

By intercepting and analysing the emissions an opponent could reconstruct the original plain text of an encrypted message. In a worst case, compromising emissions can expose the internal processes of the crypto machine and reveal the cipher key.<sup>12</sup>

## The discovery of Tempest

The compromising emissions problem was discovered independently by the United States, Britain and Nazi Germany between 1943 and 1948, although the American authorities did not fully appreciate the dangers it posed until the 1950s. All three countries became aware of the issue through the development of a new kind of electromechanical cipher machine – the one-time tape cipher machine. These devices worked by generating a randomised key for teletypewriters that would never be repeated within messages and never reused.<sup>13</sup> Theoretically, one-time tape cipher machines were completely secure for if they had a truly random key and were employed correctly, they could create codes that were impossible to solve through cryptanalysis.<sup>14</sup> Their Achilles heel, it transpired, was that they were prone to producing compromising emissions. The first to spot this weakness was a group of researchers at Bell Telephone Laboratories in the United States in 1943. Bell was testing a teletypewriter tape mixer, the 131-B2, which was part of Sigtot, a one-time tape cipher machine just coming in service with the American army.<sup>15</sup> There were high expectations for Sigtot; an ASA report declared in 1946 that it could provide 'absolute security from cryptanalytic compromise.'<sup>16</sup> Unfortunately, Sigtot also copiously leaked compromising emissions.<sup>17</sup> The Bell engineers found that by analysing radiated and conducted signals from the 131-B2 and changes

in its magnetic field, they could recover most of the plain text of an encrypted message. In effect, they could bypass Sigtot's formidable one-time encryption.

Bell told the Army Signal Corps of its discovery and proposed adding shielding and filters to the 131-B2 mixer to reduce the compromising emissions but these modifications caused problems with heat dissipation and would have made Sigtot more difficult to operate and maintain.<sup>18</sup> The Signal Corps therefore rejected Bell's proposed solution and simply instructed military commanders to prevent enemy interception of emissions by securing an area 100 feet in diameter around their communications centres. Surprisingly, little further attention was paid to the issue. David Boak, an NSA Comsec specialist, later claimed in a classified lecture on Tempest that as the Second World War ended, 'most of the people involved went back to civilian life; the files were retired, dispersed, destroyed. The whole problem was plain forgotten.'<sup>19</sup>

Sigtot though was not unique. During the Second World War Germany and Britain also secretly developed one-time tape cipher machines, the Siemens T43 and Rockex, and these exhibited similar flaws. The Germans found that the T43 produced compromising electromagnetic emissions and in 1945 German prisoners of war revealed this fact to American interrogators, who seem not to have realised its significance.<sup>20</sup> Britain ran into the Tempest problem three years later with Rockex.<sup>21</sup> The body responsible for British Comsec, the Cypher Policy Board, reported a discovery that Rockex 'produces severe electrical radiation which can be readily intercepted in the vicinity of the machine, when decyphering, this radiation is such that clear text may be read directly without cryptanalysis.'<sup>22</sup> This was a major setback. Rockex had promised to give Britain fast, unbreakable encryption and since 1944 the Foreign Office had been installing the new equipment in its embassies, including sensitive posts such as Moscow and Washington.<sup>23</sup> Rockex was also being operated by GCHQ, the Secret Intelligence Service (SIS), the Canadian Department of External Affairs and the CBNR.<sup>24</sup> All these machines now appeared vulnerable.

In June 1948 GCHQ warned the CBNRC that Rockex was insecure in certain operating conditions because of its radio frequency radiation.<sup>25</sup> It is likely that the British passed on a similar warning to the American Army Security Agency. The United States and Britain closely cooperated in the collection of communications intelligence and GCHQ had supplied the ASA with several Rockex machines to use for exchanging Comint.<sup>26</sup> GCHQ would have needed to warn the ASA about Rockex's security flaw in order to protect the shared intelligence product. Certainly by 1949 the ASA was conscious of the dangers of compromising electromagnetic emissions: in December ASA specifications for a new American rotor cipher machine stipulated, under the heading 'Spurious Radiation of Clear Text', that 'There shall be no perceptible radiation of the clear text signal'.<sup>27</sup>

Nevertheless, the American Comsec authorities only seemed to grasp how serious the problem was when the CIA rediscovered the fault in Sigtot in 1951.<sup>28</sup> The agency had started deploying Sigtot to some of its embassy stations and CIA technicians encountered the same issues as Bell with the 131-B2 tape mixer.<sup>29</sup> They found that conducted signals from the mixer created a readable plain text of messages up to a quarter of a mile down the signal line. This time the discovery caused a much greater stir because Sigtot had been used since 1943 to encrypt presidential and high level army, air force and State Department communications. It was integrated into the Signal Corps' global teletype network in World War Two and operated by the military and State Department in London, Paris and Moscow.<sup>30</sup> Sigtot was also installed in the White House and put on the presidential aeroplane, railway carriage and yacht.<sup>31</sup> During the 1948–9 Berlin Blockade Sigtot was issued to the headquarters of the United States Air Force, the headquarters of Strategic Air Command and the 3rd Air Division deployed to Britain with Boeing B-29 bombers.<sup>32</sup> The device was still encoding air force communications in the on-going Korean War.<sup>33</sup> In short, some of the United States' most important and sensitive messages had been and were being sent via an insecure cipher system. A CIA internal history later recorded that 'A severe blow was struck when the 131B-2 one-time tape machine (SIGTOT) was declared vulnerable.'<sup>34</sup>

The Americans and British urgently sought to fix the security weaknesses of Sigtot and Rockex but although filters and shielding could be fitted to the machines, it was hard to stop the radiation of

compromising emissions.<sup>35</sup> The Armed Forces Signal Agency (AFSA) directed American military commanders to either establish a 200 foot security zone around communication centres or mask the emissions by operating at least 10 teletype devices at the same time.<sup>36</sup> Obviously, this was impossible in many locations and the AFSA recognised that they might have to get security waivers based on operational necessity. Furthermore, Boak later admitted that the '200 feet figure ... was quite arbitrary. It was not based on any empirical evidence that beyond such distance interception was impractical.'<sup>37</sup> Sigot struggled on in service till the late 1950s but it had to go through four major security modifications and many procedural changes.<sup>38</sup> The British produced three different models of Rockex in quick succession to try to iron out its Tempest weaknesses but it still proved difficult to operate the machine in some overseas posts because of the radiation danger.<sup>39</sup> The Americans and British also started to investigate the wider risks posed by compromising emissions. An Anglo-American Comsec conference in November 1953 agreed that 'radiation, conduction and induction from communication and crypto devices are potentially grave sources of insecurity' and noted that the topic was 'receiving detailed examination by both countries.'<sup>40</sup>

Much of this work was done by new communications security organisations in the United States and Britain. In October 1952 the NSA was set up by President Harry Truman, replacing the AFSA, and the following year it was given the lead role in communications security. Together with the ASA and the other service cryptologic agencies, the NSA tested American equipment for compromising emissions.<sup>41</sup> The process acquired the name Tempest. An NSA document in April 1954 gave Tempest as the cover name for 'General Studies on Radiation Suppression'.<sup>42</sup> 'Cadet' was the cover name of the NSA's more specific 'Radiation and Conduction Study on Cryptographic Equipments'.<sup>43</sup> On the British side, many of GCHQ's communications security functions were transferred in 1954 to a new Comsec body, the London Communications Security Agency (LCSA).<sup>44</sup> The LCSA had a Radiation Advisory Panel which examined the problem of radiation from cryptographic equipment.<sup>45</sup> The actual cipher machine testing and research was largely carried out by the Services Communication Development Unit (SCDU). The Treasury was periodically asked to provide the SCDU with more staff and facilities to help it test cipher machines for radiation and develop counter measures.<sup>46</sup>

The Anglo-American research effort slowly revealed the monumental scale of the problem. Studies showed that other cipher machines were insecure due to their radiation of plain text, including more of the supposedly impregnable one-time tape machines such as the American ASAM 2-1, which was in service with the US army, and the British Apparatus 5 UCO, operated by GCHQ and the NSA.<sup>47</sup> The NSA also found new vulnerabilities in crypto equipment. Testing electro-mechanical rotor cipher machines the agency realised that their rotor movements could be correlated with tiny fluctuations of voltage on the power line.<sup>48</sup> An ASA conference in June 1956 therefore included powerline modulation as one of the categories of compromising emissions, along with radiation, conduction and magnetic fields.<sup>49</sup>

NSA researchers then discovered the acoustic issue. An ASA internal history for fiscal year 1957 reported that investigations of acoustic emanations from cryptographic and communications equipment had 'showed approximately the same analytical results as the analysis of electrical emanations. Analysis of acoustical radiation, accomplished by NSA, enabled the reading of plain text.'<sup>50</sup> Cipher machines produced sonic as well as electromagnetic emissions and these could also betray the contents of messages.<sup>51</sup> For example, each key on a keyboard might have a unique acoustic signature making it possible to read the plain text of a telegram as it was typed into the cipher machine. It was not easy to capture acoustic emanations with sufficient fidelity – generally the microphone would need to be in the same room as the cipher machine – but microphones capable of detecting machine sounds had already been found concealed in American embassies in the Soviet Bloc.<sup>52</sup> The NSA and LCSA were particularly concerned about the acoustic vulnerability of the American TSEC/KL-7 and British Typex rotor cipher machines.<sup>53</sup> The KL-7 was widely used by the United States' army and other NATO militaries and in 1957 the NSA advised GCHQ and the CBNRC that it should only be operated in areas where the sounds of the machine could not be detected or

recorded by unauthorised persons.<sup>54</sup> The walls, floors, ceiling, electrical outlets and fixtures of the machine's cipher room needed to be checked as often as possible for hidden microphones. Any telephones within audible range of the KL-7 had to be inspected as well because they could be secretly tampered with to permit on the hook transmission and act as microphones. It was starting to appear that everything radiated.<sup>55</sup> An NSA official told the ASA that 'all crypto equipment was affected' by 'spurious radiation'.<sup>56</sup> A LCSA paper declared that 'spurious compromising signals' were 'radiated to some extent by all crypto equipment'.<sup>57</sup> The NSA later summed up the process of discovery in the 1950s as a 'Frankenstein House of Horrors'.<sup>58</sup>

## Countering Tempest

Gradually though researchers devised counter measures. In addition to shielding cipher machines and filtering and masking emissions, agencies developed low powered circuits that would inherently emit less electromagnetic radiation. In 1956 the United States Naval Research Laboratory built a low powered key device, the NRL Keyer, and installed it in the 131-B2 mixer. With some filtering and shielding this cut the mixer's compromising emissions range from half a mile to 20 feet.<sup>59</sup> The NSA quickly incorporated the NRL Keyer circuit into a new cipher machine, the TSEC/KW-26, which came into service in 1957. The KW-26 was fully electronic and with the NRL Keyer it produced less emissions than its electromechanical forebears like Sigto. According to an NSA history, if the KW-26 was employed in a low keying mode it 'was reasonably well protected' against Tempest emissions.<sup>60</sup> The machine went on to become the mainstay of American point to point cryptography in the 1960s. Over 14,000 KW-26s were built and it was taken up by the NSA, the CIA, the army, navy, air force and to a limited extent, the State Department.<sup>61</sup> The machine was also used by the British military and GCHQ.<sup>62</sup> As well as producing technical solutions, the NSA established the policy and institutional framework for improving emission security in the United States.<sup>63</sup> It created a joint policy on Tempest with the American armed services and issued document NAG-1, which set out Tempest measurement techniques and standards. A Special Committee on Compromising Emanations, led by the NSA, became responsible for applying these Tempest standards to American government and military cryptographic and communications equipment.

The American joint policy on Tempest was adopted by Britain and Canada as well but setting standards for the rest of NATO was a more complicated task, as it had to balance the conflicting requirements of Comsec and Comint.<sup>64</sup> While the Americans and British sought to improve NATO states' emission security and prevent the Soviet Union from reading their traffic, they also secretly spied on their European allies' encrypted messages and wanted to maintain this access. By the mid-1950s several NATO states had developed one-time tape teletype cipher machines and NATO had issued limited guidance in Allied Military Security Publication (AMSP) 292(B) on the precautions that should be taken when installing and operating one-time tape cipher systems to prevent compromising emissions.<sup>65</sup> The West German manufacturer Siemens had also discovered the problems of electromagnetic and acoustic radiation and it shared its findings with Crypto A. G., a Swiss cipher machine firm.<sup>66</sup> The two companies built safeguards into their machines to reduce emissions and this was potentially a threat to Anglo-American Comint because Crypto A. G. sold to many governments in Western Europe and the developing world. In 1953 its customers included France, Italy, the Netherlands, Belgium, Denmark, Norway, Turkey, Portugal, Spain, Sweden, Finland, Yugoslavia, Egypt, Iraq, Syria, Jordan, Lebanon, Ethiopia, Indonesia, Argentina, Brazil and Chile.<sup>67</sup> But with Tempest the devil was always in the detail and the Americans and British knew more about the phenomenon than the West Europeans. Furthermore, the United States had a privileged relationship with Boris Hagelin., the head of Crypto A. G.<sup>68</sup> At American request, he withheld his most secure equipment from sale to countries hostile to the West and he supplied sensitive information about Crypto A. G.'s customers. In 1957 Hagelin confided to an NSA representative that the French 'really weren't too knowledgeable' about compromising emissions.<sup>69</sup> He said the French had tested some

Crypto A. G. equipment and passed it as radiation secure even though it had not been fitted with all of the required Siemens' anti-radiation protection.

Richard Aldrich has shown that the LCSA and NSA used their superior knowledge of Tempest to preserve vulnerabilities in their allies' cipher machines.<sup>70</sup> They gave NATO members selective and incomplete security advice about compromising emissions that left scope for the Americans and British to carry on reading European traffic. The Director of the LCSA, Fred Stannard, explained to the Canadian Cipher Policy Committee in 1958 that with Tempest there were questions of 'how we may best distribute our responsibilities for advising our allies, particularly in NATO'.<sup>71</sup> GCHQ did not want information about compromising emissions to spread to 'countries or organisations from which signal intelligence is required'.<sup>72</sup> In March 1959 NATO published revised Tempest guidance, AMSP 522, but the paper appeared to omit crucial details.<sup>73</sup> According to a CBNRC internal history, 'It was considered necessary to reveal some general aspects of the radiation hazard to NATO nations; this resulted in ... AMSP 522, which dealt in general terms with the teletype problem only'.<sup>74</sup> The LCSA directed that for American, British and Canadian users the NATO guidelines should be supplemented by 'advice on certain aspects of the problem which it is undesirable to disseminate to NATO at large'.<sup>75</sup>

There was an element of hubris in all of this, for while the LCSA and NSA were scheming to keep their allies' cipher machines insecure, the Soviet Union was already exploiting Tempest weaknesses in British and American diplomatic crypto systems. The Soviets probably learned about compromising emissions from German prisoners captured in the Second World War and they called it PEMIN, an acronym in Russian of collateral electromagnetic radiation and interference (*pobochnye elektromagnitnye izlucheniia i navodki*).<sup>76</sup> In the 1950s the Soviets made offensive use of PEMIN, particularly in Moscow where the KGB could get in close to Western embassy buildings to intercept electromagnetic and acoustic emissions.<sup>77</sup> The Foreign Office recognised the danger and by 1959 it no longer used the Rockex cipher machines in its Moscow embassy for messages with a high security grade. Prime Minister Harold Macmillan was told in February 1959 that the embassy had to manually encrypt sensitive telegrams with book ciphers, probably one-time pads which were secure but considerably slower than machine encryption by Rockex.<sup>78</sup> The cipher clerks were not even allowed to speak to each other while coding in case they gave away something to Soviet eavesdroppers. In October 1959 the Foreign Office's fears were confirmed when microphones were found in the embassy's former cipher room and registry.<sup>79</sup> A subsequent inquiry concluded that the KGB bugs had intermittently compromised top secret and secret material between 1943 to 1958, apart from periods from 1945 to mid-1947 and November 1953 to January 1954 when the cipher room was located elsewhere in the embassy.

The KGB targeted the American Moscow embassy as well. In 1953 Soviet workers refurbishing a new embassy building for the United States secretly implanted a network of microphones, with one bug hidden in the wall of the military attaché's code and communications centre.<sup>80</sup> They also turned part of the building into an antenna by setting a large metal grill, 4 feet by 16 feet in size, into the concrete ceiling of a room next to the State Department communications centre.<sup>81</sup> A KGB team led by the cryptologist Nikolai Andreev analysed emissions from the embassy and constructed equipment to convert them into readable plain text.<sup>82</sup> The embassy still relied on a rotor cipher machine, the MEC, and Andreev later recalled that 'The main difficulty was to find the "weakness" of the electro-mechanical cipher machine standing in the US Embassy in Moscow: to determine, which parts of the machine produce[d] spurious emissions'.<sup>83</sup> By 1959 this had been done and the KGB was able to read some of the embassy's encrypted traffic.<sup>84</sup>

The Americans did not know about Andreev's breakthrough but like the British they feared for the security of their communications in Moscow. In September 1960 the State Department ordered its embassies in Moscow, Bucharest, Prague, Sofia and Warsaw to use manual one-time pads instead of cipher machines to encrypt all telegrams classified as secret or higher.<sup>85</sup> However, given the importance and volume of traffic from their Moscow embassies the Americans and British could not rely indefinitely on laborious, time consuming one-time pads for encryption. The solution they



came up with was to create special secure enclosures for embassy cipher machines, rooms within rooms, that would be shielded against acoustic and electronic eavesdropping. With the help of Bell Telephone Laboratories, the State Department and CIA built and tested prototype secure rooms in 1960–1 that could contain the emissions from cryptographic equipment.<sup>86</sup> The CIA's MK II secure room, which preformed best in the tests, had walls, ceiling and floor made of three layers of aluminium with the middle layer acting as a radio shield and an inner-most layer on soft rubber strips providing sound proofing.<sup>87</sup> The secure room was designed to be set up on acrylic pillars within an embassy room with enough clearance on all sides for a person to pass. Secure rooms were expensive, heavy and difficult to install – the MK II secure room weighed three tons – but the State Department, CIA and armed services started to place them in their most vulnerable overseas posts in the early 1960s.<sup>88</sup> The Foreign Office did the same, putting a secure room in Britain's Moscow embassy to house the cipher machines.<sup>89</sup>

The secure room programme was given extra impetus by a series of discoveries in 1964–65. In April State Department investigators discovered the concealed Soviet bugging and surveillance system in the American Moscow embassy.<sup>90</sup> The embassy code room had been shielded in 1962 or 1963 but the NSA and CIA believed that through the bugging 'the Soviets had achieved a major intelligence breakthrough, i.e. for period of years they had the capability to read most, if not all, of our telegraphic messages between Washington and Moscow'.<sup>91</sup> The United States briefed its NATO allies on the bugging system and advised them to review the security precautions in their Moscow embassies.<sup>92</sup> The West Germans accordingly swept their mission and found that the Soviets had secretly attached an electronic device to the embassy's teletype cipher machine.<sup>93</sup> The device appeared to amplify Tempest emissions and broadcast the text of a message as it was typed into the cipher machine, enabling the KGB to bypass the encryption. In late 1964 or early 1965 the French discovered something similar in their Washington embassy.<sup>94</sup> A fuse in the cipher room had been modified to act as a transmitter and relay Tempest radiation outside the embassy. The fuse was of non-Western specification and had sufficient transmission range to reach the house of the Soviet military attaché across the road. The device appeared to be effective, for in the 1962 Cuban Missile Crisis the KGB was able to give the Soviet leadership verbatim copies of French diplomatic traffic from Washington, although these might have come from a KGB agent code named JOUR in the French foreign ministry.<sup>95</sup>

Clearly, the Soviets were alarmingly proficient in using Tempest to break the ciphers of Western embassies and the discoveries in Moscow prompted the United States to accelerate and expand the roll out of secure rooms. By August 1964 electronically and acoustically shielded communication rooms had been installed at eight State Department and CIA overseas posts.<sup>96</sup> This increased to 15 by December 1965 with secure rooms in all the Soviet Bloc countries and there were plans to install a further 14 rooms in Latin America and Western Europe by July 1966. The British also deployed more secure rooms and by 1969 the Foreign Office had 25 cipher secure rooms in overseas posts.<sup>97</sup> As an additional defensive measure, the Foreign Office and State Department brought into service new, more secure cipher machines. With the help of the Canadians, GCHQ had developed a miniaturised version of Rockex, called Noreen, which was designed for use in areas where the threat of Tempest exploitation was most acute.<sup>98</sup> The machine produced few compromising acoustic or electromagnetic emissions and during the 1960s the Foreign Office installed Noreen in many of its Soviet Bloc embassies.<sup>99</sup> Similarly, in 1965 the State Department replaced all its elderly rotor and one-time tape cipher machines with new crypto equipment, the HW-28 and the TSEC/KW-7, which were engineered to minimise Tempest problems.<sup>100</sup> The combination of new cipher machines and secure rooms made State Department and Foreign Office communications far safer than they had been in the 1950s.

By the mid-1960s then the Americans and British had devised the technology and procedures to protect their cipher systems against Tempest attack. They fitted shielding and filters to their old cipher equipment, brought in a new generation of machines with low level keying modes, and installed acoustic and electromagnetic secure rooms in their most exposed embassies. This did not

mean that the Tempest threat to cipher machines had been totally vanquished. It was still necessary to ensure that equipment across all the different parts of government and military was properly protected and operated. Worrying gaps in security continued to emerge. For instance, a check of the communications at President Lyndon Johnson's ranch in Texas in 1965 showed that the cipher machine there leaked Tempest radiation.<sup>101</sup> Clear text radiations from classified messages sent or received by the ranch were getting into the open wire telephone carrier and microwave system to the city of Austin. Army technicians obtained readable signals near an overhead powerline ¾ mile from the ranch. Clearly more work needed to be done. But at least now the United States and Britain had the framework of a solution.

## Anglo-American offensive use of Tempest

Tempest was very much a double edged sword. While it posed a serious challenge to Anglo-American Comsec in the early Cold War, it also opened up new ways for the NSA and GCHQ to break into other states' encrypted communications. The American and British governments have not declassified any documents on this side of Tempest but accounts by former CIA and British Security Service (MIS) officers suggest that they were quick to seize upon its offensive potential. The first alleged case of the United States exploiting Tempest emissions was in an Anglo-American cable tapping operation in Berlin. In the late 1940s/early 1950s SIS secretly dug a series of tunnels in Vienna to tap underground telephone and telegraph landlines that carried Soviet communications.<sup>102</sup> Encouraged by the haul from the Vienna tunnels, SIS and the CIA tunnelled into the Soviet occupation zone in Berlin to also tap telecommunications cables there, in an operation codenamed PBJOINTLY. The Berlin tunnel tap became active in February 1955 and the CIA and SIS harvested a huge amount of Soviet voice and teletype traffic, with the encrypted material being sent to the NSA to try to decode.<sup>103</sup> Unfortunately, PBJOINTLY had been betrayed to the Soviets before digging even began.<sup>104</sup> The KGB had an agent in SIS, George Blake, and he passed on to Moscow details of the tunnel plan. To protect Blake from suspicion, the KGB allowed the operation to run for over a year but in April 1956 the Soviets staged a discovery of the tunnel and shut it down.

In a 1980 book on the CIA the journalist David Martin claimed that compromising emissions had played a part in PBJOINTLY.<sup>105</sup> Martin recounted how Carl Nelson, the head of the CIA's Office of Communications, had discovered that the Sigtot cipher machine gave off faint echoes of plain text, which he called transients, when it encrypted a message. The transients travelled down the wire with the encrypted messages for up to 20 miles and with the right equipment they could be intercepted and turned into copies of the original plain text. This is a clearly a description of Tempest emissions although Martin did not name it as such in his book and the claimed 20 mile range is an exaggeration. Nelson tested the material being intercepted in Vienna and found that he could detect transients of encrypted Soviet messages. It was supposedly this discovery that inspired the CIA's interest in tapping Soviet landlines in Berlin. Nelson built special equipment in Washington to convert the transients from the Berlin tap into plain text. According to Martin, the CIA did not inform the SIS that it had found transients in the Vienna traffic and Nelson never disclosed to Blake or any other British intelligence officer his technique for picking out plain text transients from encrypted messages.

Martin's book was based upon interviews with retired CIA personnel including, it appears, Nelson, but his claims have been contested. Other former CIA officers complained that Nelson had inflated his real role in PBJOINTLY and they denied that the CIA withheld any information from SIS.<sup>106</sup> The CIA's leading cryptanalyst Frank Rowlett, who was involved in the operation, later said that the tap did not pick up an echo effect in the traffic and it played no part in the processing of the telegraphic circuits at the CIA's Washington headquarters.<sup>107</sup> However, Rowlett was interviewed in the 1990s, before the NSA or CIA had released much material relating to Tempest and he may have wished to maintain official secrecy on the subject. As this essay has shown, the CIA did discover in the early 1950s that Sigtot produced compromising emissions and a recently declassified article in an NSA



internal publication, *Cryptologic Almanac*, substantiates some of Martin's claims.<sup>108</sup> Describing the origins of PBJOINTLY, the article stated that in the early 1950s, 'a CIA scientist discovered a flaw in a Soviet teleprinter system that rendered its encrypted traffic exploitable'.<sup>109</sup> Though Blake knew about the tunnel and the tapping of Soviet telephone lines 'he apparently had not been informed of the flaw on Soviet teleprinters that allowed analysts to exploit encrypted messages'.<sup>110</sup> The Soviets tried to institute better telephone security procedures on Berlin lines but they did not alter their teleprinter communication habits. As a result, the intercepted telephone conversations from the wiretap 'yielded only routine – but sometimes still interesting – information while decryption of teleprinter traffic produced high-quality intelligence'.<sup>111</sup> Sections of the *Cryptologic Almanac* article are still redacted and the declassified text does not make clear the nature of the flaw in the Soviet teleprinter but given the propensity of teletypewriters to produce spurious radiation, it does seem possible that the CIA and/or the NSA were exploiting Soviet Tempest emissions on the Berlin telephone or telegraph cables, perhaps picking up faint impulses from the electromagnets on teletype machines as they printed the plain text.<sup>112</sup>

At around the same time as PBJOINTLY, the British began to exploit the acoustic properties of rotor cipher machines in foreign embassies.<sup>113</sup> Embassy cipher clerks would normally reset their machines' rotors every morning before starting transmissions and by experimenting with Crypto A. G. machines, MI5 and GCHQ found that microphones could detect the sounds of these settings being made and differentiate between them. From this information GCHQ could determine the core position of the rotors and break the cipher. In spring 1956 an MI5 officer, Peter Wright, and an engineer gained access to the code room of the Egyptian embassy in London and modified a telephone next to a Crypto A. G. cipher machine to act as a microphone. The telephone bug captured the daily changes in the rotor settings and enabled GCHQ to read the embassy's communications throughout the Suez Crisis of October-November 1956. This technique of breaking ciphers through technical surveillance of the machines was codenamed Engulf. The Egyptians operated Crypto A. G. machines in all their embassies but globally they were divided up into four cipher key groups, each with different rotor starting settings.<sup>114</sup> So SIS carried out Engulf operations against selected Egyptian diplomatic posts abroad and within a year GCHQ had broken into every cipher group. Engulf was employed against other targets as well; probe microphones planted in the Greek and Indonesian embassies in London allowed GCHQ to read their traffic during the latter part of the Cyprus Emergency in the 1950s and the 'Confrontation' with Indonesia in the mid-1960s.<sup>115</sup>

GCHQ and MI5 next targeted the electromagnetic emissions of embassy teletype cipher machines. In the late 1950s Wright tapped the telecommunications cables of the French embassy in London and saw echoes of the plain text being carried along the output cable along with the enciphered message.<sup>116</sup> He could simply connect a teleprinter to the tap, amplify the signal and print out the plain text of top secret French diplomatic telegrams. By this method, between 1960 and 1963 GCHQ read the encrypted communications of the French embassy in an operation codenamed Stockade. The great success of Engulf and Stockade led the British government to create a Radiations Operations Committee (ROC) in 1960 which was chaired by Wright and had representatives from GCHQ, SIS and MI5.<sup>117</sup> The ROC organised and coordinated further Engulf operations in the United Kingdom and abroad. Wright later claimed that it 'was one of the most important committees in postwar British Intelligence. For ten years, until the new generation of computers came in at the end of the 1960s, ROC was crucial to much of the success of GCHQ's cryptanalytical effort'.<sup>118</sup> Tempest had become a central part of British Comint collection.

The British shared information about the Engulf and Stockade techniques with the NSA, CIA and Federal Bureau of Investigation (FBI) and these agencies carried out similar operations against diplomatic premises in the United States and internationally.<sup>119</sup> For example, in 1960 the FBI mounted a Stockade attack on the cipher machine of the French embassy in Washington and in 1966 the CIA and NSA bugged the Egyptian embassy in Montevideo in Uruguay.<sup>120</sup> The Montevideo embassy used a Crypto A.G. cipher machine that was on the same communications circuit as the Egyptian embassies in Moscow and London and if the NSA could break the machine's cipher, it

would be able to read all the encrypted messages on this circuit. One of the CIA officers in Montevideo, Philip Agee, recalled in his memoirs that the NSA:

... cannot break this code system mathematically but they can do so if sensitive recordings can be obtained of the vibrations of the encrypting machine when the [internal] discs clack to a stop. The recordings are processed through an oscilloscope and other machines which reveal the disc setting. Knowing the settings, NSA can put the encoded messages ... into their own identical machines with identical settings, and the clear text message comes out.<sup>121</sup>

In February 1966 two technicians from the CIA's Division D, which handled 'black bag' Comint jobs, secretly installed two contact microphones in the ceiling of an office directly below the Egyptian embassy's code room.<sup>122</sup> By analysing the recorded noises of the cipher machine the NSA could determine its settings. The following year, during the build up to the Six Day War between Egypt and Israel, the NSA was able to decrypt messages between Cairo and the Egyptian ambassador in Moscow.<sup>123</sup>

In their operations against the Egyptians the NSA and GCHQ benefitted from the fact that they already had sample copies of Crypto A. G. cipher machines and could probe them under laboratory conditions for Tempest weaknesses. Boak explained in a declassified NSA lecture that:

... the ideal way to exploit the radio frequency or acoustic emissions from a cipher equipment is to get the thing in a laboratory and test it very thoroughly and minutely to find out in what part of the spectrum, if any – the emissions are escaping and just what their characteristics are. Having done this, you know how to zero in your intercept equipment in the much more difficult environment where machines are actually operating, and your chances of success is much greater than if you have to go at it blind.<sup>124</sup>

It was obviously far harder for the NSA and GCHQ to acquire Soviet cipher machines as test samples and this probably hindered their efforts against Soviet targets. After PBJOINTLY many more attempts were made to exploit the Tempest emissions of Soviet military and diplomatic cipher machines. In 1959 Wright took part in an Engulf operation against the Soviet cruiser *Ordzhonikidze* while it was moored in Stockholm harbour.<sup>125</sup> Although the Anglo-Swedish surveillance team detected sounds from the ship's cipher machine, they never broke the cipher. During the Cuban Missile Crisis in October 1962 an NSA spy ship, USS *Oxford*, sailed in close to Cuba to capture electromagnetic and acoustic emissions from Soviet cipher machines on the island.<sup>126</sup> In the mid-1960s CIA technicians armed with Tempest detection equipment periodically visited agency owned properties next to the Soviet embassies in Montevideo and Mexico City.<sup>127</sup> From these clandestine observation posts they tried to intercept radiation from the embassies' cipher machines, though with meagre results. Agee wrote in his memoirs that in Mexico City 'attempts to pick up radiation from Soviet cryptographic equipment have been unsuccessful.'<sup>128</sup> The Soviet cipher machines may simply have been too well shielded.<sup>129</sup> When the danger from Tempest radiation was first discovered the KGB immediately built metal mesh cages to encase cipher clerks and their machines. By the 1970s counter measures in Soviet embassies mirrored those of the United States and Britain, with fully shielded enclosures and low-powered cipher machines that emitted weaker signals.

Tempest had a major impact on Anglo-American communications security and intelligence in the early Cold War. It rendered vulnerable many American and British crypto systems, including high level cipher machines like Sigtot and Rockex, and forced the allies to spend over a decade devising new ways to protect their communications. By the mid-1960s the NSA and LCSA had considerably improved American and British Comsec; a new generation of crypto equipment produced less Tempest radiation and secure rooms shielded cipher machines in exposed locations. But prior to this the Soviets were able to exploit compromising emissions from the American and British embassies in Moscow and spy on their diplomatic traffic. This raises the question of whether the United States exposed itself to attack by squandering an early lead over the Soviets in discovering compromising emissions. Serious American research into Tempest did not start until the early 1950s despite Bell reporting the fault in Sigtot back in 1943. The documents presently available do not fully explain why there was this delay and apparent amnesia around compromising emissions, but the

sequence of events that in the 1940s suggests that the Signal Corps and the American service Comint agencies failed to disclose critical security information with the British and the CIA. Certainly, in the Second World War and early Cold War the United States was still wary of sharing its Comsec secrets with the British.<sup>130</sup>

Once Tempest was properly discovered, the NSA and GCHQ quickly took it up as a tool for breaking into the communications of other states. It worked best when surveillance teams could get in close to a cipher machine in a fixed location, like an embassy, and the Comint agencies had to work with the CIA, FBI, SIS and MI5 to covertly place microphones and monitoring equipment. The Soviet Union was their priority target in the Cold War and the new evidence in *Cryptologic Almanac* supports Martin's claim that the CIA and NSA used compromising emissions to read encrypted Soviet traffic in Berlin. The greatest Anglo-American Tempest success though, seems to have been in operations against developing world and West European states in the late 1950s and 1960s. The memoirs of Wright and Agee show that GCHQ and the NSA exploited the acoustic and electromagnetic emissions from ciphers machines to read the secret messages of Egypt, Indonesia, France and Greece. It is highly likely that NSA and GCHQ employed these techniques against other countries as well. Crypto A. G. cipher machines were clearly vulnerable to acoustic attack and they were operated by many states of interest to American and British intelligence.

More fundamentally, Tempest helped redress the balance at a time when cryptography appeared to be gaining a decisive advantage in its continuous battle with cryptanalysis. In the late 1940s and 1950s technological advances made ciphers much harder to solve; one-time tape cipher machines held out the promise of complete security and the cryptographic strength of rotor machines was also improving as new machines were armed with more rotors and irregular rotor stepping movements.<sup>131</sup> A LCSA paper estimated in 1956 that 'The security of modern general purpose crypto systems is so high that cryptanalytic success against them will be extremely difficult, if not impossible.'<sup>132</sup> Tempest opened up an new avenue of attack: the NSA, GCHQ and KGB could bypass extremely secure ciphers and instead exploit the electrical or mechanical weak points of a crypto system. These types of side channel attacks would become a permanent feature of modern cryptanalysis, thwarting cryptologists' dreams of total security and making even the best cipher machines vulnerable

## Notes

1. Anderson, *Security Engineering*, 305–20; and Gehling, Ashley and Griffin, "Electronic Emissions Security," 305–10.
2. van Eck, "Electromagnetic Radiation from Video Display Units," 269–86.
3. Aldrich, *GCHQ*, 173, 215–8; Budiansky, *Code Warriors*, 199–201; and Sweetman, "TEMPEST and the Bank of England," 1086–7.
4. National Security Agency, Declassified Documents (NSA), William F. Friedman Collection of Official Papers, <https://www.nsa.gov/news-features/declassified-documents/friedman-documents/>; NSA, History of the Army Security Agency, <https://www.nsa.gov/news-features/declassified-documents/army-security-agency/>.
5. Canadian Foreign Intelligence History Project database (CFIHP) <https://carleton.ca/csids/canadian-foreign-intelligence-history-project/>.
6. NSA, Friedman Collection, A70072, Memorandum Engstrom to Friedman, Attachment: 'Office of Research and Development Task List', 16 June 1952.
7. CFIHP, Kevin O'Neil and Ken Hughes, History of the CBNRC, 1987, Volume V, Chapter XXIV, 3; and NSA, Donahue, "Static Magic," 1–2.
8. Bauer, *Secret History*, 343; Haslam, *Near and Distant Neighbours*, 241; and "The Tempest Surrounding Tempest," *Forbes*, 10 August 2000, <https://www.forbes.com/2000/08/10/mu9.html#3c0f3c5b1004>.
9. NSA, Donahue, 'Static Magic', 1.
10. CIA Freedom of Information Act Electronic Reading Room (CIA FOIA), Briefing paper on 'Hostile Exploitation of US Communications and Related Automated Systems', Annex C Glossary, May 1984.
11. *Ibid.*
12. National Archives and Records Administration (NARA), ISCAP Releases, A History of U.S. Communications Security (The David. G. Boak Lectures), Tenth Lecture – TEMPEST, July 1973, <https://www.archives.gov/files/declassification/iscap/pdf/2009-049-doc1.pdf> (Accessed 9 October 2019).

13. Government Attic, [www.governmentattic.org](http://www.governmentattic.org), The Achievements of the Signal Security Agency in World War II, Army Security Agency, 20 February 1946.
14. Kahn, *The Codebreakers*, 394–403.
15. Budiansky, *Code Warriors*, 199–200; and Sweetman, “TEMPEST and the Bank of England,” 1086–7.
16. Government Attic, The Achievements of the Signal Security Agency in World War II, Army Security Agency, 20 February 1946.
17. NARA, A History of U.S. Communications Security, Tenth Lecture – TEMPEST, July 1973.
18. *Ibid.*
19. *Ibid.*
20. Pröse, “Chiffriermaschinen,” 89–91; TICOM Archive, <http://www.ticomarchive.com/>, Report ‘OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cipher Teleprinter Machines’, TICOM I-45, 1 August 1945; NSA, Report “European Axis Signal Intelligence in World War II as revealed by “TICOM” Investigations and by other prisoner of war interrogations and captured material, principally German, Volume 2, Notes on German high level cryptography and cryptanalysis,” Army Security Agency, 1 May 1946.
21. Easter, “Protecting Secrets,” 159.
22. *Ibid.*
23. *Ibid.*
24. The National Archives (TNA), HW 9/27, CPB (48) 1, ‘Report by the Secretary for the year ended 31st July 1948’, 19 February 1949; CFIHP, O’Neil and Hughes, History of CBNRC, Volume IV, Chapter XIV, 13, Aldrich, *GCHQ*, 57–8.
25. CFIHP, O’Neil and Hughes, History of CBNRC, Volume V, Chapter XXIV, 3.
26. NSA, Annual Report Army Security Agency, Fiscal Year 1949, Historical Section G-2, 1952; NSA, Friedman Collection, A67163, Memorandum for Director Communications-Electronics, by Earl Stone, Enclosure, 4 November 1950.
27. NSA, Friedman Collection, A43478, Minutes of Army Security Agency Technical Committee Meeting No. 6, Item 47, 2 December 1949.
28. See note 17 above, 1973.
29. *Ibid.*; CIA FOIA, History of the Office of Communications, Chapter II, Section 2, Organisation and Administration, not dated; Johnson, *American Cryptology during the Cold War*, 221.
30. Thompson and Harris, *The Signal Corps*, 610, footnote 15.
31. *Ibid.*
32. NSA, Summary Annual Report, Army Security Agency and Subordinate Units, Fiscal Year 1949, Historical Section G-2, 1952.
33. Blood, *The Three Wars of Lt. Gen. George E. Stratemyer*, 80.
34. CIA FOIA, History of the Office of Communications, Chapter III, Section F, The Headquarters Signal Center, not dated.
35. See note 17 above, 1973.
36. *Ibid.*; NSA, Friedman Collection, A4045960, Circuit Discussion, not dated.
37. See note 17 above, 1973.
38. *Ibid.*, Fourth Lecture, One-Time Tape Systems, July 1973.
39. Easter, “Protecting Secrets,” 159; CFIHP, O’Neil and Hughes, History of CBNRC, Volume V, Chapter XX, 21.
40. NSA, Friedman Collection, A523031, Memorandum for members of AFSAC by Statler, Enclosure B, 15 February 1954.
41. Johnson, *American Cryptology during the Cold War*, 215–7, 222.
42. See note 6 above, 1952.
43. *Ibid.*
44. Aldrich, “Whitehall wiring,” 182; and Easter, “Protecting Secrets,” 158.
45. TNA, CAB 21/4970, Memorandum S(PM)(59) 21, “The Threat from Eavesdropping Devices,” 25 February 1959.
46. TNA, T220/1406, Letter L/192A/0124, Cypher Policy Board to Treasury, 17 December 1952; Letter AB 18 LCESA to Wyatt, 26 October 1959.
47. NSA, Friedman Collection, A522530, U.S Communication Security Equipment and U.K. Cryptographic Equipment, 1953; A44757, Official Report National Security Agency Field Commanders Conference, 28 March to 1 April 1955; CFIHP, O’Neil and Hughes, History of CBNRC, Volume V, Chapter XX, 24.
48. See note 17 above, 1973.
49. NSA, History of the Army Security Agency and Subordinate Units, Fiscal Year 1956, Assistant Chief of Staff, G2, 1958.
50. NSA, History of the United States Army Security Agency and Subordinate Units, Fiscal Year 1957, Assistant Chief of Staff, G2, 1959.
51. See note 17 above, 1973.
52. NSA, “TEMPEST: A Signal Problem,” 28.

53. CFIHP, CSE Documents – Cipher Security Group, 56–07-12 to 57–07-29, Telegram Director NSA to GCHQ, 6 June 1957; CSE Documents – Cipher Security Group, 57–06-14 to 57–07-30, Letter LCSA to Secretary, Cypher Security Group, 17 July 1957.
54. CFIHP, CSE Documents – Cipher Security Group, 56–07-12 to 57–07-29, Telegram Director NSA to GCHQ, 6 June 1957.
55. Johnson, *American Cryptology during the Cold War*, 221.
56. See note 49 above, 1958.
57. TNA, T220/1406, Letter LCESA to Wyatt, 26 October 1959.
58. Johnson, *American Cryptology during the Cold War*, 222.
59. NARA, A History of U.S. Communications Security, Tenth Lecture – TEMPEST, July 1973; and Johnson, *American Cryptology during the Cold War*, 222.
60. Johnson, *American Cryptology during the Cold War*, 222.
61. Klein, *Securing Record Communications*, 10–1.
62. TNA, DEFE 59/16, Report by the Defence Cryptographic Committee on “Standardisation of On-Line Cryptographic Equipment,” DSS 23/64 (Final), 26 May 1965.
63. NARA, A History of U.S. Communications Security, Tenth Lecture – TEMPEST, July 1973; NSA. Friedman Collection, A44645, Memorandum Frost to U.S. Communications Security Board, 6 December 1960.
64. See note 17 above, 1973.
65. CFIHP, O’Neil and Hughes, History of CBNRC, Volume V, Chapter XX, 25; NATO Archives Online, [https://archives.nato.int/Memorandum\\_SGM-645-56\\_Sampson\\_to\\_the\\_Chairman,\\_European\\_Communications\\_Security\\_Agency,\\_14\\_September\\_1956;NSA,\\_History\\_of\\_the\\_United\\_States\\_Army\\_Security\\_Agency\\_and\\_Subordinate\\_Units,\\_Fiscal\\_Year\\_1957,\\_Assistant\\_Chief\\_of\\_Staff,\\_G2,\\_1959](https://archives.nato.int/Memorandum_SGM-645-56_Sampson_to_the_Chairman,_European_Communications_Security_Agency,_14_September_1956;NSA,_History_of_the_United_States_Army_Security_Agency_and_Subordinate_Units,_Fiscal_Year_1957,_Assistant_Chief_of_Staff,_G2,_1959).
66. NSA, Friedman Collection A60669, Memorandum for the Record, Hagelin Negotiations by Friedman, 18 December 1957.
67. NSA, Friedman Collection, A4146578, “List of countries using Hagelin machines,” December 1953.
68. Mainwaring, “Division D,” 627–9.
69. NSA, Friedman Collection A60669, Memorandum for the Record, Hagelin Negotiations by Friedman, 18 December 1957.
70. Aldrich, *GCHQ*, 216–7.
71. *Ibid.*, 217.
72. *Ibid.*
73. See note 25 above, 14.
74. *Ibid.*
75. Aldrich, *GCHQ*, 217.
76. Johnson, *American Cryptology during the Cold War*, 221; Emelyanov, Larin and Butyrsky, ‘Prevrashchenie Kriptologii’; Haseltine, *The Spy in Moscow Station*, 237. Haslam and Easter give the acronym as PEMNI but that is not supported by Emelyanov, Larin and Butyrsky or Haseltine. See Haslam, *Near and Distant Neighbours*, 241; and Easter, “Protecting Secrets,” 164.
77. Johnson, *American Cryptology during the Cold War*, 221.
78. TNA, CAB 21/3233, Letter Millar to Brook, 11 February 1959; Minute Brook to Macmillan, 18 February 1959.
79. Easter, “Soviet Bloc and Western Bugging,” 43–4.
80. *Ibid.*, 34–6.
81. *History of the Bureau of Diplomatic Security*, 178.
82. Emelyanov, Larin and Butyrsky, “Prevrashchenie kriptologii”.
83. NARA, RG 59 State Department Central Decimal File, 1955–59, Box 493, File 116.11/1-59, Letter A-147 Dillon to Moscow, 13 February 1959; Central Foreign Policy File, 1963, Box 3140, File CR 12-3-US-USSR CR 12–3. Telegram 413 Moscow to State Department, 31 July 1963; and Emelyanov, Larin and Butyrsky, “Prevrashchenie kriptologii”. Translation by author.
84. Haslam, *Near and Distant Neighbours*, 241.
85. NARA, RG 59 Central Decimal File, 1960–1963, Box 208, File 116.1/1-162, Telegram 678 State Department to Moscow, 28 September 1960.
86. *Ibid.*, File 116.13/1-1460 Memorandum Haines to Dwinell, 3 October 1960; NARA, A History of U.S. Communications Security, Tenth Lecture – TEMPEST, July 1973; CIA FOIA, Memorandum by Executive Officer, 10 March 1961; CIA FOIA, Bell Telephone Laboratories, Final Test Report, Shielded Soundproof Booths, Contact SCC-28,160, 27 April 1961.
87. CIA FOIA, “MK II SECURE ROOM,” not dated.
88. *Ibid.*; NARA, A History of U.S. Communications Security, Tenth Lecture – TEMPEST, July 1973.
89. FO 366/3359, Brief for Secretary of State’s visit to Moscow, “British Embassy Building, Moscow,” 16 July 1964.
90. Easter, “Soviet Bloc and Western Bugging,” 44–45.

91. *History of the Bureau of Diplomatic Security*, 176; Foreign Relations of the United States, 1964–1964, Volume XIV, Soviet Union, Document 47, Report by State Department, “Estimate of Damage to U.S. Foreign Policy Interests,” 2 October 1964.
92. NARA, RG 59, Central Foreign Policy Files, 1964–66, Buildings and Grounds, Box 8, File BG Buildings & Grounds, Moscow 11/30/66, Telegram 1985 State Department to Paris, 19 June 1964; Telegram 1996 Paris to State Department, 27 June 1966.
93. Barron, *KGB*, 10–1.
94. Wright, *Spycatcher*, 241. Wright implies this was separate from the American Tempest attack on the French Washington embassy discussed below.
95. Fursenko and Naftali, “Soviet Intelligence and the Cuban missile crisis,” 70–1; and Andrew and Mitrokhin, *The Mitrokhin Archive*, 601.
96. Gale, U.S. Declassified Documents Online, <https://www.gale.com/intl/c/us-declassified-documents-online/>, Minute for President’s Foreign Intelligence Advisory Board, ‘Secure Room Installations’, 7 January 1966.
97. TNA, FCO 19/86, Minute by Askew, 25 June 1969.
98. CFIHP, O’Neil and Hughes, *History of CBNRC*, Volume V, Chapter XXII, 4.
99. *Ibid.*; Easter, “Protecting Secrets,” 160.
100. NARA, RG 84, Classified Central Subject Files, CR 7 Telecommunications, Services 1965, Airgram CA-5269 State Department to various posts, 6 January 1965, <https://catalog.archives.gov/id/75583397> (Accessed 10 October 2019); Kahn, *The Codebreakers*, 714; CFIHP, O’Neil and Hughes, *History of CBNRC*, Volume V, Chapter XX, 34.
101. Lyndon Johnson Presidential Library, National Security Action Memorandums, NSF, Box 5, NSAM 315: Communications Security Survey, 10/29/1964, Survey of Technical and Physical Security Protection for the Presidency, 30 April 1965.
102. Stafford, *Spies Beneath Berlin*, 18–32.
103. Aldrich, *GCHQ*, 172–173; Vogel, *Betrayal in Berlin*, 210–1; Stockton, *Flawed Patriot*, 93.
104. Vogel, *Betrayal in Berlin*, 125–7, 252–3, 277–83.
105. Martin, *Wilderness of Mirrors*, 72–6, 84–5, 100–1.
106. Stafford, *Spies Beneath Berlin*, 33–7; and Bayard, *Flawed Patriot*, 94–5.
107. Murphy, Kondrashev and Bailey, *Battleground Berlin*, 206–7; and Stafford, *Spies Beneath Berlin*, 37.
108. NSA, *Cryptologic Almanac 50th Anniversary Series*, ‘The Berlin Tunnel Part 2: The Rivals’, March–April 2002.
109. *Ibid.*
110. *Ibid.*
111. *Ibid.*
112. *Cryptome* website, e-mail Dave Emery to John Young, 15 January 2000, <https://cryptome.org/tempest-old.htm> (Accessed 10 December 2019).
113. Wright, *Spycatcher*, 81–5.
114. *Ibid.*, 84, 109.
115. *Ibid.*, 113.
116. *Ibid.*, 109–12.
117. *Ibid.*, 114.
118. *Ibid.*
119. *Ibid.*, 145–8, 241.
120. *Ibid.*, 146, 241; Agee, *Inside the Company*, 474–8.
121. Agee, *Inside the Company*, 475.
122. *Ibid.*, 474, 478, 480.
123. Aid, *The Secret Sentry*, 134.
124. NARA, A History of U.S. Communications Security, Fourth Lecture, One-Time Tape Systems, July 1973.
125. Wright, *Spycatcher*, 113–4.
126. Bamford, *Body of Secrets*, 110.
127. Agee, *Inside the Company*, 350–1, 528.
128. *Ibid.*, 528.
129. Sheymov, *Tower of Secrets*, 76, 86, 141, 146.
130. Aldrich, *GCHQ*, 98–99.
131. Budiansky, *Code Warriors*, 184–188.
132. TNA, CAB 21/4003, Memorandum COMSECA (56) 5, LCSA, 30 July 1956.



## Acknowledgements

The author is grateful to the generous assistance of Professor Michael Goodman, Alan Barnes and the Canadian Foreign Intelligence History Project

## Disclosure statement

No potential conflict of interest was reported by the author.

## Notes on contributor

*Dr David Easter* is a Lecturer in the Department of War Studies at Kings College London. His research interests are intelligence, communications security and the Cold War. He is currently writing a book on GCHQ and Britain's withdrawal from empire.

## ORCID

David Easter  <http://orcid.org/0000-0001-6561-7851>

## Bibliography

- Agee, P. *Inside the Company: CIA Diary*. Harmondsworth: Penguin, 1975.
- Aid, M. *The Secret Sentry: The Untold History of the National Security Agency*. New York: Bloomsbury Press, 2009.
- Aldrich, R. *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. London: Harper Press, 2010.
- Aldrich, R. "Whitehall Wiring: The Communications Electronics Security Group and the Struggle for Secure Speech." *Public Policy and Administration* 28, no. 2 (2012): 178–195. doi:10.1177%2F0952076712458111.
- Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: Wiley Computer Publishing, 2001.
- Andrew, C., and V. Mitrokhin. *The Mitrokhin Archive: The KGB in Europe and the West*. London: Allen Lane, 1999.
- Anonymous. "TEMPEST: A Signal Problem." *Cryptologic Spectrum*, 2, no. 3 (1972): 26–30. <https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf>
- Anonymous. *History of the Bureau of Diplomatic Security of the United States Department of State*. Washington D.C.: Global Publishing Solutions, 2011.
- Ashley, R., R. Gehling, and T. Griffin. "Electronic Emissions Security: Danger in the Air." *Information Systems Management* 22, no. 4 (2007): 305–310. doi:10.1080/10580530701586011.
- Bamford, J. *Body of Secrets*. London: Arrow Books, 2002.
- Bauer, C. *Secret History: The Story of Cryptology*. Boca Raton: CRC Press, 2016.
- Blood, W., ed. *The Three Wars of Lt. Gen. George E. Stratemeyer: His Korean War Diary*. Washington D. C.: United States Government Printing Office, 1999.
- Budiansky, S. *Code Warriors: NSA's Codebreakers and the Secret Intelligence War against the Soviet Union*. New York: Alfred A. Knopf, 2016.
- Donahue, T. "Static Magic: The Wonderful World of Tempest." *Cryptolog* 10, no. 11 (1983): 1–2. [https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologs/cryptolog\\_84.pdf](https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologs/cryptolog_84.pdf)
- Easter, D. "Soviet Bloc and Western Bugging of Opponents' Diplomatic Premises during the Early Cold War." *Intelligence and National Security* 31, no. 1 (2016): 28–48. doi:10.1080/02684527.2014.926745.
- Easter, D. "Protecting Secrets: British Diplomatic Cipher Machines in the Early Cold War." *Intelligence and National Security* 34, no. 2 (2019): 157–169. doi:10.1080/02684527.2018.1543749.
- Emelyanov, G., D. Larin, and L. Butyrsky. "The Transformation of Cryptology into a Fundamental Science' [Prevrashchenie Kriptologii V Fundamental'nuĭ Nauku]." *BIS Journal* 10, no. 3 (2013). <https://ib-bank.ru/bisjournal/post/228>.
- Fursenko, A., and T. Naftali. "Soviet Intelligence and the Cuban Missile Crisis." *Intelligence and National Security* 13, no. 3 (1998): 64–87. doi:10.1080/02684529808432494.
- Haseltine, E. *The Spy in Moscow Station*. London: Icon Books, 2019.
- Haslam, J. *Near and Distant Neighbours*. Oxford: Oxford University Press, 2015.
- Johnson, T. *American Cryptology during the Cold War, 1945-1989, Book 1: The Struggle for Centralisation, 1945-1960*. Fort Meade: Center for Cryptologic History, NSA, 1995.
- Kahn, D. *The Codebreakers: The Story of Secret Writing*. New York: Scribner, 1996.
- Klein, M. *Securing Record Communications: The TSEC/KW-26*. Fort Meade: NSA, 2003.

- Mainwaring, S. "Division D: Operation Rubicon and the CIA's Secret SIGINT Empire." *Intelligence and National Security* 35, no. 5 (2020): 623–640. doi:10.1080/02684527.2020.1774854.
- Martin, D. *Wilderness of Mirrors*. New York: Harper & Row, 1980.
- Murphy, D., S. Kondrashev, and G. Bailey. *Battleground Berlin: CIA Vs KGB in the Cold War*. New Haven: Yale University Press, 1997.
- Pröse, M. "Chiffriermaschinen und Entzifferungsgeräte im Zweiten Weltkrieg: Technikgeschichte und informatikhistorische Aspekte." PhD diss., Leipzig University, 2004.
- Sheymov, V. *Tower of Secrets: A Real Life Spy Thriller*. Annapolis: Naval Institute Press, 1993.
- Stafford, D. *Spies Beneath Berlin*. London: John Murray, 2013.
- Stockton, B. *Flawed Patriot*. Washington D.C.: Potomac Books, 2006.
- Sweetman, A. "TEMPEST and the Bank of England." *Intelligence and National Security* 33, no. 7 (2018): 1084–1091. doi:10.1080/02684527.2018.1499356.
- Thompson, G. R., and D. Harris. *The Signal Corps: The Outcome (Mid-1943 Through 1945)*. Washington D.C.: Center of Military History, United States Army, 1991.
- van Eck, W. "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" *Computers and Security* 4, no. 4 (1985): 269–286. doi:10.1016/0167-4048(85)90046-X.
- Vogel, S. *Betrayal in Berlin*. London: John Murray, 2019.
- Wright, P. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. Toronto: Stoddart Publishing, 1987.