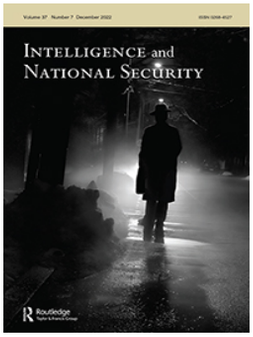

Intelligence and National Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fint20

Project Spaceman: early British computer security and automatic data processing

Richard J Aldrich & JD Work

To cite this article: Richard J Aldrich & JD Work (2022): Project Spaceman: early British computer security and automatic data processing, Intelligence and National Security, DOI: 10.1080/02684527.2022.2139342

To link to this article: https://doi.org/10.1080/02684527.2022.2139342

Published online: 10 Nov 2022.

INTELLIGENCE AND NATIONAL SECURITY
https://doi.org/10.1080/02684527.2022.2139342

Routledge
Taylor & Francis Group

ARTICLE

OPEN ACCESS Check for updates

Project Spaceman: early British computer security and automatic data processing

Richard J Aldrich and JD Work

ABSTRACT

Much has been written about the prehistory of 'cyber' and computer security in the United States, but we know less about other countries. This essay seeks to examine early British efforts in this field and especially attacks by 'Tiger Teams' against ICL mainframe computers that were being deployed by MI5 and other agencies. Over 2 years, a sophisticated programme was completed. It argues that a severe expertise shortage ensured a degree of convergence and later outsourcing to ICL. This pioneering work also paved the way for 'Project Spaceman' which offered government highly secure options together with encryption in the mid-1980s.

The pre-history of computer security

As Michael Warner has argued, the 'cyber' issue is not new, but instead has taken over 50 years to develop. By the time, the general public finally noticed the importance of this subject, a circle of *cognoscenti* had already been working on these problems for decades. A somewhat linear path can be traced characterised by rapid acceleration in the 1970s since previously computers were viewed mostly as mere 'filing cabinets' or calculating machines, but then quickly became integrated into a wide variety of government operations as automatic data processors and then management information systems. The most critical function was perhaps strategic warning at locations such as NORAD.[1] Not only were these among the earliest mission critical systems in which failure could not be tolerated, early warning and other nuclear command and control architectures represented some of the most complex compute environments then yet assembled.[2] Exploitation of these environments in order to alter nuclear release orders or shift aircraft mission taskings was very much on the minds of forward-looking observers – with speculative fiction raising the potential of what we would now call offensive cyber operations executed through self-propagating malware as early as 1975.[3]

The United States took the lead in encouraging the then nascent focus on computer security to protect these systems, hosting an annual government computer security conference. By 1990s, a series of extended debates had not only set standards for computer security but also framed the options available to policy-makers. In each decade the horizon expanded, with government computers no longer serving as mere reservoirs of data and gradually becoming incorporated into military arsenals.[4] Similar developments were taking place within the superpower competitor, and the questions of advancement and security of computers for air defence, troops control, and strategic nuclear missions in the Soviet Union became of great importance to the Western intelligence community.[5]

One of the most important dynamics was the early rejection of a simple technical fix. By late 1960s, it was clear that the issue of securing data was not strictly mechanical, since humans and technical systems increasingly interacted around multiple levels of classification. Moreover, those

CONTACT Richard J Aldrich r.j.aldrich@warwick.ac.uk

who accessed the data were no longer a few specialists but consisted of larger numbers of communicators. As those with necessary access to the information that computers stored and transmitted grew exponentially, so did the possibilities for criminal activity and even espionage. The 1970s were especially important and saw a number of computer programming innovations to improve security, such as administrator privileges, file system permissions and hashed passwords. Another innovation was encryption of data flowing between computers.[6] These controls were introduced following penetrating testing and red team reviews, and through the early development of formal models of weakness and exploitation – driven by work on classified US government activities for the Defense Advanced Research Projects Agency (DARPA), the National Science Foundation, and the US Atomic Energy Commission that were only just emerging into open publications.[7] In short, computer security and privacy would have to depend on 'hygiene' as well as hardware. This was not viewed as a simple matter of security but also of privacy, something that Capitol Hill was already deeply interested in. But while this fascinating landscape of early computer security is now being explored – as yet it remains a mostly American story.[8]

Creating Bureau West

Britain was a significant post-war computer pioneer with more companies than the United States. Much has been written about this early British computing boom, but rather less on early British computer security.[9] In terms of cutting-edge developments, historians have often associated the use of mainframe computers with Government Communications Headquarters (GCHQ) and the Atomic Weapons Research Centre at Aldermaston (AWRE). But while these bodies certainly took care over to protect their own installations, they did not take a national lead on computing security.[10] GCHQ's security component, the Communications-Electronics Security Group (CESG), was mostly concerned with the design and defense of encryption machines for government, working with other bodies to defeat electronic eavesdropping and 'tempest' problems.[11]

Electronic defence and attacks, including infosec and compusec, were in fact a highly disaggregated field in post-war Britain. It included important players like the Post Office who were taking the lead on secure speech and who were moved into the private sector in 1980s. While GCHQ boasted about 500 scientists and technicians, British Telecom sometimes commanded almost 10 times that number, many of them based at its impressive research centre in Martlesham in Suffolk. Even larger was the Ministry of Defence, with numerous research establishments, including the Royals Signals and Radar Establishment at Malvern, which developed a great range of projects including the electronic aspects of counterterrorism.[12] Indeed, the Ministry of Defence was simply a huge centre of post-war government science and intelligence.[13] Employing 200,000 civilians and over 300,000 service personnel, it was five times the size of the largest of the civil departments. By 1960s, its computers had mostly been used for mundane activities, such as personnel, payroll records and tracking stores. But by 1970s, their application was much wider ranging from battlefield surveillance to data processing for Britain's Polaris missile system. Moreover, with a budget of about £4 billion it superintended about a dozen defence research establishments, most of which had some computing capacity. Computers were increasingly a core activity for the Ministry of Defence and with this came security concerns.[14]

In 1972, reflecting these wider developments, the government set up the Central Computer Agency to advise across Whitehall. Its public role was to act as an agent for Government Departments purchasing computer equipment, but privately it also enjoyed other functions, including co-ordinating with the United States in the area of computer security.[15] It was divided into six sections: C1 looked after departmental projects across Whitehall. C2 superintended general policy. C3 was technical and was largely concerned with validation of the ICL 2900 range. C4 was based in Norwich and did the contracting for government computers. C5 focused on telephones and telecommunication. C6 was effectively a small stable of consultants who had extensive experience in the private sector, who were used to give advice on individual ministry projects.[16]

Alongside this, the MoD created an Automated Data Working Party under Admiral James Eberle to coordinate policy across all three services. Conversations with the major computer companies, including Britain's leader – International Computers limited (ICL) – suggested that computing power would accelerate fast, the cost of hardware would decrease and software would also be relatively cheap, which was true. The ICL also argued that the future was big mainframes with 'dial in' access, not mini-computers or networks, which in the long term proved to be wrong. This led to the growing demand for a small number of centralised computer bureaus with high-speed data links. The MoD's first proposed site was 'Bureau West' near Devizes in Wiltshire.[17]

Bureau West was envisaged as the first of a number of hubs. This view was underpinned by the MoD's 'Grid 77' study that predicted an expected tenfold increase in defence computing by early 1980s. It suggested four major computer centres as the focal points of a massive bureau grid that would take over all MoD data processing activities then handled by about 60 separate computers.[18] Predictably, there were multiple rivalries over location. Initially, the proposed site at Bureau West competed with the possibility of developing RAF Rudloe Manor, another centre of secretive defence science near Corsham. On 1 April 1974, work began, but the new centre also competed with a rival computer complex at Bath focused on naval logistics.

The first computer system delivered to Bureau West was accepted and brought into operational use in late 1976.[19] Opened with fanfare by Sir Frank Cooper, the MoD's permanent undersecretary, the project cost £5.5 million and centralized the work hitherto undertaken by 16 departments. Cooper boasted that the centre was equipped with one of the most powerful computers in Europe. It used ICL 2980 machines, the largest model in the 2900 range, and these were linked to terminals at various user locations. The 2980 was in fact installed at Devizes in mid-1975, but it took some time to pass its initial site trials and to work well enough to be accepted by the Central Computer Agency. Dr Peter Nutter, director of the bureau, admitted that the failures to pass the site trials were caused mainly by hardware reliability problems and these sorts of problems would continue to dog Bureau West.[20]

The problems were not local. Created in 1969 by Harold Wilson, ICL, who supplied the machine, it was a state-sponsored amalgam of many British computing firms, effectively the British Leyland of the data processing world. The main ingredients were several competing British computer manufacturers: ICT, English Electric-Leo-Marconi and Elliott Automation, themselves the products of previous mergers. The intention was to persuade them to join forces against American competition.[21] ICL was not commercially successful and by 1972, amid a world-wide recession, the Cabinet Office was panicking about the level of government subsidy ICL required to stay afloat at a time of austerity, together with the poor performance of the machines. Edward Heath's Central Policy Review Staff conducted an investigation and took initial advice from Joe Hooper, the Intelligence Coordinator in the Cabinet Office, who had previously served as Director of GCHQ. For the purposes of their review, Hooper offered them the services of Teddy Poulden, a naval officer who had been Senior UK Liaison Officer Washington (SUKLO) and later head of technology at GCHQ.[22]

Poulden enjoyed a unique comparative perspective on ICL as GCHQ was one of the few British government organisations that was allowed to buy the rather better IBM machines. He was also familiar with the position of the National Security Agency on computer procurement, and therefore understood what ICL's main competitor was doing. Accordingly, he argued that ICL was just not selling enough machines to generate the revenue to support effective research and development. Only a merger with a foreign competitor like Honeywell, he argued, would resolve this problem. Ministers were dismayed and rejected his advice, bringing in new management with past IBM experience. But his thoughtful recommendations eventually proved prescient, with ICL gradually being taken over by Fujitsu in late 1980s and 1990s.[23]

Partly for this reason, GCHQ had maintained a deliberately distant relationship with ICL. Although they had one ICL machine they treated it like a classic car that required special care and maintenance. Instead, their large-scale data processing was undertaken using US machines, mostly IBMs, but also

UNIVAC and Crays. Because of the limitations and problems encountered with ICL machines, GCHQ had progressively less and less influence on overall UK computer policy, indeed John Ferris documents a rather frosty relationship that resulted between GCHQ and the UK computing industry in 1970s. This effectively ceded the landscape of mainstream computer security to the MoD and the Home Office.[24]

Meanwhile, ICL promised better performance from its New Range 2900 machines and on this basis, they were purchased by not only Bureau West but also many other government departments, including RRE Malvern.[25] Therefore, 'Bureau West' was in a sense a test-bed for the concept of using a large bureaux to handle a variety of intelligence, security and defence work, emerging as the first of four such planned defence computing centres.[26] In fact, it became the only hub and grew ever bigger. Bureau West existed as an independent entity until early 1984, when it was amalgamated with Defence Data Processing Service, together with the small systems capability of Defence Administrative Computer Division to create the Directorate of Central Computer Services, a powerful central facility for the exploitation of all aspects of computing and communications in the defence information technology area.[27] However, even in the 1990s, defence officials still habitually and affectionately referred to their Devizes computing facility as 'Bu West'.

Tiger teams

Because of the wider range of tasks being allocated to computers, not least work for Britain's independent nuclear deterrent, security was becoming vitally important. The government's purchase of a number of New Range machines provided an obvious moment for security testing. It was not just the scale but the sensitivity of their employment. In late 1975, MI5 was moving its registry into a new building at Curzon Street House while also upgrading its computer systems.[28] Hitherto, it had run the ICL 1900 series, but it was now moving to a dual 2900 with additional memory provided by 100 disks. Remarkably, this vast arrangement provided less memory than a basic smart watch has today – but still vast for its time.[29] Meanwhile, a new ICL 2966 mainframe computer was being installed at Jubilee House, Putney, which was used to run the national crime statistics database.[30] Security testing was therefore required rather urgently, including deliberate red teaming efforts to model attacks.

The biggest problem was capacity. Because Nutter already had 'practical experience in the past of operating attack teams', he knew that the real challenge was finding competent members for his team, since most of the likely people were over-stretched and busy implementing the very systems that he needed to test. Because the 'specialist expertise required by members of such attack teams was in very short supply', he suggested that they undertake the exercise 'on as broad a front as possible' and in cooperation with 'all others with a similar problem'. Accordingly, the 'prime function' of his working group of five people was not so much planning the various attacks in detail but 'negotiations' with a range of departments for the full-time or part-time release of those he needed.[31] Many found the task interesting and were keen to help, but few were available, with the eventual team being drawn from Bureau West, the Defence Operational Analysis Establishment and the maths lab at RSRE Malvern.[32] Two further 'Tiger Tests' were run at DOAE and RSRE. Nutter had the final reports completed and finalised by April 1978.[33]

Who were the best potential attackers for these red teaming efforts? They tended to be self-taught enthusiasts from the Army's Royal Signals Regiment. Two officers, Kenneth Hunt and Tony Sammes, had seen the future, and even in the 1960s were running volunteer evening courses in systems analysis at the Royal School of Signals at the Blandford Forum. These two figures would become sequentially Professor of Computer Science at Shrivenham. Sammes would preside over the introduction of the pathbreaking 'Project Wavell' in the 1970s. Later, he would become Britain's pioneering professor of digital forensics.[34] Nutter wanted Sammes to join the attack team but was too busy with Wavell and Hunt could only make a small contribution.[35]

'Project Wavell' was a large-scale battlefield surveillance system and automatic data processing systems for the British Army of the Rhine.[36] Planned and developed through the 1970s this was an especially ambitious system, and its primary task was combat intelligence, storage and retrieval.[37] Alongside it was 'Project Bates', short for the 'British Artillery Target Engagement System'.[38] Both were linked to Ptarmigan, the new Army communication system. In other words, in the late 1970s and early 1980s, the British Armed Forces were going through nothing short of an electronic revolution.[39] Therefore, as early as 1976 the Army were requesting specific 'Tiger Team' attacks on all their new systems under development including Ptarmigan, Wavell and Bates.[40]

Around this time, Bureau West advertised in the *New Scientist* magazine as a software development specialist. But it was competing with adverts from the computer services of the Army's Directorate of Supply, who wanted a head of operation research for its computer centre at Bicester, the RAF medical facility at Halton in Aylesbury that was seeking a computer programmer/interface development engineer and the Royal Navy Engineering College at Manadon in Plymouth that wanted a speciality in structural mechanics and computing techniques. All four posts were advertised on the same page.[41] Officials bemoaned the fact that the numbers available for the 'Tiger Team' were 'very small' compared to the effort going into automated data processing.[42] By October 1976, several groups of managers across Whitehall were panicking and wanted to converge on their security plans to achieve 'a joint effort'.[43]

Despite these formidable problems, over 2 years, Nutter's team probed every aspect of the ICL 2900. The machine they attacked was described as a 'hardened' version. The programme ranged from straightforward functional testing of security features to examination of source code listings, sometimes aided by automatic tools. There were also attacks in which security experts attempted to penetrate the system in a simulated real-life situation, together with consideration of architectural and design quality. Nutter's research gave considerable attention to the operating system. When ICL's New Range was first launched in October 1974, its operating system was referred to as 'System B'. By the time it was first delivered, it had become a VME/B. To the surprise of Nutter's team, it proved remarkably robust and impressive.[44]

Instead, Nutter's anxieties focused on two areas that he deemed rather urgent. First, the now familiar problem of 'mixed mode' processing, in other words having material at different levels of classification in the same system, allowing the possibility of access by people with limited clearance to high-grade material. A deeper issue was 'the possibility of "sleepers" being implemented into the system software' during its production. In modern parlance, a sleeper is a backdoor – in other words, computer instructions that deliberately introduce a flaw that drives the machine into an unanticipated weird state, or that will allow a mechanism of abuse that bypasses normal security features – thus allowing for malicious control.[45] Backdoors are often small and hard to find, requiring only a small number of lines of code in a codebase that is much larger and more complex by orders of magnitude. Backdoors may also be introduced via 'bugdoor', which is deliberately constructed programming error that creates vulnerability that may be exploited in a specific manner.[46] Prevailing ideas at the time, expressed in the older language of the period, encompassed both possibilities – not yet making the same distinctions that modern analysis might draw between different attack typologies. Having identified a human aspect to the problem, Bureau West was keen to hand this issue to others, adding that 'the likelihood of this occurring is a matter of speculation at this stage, and any assessment of the threat from this source is seen as 'the responsibility of the Security Services'. By August 1976, they had already contacted MI5 and requested assistance.[47]

There was wide disagreement about the 'sleeper' problem, with some worrying that neither Bureau West nor MI5 had the capability to detect sleepers embedded in the software. Others were sanguine and argued that the impressive 2900 software was designed with security in mind, and so they would be easily detected at the design and testing stage. Some suggested that even if sleepers were in place, there was still a lot of collusion required, and a very detailed knowledge of the system was needed to get anything useful in terms of regular flows of data. This argument of 'security by obscurity' would remain a foundational area of debate between differing computer security

approaches for decades to come across multiple technology areas.[48] Amid this ongoing debate, in the summer of 1976, the Central Computer Agency and MI5 sent a joint team to Washington to study computer security methods with the US Air Force.[49]

The USA was less optimistic about the mainframes generally. In 1979, Colonel Roger Schell of the US Air Force Systems Command, whom ICL interacted with, listed numerous ways of gaining access, drawing on his own experience on Tiger Teams testing the security of Air Force information security. If anything, he noted, the ease with which these teams penetrated real military computers holding sensitive data masked the depth of the problem, as they largely missed the possibility of intentional compromise of the systems in question. Schell argued that most tiger teams concentrated on accidental flaws that anyone might happen to find, but the deliberate flaws or 'sleepers' are dormant until activated by an attacker. These errors can be placed virtually anywhere and are carefully designed to escape detection. Yet most military systems include programmes not developed in a secure environment, and some are even developed abroad. In fact, some systems can be subverted by an anonymous remote technician with no legitimate role in the system development. He argued these errors could be activated by essentially any external actor.[50] Schell, who eventually became the founding deputy director of NSA's computer security centre, consistently took the view that computer companies and their customers had a vested interest in taking an optimistic view of the security of their mainframes.[51]

Schell's views were almost certainly informed, in no small part, by the foundational 'Computer Security Technology Planning Study' led by James Anderson – convening a panel of experts from industry, academia, and the National Security Agency – which submitted its findings in 1972.[52] This, in turn, incorporated concepts of vulnerability first developed within the then still heavily classified 'Ware report' issued by RAND, the earliest look at security in multiuser mainframe environments for the Defense Science Board.[53] The extent to which the UK and US teams were collaborating on these problems remains mysterious and a subject for future historical investigation.

Icl's high security option

In 1970s, security for British government computer projects was effectively led by Bureau West. But in 1980s this was increasingly outsourced to external providers or else combined 'joint' approaches were employed. They key driver for this outsourcing was the increasing shortage of in-house specialist IT project development staff as the private sector proved increasingly attractive to them. The problem was made worse by the fact that almost all the defence research establishments were less than a hundred miles from London, many of them along the M4 motorway corridor where Britain's new technology towns like Reading and Swindon were booming. This was reinforced by a political preference under the new Thatcher administration to buy in many public sector services, which drove the movement of significant IT development projects to external consultants and contractors.[54] Arguably things were moving in the same direction in the United States.[55]

The security for Britain's ICL 2900 machines travelled in this direction. ICL, although still struggling in a fiercely competitive international market, was now at its peak, employing some 33,000 staff.[56] In 1980s, responsibility travelled from Peter Nutter at Bureau West towards ICL's new Defence Technology Centre. This was led by Tom Parker who had joined ICL in 1971 after working for Ferranti. He initially worked on the early design and production of ICL's proprietary VME Operating System. In 1978, he began specialising in computer security at ICL, occupying this role for more than a decade, until he left the company in October 1999 to become an independent consultant.[57]

Parker was complimentary about Nutter's work and also optimistic about the security of ICL machines. His view was that the operating system was well designed and so intrinsically demonstrated 'a reasonable degree of security' adding that the Tiger Teams had failed to achieve their major penetration objectives. Perhaps, this was not the whole story as there were already a number of known defects that could have been exploited and were therefore declared 'no go areas' to the attackers, moreover there were other weak spots that could only be defended by asserting rather

restrictive procedural controls. (The tensions in defining what will be in scope, and what will remain out of scope, for red team efforts remain quite familiar to modern practitioners.) The immediate value of Nutter's previous work, was to allow ICL to remedy some of these defects. Parker did not claim that the improved system was 'totally secure', but he did feel that with these improvements it was difficult to attack. He added that the great majority of successful penetrations of other systems have been by teams consisting of top-class systems penetration specialists who knew their target inside out.[58]

Parker was a pragmatist who asserted that security 'is not a binary property', a widely repeated common maxim even today. He observed that with a large commercial system like VME/2900, all that could be done was to eliminate as many potential loopholes as their expertise and the state-of-the-art technology allowed. Obvious security facilities, such as privacy mechanisms and the checking of login passwords, were of little use if they could be corrupted or by-passed. So ICL had focused on advanced software technology that they had used in the production of the system and further work on security assurance that has been done to maximise the integrity of the security features, in other words security correctness.[59]

Some of the ICL machines have already been given additional protection such as those installed for MI5. Parker observed that 'a substantial number of extra security features have been developed' to satisfy these special customers. Work has been done also on 'hardening' VME/2900, not only from the point of view of providing extra facilities but also from that of security correctness. Some of these special options have since become standard product-line items. ICL had attempted to automate the security analysis as far as possible and some of the tools developed in this work were incorporated into a 'security test package' which also included tests of those standard security facilities that were visible to the user. ICL claimed its VME Operating System has established itself over the years as being one of the most secure commercial operating systems available.[60]

One of Parker's interesting observations was the problem of measuring security, a challenge that has never fully been resolved even today. Until 1980s there was no way of obtaining a reliable standard measure from these techniques since there was no concept of 'marks out of ten' on a scale of security. Addressing a US Department of Defence seminar on computer security in August 1981, he dismissed some of the proposed high-level criteria as a 'fairy-tale fantasy'.[61] However, only 2 years later the first official set of standard criteria for the evaluation of computer security was published by the US Department of Defense. This standard was first applied in US Government procurements of secure systems and its influence slowly pervaded European government and commercial requirements.[62] By the late 1980s, an evaluation scale had also been developed by the British Government. This has built on the experience obtained from the American work but was more flexible in its application. One important feature was its ability to separate out the issue of what the system claimed to do from how well it actually performed.[63]

ICL was quick to recognise that high security constituted a new and expanding market. In 1983, ICL made initial proposals to the Department of Industry for a subsidy to research and develop an advanced set of security enhancements. Codenamed 'Project Spaceman', this was aimed mostly at the government but also at commercial users given that bank security was becoming more important. The emphasis was on 'usable security' and providing flexibility in the choice of security policy. With the rise of independent security quality standards, it also aimed to be something that could be evaluated by a recognised authority that had credibility in the marketplace. In late 1984, ICL received government approval and this development came to be known as the VME High Security Option, usually called the VME HSO.[64]

The High Security Option boasted three major innovations over prior ICL systems. It permitted the security manager to determine and mark the levels of confidentiality of data held by the system. It also allowed the manager to determine and mark which users are cleared to access what data according to its confidentiality markings. It ensured that only if a user is 'cleared' to the level of confidentiality of the data is he permitted to read it. In other words, they addressed the multi-level user problem identified by Nutter as a key issue in 1976. Moreover, there was a more robust defence

against certain kinds of 'Trojan Horse' attacks. This implemented a type of information flow control, preventing untrusted application code from circumventing security checks by maliciously copying data from a highly confidential file across memory security boundaries to a less confidential file, to which a user with a low clearance could subsequently access discreetly.[65] This memory separation prevented user processes from directly interacting with each other, and explicitly limited which user processes could interact with core systems functionality.

More broadly, introducing additional security options delivered significant success for ICL. Previously, the firm had struggled with sales. Its marketing reflected these challenges, with the firm able to cite only limited prior performance successes, such as accounting functions for ship-building firm responsible for construction of the Queen Elizabeth 2 ocean liner,[66] or pilot projects, with local police services deploying the ICL 1900 series system for crime analysis tasks.[67] Although unable to compete with IBM in the standard mainframe business, its strong involvement with the delivery of computer services to the government, in particular those with special security requirements, such as MI5, accelerated its expertise in all secure and hardened systems required by defence customers. This was later applied to the Royal Navy's Operational Control Command Control and Information System (OPCON CCIS), an automated message handling system and database for use by the Commander-in-Chief Fleet (CINCFLEET) headquarters at Northwood using ICL's commercial ADP equipment at a cost of some £40 million. It proved its value during the Falklands War, with fielded systems surviving even through the most serious kinetic attacks against the vessels on which it was deployed, and evolved to provide joint use in the mid-1980s. The firm would shift its marketing campaigns accordingly to emphasise military themes, undoubtedly leveraging these successes.[68]

More broadly, Project Spaceman provided a path for ICL's future activities in the secure systems arena. It has the advantage that VME is one of the last large-scale operating systems ICL ever designed, and one that is revolutionary rather than evolutionary in design. Almost by accident, its underlying architecture encompassed many of the elements needed to develop a secure systemin particular, the hardware-assisted Access Control Registers to limit the privileges that can be taken by users. Project Spaceman in fact gave birth to a pair of complementary products, with the commercial release being called High Security Option and the public sector version, with encryption technologies, designated the Government Security Option.[69] Both were formally tested under the CESG UK (Security) Evaluation Scheme and in fact became the first mainstream operating system to be formally certified in Britain.[70] The VME/2900 system was sufficiently innovative that it became a comparative benchmark for study in one of the first computer security courses ever taught in the United States (by an engineer noted for prominent involvement in information assurance efforts for Department of Defense networks for decades after).[71]

Computer security suddenly caught the attention of Downing Street in 1982. *The Times* reported that this was being tightened up asresponsea response to 'allegations in the United States that British computers containing classified information have been penetrated by the Russians'. [72] In fact, the changes reflected recommendations by the Security Commission in the wake of the Geoffrey Prime espionage case at GCHQ. The Commission had decided there was a need to upgrade the Security Committee on Electronic Information Processing (SCEIP), one of a number of Cabinet official committees on security, and its membership now included people with experience of computing from the Treasury, Home Office, Foreign Office, MoD, GCHQ and CESG. Its role included liaising with equivalent bodies in the United States.[73] With characteristic thoroughness, Margaret Thatcher repeatedly probed the technical qualifications of each of the members, casting doubt on whether even membership of the British Computer Society offered evidence of proper capability. The Cabinet Secretary, Robert Armstrong, tried to reassure her, but she replied, 'my doubts remain'.[74] To placate the prime minister, Adrian Norman, a computer consultant from the Information Technology Unit at the Cabinet Office, was eventually added to the committee.[75] The presence of an external consultant on such a security committee in 1982 is interesting.

Conclusion

The full story of Bureau West as a pioneer of early British computer attacks and automatic data processing remains to be told. However, it illustrates the importance of the Ministry of Defence as an early player in the field of information security and computer security.[76] Meanwhile ICL, its close collaborator, presents a fascinating case of successful failure. Despite being the world's second-biggest mainframe manufacturer, ICL struggled in international markets because of the high costs of R&D and so was dependent on both direct and indirect subsidies, partly in the form of a preferential position as a supplier to the British government.[77] It often struggled to deliver its intelligence, security and defence projects on time and there were big cost overruns.[78] However, that close relationship also delivered a fruitful partnership that specialised in secure systems. This in turn gave Britain an early lead in this specialist field and, as with other areas of intelligence and information technology, its technicians were often praised by their American allies for finding ingenious and low-cost solutions to difficult problems.

Given this early success, it is surprising that Britain struggled with some of its later projects. This included 'Project Trawlerman', a new database for the Defence Intelligence Staff that was already being considered in 1980s. It would revisit many of the problems anticipated by Nutter and Parker with the security of multi-level multi-user databases.[79] Trawlerman began in 1988 with a £32 m contract to be delivered in October 1991. The project experienced substantial delays and the contractor requested additional funds. Trawlerman was eventually delivered in November 1993, some two years late, but was rejected as unsatisfactory. After further remedial work, it ran for only 2 years before being written off and replaced by a commercial off-the-shelf system at a fraction of the cost.[80]

As yet we know little about Britain's first forays into the exciting world of Computer Network Exploitation. We do not know much about the British agencies or departments that developed early efforts to collect intelligence using offensive computer techniques.[81] The interaction between humans and the technical systems in this area is especially fascinating.[82] The archives on this subject are yet to be declassified, and we are unlikely to see them anytime soon. But in the late 1970s, Teddy Poulden, GCHQ's head of technology, retired from Cheltenham and took on a new part-time role as MI6's first computing officer. Perhaps, this indicated the first stirrings of an interest on the part of Century House.[83]

Notes

1. Broad, "Computers and the US Military Don't Mix," 1183.
2. Astrahan and Jacobs, "History of the Design of the SAGE Computer-The AN/FSQ-7," 340–349.
3. Brunner, "The Shockwave Rider."
4. Warner, "Cybersecurity," 781–799.
5. Work, "Early Intelligence Assessments of COMBLOC Computing," 172-190.
6. Ibid. See also Yost, "Computer Security, Part 2," 10–11.
7. Conn and Yamamoto, "A Model Highlighting the Security of Operating Systems," 174–179; and Jones and Lipton, "The Enforcement of Security Policies for Computation," 197–206.
8. However, see Subramanian, "Historical Consciousness of Cyber Security in India," 71–93; and Baumard, *Cybersecurity in France*.
9. See for example: Agar, *The Government Machine*; Hicks, *Programmed Inequality*; Lavington, *Early Computing in Britain*; Lavington, *Moving Targets*; and Lean, *Electronic Dreams*.
10. Lavington, *Moving Targets*, 81–99; and Agar, "Putting the Spooks Back in?" 102–124.
11. Easter, "Protecting Secrets," 157–169; and Ferris, *Behind the Enigma*, 705–6.
12. Aldrich, "Whitehall Wiring," 178–195.
13. Davies, "The Problem of Defence Intelligence," 797–809.
14. Bell, "Management Audit in the Ministry of Defence," 311–321.
15. Slater, "Budgeting in a time of inflation," 5. See also ADP Report No.113, "Visit to US Police Computer Installations 1969," HO 337/119, TNA.

16. Andrew Stott, interviewed by Ian Symonds, 28th March 2019, Archives of IT https://archivesit.org.uk/wp-content/uploads/2019/09/AIT-Andrew-Stott-final-for-web.pdf accessed October 11, 2022.
17. Eberle, *A life on the Ocean Wave*, 223–4.
18. "Grid 77 plan to aid Defence Operations," *Computer Weekly*, February 10, 1972.
19. The MoD computer directorate in fact occupied two locations: 'Bureau London', the name given to a diverse range of computer suites in the Old War Office and Metropole Buildings, and Bureau West, which was mostly based at a new purpose-built facility at Horton Road but which also had space at Le Marchant Barracks in the centre of Devizes.
20. Cabinet Committee on Economic and Industrial Policy, E1(77)10th Meeting, July 15, 1977, DEFE 47/30, TNA.
21. Campbell-Kelly, "ICL and the Evolution of the British Mainframe," 408.
22. Aldrich, "GCHQ and Computing"; and Ferris, *Behind the Enigma*, 436.
23. Ibid.
24. Ibid.; and Ferris, *Behind the Enigma*, 428–36.
25. Valentine to Merrett, "Replacement Computer for the Royal Radar Establishment, Malvern," September 19, 1975, T 225/4003, TNA.
26. "Bureau West" Centre, *Computer News*.
27. Clarke and Baker, "Bureau West Devizes, Wiltshire," 251–61.
28. Howard and Wight, "For your eyes only." See also Andrew, *Defend the Realm*, 551.
29. Campbell and Connor, "The Monster that Keeps on Growing," 6–7.
30. Summary of operational requirements for the provision of two additional computers for Home Office and Metropolitan Police, September, 1975, HO 337/163.
31. DGERPA/246/76, DGERPA to Sabatini, "Computer Security – Attack Teams," October 5, 1976, DEFE 68/287, TNA.
32. ACDS (Ops) 56/8/5, Thom to AD of S (Pol), "Note of Action – Computer Security Attack teams," December 10, 1976, DEFE 68/287.
33. Talbot to DCCIS, "Computer Security," March 3, 1977, DEFE 68/287, TNA.
34. Warner, *The Vital Link*, 316–7.
35. Talbot to DCCIS, "Computer Attack Teams," January 13, 1977, DEFE 68/287, TNA.
36. Feasibility study report JOCPT, Trenchard/Haig/Wavell, June 18, 1970, DEFE 10/1215, TNA. See also. JOPCT, "Feasibility Study on Project Wavell," May, 1970, DEFE 10/1213.
37. Army Staff Targets and Requirements: GST 3668, Operational Command and Control, Automatic Data Processing System (Project Wavell) April 10, 1979, DEFE 70/1404.
38. RARDE 3/74, "Report on Preliminary Studies and Proposals for Future Work in Support of Project Bates," March 31, 1974, DEFE 15/2214.
39. Rice and Sammes, *Communications and Information Systems for Battlefield Command and Control*. See also Ricem and Sammes, *Command and Control: Support Systems in the Gulf War*.
40. "Computer Security Attack Teams: Meeting," December 6, 1976, DEFE 68/287, TNA.
41. *New Scientist*, September 6, 1979, 763.
42. D/Man C 2900/13/2/1, Annex A, "Guidelines on 2900 Security," May 25, 1976, DEFE 68/287, TNA and minute.
43. Sabatini to DGERPA, "Computer Security – attack Teams," October 27, 1976, ibid.
44. D/Man C/4/221, "Defence ADP Development Board Working Group on Testing of Computer Security, Note by Secretary," Downes, January 21, 1977, ibid.
45. Thomas and Francillon, "Backdoors: Definition, Deniability and Detection"; and Dullien, "Weird Machines, Exploitability, and Provable Unexploitability," 391–403.
46. Samuel Jungie Tan, Sergey Bratus, Travis Goodspeed, "Interrupt-oriented Bugdoor Programming: A minimalist approach to bugdooring embedded systems firmware," Annual Computer Security Applications Conference (ACSAC), December 08–12, 2014, New Orleans, USA.
47. D/Man C 2900/13/2/1, Annex A, "Guidelines on 2900 Security," May 25, 1976, DEFE 68/287, TNA and minute. MI5 was also taking the lead on personnel security threat for police national computer, HO to Todd, November 30, 1972, HO 521/1.
48. Anderson, "Why Cryptosystems Fail," 215–227; Schneider and Bellovin, "Inside rIsks: Evolving Telephone Networks," 160; and Mercuri and Neumann, "Security by Obscurity," 160.
49. DAPDB/M(76)2, Minutes of the 22nd Meeting of the Defence ADP Development Board, item 3, "2900 Security," September 17, 1976, DEFE 68/287, TNA.
50. Warner, "Cybersecurity," 785.
51. Machine Intelligence Research Institute, Conversation with Luke Muehlhauser, "Roger Schell on Long-term Computer Security Research," June 23, 2014, https://intelligence.org/2014/06/23/roger-schell/.
52. Anderson, "Computer Security Technology Planning Study."
53. Ware, "Security Controls for Computer Systems".
54. Brown, "Modernisation or failure?" 363–81.
55. Admiral Bobby Inman, DDCI, Computer Security Initiative, "Keynote Address," Proceedings of the Fourth Seminar on the DoD Computer Security Initiative, August 10–12, 1981, B 1–4, https://csrc.nist.gov/CSRC/media/

Publications/conference-paper/1981/08/10/proceedings-4th-seminar-dod-computer-security-initiative/documents/1981-4th-seminar-proceedings.pdf.

56. Campbell-Kelly, "ICL and the Evolution of the British Mainframe," 410.
57. Parker, "Security in a Large General-purpose Operating System," 28–42.
58. Ibid.
59. Ibid.
60. Ibid.
61. Tom Parker, "ICL Efforts in Computer Security", Proceedings of the Fourth Seminar on the DoD Computer Security Initiative," August 10–12, 1981, L1–12, https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1981/08/10/proceedings-4th-seminar-dod-computer-security-initiative/documents/1981-4th-seminar-proceedings.pdf.
62. DOD 5200.28-STD: Trusted Computer Systems Evaluation Criteria, Fort George Meade MD USA: National Computer Security Center, December 1985.
63. CESG: UK Systems Confidence Levels, CESG Computer Security Memorandum No.3, Issue 1.1, Feb. 1989.
64. Parker, "The VME High Security Option," 657–70.
65. Ibid.
66. Yarrow – Admiralty Research Department (Y-ARD) at the yard in Govan was in the mid-60s operating an advanced ICL machine for warship design (funded by MOD) and used by key defence contractors.
67. Advertisement, "What helped the Queen Elizabeth 2 take the plunge like a lady?" International Computers Ltd, circa 1968; and Advertisement, "What will tell British police where a thief's going before he knows himself," International Computers Ltd, circa 1968.
68. Advertisement, "Send Reinforcements," ICL, circa 1984.
69. The Government Security Option offered extra controls restricting some actions to authorised users, improved auditing and a password handling package to enable it to use government-approved password generation and encryption algorithms.
70. CESG, "Certified Product List UKSP 06 UK IT Security Evaluation and Certification Scheme", April 2000, 56, ftp.scs-trc.net.
71. William Neugent, "A University Course in Computer Security," ACM SIGSAC Review 1 Issue 2 (Spring 1982): 17–33.
72. Pearce Wright, "Security Review Ordered on Computer Files," *The Times*, November 8, 1982.
73. Whitmore to Armstrong, July 26, 1982, attaching Annex A "Security Committee on Electronic Information Processing (SCEIP) Departmental Representatives," PREM 19/2219, TNA.
74. Margaret Thatcher minute, ibid. n.d. presumed July 26, 1982.
75. Armstrong to Butler, "Security Committee on Electronic Information Processing," A09692, 11 October, 1982, PREM 19/2219. See also Norman, *Computer Insecurity*..
76. "Bureau West" as a name vanished in January 1984 when it joined the Defence Data Processing service and the Defence administrative Computer Division to form the Directorate of Central Computer services. The facility itself closed in 1999, see Clarke and Baker, *Bureau West*, 261.
77. "Computers: Preference for ICL Intensified," *Financial Times*, May 6, 1975.
78. Whicher (Dir D Sc 8) to ACSA (P), "Wavell," June 4, 1981. DEFE 70/1404, TNA.
79. "Project Trawlerman: Consultancy Study of Future ADP (computer) Requirements of the Defence Intelligence Staff (DIS)," March 1, 1983, DEFE 31/274, TNA.
80. Brown, "Modernisation or failure?" 367.
81. An MI6 officer employed in 2007 was later convicted of trying to sell his information gathering software, see Fiona Hamilton," MI6 worker given 12 month sentence for trying to sell secrets," *The Times*, September 3, 2010.
82. Gioe, Goodman and Stevens, "Intelligence in the Cyber Era," 191–224.
83. Aldrich, "GCHQ and Computing," 252–3.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Richard J. Aldrich is Professor of International Security at the Department of Politics and International Studies, University of Warwick, and a Fellow of the Royal Historical Society. He is the author of several books including The Hidden Hand and GCHQ. His most recent books are The Black Door (2016) and The Secret Royals (2021) co-authored with Rory Cormac. Between 2016 and 2020 he was a Leverhulme Major Research Fellow working on the future of secrecy. He is

now working on the ERC 'Demoseries' and H2020 'DigiGen' projects, together with the Jean Monnet 'Cydiplo' programme.

JD Work is a professor at the National Defense University, College of Information and Cyberspace. He has over two decades of experience working in cyber intelligence and operations roles for the private sector and the US government. He holds additional affiliations with the Saltzman Institute of War and Peace Studies at the School of International and Public Affairs at Columbia University, the Atlantic Council's Cyber Statecraft Initiative, and the Krulak Center for Innovation and Future Warfare at Marine Corps University.

References

Agar, J. *The Government Machine: A Revolutionary History of the Computer*. Cambridge MA: MIT Press, 2003.

Agar, J. "Putting the Spooks Back In? The UK Secret State and the History of Computing." *Information & Culture* 51, no. 1 (2016): 102–124. doi:10.7560/IC51105.

Aldrich, R. J. "Whitehall Wiring: The Communications-Electronics Security Group and the Struggle for Secure Speech." *Public Policy and Administration* 28, no. 2 (2013): 178–195. doi:10.1177/0952076712458111.

Aldrich, R. J. "GCHQ and Computing: Teddy Poulden, IBM and ICL." In *Shaping British Foreign and Defence Policy in the Twentieth Century*, edited by M. Murfett, pp. 240–253. London: Palgrave, 2014.

Anderson, J. P. "Computer Security Technology Planning Study." US Air Force, Systems Command, Electronic Systems Division, ESD-TR-73-51, October, 1972.

Anderson, R. "Why Cryptosystems Fail." Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS), December, 1993: 215–227. doi: 10.1145/168588.168615.

Andrew, C. M. *Defend the Realm: The Authorized History of MI5*. New York: Knopf, 2009.

Astrahan, M. M., and J. F. Jacobs. "History of the Design of the SAGE Computer-The AN/FSQ-7." *IEEE Annals of the History of Computing* 5, no. 4 (1983): 340–349. doi:10.1109/MAHC.1983.10098.

Baumard, P. *Cybersecurity in France*. London: Springer International Publishing, 2017.

Bell, M. J. V. "Management Audit in the Ministry of Defence." *Public Administration* 62, no. 3 (1984): 311–321. doi:10.1111/j.1467-9299.1984.tb00565.x.

Broad, W. J. "Computers and the US Military Don't Mix: After 9 Years and More Than $1 Billion, the Pentagon's Global Computer Network is Still on the Blink." *Science* 207, no. 4436 (1980): 1183–1187.

Brown, T. "Modernisation or Failure? IT Development Projects in the UK Public Sector." *Financial Accountability & Management* 17, no. 4 (2001): 363–381.

Brunner, J. *The Shockwave Rider*. New York: Harper & Row, 1975.

""Bureau West" Centre." *Computer News*.

Campbell, D., and S. Connor. 1981. "The Monster That Keep on Growing." *New Statesman*, March 5.

Campbell-Kelly, M. *ICL: A Business and Technical History*. Oxford: Oxford University Press, 1989.

Campbell-Kelly, M. "ICL and the Evolution of the British Mainframe." *The Computer Journal* 38, no. 5 (1995): 400–412. doi:10.1093/comjnl/38.5.400.

"CESG: UK Systems Confidence Levels." CESG Computer Security Memorandum no. 3, Issue 1/1, February, 1989.

Clarke, B., and W. Baker. "Bureau West Devizes, Wiltshire: An Early Component of the British Computer Landscape." *Wiltshire Archaeological & Natural History Magazine* 113, no. 1 (2020): 251–261.

Conn, R. W., and R. H. Yamamoto. "A Model Highlighting the Security of Operating Systems." Proceedings of the Association for Computing Machinery annual conference, January, 1974, 174–179. doi: 10.1145/800182.810399.

Davies, P. H. "The Problem of Defence Intelligence." *Intelligence and National Security* 31, no. 6 (2016): 797–809. doi:10.1080/02684527.2015.1115234.

Department of Defence'5200.28-STD: Trusted Computer Systems Evaluation Criteria. Port George Meade, MD: National Computer Security Center, December, 1985.

Dullien, T. "Weird Machines, Exploitability, and Provable Unexploitability." *IEEE Transactions on Emerging Topics in Computing* 8, no. 2 (2020): 391–403. doi:10.1109/TETC.2017.2785299.

Easter, D. "Protecting Secrets: British Diplomatic Cipher Machines in the Early Cold War, 1945–1970." *Intelligence and National Security* 34, no. 2 (2019): 157–169. doi:10.1080/02684527.2018.1543749.

Eberle, S. J. *A Life on the Ocean Wave*. Durham: Roundtrip, 2006.

Farquhar, G. "The Defence Research Information Centre: Services and New Developments." *ASLIB Proceedings* 41, no. 5 (1989): 169–178. doi:10.1108/eb051137.

Ferris, J. *Behind the Enigma: The Authorised History of GCHQ - Britain's Cyber-Intelligence Agency*. London: Bloomsbury, 2020.

Gioe, D. V., M. S. Goodman, and T. Stevens. "Intelligence in the Cyber Era: Evolution or Revolution?" *Political Science Quarterly* 135, no. 2 (2020): 191–224. doi:10.1002/polq.13031.

Hicks, M. *Programmed Inequality: How Britain Discarded Women*. Cambridge MA: MIT Press, 2017.

Howard, H., and E. Wight. "For Your Eyes Only: MI5 Shares Unseen Images of Its Former Mayfair HQ, Where "Registry Queens" Carried Out Phone-Tapping." *Daily Mail*, July 9, 2021. https://www.dailymail.co.uk/news/article-9769759/MI5-shares-unseen-images-former-Mayfair-HQ-Registry-Queens-carried-phone-tapping.html

Jones, A. K., and R. J. Lipton. "The Enforcement of Security Policies for Computation", Proceedings of the fifth Association for Computing Machinery symposium on operating systems principles (SOSP), November, 1975, 197–206. doi: 10.1145/800213.806538.

Lavington, S. *Moving Targets: Elliott-Automation and the Dawn of the Computer Age*. London: Springer, 2011.

Lavington, S. *Early Computing in Britain: Ferranti Ltd. and Government*. London: Springer, 2019.

Lean, T. *Electronic Dreams: How 1980s Britain Learned to Love the Computer*. London: Bloomsbury, 2016.

Mercuri, R. T., and P. G. Neumann. "Security by Obscurity." *Communications of the ACM* 46, no. 11, November (2003): 160. doi:10.1145/948383.948413.

New Scientist, MoD Computer Post Advertisements, September 6, 1979.

Norman, A. R. D. *Computer Insecurity*. London: Chapman & Hall, 1983.

Parker, T. A. "Security in a Large General-Purpose Operating System: Icl's Approach in VME/2900." *ICL Technical Journal* 3, no. 1 (1982): 28–42.

Parker, T. A. "The VME High Security Option." *ICL Technical Journal* 6, no. 4 (November, 1989): 657–670.

Rice, M. A., and A. J. Sammes. *Communications and Information Systems for Battlefield Command and Control*. London: Brassey's, 1989.

Rice, M. A., and A. J. Sammes. Command and Control: Support Systems in the Gulf War*: An* account of the Command and Control Information Systems Support to the British Army Contribution to the Gulf War. London: Brassey's, 1994.

Schneider, F. B., and S. M. Bellovin. "Inside Risks: Evolving Telephone Networks." *Communications of the ACM* 42, no. 1, January (1999): 160. doi:10.1145/291469.291485.

Slater, J. B. "Budgeting in a Time of Inflation and Austerity-Some UK Experiences." Proceedings of the 8th annual ACM SIGUCCS conference on User services, 1980. https://dl.acm.org/doi/pdf/10.1145/800086.802741.

Subramanian, R. "Historical Consciousness of Cyber Security in India." *IEEE Annals of the History of Computing* 42, no. 4 (2020): 71–93. doi:10.1109/MAHC.2020.3001215.

Tan, S. J., S. Bratus, and T. Goodspeed. "Interrupt-Oriented Bugdoor Programming: A Minimalist Approach to Bugdooring Embedded Systems Firmware." Annual Computer Security Applications Conference (ACSAC), New Orleans, USA, December 08 - 12, 2014

Thomas, S. L., and A. Francillon. "Backdoors: Definition, Deniability and Detection." In *Research in Attacks, Intrusions, and Defenses (RAID). Lecture Notes in Computer Science*, edited by M. Bailey, T. Holz, M. Stamatogiannakis, and S. Ioannidis. Vol. 11050, p. 1-21. Cham: Springer, 2018.

Ware, W. "Security Controls for Computer Systems." RAND, Defense Science Board Task Force on Computer Security, R-609-PR. DECLASSIFIED, 1972.

Warner, P. *The Vital Link: The Story of Royal Signals 1945-1985*. London: Leo Cooper, 1989.

Warner, M. "Cybersecurity: A Pre-History." *Intelligence and National Security* 27, no. 5 (2012): 781–799. doi:10.1080/02684527.2012.708530.

Wells, P. "The Military Scientific Infrastructure and Regional Development." *Environment & Planning A* 19, no. 12 (1987): 1631–1658. doi:10.1068/a191631.

Work, J.D. "Early Intelligence Assessments of COMBLOC Computing." *Journal of Intelligence History* 21, no. 2 (2022): 172–190. doi:10.1080/16161262.2021.1884791.

Yost, J. R. "Computer Security, Part 2." *IEEE Annals of the History of Computing* 38, no. 4 (2016): 10–11. doi:10.1353/ahc.2016.0040.