Capturing the Past, Inspiring the Future

Sir Edmund Burton

Interviewed by

Elisabetta Mori

26th February 2019

At the

BCS Offices

5 Southampton Street, London, WC2E 7HA

Kindly provided by The British Computer Sociry

Welcome to the Archives of Information Technology. It's 26th of February 2019 and we're in London at the British Computer Society. I am Elisabetta Mori, an interviewer with Archives of IT. Today I'll be talking to Lieutenant General Professor Sir Edmund Burton, Knight Commander of the Most Excellent Order of the British Empire. Sir Edmund Burton is a retired general and an experienced and highly innovative senior executive with extensive experience within the UK defence and security community operating at both ministerial and board level. He has been a staunch advocate of the importance of treating information as a key business asset and of protecting it accordingly. Formerly executive chairman of the UK national Police IT Organisation leading a major business improvement programme, a knowledge adviser to the Cabinet Office, other government departments, private sector and academia on information assurance processes and the need for education and training. He has represented the UK in NATO panels. His areas of expertise include integrated national defence and police equipment strategies, management of information risk at board level, effective communication at international board levels, and at the interface between the private and public sectors. He is experienced in information assurance and information risk and cybersecurity. He was chairman of the Information Assurance Advisory Council and joint chairman of the Telecommunication Industry Security Advisory Council, TISAC. He was awarded two doctorates of science (honoris causa) at Cranfield University and at the University of Chester. He is a Fellow of the British Computer Society and of the Institution of Engineering and Technology. He is now chairman of the Cyber Security Body of Knowledge, CyBOK, professional advisory board.

Welcome Sir Edmund. Can you tell us about your childhood and the important influences on you in your early life?

[0:02:24]
Thank you, Elisabetta. All the male members of my family have followed a military career since the 19th century, and I made the decision at the age of fifteen to apply for a commission in the army.

What can you tell us about your early education?

Well, I left school at eighteen and went to Sandhurst for the two-year commissioning course, during which I took the Cambridge University mechanical sciences qualifying exam. I was commissioned into the Royal Regiment of Artillery and posted to one of the UK's two army missile regiments, based in West Germany. So my university education was deferred for eighteen months. That tour of duty in Germany, which comprised education and training, provided my first experience of leading soldiers and of managing a key component of a complex system of systems. We'll be developing this theme if it's of interest, because it will recur as our conversation develops. I comment at this point that the practical experience with surveying, meteorology, radar and analogue computers that I gained from this initial period of service in the Missile Regiment was to provide me with an invaluable foundation for my degree course at Cambridge. I should also add that the young soldiers who manned these systems had few, if any, form of technical education or qualifications prior to enlisting, yet they were able to accomplish their task with calmness and efficiency, and again, this theme is to continue over the following years.

[0:04:14]
Have you got any other special memory of the time?

Well, it's many years ago. Although the regiment was stationed in West Germany, it undertook its live firing of missiles in the Outer Hebrides. The successful firing of an inert practice missile 80 miles into the North Atlantic from the island of Benbecula in the Outer Hebrides was a significant experience. It's worth adding that this period – and we're talking about the early 1960s – was barely twenty years since the end of World War Two. The threat from the Soviet Union and Warsaw Pact forces stationed in East Germany was very real and the British Army of the Rhine as a significant component of NATO was held at two hours' readiness to deploy from barracks.

How did that experience in Germany change your relationship with technology?

As I've just outlined, this is my first introduction to technology and to what is now described as the system of systems. That comprising the integration of command and control functions, missile guidance, missile propellants, computation, radar tracking, surveying, radio communications, and significantly, a nuclear warhead.

[0:05:41]
You have just mentioned the expression, system of systems, can you tell us more about that?

Well, this is a major subject. However, for the purposes of this interview I'm asserting that military platforms, sensors, warheads and information, logistic support infrastructure are system of systems which represent key components of a military capability. They have to be integrated in the domain of operational effects, sometimes termed 'capability integration'. An example might be the conceptual approach to enabling the deployment of fixed-wing aircraft, attack helicopters, troop carrying helicopters, drones, guided weapons and sensors in the complex electromagnetic environment, say, of an aircraft carrier. In the technical domain, systems and subsystems must be integrated, ie, systems integration, in order to operate together in a highly complex environment in order to deliver the desired operational effects. Systems engineering is the approach adopted to achieve this. And this issue will arise later when we talk about smart procurement.

[0:07:05]
So I notice that you attended the Regimental Signals Officer course at the School of Artillery. Have you got any particular memory you would like to share with us?

Well, the first point to be made is that secure, reliable and resilient communications are essential to all defence and security capabilities on land, at sea, in the air and in the space environment. As an aside, this is true of public and private sector organisations to this day. In those days, and we're still talking about the 1960s, every British regiment had a Regimental Signals Officer who was responsible for all aspects of ensuring the availability of communications. This included the siting of headquarters and the planning and delivery of appropriate training for all users of HF – high frequency – and VHF – very high frequency – radios. You've asked for any particular memory. I believe that the responsibility for effective regimental communications confirm the principle that – and I'm really quoting – information, knowledge and data are critical enterprise assets to be developed and protected

accordingly. Now, that reality is receiving belated recognition some 50 years later and this theme will develop and recur during our conversation.

[0:08:43]
I also noticed that your service included periods in West Germany. How has that influenced your thinking?

I choose two main areas. The first one is the reality of the threat. As I've already mentioned, the first British corps was stationed in West Germany in the post-war years. In the 1960s these troops numbered over 55,000. These forces were maintained at two hours' notice to move out of barracks to operational deployment areas. The reality and the scale of the threat was clear. The forces of the Warsaw Pact and of the Soviet Union were visible across the inner German border, which was marked by a high barbed wire fence, minefields and watchtowers, which stretched from the Baltic to the Adriatic. My second point is that of crucial importance of physical and information security. The proximity of the threat presented by the forces of the Warsaw Pact and Soviet Union and their recognised expertise in monitoring and interfering with NATO communications obliged us to take communication security very seriously. However, this capability and its underpinning principles were lost in the years that followed the collapse of the Soviet Union.

What technology did you manage to become competent with during your course for mid-career officers at the Royal Military College of Science in Shrivenham, Wiltshire?

In 1975 I attended the Army Staff course. This was a one-year postgraduate science and technology course addressing a wide range of technologies. These included lasers, image intensification, infrared imaging, IT and communications, guns, ammunition, armoured vehicle design and operation analysis. I realised in later years that this unique educational experience was to provide me with a foundation of knowledge and understanding for the rest of my professional career. In a nutshell, education is for life and it delivers understanding. When a system and set of processes fail, it is usually attributable to a lack of understanding.

[0:11:27]
Have you got any particular memory of that time?

We're now talking about the early 1970s and my memories are the contrast between the two and a half years that I'd spent in Northern Ireland and the calm, domestic and academic environment of the Shrivenham campus of the Royal Military College of Science. Professionally I recall the extraordinary advances in light imaging equipment that were emerging from the UK's R&D establishments. It was clear that these would transform tactical operations in the short term and offer major operational benefits in the longer term.

So what led you to attend a Royal Navy staff course in Greenwich?

The selection process for staff training allocated officers to courses. In my case I was posted to the Royal Navy staff course, possibly because of my responsibilities in the operation centre in Northern Ireland which included briefing Royal Navy warships on coastal operations.

And what was your first role for the Ministry of Defence?

Well, after attending the staff course in the mid-1970s I was appointed to a role which bore responsibility for the current and future specification and programming of equipment capabilities required for the accurate employment of artillery. These capabilities included the early generations of IT, survey, meteorology, muzzle velocity measurement and their integration in order to deliver optimal effects from the UK's reducing force structure. At that time the most significant advance in gunnery was the Battlefield Artillery Target Engagement System known as BATES. As its name implies, this was conceived as a means of integrating the elements of the artillery target engagement system from observer, through the fire control system to the gun platforms. It was to replace the very successful ballistic computation equipment and represented a huge leap in thinking and in IT engineering. Indeed, in retrospect I believe the scope of that requirement far exceeded the computing capability of the technologies of the day. The development of BATES project was also to demonstrate many of the failures of subsequent major IT systems. The issue

of complexity, the difficulty of capturing and stabilising requirements and the limitations of processor technology were major handicaps.

[0:14:22]
I noticed that you returned to Germany at this stage.

Yes. I was posted to an artillery regiment close to the inner German border in 1978 in command of a gun battery of six tracked self-propelled guns. It also provided a real reminder of the importance of effective radio discipline in a hostile electromagnetic environment. Very shortly after my arrival the regiment was warned for a five-month tour of duty in Northern Ireland in the infantry role. This involved a comprehensive, well-developed training package and significant organisational changes. In the context of today's conversation this operational tour in Belfast involved developing tactics, techniques and procedures for the use of newly fielded technologies. These included a new generation of weapon sights and an Automatic Number Plate Reading system, ANPR. This is an excellent example of the effective appliance of science and technology to deliver improved operational effectiveness. Some 40 years later, Automatic Number Plate Reading systems are well deployed by UK police forces and indeed in the commercial sector by large car park businesses such as in airports

[0:15:55]
You then returned to the Ministry of Defence in 1980 to an appointment which seems to me human relations, HR. Was this an important stage?

I believe that people are a key component, if not the key component within every enterprise, whether it's defence, security or in the field of commerce. This particular appointment was responsible for the career management of all majors in the Royal Artillery. At this stage the army had a severe shortage of people who understood what was then called ADP, Automatic Data Processing, and the Royal Artillery was in need of a qualified and confident generation of ADP IT experts. In the context of this particular job I was able to guide selected officers towards ADP and IT programme management career paths and this was to be an important initiative to meet the increasing need for IT programme staff. And furthermore, it provided new career opportunities for the individuals concerned. The cyber security risks and threats

currently facing all enterprises obliges us to ensure that our education system is adapted to enable our young people to use the internet safely and to benefit from and contribute to our evolving information economy. A major initiative is underway now and deserves our full support and engagement. Let me make a comment here. Careful strategic career management is a core responsibility of leaders and managers today. There is much still to be done in aligning what is taught in education and training with what is needed by employers. A matter of current importance to the UK is the need for a national approach to the creation of a career path for those with aptitude for a career in the information economy. That should include a spectrum of academic and practical disciplines across science, technology and the humanities.

[0:18:25]
So, going back to your career, you then became an instructor at the Royal Military College of Science?

Yes. Continuing from my previous comment about the importance of education and training, I believe that those in leadership positions must have a sound understanding of the potential benefits and the risks of technology. I firmly believe that education delivers that understanding. In those days the Royal Military College of Science delivers science and technology and management education to officers and civilians through bachelor and masters level programmes and through specialist short courses. The role of the Royal Military College of Science directing staff – those are the military officers teaching – teaching army mid-career students on Army Staff courses at the postgraduate level. Additionally, I managed a Master of Science course in gun systems design. This was to prove extremely useful for all parties as I was able to host students in later years in my artillery regiment, providing them with real experience of firing real guns as members of gun detachments in a realistic tactical environment. In my view that practical experience is fundamental to those engaged in gun and fighting vehicle design. It also provided me with invaluable links with gun technology experts, expertise that I drew on in the subsequent gun replacement project. This period also included the Falklands War, as a result of which many fundamental lessons were learned and relearnt by the British army, leading to the development of the British Army's doctrine. This was to shape the nature of

education and the approach to career planning and procurement of equipment capabilities.

[0:20:34]
So I understand that all officers see command of a regiment as being the ultimate goal of their career.

Indeed it is. And that appointment enabled me to develop and apply all that I'd learnt in the previous twenty years of my career. The practical integration of capabilities to deliver combat effectiveness of an operational artillery unit. The experience of leading, training and developing the talents of men and women, taking responsibility for all aspects of their wellbeing and performance is a demanding and rewarding experience. This might be summarised as ensuring that each person is able to achieve their full potential and in so doing to enable the regiment to deliver optimal operational effectiveness.

[0:21:30]
What do you remember of your experience at the British Embassy in Washington DC?

Before I answer that question I just need to mention as an aside that we've leap-frogged four years, during which I was responsible for sponsoring the British Army's surface-to-surface weapons and air defence and related IT capabilities in the Ministry of Defence, and then two years as Commander Artillery in support of the UK's largest armoured division deployed in West Germany. So back to Washington DC, I was posted to the British Embassy in Washington DC as the Military Attaché and Commander British Army Staff, arriving just before Christmas 1988, a date of significance. My role was as the representative of the Chief of the General Staff to his opposite number of the US Army. This proved to be particularly significant in the timing of the UK and US relationships as the UK became a key contributor to the Desert Storm operation. This was a milestone in international affairs, also termed as the first Gulf War. So the context of the time was the collapse of the Soviet Union, which came as a surprise to virtually everybody, the invasion by the US of Panama over the Christmas, 1989, the Iraqi invasion of Kuwait in the summer of the following year and Operation Desert Storm, August 1990 to, I recall, May 1991. So,

impressions that I would choose to extract and share would be as follows. First, to an experienced member of the British Army I was impressed by the huge scale of the US military and reserve forces. I was impressed by the US intellectual rigour, by which I mean their approach to their operational doctrine, their operational analysis and the rigour of their planning, both in the approach to the post-war, post-Cold War force reductions and the closure of many military bases around the world and in the continental US, and in their application of what the Brits called operation analysis in the conduct of Desert Storm. I was impressed by the major scale of investment in research and development in the US and the appliance of science and technology to war fighting. I was impressed by their single-mindedness in their approach to what they called digitisation of military capability, and it was that observation during my time in Washington that enabled me to develop the theme in my next appointment as Commandant of the Royal Military College of Science at Shrivenham and subsequently in the Ministry of Defence.

[0:25:00]
How did the end of Cold War affect you personally or your career?

I guess that the end of the Cold War and the experience from the Gulf War operations represented the end of the first twenty-five years of my professional career. So I'd had comprehensive education and training and practical experience that was to carry me into the second twenty-five year period of my professional career.

What was your role in the Desert Storm operation? Were you involved, at which level?

I was involved, as I've explained, with the staff of the Chief of the US Army and making a link back to the Chief of General Staff of the British Army. So it was a close relationship, and as an aside, illustrated to me the importance of establishing trust, not only within enterprises, but across national and international boundaries and there were many examples where that degree of trust bore fruit for our deployed forces.

[0:26:18]

So then between 1991 and 1994, as you have already told us, you became Commander of the Royal Military College of Science in Shrivenham. What do you recall of that experience?

During that period the College was a well-established partnership between the services and Cranford University, providing postgraduate education, principally to officers of all three services, and to MoD civilians. The term partnership is significant. The ability to develop and sustain an efficient and effective partnership approach to delivering an outsourced service is crucial to delivering value for money to the taxpayer. So a number of headings cover the themes that emerged from that period. The first I've selected is the spread of subjects. The courses delivered by the Royal Military College of Science range from a suite of short specialist courses on topics as diverse as bomb disposal and military operation analysis, to a programme of ten undergraduate and fourteen Masters courses in science and technology management, underpinning the principal Army Staff courses in defence technology and military studies. In terms of scale of the operation, taking a typical year in the early 1990s, over three and a half thousand individuals attended courses, including 1600 officers from the army, navy and air force and 220 officers from overseas. And the college attracted over 1600 civilians on short courses. Innovation was a key feature and the lecturers who taught this range of courses were selected as key academics with a substantial knowledge of the military context within which technology would be applied to delivering operational effects and capabilities. The military directing staff were also handpicked, either direct from having commanded a regiment, or immediately prior to commanding a regiment, so they were high quality individuals. This breadth and depth of expertise enabled the military and civilian staff to provide a unique mid-career educational stimulus for the services in the manage of science and technology. This would be a key component of their knowledge base for all their future assignments. Science and technology provided a catalyst for the transformational changes needed then in the post-Cold War years of the early 1990s and now in the latter years of this decade. The Royal Military College of Science in those years introduced new approaches to thinking and problem solving, such as brainstorming and mind-mapping, and provided every staff course student with a laptop, now very much taken for granted, but was then a radical step. And all these

issues offered a revolution in capability for busy staff officers in operational and support headquarters. An early step in rationalisation was the co-location of the British Army ADP training centre at Shrivenham, blurring the divide between training and education, but seeking to gain benefit from the sharing of knowledge.

[0:30:11]
Thank you. We agreed at the outset that this interview lent itself to a chronological approach, acknowledging that there is a key intellectual theme underpinning it. Now would be a good time to outline that approach.

Thank you. I'm going to start by making assertions and offering some definitions. The first point is to emphasise the importance of our people and the fact that our people and our information, knowledge and data are key enterprise assets, therefore to be developed and protected accordingly. My second point is about the context of these thoughts. Our environment is increasingly complex and uncertain. Technology is advancing at an increasing rate and it's available to law abiding users and villains alike. Worth noting here that procurement decisions for criminals with money to spend are made more rapidly than in most government departments, which are answerable for ethical practice, seeking best value for money through competition. Success may well depend on how effectively technology is applied in an operational environment. In this uncertain and fast moving environment, I advocate the adoption of what I termed a capability approach, to which I alluded in my earlier remarks, and this was the approach that we adopted during the build-up to the Strategic Defence Review in the mid-1990s. The adoption of such a capability approach enables us to manage threats and opportunities – definition: a capability in this context is a function or set of functions that deliver a business or operational effect or outcome. This approach contrasts with a traditional approach of, for example, replacing manned platforms with manned platforms, rather than with a mix of manned and unmanned platforms. In this approach, programme and project managers need to understand and manage the integration of capabilities across enterprises and across enterprise boundaries. That topic I would term capability integration. So consider the mix of combat systems in a modern warship. Highly complex electromagnetic environment and in technical systems, each of which should be able to work in the context of the whole without interference. Almost all capabilities defend on effective partnering

within and across enterprise and business boundaries. I offer the following principles for effective partnering. It's important to note that every joint enterprise must fulfil each and every principle. Evidence over the past decades indicates that failure to comply leads to eventual failure, and I'm going to list them. The first one is absolute clarity in the objective. Second, absolute clarity over accountabilities; who is accountable for delivering what. Absolute clarity over the schedule and milestones. Provision of sufficient appropriate resources. Those may be information infrastructure, they may be bright people, may be financial resources or office space, research laboratories, whatever. Provision of sufficient appropriate resources. Importantly, and this is the fifth principle, the alignment of authority to apply resources with accountability. It is not appropriate for individuals to be held accountable for delivery unless they are given the authority to apply the resources to do that. The sixth principle: clear governance and a lean management structure. Keep it simple. Finally, effective leadership at all levels, an absolute determination to succeed. So there you have Burton's seven principles for effective partnering. I just need to remind you, as I said before I introduced them, that if any one of those is missing on the list on your programme, I can guarantee it will fail.

Okay.

[0:35:12]
On leadership, everybody has a view of good, bad and indifferent leadership from their work experience. They'll also have an apt definition that captures their expectations, and I've found this definition useful. The capacity and the will to rally men and women to a common purpose and the character which will inspire confidence. Now, the proponent of that approach knew a thing or two about leadership. That was Field Marshal Lord Montgomery of Alamein. Other wise and successful men and women have developed their own approach, appropriate to the context of the business, and so will you.

Can you tell us a little about the land digitisation programme?

Certainly. As the Cold War ended the democracies were quick to seize their peace dividend. This feature became evident in 1989 when I joined the British Embassy in

Washington DC as the Military Attaché and Commander British Army Staff. Bold assumptions were being made by politicians and military commanders were responding in order to deliver mandated savings. The core assumption was that the world had seen the end of conventional armoured warfare, the future would be asymmetric operations, for which light, agile forces would be the dominant capability. None foresaw the invasion of Kuwait and the deployment of large-scale, multi-national, heavy armoured formations to the Gulf in order to liberate Kuwait. The outcome is well known, but the repercussions continue across the Middle East. One consequence of the Desert Storm operation was a comprehensive study of lessons identified by the US forces and by their allies. The US Army and other services were well ahead of the British Army in their exploitation and deployment of commercial IT. However, when they deployed formations and units from around the globe and reserve forces from continental United States, the non-interoperability of these systems within the US force structure and with their foreign allies became a major issue. With characteristic thoroughness the US leadership tackled that and many more themes, including what they termed digitisation, and I was clear that the British Army had much ground to catch up. As a generalisation the British Army ICT capabilities lay well behind those of the Royal Navy and the Royal Air Force. The Cold War deployment of the bulk of UK armoured forces in West Germany had concealed the shortcoming. The Royal Navy main effort was devoted to the North Atlantic and the RAF was closely integrated into NATO's air defence capability. The British Army had little expectation of timely ground attack support from NATO air forces, so the modest nature of ground-air communications, for example, was put up with. However, such inadequacies could not continue as the UK sought to adapt its military capability to the new environment. For the British Army, the integration of information and data across the battlespace became a priority. This had to include the management of a legacy of stand-alone Cold War systems. The new capability, the integration of information, data and effects across the battlespace was, and is today, essential for the British Army to fulfil its operational doctrine. Make an aside; I'll define doctrine. Doctrine is a fundamental principle by which military forces guide their actions in support of objectives. It is authoritative but requires judgement in application. The initiative had to involve the whole British Army and constituted a major transformation programme. It also represented unfamiliar territory. We've therefore sought and benefited from advice from external experts in the Ministry of

Defence research community, the Defence Evaluation Research Agency, DERA, and industry. The emerging thinking proved to be useful in our subsequent development of the Joint Battlespace Digitisation Initiative, of which more later.

[0:40:04]
Yes, we're going to talk about the Joint Battlespace Digitisation a bit later, but before I would like to ask you, during which years did you develop the process which led to the Ministry of Defence smart procurement initiative?

Good question. In 1997 I was appointed Deputy Chief to the Defence Staff (Systems) in the Ministry of Defence. That post held responsibility for the sponsorship of the equipment capabilities of the UK armed forces out to 2020. And the underpinning applied research programme. It was clear that all future operations would involve all three services, the term is joint service. It followed that the traditional processes of requirements definition, procurement, acceptance into service and through service support should also be joint. For this to be a practical proposition there was a need for a jointly agreed set of principles to guide thinking and to deliver coherence. In this context the UK joint doctrine provided the approach. For clarification, once again, doctrine represents fundamental principles by which military forces guide their actions in support of objectives. It is authoritative but requires judgement in application. So at the heart of British defence doctrine lay the manoeuvrist approach, a key enabler of which is the concept of information superiority. This approach has been developed in the MoD's thinking on what was originally termed Network Enabled Capability. The exploitation of information and its protection are therefore fundamental to the business of the MoD, the armed forces and their commercial partners. This dependence on accurate and timely information throughout the battlespace required that serious consideration should be given to the interoperability of systems and platforms. Since weapons, sensors, platforms and information systems are of different generations, this becomes a major systems integration challenge for programme and project managers. The systems area advocated the establishment of an integration authority within the procurement community with the authority to mandate interoperability standards. The outcome of this substantial transformational thinking was the systems area team developed four capability areas, comprising all the former projects and programmes. As I recall, some twenty years on, these were the

following: Strike, Manoeuvre, Support and Information Superiority. Each of these capability areas was staffed by officers from all three services. Now, systems engineering principles obliged the system staff to integrate their thinking with the defence procurement staffs and with the then Defence Evaluation Research Agency, DERA, to which I've just referred. And this undertook the MoD's applied and corporate blue skies research programme. So DERA was running on the MoD's behalf the applied research programme and also the blue skies corporate research. This harmonisation of thinking was subsumed by the UK Strategic Defence Review and within that the Smart Procurement Review, tasked by the MoD and undertaken by McKinsey's, with significant input from the systems and procurement staffs as I've just described. And that led eventually to the new acquisition process, integrating processes across the partner communities.

[0:44:21]
You have already mentioned the land digitisation programme. What can you tell us about the Joint Battlespace Digitisation programme?

Fine. The Joint Battlespace Digitisation Initiative stemmed from the land digitisation thinking and was concurrent with the transformational changes that I've just described which led to smart procurement. Evolving joint doctrine required the effective timely integration of information throughout the battlespace and the ability to present it in an intelligible format to all entitled decision makers. While this integration of information offered a significant increase in the effectiveness of defence assets, it also presented new security risks. Integrating legacy systems implied the integration of their embodied risks. In an increasingly inter-dependent world, this remains a major risk area for government and commercial enterprises.

[0:45:32]
When did you start working as a consultant for the government communication headquarters, GCHQ? What was your aim?

In 2000 I was tasked by the Cabinet Office and Director GCHQ to undertake two reviews and to make recommendations. In the first case, recommendations around the arrangements for managing GCHQ new accommodation project in Cheltenham. The

project addressed the provision and commissioning of the building now known as The Doughnut. The second review addressed national information security. I was subsequently tasked to provide strategic advice to the director over the implementation of the recommendations. It's worth noting that the review of national information security led to the appointment of the then e-Envoy, Andrew Pinder, as the Central Sponsor for Information Assurance, abbreviated as CSIA. And he would have been supported by a small team of experts embedded in the Cabinet Office. And the Central Sponsor and his team provided the foundations for the current cyber security initiative.

[0:46:53]
Maybe we can talk about your experience in the Police IT Organisation?

PITO, yes. Police IT Organisation, PITO. This is a subject in its own right, but it offers some interesting insights. I was appointed by the Home Secretary, Jack Straw, to be executive chairman of the Police IT Organisation in 2001 for a three-year assignment. This period would see the start of the most significant re-equipment programme in the history of the police service. PITO was termed by the Cabinet Office as a Non-Departmental Public Body, NDPB. It was answerable to the Home Office and its role was to provide IT and communication systems and services to the police and other criminal justice organisations within the UK. This included operating and maintaining the Police National Computer, known widely as PNC. The challenge presented several key features. These included the police service customer and user community, which comprised three major constituencies: over 50 independent police forces, including Scotland, Wales and Northern Ireland; 52 police authorities; and the Home Office as the sponsor department. An increasing need for interoperability, facilitated by the deployment of the new Airwave nationwide secure communication system, the incoherent legacy approach to requirements definition, procurement and through life support, there was a noticeable absence of an identifiable central customer to define current emerging future requirements. There was an absence of what I call a doctrine for policing. There was an absence of strategic governance and a management structure for the efficient and effective delivery of ICT capabilities for policing. And as a result of these facts and some deficiencies, the police user and customer community were thoroughly dissatisfied

with the service that was being provided for them. So this business context implied a fundamental review and redesign of the whole process for police ICT requirements definition, procurement and through service support. The intent was to accelerate the tempo of delivery of those operational capabilities that would offer the greatest operational and business benefit while delivering projects on time, meeting performance and the cost criteria. All of this necessitated clarity in requirements capture and in the prioritisation of programmes and the continuous improvement of all business processes. Acknowledging the principle that intellectual change must precede organisational transformation, the first priority was to work with the Association of Chief Police Officers, ACPO, to develop a doctrine for policing. This was to provide the underlying approach for the transformation. And the solution included the following features. First the preparation of a draft doctrine for policing, accepted by the Association of Chief Police Officers, and I already mentioned doctrine in another context, but just to remind you once again, doctrine, a fundamental set of principles which police forces could use to guide their actions in support of objectives. It should be authoritative but requires judgement in application. The next feature was transforming the structure of the organisation to reflect the distinct characteristics of the police user and requirements definition process to establish capability teams and project teams whose core business was programme management and through service support. So the five capabilities that we adopted were as follows: the first was communications; the next criminal justice, ICT support; the third was the whole issue of identification, such as fingerprinting. The fourth was business support services, which basically swept up all the other ICT capabilities required for delivering policing. And the final capability was intelligence and investigation. Now, the new structure and processes were enabled by the appointment of a serving Deputy Chief Constable as the representative central customer for those police service ICT capabilities, with the role of gaining agreement of forces for the statement of requirement and for acceptance into service. The central customer was also responsible for addressing the information assurance of current and future systems and this of course was complicated by the fact that the individual forces were interdependent and independent and agreement and conformity to stand as related information assurance had to be addressed on a one-to-one basis, so that is central customer to each of the 52 police forces. Significant police ICT capabilities introduced in the early years of the millennium included Airwave, the new secure

digital police radio communication system, HOLMES 2, which was the Home Office large major enquiry system, the National Automative Fingerprint Identification System, NAFIS, and software improvements for the Police National Computer.

[0:53:19]
So, what led you to set up the UK Telecommunication Industry Security Advisory Council?

Government, individuals and businesses seek assurance of reliable, secure and resilient Critical National Infrastructures, CNI. In the early 1990s the major UK based global communication service providers began to address the upgrading of their information systems and telecommunication services. Commercial pressures to reduce costs led these Communication Service Providers, CSPs, to consider procuring major components from hitherto untrustworthy sources. In doing so, they sought Her Majesty's government's advice on how best to assure reliability, security and resilience in the new infrastructures which would be embodying new technologies. I was invited by the Cabinet Office to establish a forum within which the principal CNI providers could exchange information and contribute to the development of policy on mutual regional, national and international security issues in order to provide a high degree of confidence in the reliability, security and the resilience of the UK's Critical National Infrastructure. And this became the Telecoms Industry Security Advisory Council, TISAC. The Council met three or four times a year at chairman, chief executive level, with comparable representation by government officials. It was jointly chaired by a senior leader from industry - initially that was the chairman of BT - and by a senior representative of government and the Cabinet Office, and initially that was me. This unique joint private/public sector body proved to be an invaluable forum for the discussion of issues of crucial importance to the reliability, security and resilience of UK's Critical National Infrastructure.

[0:55:34]
What is the Information Assurance Advisory Council? What was your role?

In 2007 I was invited to relieve Baroness Neville-Jones as chairman of IAAC, the Information Assurance Advisory Council, and that was a role that she'd undertaken

for several years. IAAC is a unique not-for-profit organisation that brings together a community of some 600 or so professionals. It includes corporate leaders, government officials, members of the defence, security and law enforcement communities, academics and scientists and technical experts, in order to address information assurance and related challenges and opportunities faced by our information society. It was originally set up in 1999 and since then it's been at the leading edge of many of the developments in IA and cyber security thinking in the UK, maintaining a non-partisan position on matters affecting the way society uses and protects information. The board comprises a chairman, vice-chairman and company secretary, all in a pro bono capacity. Government officials from the Cabinet Office, National Cyber Security Centre and the Department for Culture, Media and Sport, and a number of private sector sponsors who pay an annual subscription that funds the IAAC programme of research, discussion, workshops, projects and related activities. IAAC's activities fall into six broad categories. We have private discussion meetings which are held quarterly as dinners with a senior speaker under the Chatham House Rule. We have a number of research themes. Examples over recent years include implications of cloud and mobile device standards and the need for revision, the issue of identity assurance, organising against cybercrime, addressing the risks and opportunities of social networking and social behaviour, looking at the impact between the citizen and the Internet of Things. And currently and very importantly, development of the information assurance and cyber profession. The academic liaison panel which we've formed, established and supported a group of academics from the most active cyber security education providers, developing ideas and improving co-operation between them. We ran a series of workshops and those are still running today, a regular programme with scope for impromptu events to meet urgent needs. So IAAC's an agile organisation and can respond very rapidly to new thinking. The projects IAAC has undertaken include developing a framework for a young IAAC, now called IAAC Access, for young emerging cyber professionals. Project includes supporting the North West young people's cyber security safety initiative and undertaking a cyber security internship pilot scheme for the former Department of Business, Industry and Skills.

[0:59:12]
So 2008 was a critical year for the Ministry of Defence because of the losses of data that occurred. So what can you tell us about these losses of data and about the subsequent data handling review and the Burton Report which bears your name?

Yes. First point to make is that the entire Burton Report has been published on the internet, you can find it on the Ministry of Defence website. I believe it's also on the Hansard website. So it's open to all to see.

Yes, I downloaded it.

And I strongly recommend it, because the 51 recommendations are still of relevance today. So my first recommendation is that the Burton Report into the loss of MoD personal data, which was published on 30th April 2008, merits reading in detail. Why, you may ask. To which my answer is, because the majority of the recommendations are relevant to most government and private sector enterprises today and should be understood by all in leadership and managerial roles – underline 'all in leadership and managerial roles'. The data handling review, also known as the Hannigan Report, sought to collate the findings of four major reviews into government data losses in 2007/2008 and to issue guidance and direction. I was invited by the Secretary of State for Defence and the Permanent Secretary of the Ministry of Defence in January 2008 to undertake the review of the circumstances that led to the loss of the data and considered a broader MoD approach to data protection. The detailed terms of reference were to establish the exact circumstances and events that led to the loss by MoD of personal data. To examine the adequacy of the steps taken to prevent any recurrence and of MoD policy, practice and management arrangements in respect of the protection of personal data more generally, to make recommendations and to report to the MoD's Permanent Secretary not later than the 30th April. The report was published in two parts with an executive summary. The first part set out events leading to the loss of data on 9th January 2008, covering issues relating to the Training, Administration and Financial Management Information System, TAFMIS, and the related policies and procedures. The second part to address the broader MoD approach to personal data protection. My 51 recommendations are summarised in Annex 8 of the report, and again, I strongly recommend IA and cyber professionals

should revise or read them for the first time if they haven't already done so. The Secretary of State and the Defence Board accepted all 51 recommendations and directed that the Board should supervise their implementation. In this brief overview it's worth making four major observations. First, information, knowledge, data and our people are critical enterprise assets to be developed and protected accordingly. A recurring theme in my last remarks. However, information risk was not on MoD's risk register. Unknown to the user – second point – the lost laptop, which is one of several stolen from parked cars, in clear breach of security regulations, contained some 600,000 personnel records and up to 400,000 records of family and next of kin.

That's impressive.

The database, which was not encrypted, breached most of the principles underpinning the Data Protection Act. Fourth point, the recommendations fell into four main categories: processes, 31 recommendations; people, eleven recommendations; training and education, five; and significantly, technology only three. I suspect that many people thought that technology was a major issue, it was not. The lessons are there for you to see; processes and people were dominant, but training and education, delivering understanding and proper processes are key. So my comment is, technology is a neutral issue, education delivers understanding, training shapes behaviours, effective leadership of well-motivated people and careful management of resources, processes and contracts enables information risk to be minimised.

[1:04:44]
Thank you. So, what do you think are the main issues in regards to cybersecurity today?

I believe the UK must concentrate on delivering the objectives set out in the cybersecurity strategy which was published in 2016. In particular, concentrating on achieving a real improvement in the coverage and quality of the provision of cybersecurity education and training. Work is in hand to tackle this important issue but progress since the launch of the first information assurance strategy in 2003 has been disappointingly slow. The tempo must be raised with close attention being

applied by the leadership across schools, colleges, universities and enterprises, all are involved.

[1:05:37]
So let's think a little bit about the future. What do you think are the biggest challenges and issues related to IT and security for the next five years? And what do you think will change in twenty years?

Prediction is an uncertain business, but I can envisage the following. Increasing emphasis and resources being given to addressing ICT and the cybersecurity understanding the skills, both for the benefit of society and to meet the needs of employers across the public and private sectors. Legislation and regulation continue to lag technological advances. The gap may narrow, but will continue to be a concern. The ethical issues arising from ICT innovation are not being addressed with sufficient vigour or rigour. The medical profession has tackled emerging ethical issues over recent years. The ICT communities must do likewise, seeking good practice and appropriate insights from other disciplines and professions. Users of ICT systems and services are being presented with flawed software. This is unacceptable. Legislation and regulation have addressed this issue in the hardware domain, increasing attention must be given by private sector providers, and by customers to insistence on trustworthy software. Traditionally, professional institutions have evolved to support the development of professions and to encourage a good proportion of well-motivated young people to join. However, the reality of interdependence across national, international and enterprise boundaries and the dependence of all on the integrity, resilience, availability and assurance of our ICT infrastructures and the data they carry obliges nations, enterprises and individuals to treat cybersecurity and resilience as a cross-disciplinary, cross-community issue of vital importance. The professional institutions must develop means of working co-operatively to ensure that technical and ethical issues are identified and resolved jointly.

[1:08:11]
Thank you. And to conclude I would like to ask you, what was your proudest achievement during your whole career?

Well, that's an excellent question. I think as I look back on several decades of professional work, I think that being allowed to work with teams of well-motivated, highly capable and committed young people who are determined to make a real difference and an enduring difference has been the most memorable and proudest aspect of my whole career.

Thank you, Sir Edmund, it's been a real pleasure talking to you.

Thank you, Elisabetta.

[1:08:58 recording ends]