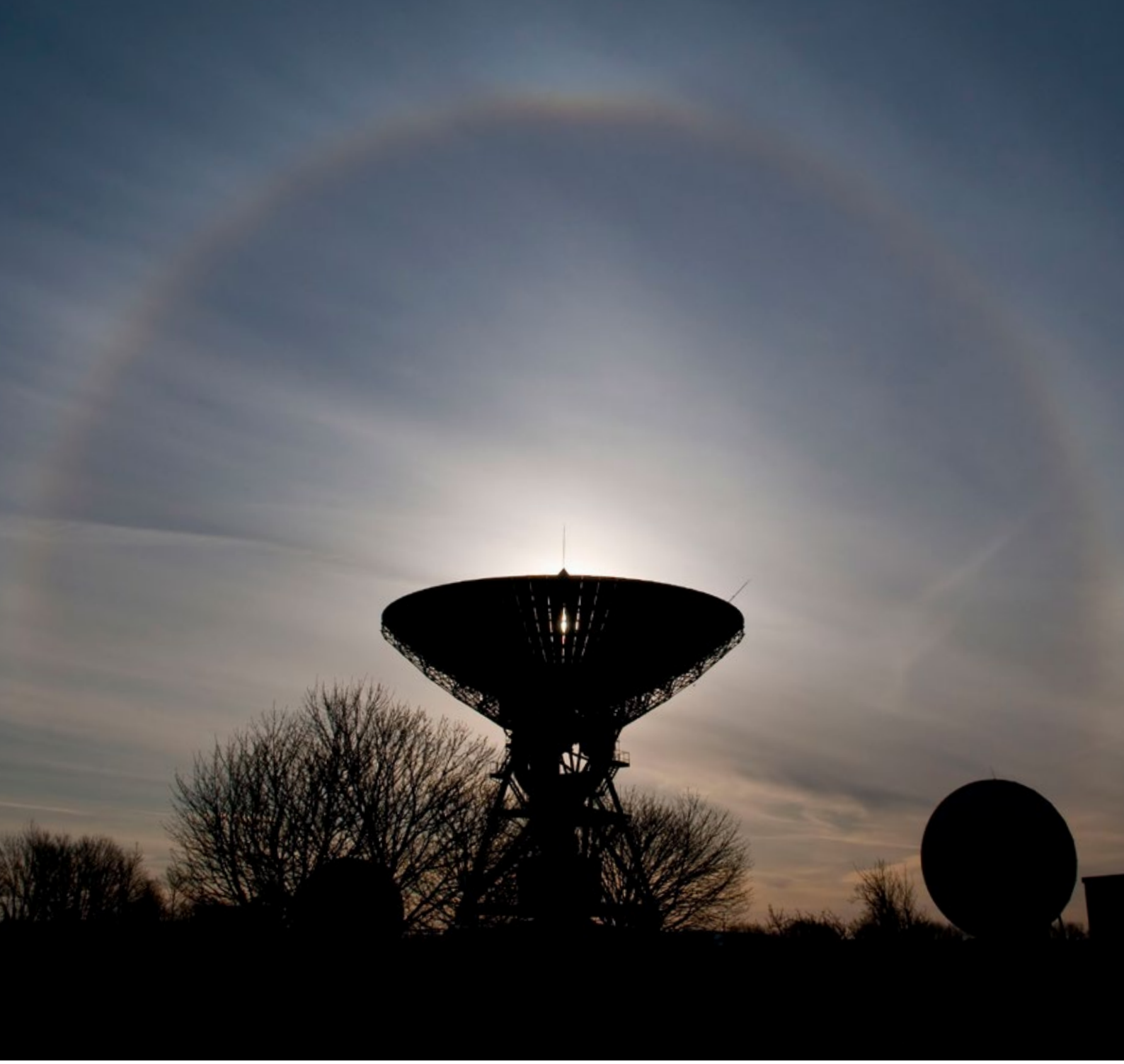


Protecting the UK's Critical National Infrastructure

Defence and Security Information Circle

BT

“We are threatened by adversaries exploiting pervasive new technologies. It is only through trusted partnerships across Government and industry that we will be able to counter this threat.”

We would like to thank the following contributors
Air Marshal Phil Osborn CBE, Chief Defence Intelligence
Group Captain Ian Chesworth, Deputy Head Ops, Joint Force Command
Professor William Buchanan, Edinburgh Napier University
David Ferbrache OBE, Technical Director – Cyber Security, KPMG
Mark Hughes, CEO, BT Security
Alex Healing, Chief Researcher, BT
Richard Baker, Cloud Security & Futures Architect, BT
Rob Partridge, Head of Cyber Academy, BT
As well as Professor Michael Clarke for his contribution and facilitation at DSIC17

Improving Our Individual and Collective Cyber Resilience

Phil Osborn
Air Marshal CBE

I was privileged to be the keynote speaker at BT's annual Defence and Security Information Circle, to discuss how industry and MOD could work better together on protecting the UK's National Critical Infrastructure from cyber-attack. The Government and MOD continue to invest significantly in the protection of critical UK Defence and security assets, and the National Cyber Security Centre is already a major player in this arena. However, in a world where attackers continue to seize any opportunity to exploit vulnerable systems, there is no room for complacency. The recent series of cyber events serve as yet another indicator, if one were needed, of the threat to Government, and to our key capabilities and public services.

Hence, as our operational environment shifts to include virtual as well as physical threats at home and overseas, we need to ensure that we properly understand the robustness and resilience of our military capabilities, as well as their battle-winning advantage. Indeed, the security challenges we face and the nature of our potential adversaries demands that information and data are placed at the heart of our thinking about operational capability and resilience. In this, we must aggressively exploit emerging technologies such as artificial intelligence, big data and quantum computing. We must also be even more imaginative in building a national cadre of cyber specialists and to ensure that the recruitment of vitally skilled individuals does not become a zero-sum game between Government and industry; this should of course include even greater use of the already highly successful approach to reservists.

However, the threat is moving at pace, which leads me to the need for openness and transparency; not always easy in a security environment, but nevertheless critical for all of us who are focussed on defence and protecting the nation. We know that, in addition to enjoying the advantages of today's information age, we are also threatened by adversaries exploiting pervasive new technologies. It is only through trusted partnerships across Government and industry that we will be able to counter this threat. We will need to strive to work together more effectively, guided by the National Cyber Security Centre; we need to be more open and transparent, to more actively share information and vulnerabilities, and to work collaboratively to mitigate a threat which targets all of us.

In reviewing these extracts from the Defence and Security Information Circle, let me leave you with one question... how can we work more closely to improve our individual and collective cyber resilience? The answer to this question is at the heart of ensuring that our shared contribution is decisive against the sophisticated and growing cyber threat.

The Global Cyber Challenge

The growth of the global cyber sphere is well documented but not so well understood. In 2000 around 3% of the global population was connected via the internet. By 2010 it was 30%; by 2015 40% and by 2020 is expected to be around 80%. That translates – within the next three or four years – into internet connectivity between over 4 billion people, embodying 25 million apps, 25 million embedded and intelligent systems; probably some 50 billion connected devices containing 50 trillion gigabytes of data.

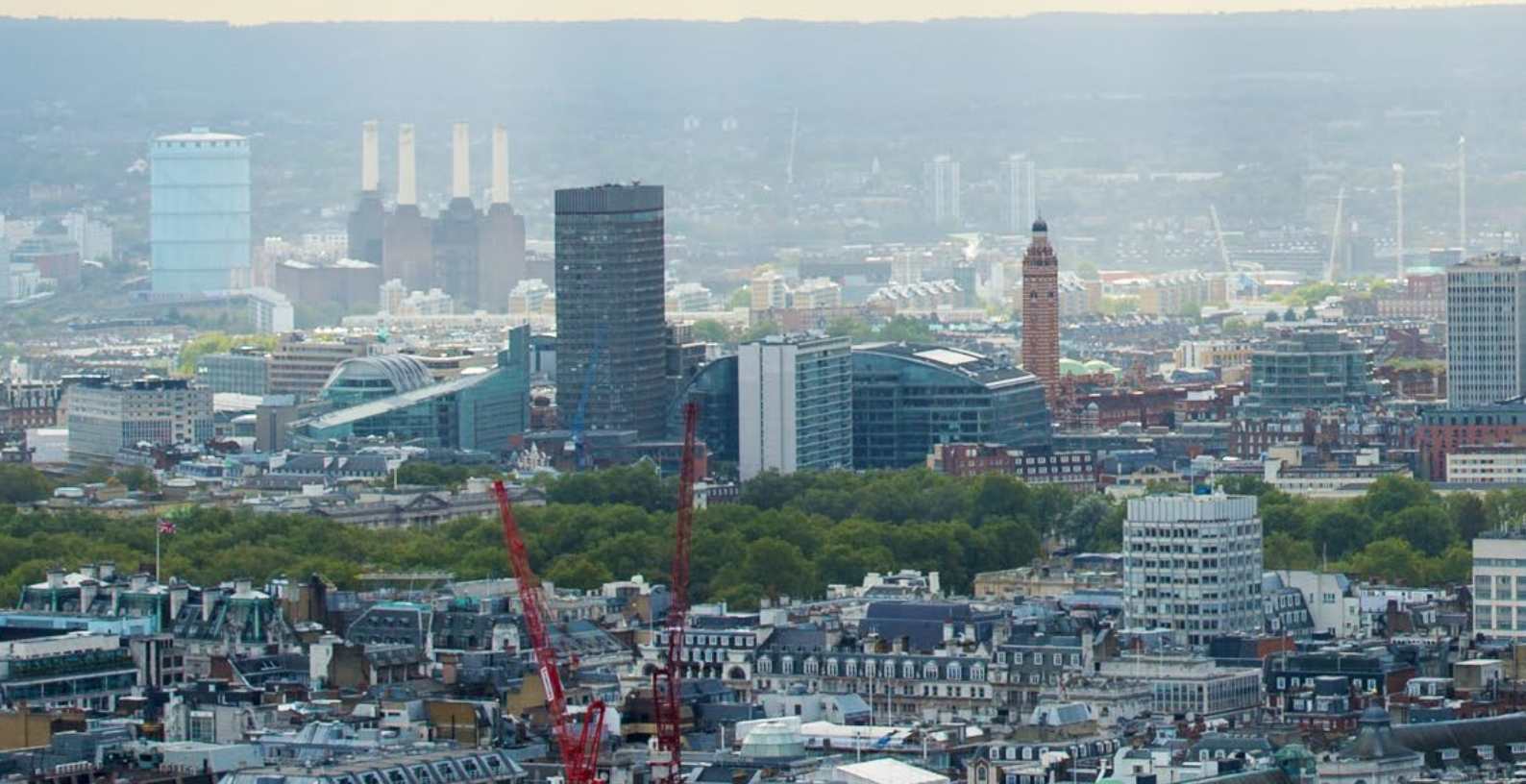
The biggest growth areas for cyber technologies in the next decade will be in Asia, Africa and Latin America. The guardians of cyber space have long been the western companies and their governments who invented and exploited it both for their own purposes and for the international common good.

But this is changing as natural economic competition becomes more global and the cyber market expands outside the sphere of the OECD countries. At present, over 80% of global internet traffic is handled by around 25 leading Internet Service Providers (ISPs). This will soon change, regardless of what the ISPs may do to protect their market positions. Not least, the manifest vulnerabilities of cyber-enabled technologies have become impossible to ignore from both security and business perspectives.

Noted examples of such vulnerabilities include

- the blackout across western Ukraine in 2015 and again in 2016 through spear phishing malware
- the historical malware that is already estimated to be embedded in Critical National infrastructure (CNI) throughout the developed world
- the 'Kemuri Water Company' hack of 2016 (anonymised to avoid panic since cleaning chemicals were switched to high levels in a major water supply by hacking into control systems)
- the massive and persistent use of botnets, in particular, across the USA
- the damage done to the German steel industry in 2014 through spear phishing malware.

The effect both of competition and vulnerability is to encourage the increasing 'balkanisation' of the internet. Authoritarian governments around the world become determined to control their citizens' use of it; and western governments and companies become increasingly anxious to ring fence secure areas of cyber space that most matter to them.



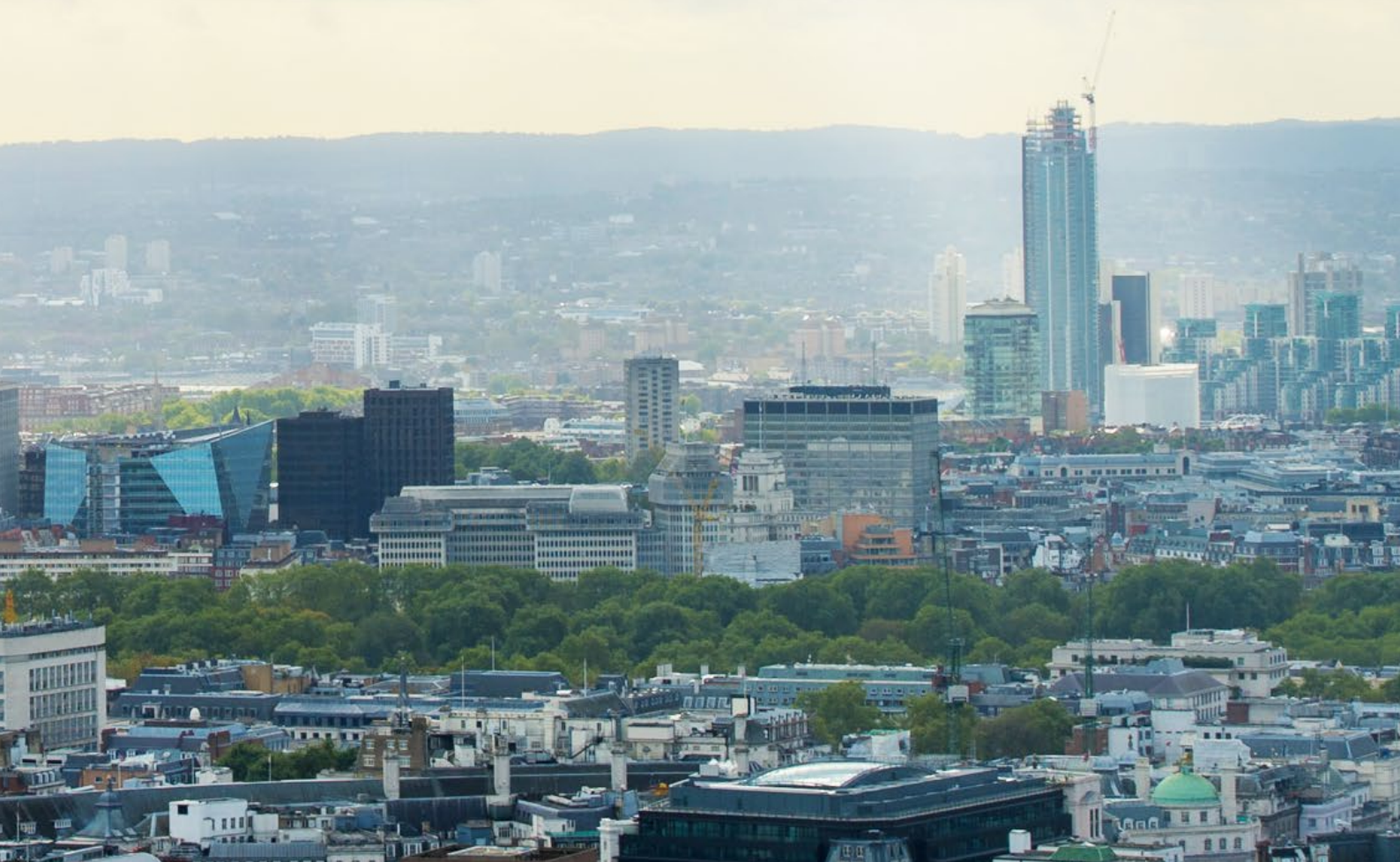
The Policy Challenge

The global economic crisis has been deep and long. The world economy is recovering from it slowly and sluggishly and is still flat-lining after almost a decade of persistent crises. Cyber-enabled economic development is the only consistent bright spot in the global economy. It is estimated that it will account for around 2-4% GDP growth in the developed economies and up to 10% GDP growth in the emerging and less developed economies.

Cyber security has always lagged behind the transformative advances in cyber technology, both in the commercial and also the military and security spheres. But if future GDP growth across the world is so driven by cyber-enabled technologies then the essential policy challenge for DSIC17 to address could not be clearer.

"It is necessary, and urgent, to align the strong economic imperatives behind cyber technologies with the security agendas that matter most to free societies and open economies."

Professor Michael Clarke, Chairman of DSIC17



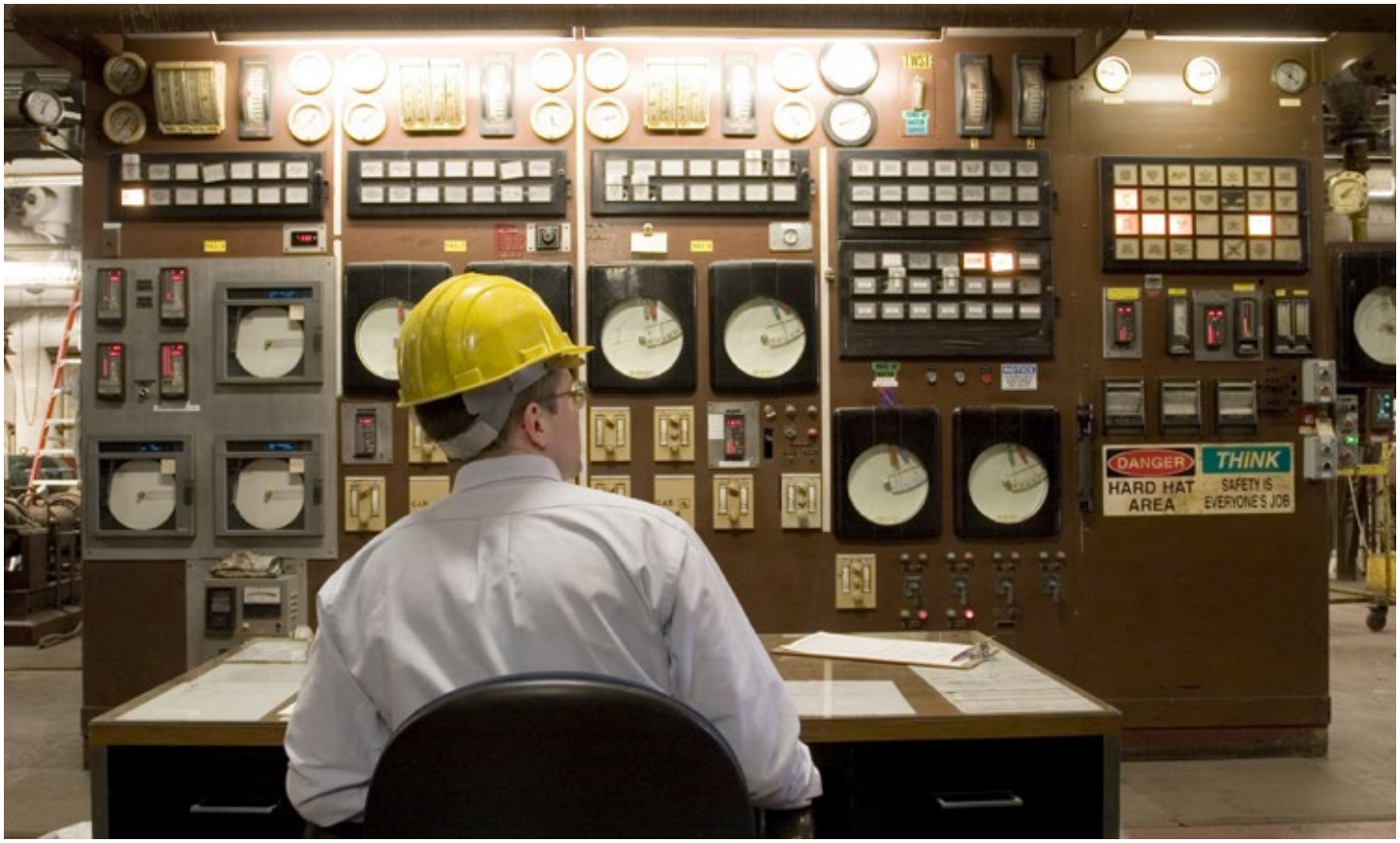
The Geopolitical Security Realm

Over the last five years a new landscape in cyber security has emerged. The teenage geeks who computer hack for fun are still operating and their skills are improving, but the most serious computer hacking lies in the realm of highly organised criminal gangs and governments around the world.

For criminal gangs there is great financial gain in targeting a small number of high value institutions for fraud or extortion, as well as in targeting high numbers of small institutions or individuals for small and marginal monetary gains. Either way, high financial returns at low risk are available for criminal investment in compromising cyber-security wherever it becomes evident. In 2016 the World Economic Forum estimated that the cost to the international economy of cyberspace crime was at least $445 billion.

For governments, strategic economic advantages, political gains and traditional espionage objectives can all be pursued at unprecedented scale and low political risk by taking advantage of cyber insecurities. Government can put a great deal into cyber hacking. For example, the massive 2015 attacks on the infrastructures of Ukraine, reliably ascribed to Russian hackers, appears to have been six months in preparation and intended as a clear demonstration of state-backed hacking powers to the leadership in Kiev. The exercise was repeated in the early months of 2016. Terrorist and malign non-state groups, too, have found that investment in their own cyber capacities add new dimensions to their operations. While 'cyber-terrorism' is not yet an established phenomenon, the potential for it to emerge is acknowledged, and cyber elements in more traditional terrorist activities make the exploitation of cyber insecurity very attractive to terrorist groups.

The global landscape in cyber-security is therefore not consistent and can be seen to revolve around four differing planes, not all of which are moving along the same trend lines, as shown opposite. It is not possible to predict how these differing planes will interact with each other but they are nevertheless interdependent and 'technologically contagious' one with another. These four planes together shape the global cyber infrastructure for the rest of the world and dominate the current politics of cyber-security.



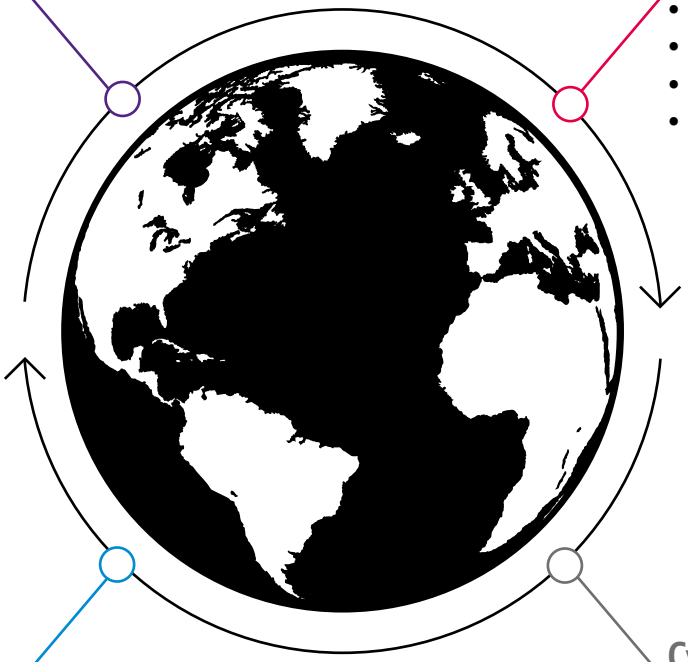
Black Swans

US-China Cyber Détente Collapses

- Relations deteriorate
- IP theft ramps up
- Many sectors targeted
- Economic warfare

US-Russian Cyber Cold War

- Sleepers installed
- Infrastructure targeted
- Signalling intent
- West held to ransom



Taking Africa Offline

- Massive botnet
- Build from IOT
- Creates large scale DDOS attack
- Overload African internet

Cyber Terrorism Arrives

- Successful example
- Infrastructure targeting
- Transport disruption
- Refinery attacks
- Rapid proliferation

Global cyber infrastructure is challenged in four different planes

China-US relations
The fragile 'cyber détente' between them is threatened by pressures created by their intense economic competition

Russia-US relations
Western security is held to ransom by cyber hacking practices between them and a new 'cyber cold war' appears already to have emerged

Africa-as an example of a digitally challenged continent
Large parts of the continent risk being taken offline by the massive use of botnets to create DDOS attacks, while certain countries offer poorly governed spaces harbouring cyber crime

Terrorism and the Middle East/South Asia
Cyber dimensions of terrorism in all its forms exist throughout the cyber infrastructure and have particular relevance to systems operating from and through many countries in the greater Middle East and many parts of South Asia and the sub-continent

UK Defence and Security: Skills and Partnership

Many public sector watchdogs as well as intelligence and cyber agency chiefs have warned that public services and important parts of the UK's critical national infrastructure will rapidly have to be made more secure. The newly created National Cyber Security Centre has pointed out that cyber threats to CNI and public services have never been higher.

More to the point, there may also be a critical skills shortage in the UK very soon. The UK's cyber skills shortage, at least measured by the number of people responding to relevant job vacancies is second worst in the developed world, next only to Israel, according to a survey by Jobsite Indeed in January 2017.

While employer demand for cyber security has grown steadily by 2-3% every year and directly relevant job vacancies increased by almost 32% between 2014 and 2016, "employer demand exceeded candidate interest by more than three times" according to Jobsite Indeed. At the very least such findings suggest that unless something is done urgently, there will be a lag, if not a long-term shortage, in the provision of key cyber skills relative to the ever-increasing demand for them. In March 2017 the outgoing Director of GCHQ, Robert Hannigan, warned of a "huge skills shortage" in the UK unless action was taken very quickly. In November 2016 the government announced that it would commit £1.9 billion over five years to promote cyber security in the UK – a figure that almost doubles the previous commitment made in 2011, and as Chancellor Philip Hammond said of this allocation, "the country's 'cyber workforce' will also be increased to improve protection against attacks".

And within the Ministry of Defence the Secretary of State announced in October 2016 a £215 million boost in funding for the development and hardening of military cyber systems, including support to the Cyber Vulnerability Investigation (CVI) programme which seeks to analyse and understand the risks across the MOD as a whole. This commitment complements the establishment of the Cyber Security Operations Centre, announced in April 2016 with £40 million in funding to protect the MOD cyber facilities and followed the signing of a US-UK Memorandum of Understanding for the two countries to work together more closely to address a range of defence cyber-security issues.

Nevertheless, Joint Forces Command and the Defence Intelligence organisation understand that there is some catching up to do, both in defining the areas and the depth of the CNI that really matters to defence and also in developing the appropriate partnerships with industry to address both human skills and new technologies. The aim is to create a more seamless coverage to make the UK as cyber secure as possible and offer cyber security as a competitive economic edge for inward investment – in the same way that the City of London and UK law have the power to attract global investment.

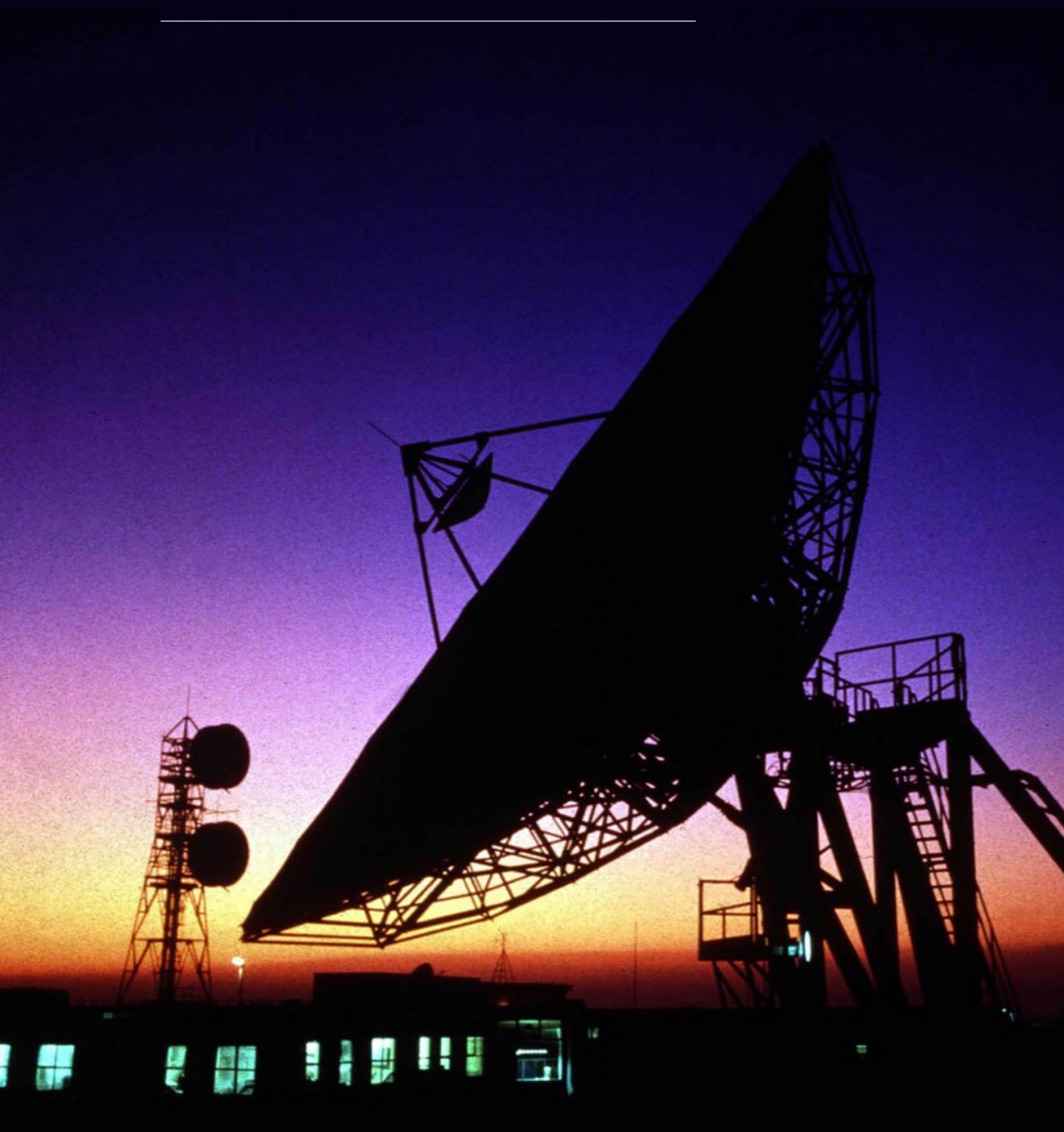
Resilience in defence, as well as in business terms, is not merely physical but based on trusted partnerships. The MOD's relationships with its industrial and commercial suppliers is a critical one and the MOD welcomes honest discussions about cyber vulnerabilities with its suppliers and commercial partners. The MOD must go beyond developing 'public safety messages' to the civil sector. Indeed its current message to its suppliers and commercial partners is clear.

"Cyber attack is one of the greatest challenges to our security. It's crucial we use our increasing defence budget to stay ahead and investing in this programme will help us protect against these threats."

Secretary of State for Defence, Sir Michael Fallon, October 2016

"You will not lose contracts with the MOD by sharing with us honest assessments of your cyber vulnerabilities – quite the opposite, in fact. We want to work with you to reduce those vulnerabilities, not discover them afterwards when you had reassured us everything was absolutely fine."

Air Marshal PC Osborn, Chief of Defence Intelligence



UK Business: New Types of Thinking

Over 12% of the UK's GDP is created through its digital economy – the highest proportion within the G20 countries – and is growing all the time. It has one of the biggest online retail sectors in the world, worth almost £11 billion last year.

In the face of such facts organisations are certainly aware of the business risks associated with cyber-security but struggle to appreciate the likely impact for themselves of cyber events that might occur. In the UK only a range of between 22% and 44% of businesses regard themselves as 'fully prepared' in the realm of cyber-security and only 23% are insured specifically against the costs of cybercrime against them. Some 45% of UK businesses lack the appropriate skills or resources to defend themselves adequately. Cyber threats tend to be regarded by business leaders as another category of business risk, like a competitor brand, which can be quantified and to which there is a commercial response.

But digital crime is rising at an astonishing rate and the increasing sophistication and tenacity of cyber criminals means that no organisation can be 100% assured that all its systems are secure.

The exponential growth of the Internet of Things (IoT) and the Industrial internet of Things (IIoT) is transformative for the cyber challenge and presents a different order of business risk that companies must deal with in different ways. The working cultures that support Industrial Control Systems (ICS) are naturally conservative but IoT working cultures are the exact opposite, valuing cross-sector connectivity and anarchic innovation at all levels. As the IoT and the IIoT technologies mature so organic growth models, cloud computing norms, third party access to systems at all levels, external maintenance providers, remote support, personal devices, and so on, will all pose new conceptual challenges to the cyber-security professional.

In essence, businesses must view their ICS and IoT/IIoT architecture in a completely integrated way, and this will require as much of a cultural shift as an intellectual one to encompass the conceptual challenges these technologies pose.

Cyber insurance will be increasingly necessary to hedge against the financial losses liable to be caused by cybercrime and this will only be obtained by companies when they have demonstrated adequate security measures. To date, the insurance industry is not fully geared up to take on this line of business to the extent that may be necessary, but ultimately, the insurance industry will largely determine levels of tolerable cyber security for different commercial and industrial sectors across the economy.

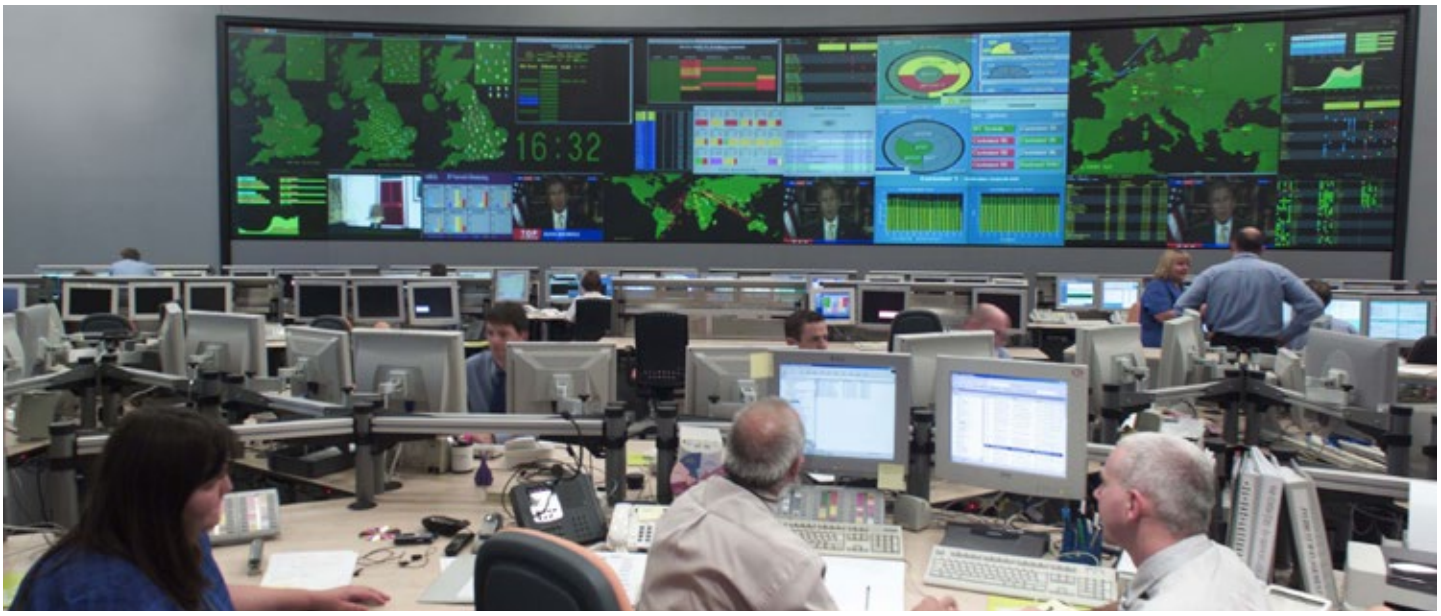
Cybercrime, in short, is not just an issue between competitors but a risk to the whole commercial community and should be seen as such.

The measures the insurance industry will use to determine tolerable levels of risk will revolve around the ability of industry to make successful cyber attacks more difficult, more costly and much less profitable. This will depend on a number of factors such as:

- decreasing the attack surface of systems by building high security into them at the design stage, not as a later addition
- increasing the speed of detection, forensics and recovery processes in the event of cyber attacks
- having personnel trained and available to deal with cyber events and the headroom for them to participate in urgent response forums
- developing partnerships with law enforcement agencies that can be quickly activated in trusted ways when the need arises
- creating systems of shared information with peers to understand emerging threats, best practice and current challenges
- understanding the conceptual challenges of the IoT/IIoT technologies alongside their transformative commercial, financial and efficiency potential.

The BT Approach: Scale and Partnerships

BT responds to these challenges in a number of ways; as a key UK business in itself, as a major provider for large parts of UK industry and society, and as a trusted partner for the MOD. In all of these domains BT is able to operate at scale and make a strategic difference to the cyber security of many sectors of UK society, from the individual customer to the largest government organisations.



An anonymous quote, widely attributed to Albert Einstein, but never actually said or written by him, encapsulates the promise perfectly:

"Computers are incredibly fast, accurate and stupid; humans are incredibly slow, inaccurate and brilliant; together they are powerful beyond imagination."

Offering resilience in everything from broadband connectivity to TV and sports content, mobile networks and services, and handling an ever-increasing volume of traffic, BT works to provide the highest levels of security and confidentiality. In this respect, BT is like the MOD and both organisations working in partnership represent 'scale' at an impressive and effective level. For these reasons, BT works closely with law enforcement and the security agencies, as well as the MOD, and draws in other commercial partners to augment its own threat intelligence and techniques.

Like the MOD, BT takes a proactive stance on cyber-security, pre-empting attackers and disrupting groups and plots rather than relying only on defensive and reactive measures. It strongly supports the work of the National Cyber Security Centre, putting people and resources into the NCSC, providing cyber defence services for its customers and helping to build cyber skills in the wider community. BT's own 'Cytadel' programme has just received a five-year investment from the company to protect its own 'crown jewels', harden BT's own business estate and create a proactive defence posture throughout the company.

Operating at such scale, BT is able to put a value on cyber risk and make clear business investment decisions on that basis. This, too, provides vital new pointers to the MOD, government organisations, BT partners and customer organisations in the sizing and evaluation of cyber risk as a new dimension in business costs, and benefits.

As it researches new technologies BT invests a great deal in investigating the potentials of artificial intelligence, of visualisation as a tool for new conceptual understanding, and petabyte (10 to the power of 15) scales of computation to identify significant relationships in highly complex datasets. In analysing ultra-complex datasets a great deal can be derived from human biology – lifting 'artificial intelligence' (AI) to 'intelligence amplification' (IA) and design automated processes to be integrated with intuitive human processes rather than set as separate entities. In a joint project with the University of Oxford, part funded by Innovate UK, BT's ability to provide visual interfaces with machine learning pattern detection has worked extremely well in helping specialists to plot essential interactions between ultra-complex datasets.

Addressing the Cyber Skills Challenge Directly

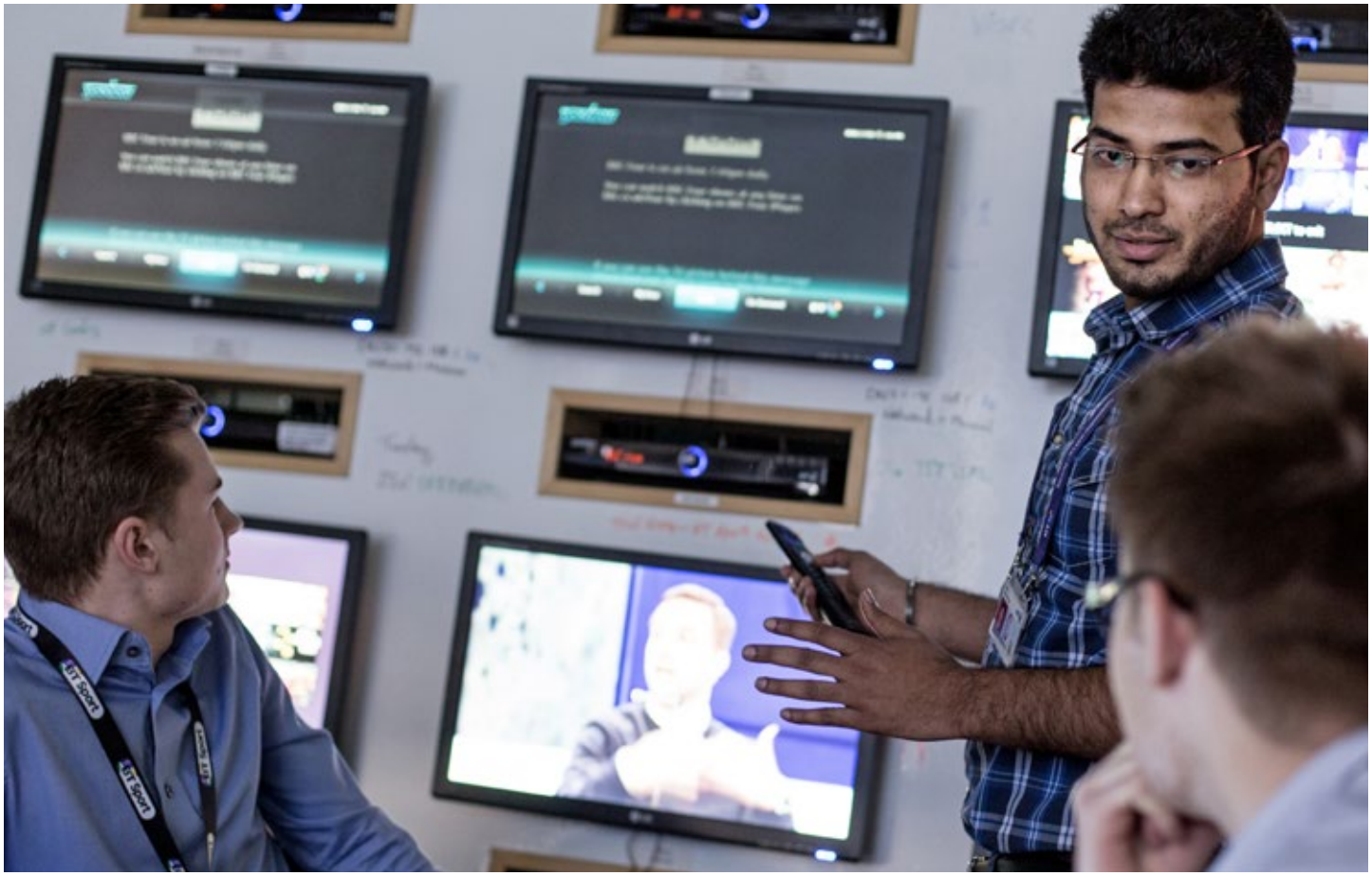
BT established the Cyber Skills Academy based on a manifest need to invest in such education and training, both for its own sake and that of the wider security and economic health of the UK.

A series of detailed studies of the cyber skills gaps among key international companies operating in the UK and abroad revealed a number of key challenges in the current situation. It is evident that recruitment to such companies of individuals with requisite cyber skills, and in particular in cyber-security skills, is a persistent – and growing – problem. There is a shortage of skills particularly in implementing secure systems, which is identified as the single greatest perceived need by most companies surveyed. Furthermore, other evident shortages are perceived in operational security management, incident management, and information risk management.

Of equal concern, however, is an anticipation among companies that the cyber skills challenge will grow exponentially with the rapidly changing pattern of work practices driven by the business use of social media, access via fully mobile platforms, the use of multiple personal devices and the burgeoning of artificial intelligence (AI) in all branches of industry and commerce. More flexibility and adaptive ways of working across an information-rich, globalised world economy – so attractive in the pursuit of lower cost efficiency – is also acknowledged by industry to require an urgent step change in the depth and extent of available cyber skills.

There are both formal and informal reasons for such growth and serious shortages. In formal terms there are limitations on what the national education system provides:

- too few school students are attracted to study the STEM subjects in general and are unaware of the burgeoning scope of cyber and cyber-security careers in the commercial sector
- even those who study STEM subjects at school go on to pursue relevant degrees in computer science, which do not normally contain up-to-date elements in cyber-security
- there are insufficient opportunities for students to gain relevant work experience in cyber skills and especially cyber-security skills and thereby in understanding their relationship to business skills and commercial success
- traditional university recruitment procedures may have the effect of excluding individuals with the right technical skills but less appropriate formal qualifications, notwithstanding their commitment to promoting more 'open access' recruitment
- in informal terms, however, some of the problems are more profound and will require big elements of cultural change across industry
- where communities of cyber graduates exist there is a notable lack of attendant soft skills and business awareness that would enable cyber-security to be more easily integrated into business planning, and be properly explained at all levels of management up to board level
- software developers, programmers and computer engineers, too, do not share enough common ground with cyber-security specialists to engender a single business culture that embeds security awareness and protocols into business models, as standard
- too little shared understanding exists to create inherently high – and dynamic – levels of security for information and control systems, for robust software and to reduce the long-term need for remedial action.



The educational challenge

Educational pathways to such an integrated approach do not currently exist, though they are acknowledged by some educational leaders in the field. Edinburgh Napier University's School of Computing, led by Professor Bill Buchanan, for example, has always accepted the validity of Benjamin Bloom's famous Taxonomy of Educational Objectives, published after 1956, that articulated the differences between cognitive, affective and psychomotor domains of learning. This was an important milestone in understanding the complexity of human learning, as well as the tasks of the educational institutions trying to promote it.

But today's cyber educational challenges, as Professor Buchanan expresses it, are far more complex and multi-layered. There is no logical distinction between academic practice and professional practice – even though there are big distinctions between them in the current climate. Incident response and management is not merely a problem for practitioners; they should be part of academic training in itself, as should cyber forensics and the integration of data for cyber security. Security Information and Event Management (SIEM) tools, for example, are intrinsically part of a proper cyber-security syllabus.

Cyber education, in short, should be about both education and training, highly practical and immersive in the way it is approached. Scenario-based educational courses are essential and the field constantly requires new skills; in operating systems, cloud architecture, incidence response, cryptography, coding, and so on. For these reasons, it is difficult at present to define a 'cyber-security professional' as the field touches every aspect of cyber applications to business. Nevertheless, it is imperative that specialists are trained and that a discipline of cyber-security is developed – fusing intellectual, technical and business skills, based on immersive educational techniques, and embodying the essence of individual learning so that the cyber professionals of the future can respond with flexibility and innovation to new cyber challenges.

Cyber challenges, in effect, take Bloom's famous taxonomy to new levels of complexity and make learning demands on individuals that he might generally recognise but could hardly have anticipated.

The BT Cyber Academy

BT is making significant contributions to help address the cyber skills gap. An important part of BT's approach is the establishment of the BT Cyber Academy, whose mission, quite simply, is to develop the workforce of today and help create the right workforce for the future. It aims to attract talent from all age groups and from all parts of the world to bridge the cyber skills gap and thereby create the momentum to implement continuous improvement.

Implementing the vision

The BT Academy subscribes to the educational approach that is based on immersive, self-learning and it translates it into practical outcomes by adopting a 70/20/10 rule. It structures its programmes around an expectation that: 70% of learning will be highly practical, on the job, education; 20% will be mentoring, which is the essential accompaniment to on the job education; and 10% will be via the classroom and self-study reading. The Academy understands that proper self-directed learning requires high levels of investment, not least in mentoring and monitoring. It also understands that formal learning is still a highly necessary – though not sufficient – condition of proper education. But the principle of Academy education is to provide the space for students to learn for themselves; to make mistakes (safely) and analyse their own failings, and to provide a 'cyber playground' that encourages individual learning, inventiveness and innovation. It intends to create a workforce whose skills are dynamic and thereby capable of moving with, or ahead of, global cyber challenges as they emerge.

"The art of learning – 'study hard what interests you most, in the most undisciplined, irreverent and original manner possible'."

Professor Richard Feynman
American theoretical physicist and Nobel Laureate

In essence, the Academy identifies lines of essential and interdependent progress to achieve these objectives:

- to articulate and enshrine a dedicated discipline of cyber-security
- to influence and further develop the workforce of today in cyber-security.
- to influence the professions in an awareness of the discipline of cyber-security
- to embed continuous learning, improvement and innovation within the development of the cyber-security discipline.

These objectives have to be approached simultaneously rather than sequentially; they are fundamentally interdependent and have to be enacted as part of an integrated design for learning that not only builds skills but also helps to change important aspects of business culture. This is expressed in the infographic opposite.

Academy Learning

Influences associated professions

To implement appropriate security knowledge levels to all stakeholders

Develops a security profession

To ensure the increased pipeline and supply of competent cyber professionals to meet growing demand levels within the industry

Promotes a learning culture

To ensure the industry is a trail blazer in integrated and effective learning solutions

Develops the workforce of the future

To increase the pipeline of cyber capable people available to the industry

Implements continuous improvement

So that Security knowledge and skills are understood and managed to exert a positive influence over the demand and supply of the security team

Develops the workforce of today

So that the industry has the right people with the right skills and knowledge to be able to do their jobs

Discovers and recruits talent

To ensure the industry has the right people with the right skills and potential to ensure a brilliant operation

These lines of progress can be broken down further into multiple sets of targets of the work and sub-tasks to be performed – in order to achieve academy integration and thus continuing learning at all levels, as outlined below:

Develop the workforce of today

Your people can do their jobs more efficiently, and keep your stakeholders more satisfied.

- Formal learning
- "Give back"
- Work based learning
- Career transition
- Social learning
- Learning perceptions
- Learning catalogue
- Skills assessment
- Academic programme

Develop the workforce of the future

You are able to be confident in resourcing the NCSC and also in your ability to successfully resource growth. You will be able to find the people we need, and recruit them quickly.

- Internships and work experience
- Skills gap closure
- Higher education
- Cyber talent
- Ease of recruitment
- BT Cyber Challenge
- Apprentices
- Mentoring
- Further education

Develop a security profession

You have a flexible team by knowing your skills and potential. You stand out in your region by being the best in our field.

- Head of profession
- Lead of profession
- Career dev. framework
- Graduate programme
- Skills based learning
- Skills framework
- Learning pathways
- Portal site
- Subject matter experts

Influence associated professions

Anything anybody does in the organisation has security embedded in it.

- Project managers
- Procurement
- Finance/Legal/HR
- CEOs/Boards/Seniors
- Software and systems engineers
- Professional and business services

Promote a learning culture

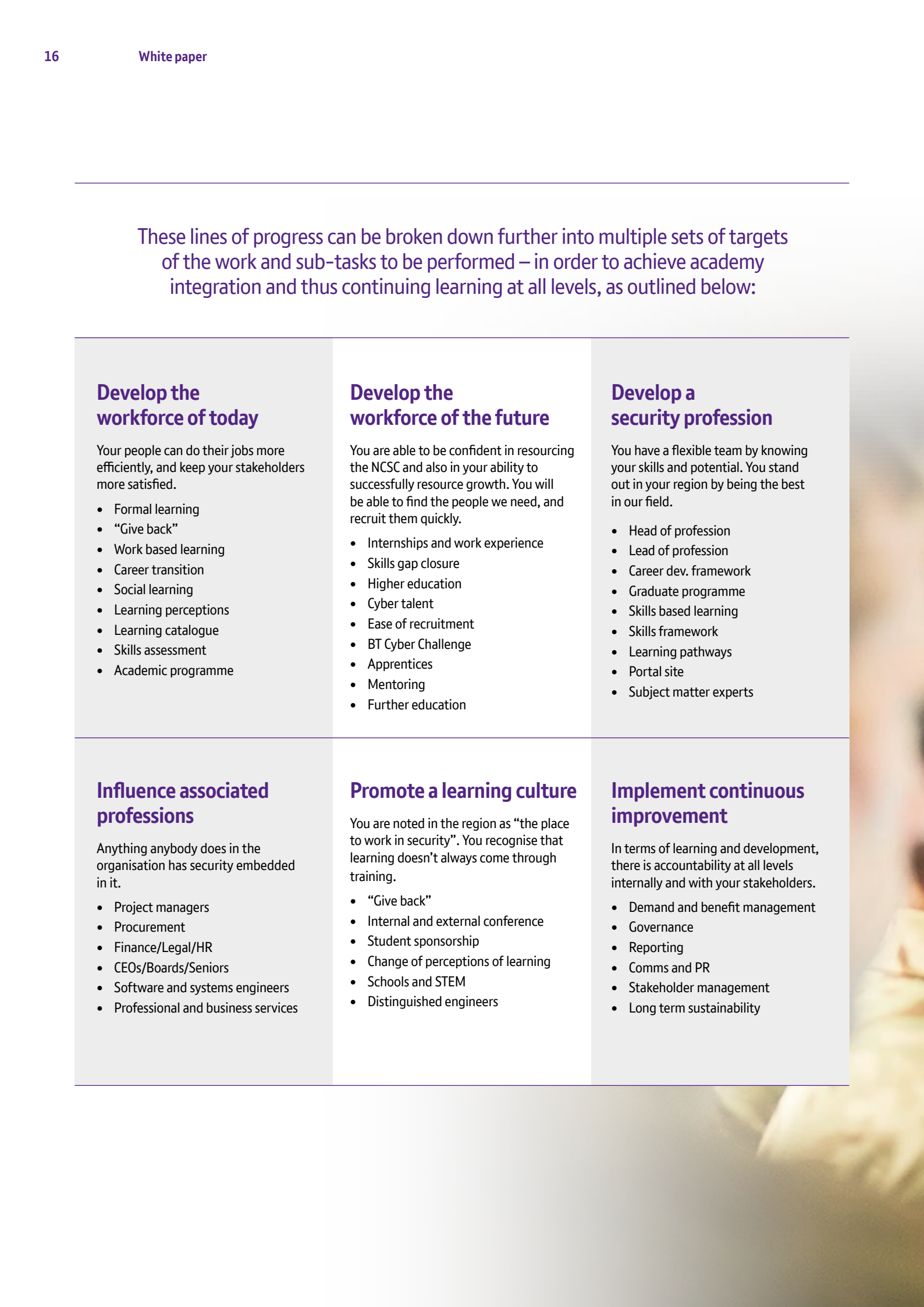
You are noted in the region as "the place to work in security". You recognise that learning doesn't always come through training.

- "Give back"
- Internal and external conference
- Student sponsorship
- Change of perceptions of learning
- Schools and STEM
- Distinguished engineers

Implement continuous improvement

In terms of learning and development, there is accountability at all levels internally and with your stakeholders.

- Demand and benefit management
- Governance
- Reporting
- Comms and PR
- Stakeholder management
- Long term sustainability



Defence and the Cyber Skills Challenge

The Ministry of Defence has a direct, parallel interest in the way the discipline of cyber-security evolves and a strong national defence imperative to access the very best available expertise in the field.

Like other employers, the MOD must decide its priorities between the needs for technical, analytical or operational skills, and the best combinations between them – and those areas where nothing less than truly integrated cyber skills will suffice.

Then, too, defence must choose where to put the weight of its technical/analytical/operational skills, into what combination of offensive, defensive or intelligence operations may be required at any given time.

This calculation is liable to alter as the international situation and the threat environment against which the MOD scales its effort naturally shifts – sometimes very rapidly.

Defence and the Cyber Skills Challenge

Current requirements for defence cyber-security and the MOD's own skills challenge also has to be set against the MOD's ongoing reorganisation as the single services are given more discretion over their own management and spending and as they assess their own needs in a significant military devolution from the centre. Nevertheless, the cyber skills challenge for the MOD is best classified as falling into three natural categories:

Recruitment
The main challenges still involve creating a satisfactory career structure for cyber specialists as all three single services reorganise themselves around the £178 billion new equipment programme being delivered over the coming decade.

The Defence Cyber Aptitude Test (DCAT), has been extensively employed, and now also in partnership with IBM; to help standardise a way of identifying relevant cyber talent across a wide range of fields. Work to put the DCAT into a game format is also underway to give it more general appeal as an international standard, as well as using it to help recruit talent into the defence field.

Training
A training review is currently underway, drawing on the work being undertaken by the Single Service Departments as they articulate their future requirements more precisely. The Defence Cyber School (DCS) is playing an increasingly key role in delivering relevant training. All training for the military must be reflected, ultimately, in its relevance to operations and this is no different in the case of cyber skills. Nevertheless, current training levels must be pushed through to the next technical iteration, where active consideration is being given to delivering such advanced material in a combination of the DCS and key commercial partners, and possibly allies, as well as recognising that which – for national security reasons – must be delivered in-house and through the DCS only.

Retentions
The military faces some unique structural problems in the matter of retaining skills, not because the military profession is in any way less attractive than civilian life, but because it has to be structured more hierarchically than civilian companies who compete for the same skills. Companies are able to accept the rapid migration of workforces from one firm to another, sideways entries, greatly differential rewards to meet skill shortages, and so on. The MOD and the Armed Forces do not have the luxury of such flexibility, though they are thinking hard about how much of their traditional legacy and hierarchy could be amended to help them retain and re-recruit cyber skills within such a naturally fluid workforce. Working within the framework of the government's public sector pay policy and the Armed Forces Pay Review Board, the MOD continues to explore options and frameworks that can reward an individual's cyber skills and worth, within innovative cyber career pathways.

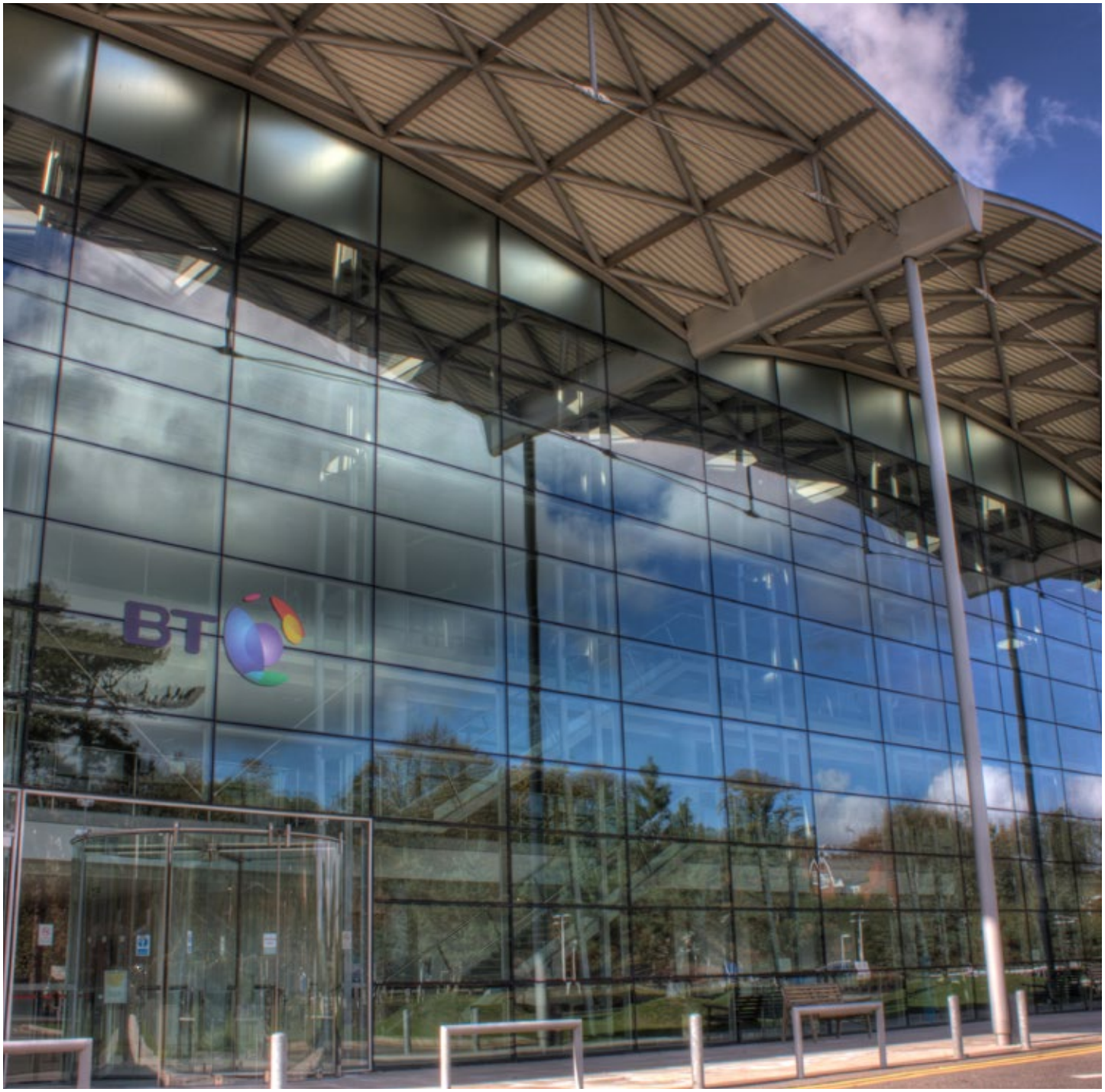
The use of reservists across all the Armed Services is a vital part of achieving all three of the objectives above, and play into recruitment, training and retention in important and different ways. The experience that skilled individuals can bring to the collective capabilities of the forces in this respect is immense. Less evident, however, is the reverse side of the coin, in the values and understanding that the Armed Forces can give to the cyber specialist – application of skills at the sharp end of operations, personal satisfaction and fulfilment in a nationally important role, and the respect of fellow professionals in a very special environment.

The truth is that cyber skills for the Armed Forces cannot simply be outsourced to the private sector. But the interaction between the Armed Forces and the private sector must be intense and fruitful, and is certain to become deeper – and without the dedicated contribution of reserve service personnel that would be impossible.

Working in Partnership

All these challenges must therefore be set within the requirement of the MOD's whole force concept, to gain the greatest synergies from the UK's investment in its Armed Forces. Of course, cyber skills, and particularly cyber-security, are a principal way in which synergies to underpin the whole force concept could be very effectively realised. But for that to be the case, settled MOD policies to recruit, train and retain the necessary skills must bear fruit, and to integrate the range of skills inherent in the regular and reserve parts of the Armed Forces. In this respect, there are many potential benefits in even greater dialogue and cooperation between Joint Forces Command and the nascent BT Cyber Academy.

BT, the Armed Forces and the MOD share much in common, even though their essential missions might be naturally different. In fact, their core values are almost identical: to be efficient leaders of national purpose, to serve the public, to embody the best technologies, and to do their utmost to promote a prosperous, secure, free and democratic United Kingdom in a confusing and darkening global environment.



Find out more
bt.com/business
0800 783 9053