Cybersecurity

Challenges and opportunities for the UK

Innovate UK
Knowledge Transfer Network

Executive summary

This strategic roadmap report, *Cybersecurity: Challenges and opportunities for the UK,* presents an evaluation of the major cybersecurity themes pertinent to industry, Government, the research base and consumers in the next 3-5 years. It sets out recommendations as to how these areas can be better understood, and how UK industry may be able to exploit these opportunities – through further investigation, policy priorities, research & development and/or other collaborative and knowledge transfer activities.

As the UK's innovation network, KTN is uniquely positioned to identify and analyse emerging areas of concern across different sectors, and to extrapolate common opportunities from that data, which may benefit from further investment in the coming years.

This roadmap has been created to support and stimulate the UK economy to grow by enabling industry, research and policymakers to extend their collaboration, direct strategic investment and cross-pollinate ideas.

It identifies ten themes for cybersecurity that will grow in importance over the next 3-5 years. Each represents an excellent opportunity for UK industry to seek or develop tools and techniques to address these problems, with a key recommendation identified for each theme.

The ten themes are:

- Bitcoin and distributed ledger
- Consumer payment and transaction systems
- Legacy systems
- IoT security
- Physical autonomous systems (including robotics)
- Building information management (BIM)
- Devices used across private and professional networks
- Increased Wi-Fi access (personal and professional networks)
- Quantum key distribution and quantum computing
- The human factor

Introduction

Cybersecurity remains a high priority for the United Kingdom. The Government has invested time and capital in the National Cyber Security Centre (NCSC) – the prospectus for which was published in summer 2016. The Cyber Growth Partnership has been established to increase UK Industry's export market understanding and access, develop the UK's offer/brand for overseas markets, catalyse research, development and innovation within the UK's cybersecurity sector, and support the provision of skills in the UK.[1] In addition, funding has been provided by Research Councils UK (RCUK) to undertake research into understanding both the nature of cybersecurity threats as well as practices that might mitigate them. This supportive strategy has helped position the UK as the third largest cybersecurity market globally.

However, gaps in understanding and capability remain and there has not thus far been an undertaking to present a coherent and aligned illustration of industrial priorities across different sectors. Consideration of the efforts made by the Transport Systems Catapult to map threats and opportunities to Intelligent Transport Systems would, for example, benefit other industries that are likely to experience related threats.

KTN's links to many of the UK's most innovative businesses has enabled it to look across sectors. This report shows where existing and/or emerging threats are likely to become common in hitherto unrelated markets. Thus, there is a strong case for collaborative R&D activities by businesses and researchers who might not ordinarily work together.

Purpose

Through this report KTN aims to:

- Highlight emerging and growing threats and opportunities for investment in cybersecurity
- Enable more UK businesses to plan their cybersecurity R&D activities
- Foster collaborations between cybersecurity businesses and other developers, and users from across a variety of sectors requiring such solutions
- Facilitate thought leadership in systems security leading on innovation for engineering complex and critical systems
- Inform policy and research funding priorities

[1] Cyber Growth Partnership: further information at *www.techuk.org/cyber-growth-partnership*

Scope

This report highlights four areas that are of sufficient maturity, and which may provide substantial opportunity for collaboration:

- Transport systems
- Defence and national security
- National infrastructure
- Financial services (FinTech)

This report intentionally focuses on the technical cyber solutions that currently lie in the Technology Readiness Level (TRL) band of 3-6, commonly referred to as the 'Valley of Death', where funding traditionally drops away from the research base but is not yet (fully) replaced by commercial investment. It is in this gap that public funders, such as Innovate UK, make their largest and most significant impact on UK business and R&D.

It is also in this area – in the gap between concept and commercialisation – that KTN routinely creates value by bringing together businesses and researchers to create innovative solutions to the problems faced by end-users.

The recommendations in this report showcase a range of options that do not necessarily all point to investment. What is clear is that cybersecurity challenges faced by Government, businesses and consumers cannot always be solved by investment alone. Funding and finance, good policy, regulation and industry-led research must be combined with softer forms of innovation that involve collaboration, knowledge exchange and the human dimensions of cybersecurity practice.

While this roadmap focuses on the emerging and growing classes of threats over the next 3-5 years, it does not consider how the academic community is channeling efforts and investment into more distant challenges.

The roadmap does not seek to duplicate efforts already made elsewhere, but rather to acknowledge this and, where appropriate, to reference work already published.

Future findings

Finally, while the outcomes of the roadmap present a coherent and well-defined opportunity, this does not present the whole picture. It would be of great benefit to the UK economy to produce a unified illustration of cybersecurity activity married to investment strategy; it is hoped that this report will act as a foundation on which future reports may be based.

There is already a great deal of work being done by RCUK, in particular through Engineering and Physical Sciences Research Council (EPSRC) funding, and there are numerous businesses operating in the commercial space. This roadmap report focuses on the TRL3-6 band, but acknowledges work being done at the research and commercial ends of the chain.

Since work on this roadmap commenced, the following activities, which are particularly relevant to this space, have taken place or are ongoing:

- The Royal Society (www.royalsociety.org) published an independent report titled *Progress and research in cybersecurity: Supporting a resilient and trustworthy system for the UK* with chapters including *Cybersecurity and the digital society*, *Trust*, *Resilience* and *Research*.
- The NCSC (www.ncsc.gov.uk) has been established as the UK's authority on cybersecurity. NCSC is part of GCHQ and acts as a bridge between industry and Government, providing a unified source of advice, guidance and support on cybersecurity, including the management of cybersecurity incidents.
- NCSC are continuing to establish CyberInvest, a partnership that brings together key players from Government and industry to invest in and support the development of cutting-edge cybersecurity research across the UK's academic sector.
- The PETRAS Internet of Things Research Hub (www.petrashub.org) has been established. This is a consortium of nine leading UK universities working together over three years to explore critical issues in privacy, ethics, trust, reliability, acceptability and security. The project runs in collaboration with IoTUK.
- The Blackett review into Quantum technologies has been published which explores how the UK could benefit from the research, development, and commercialisation of quantum technologies. "The Quantum Age : technological opportunities" (www.gov.uk/government/publications/quantum-technologies-blackett-review)
- The Transport Systems Catapult (ts.catapult.org.uk) published a report "Cyber Security and Intelligent Mobility" which recommends that the UK Transport sector needs to increase its focus on Cyber-Security in the face of rapidly emerging technological developments.
- KTN, in partnership with the Partnership for Conflict, Crime and Security Research (PaCCS) (www.paccsresearch.org.uk) has published a Policy Briefing titled *Innovation challenges in cybersecurity*.

It is hoped that future iterations of this report will tie all these strands together to create a more holistic innovation landscape for cybersecurity in the UK.

Methodology

The methods used by KTN in the preparation of this report are:

- Desk research evaluating published sector-specific cybersecurity material
- Identifying available and existing investment in cybersecurity technologies
- Speaking to cybersecurity businesses in KTN's business network
- Running industry-focused workshops

In June 2016, KTN hosted workshops on cybersecurity challenges in two of the four areas highlighted in this report: Infrastructure, and FinTech.

The Transport Systems Catapult held a similar seminar in March 2016 on Intelligent Transport Systems and since we were able to use their results and extrapolate their findings for this report, it was not considered necessary to hold a further workshop on this topic.

Defence and national security, at a certain level of activity, becomes a cross-cutting subject. For example, major, debilitating attacks upon the rail network, or the central banking system, or the utility networks or nuclear power stations, can soon escalate to become a national security problem. For this reason it was decided not to conduct a separate workshop on this topic.

Participants in the workshops included academics, industrial representatives and Government operatives, who were either experts in cybersecurity operations, or who had knowledge of the specific cybersecurity challenges and threats facing their sectors.

In preparation for the workshops, KTN used the "Well-Sorted" tool, a web-based sorting program developed by Heriot-Watt University and routinely used by EPSRC for sandpit and innovation sessions to gather and sort delegate responses to key questions, before the workshop takes place. The answers were used as the spark for the discussion sessions during the workshops.

Using this insight, KTN moderators worked towards identifying the following information relating to cybersecurity issues:

- The particular threats, challenges, and problems facing their sector, whether technological, cultural, or relating to other aspects of policy
- Where possible and relevant, the technical developments and techniques that might mitigate, defend against or repel these threats
- The non-technical (or "softer") techniques that might be deployed to mitigate, defend against or repel them
- Potential topics for R&D projects that may ameliorate them in future

Annex document

The full findings of the research and consultation activities undertaken in the preparation of this report are captured in the supplementary document *Cybersecurity: Challenges and opportunities for the UK, Annex*.

The names of organisations who participated in KTN workshops are included in the Annex.

Ten key recommendations

Based on the combination of research and industrial consultation gathered in the preparation of this report, there are ten themes which we believe will grow in importance over the next 3-5 years and which would benefit from focused support.

The justification for these themes emerges clearly from the Annex document, which comprehensively breaks down the threats by key sector, and identifies which broad areas represent the greatest challenges.

Here, they are distilled to their essence, so that the individual challenge, threat, and solution benefits are outlined. Each challenge represents an excellent opportunity for UK industry to seek or develop tools and techniques to address these problems, and the key recommendation that may enable these solutions is listed with each scenario.

The recommendations for each of the ten themes are set out in the following pages.

1 Bitcoin and distributed ledger

Distributed ledgers are being increasingly used to manage complex electronic, legal or financial assets involving multiple parties. They are attractive because of the underlying algorithmic block-chain technology, which enables ledgers to become tools that can enable, record and secure a huge amount of transactions in a very short space of time with a high degree of security. Because the basic algorithmic approach to block-chains means they are customisable, the distributed ledgers can contain smart contracts, digital signatures, authentication tools and other cybersecurity tools and techniques.

However, distributed ledgers are not uncrackable; somebody who is able to successfully and 'legitimately' manipulate one copy of the ledger will thereby have successfully manipulated every copy of the ledger, leading to huge complexities and problems. Thus, the successful commercialisation of distributed ledgers depends on demonstrating their security, performance and scalability, as well as how well the technology will be adopted by the general public.

Should these issues be resolved, the potential for efficiency savings and reduction of paperwork, bureaucracy, administration and, crucially, the time associated with these things, would be enormous. Businesses and Government would save huge amounts of money and time, while end users such as consumers, passengers and patients will have greater transparency of their transactions.

A technology demonstrator project featuring a sufficiently high-profile user (for example, a consumer-facing business or Government department) may have the potential to bring this transformative technology to greater public attention, as well as stress-test the security, performance and scalability of a bespoke distributed ledger in a high-pressure, complex, public-facing environment.

Key recommendation

The UK should invest in a large-scale technology demonstrator to accelerate the awareness and development of the technology.

2 Consumer payment and transaction systems

As devices proliferate, the reliance on EMV-payment systems – such as chip-and-pin – will wane, and the number and variety of transaction types will increase. The acceleration of different payment types has meant that some payments are happening beyond the visibility of traditional financial institutions.

A side effect of this is that authentication for the various actors participating in the transaction becomes more difficult, creating more entry points for cyber attackers to intercept, disrupt or steal the data involved in the transaction. Critically, without the infrastructure and regulatory back-up that traditional financial institutions have, there is no guarantee that consumers using new payment and transaction methods will be protected. Transactions occurring outside traditional parameters may also enable criminal activity such as embezzlement, theft, fraud or money laundering.

The growth of new transactions has introduced a variety of new stakeholders into the financial services and FinTech space. Getting these stakeholders to interact, share data and create lines of visibility will be a challenge, when the ability to manage these operations has become so socialised. Freedom from traditional financial conventions is a big selling point for many peer-to-peer platforms, and sacrificing some of that freedom for greater security may not be an easy argument to make.

Key recommendation

Develop scalable authentication and data sharing techniques. Encourage greater R&D collaboration between the traditional financial sector, digital start-up businesses and consumers.

3 Legacy systems

Large organisations in transport, business, Government and other commercial sectors frequently use hardware and software that have been in place for many years and, owing to the size, complexity or operational infrastructure of the organisation are extremely difficult to upgrade for internet connectivity.

The catch-22 presented by these legacy systems is that, while they are often outmoded, updating them would disrupt business operations, and potentially expose them to newer types of threats. This is a hugely significant obstacle that affects organisations in a wide variety of sectors. Addressing it successfully would enable a whole new generation of infrastructure to operate with a next-generation level of adaptability, flexibility and robustness that can move in accordance with the threat evolution.

There is an opportunity for the UK to demonstrate how large sectors can overhaul their infrastructure in a practical and commercially sensitive manner. This calls for investment in R&D to develop sufficiently scalable tools and techniques – such as data diodes and hard-disk firewalls – that can enable the connectivity of legacy systems from different sectors without compromising security or operability.

Key recommendation

Develop tools and techniques to enable legacy systems to be securely interconnected. Enable cross-sector knowledge exchange to highlight common concerns and capabilities.

4 IoT security

The Internet of Things (IoT) is set to be an enormous new market that will touch the majority of First World lives in the coming years, with an estimated global market size of US $661bn by 2021.[2] IoT will provide mundane devices with internet connectivity, allowing greater control and customization of our lives and the devices and products that affect it, from our computers, tablets and phones to our cars, lighting, and even our kitchen appliances.

This connectivity brings very real threats. The low computational power of most IoT-enabled devices and sensors, such as kitchen appliances, lamps and smart energy meters, means they are not fitted with sophisticated cyber defence capability. The ease with which nefarious actors could hack the devices and access the data they exchange is a cause for alarm. The consequences of hacking IoT devices range from local crime (such as burglaries in response to data revealing the movements of homeowners in their properties), to industrial sabotage (based on mass interception of data).

IoT-enabled products that have serious cyber weaknesses could create a nightmare for consumers. In a very bad case scenario – such as a Talk Talk or Ashley Madison-style large-scale theft or breach of consumer data – they could even dent consumer confidence so much as to slow the growth of the market.

The challenge is to develop encryption and authentication technologies that can operate on the very low computation power that many IoT devices will possess. Getting this right will enable the IoT market to grow without major hiccups or setbacks, as well as boosting industry and consumer confidence. It will also position UK cyber businesses that offer such solutions extremely advantageously as the market grows, and as the need for such capability becomes more apparent.

Key recommendation

Support R&D into encryption, authentication and certification technologies for IoT devices.

---

[2] *Marketsandmarkets.com* (2016). *Internet of Things Market by Software Solution & Platform – 2021*. [online] Available at: *www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html*

[3] Reference: *Autonomous Systems : Opportunities and Challenges for the UK* produced by the Aerospace, Aviation & Defence Knowledge Transfer Network (AAD KTN), 2014.

5 Physical autonomous systems (including robotics)

In 2014 it was estimated that the value of the markets applicable to autonomous systems was $264bn.[3] There are very few sectors that will not be transformed by the introduction of robotics and autonomous systems. Within the next five years we can expect robotics with advanced autonomy frameworks – by which we mean decision-making capability – to be used heavily in consumer-facing sectors such as transport and logistics, health and care, manufacturing, and consumer markets.

While the transformative power of robotics will bring new advances in quality of life, efficiency, safety, as well as new scientific capabilities, it is critical that robots and autonomous systems that have any sort of connectivity – be it telemetry, tele-robotics, tele-operation or other data uplinks – are as secure as they need to be. In many cases the robots or systems used here will be large, heavy and potentially dangerous. To cyber attackers they can represent a rich vein of pickings, offering the potential to mine or steal data, implant false data, or in some cases offer bogus commands, causing the system to fail. In public-facing environments, the consequences of a catastrophic failure, or rogue manipulation, could range from the mischievous to the lethal.

The safety of large and dangerous robotic systems is critical to the prospects of these systems being adopted by industry and accepted by the public. Robotics are already used in certain non-public-facing sectors, such as manufacturing and space, where potential catastrophic consequences can largely be measured in dollars rather than lives.

Overcoming any such weaknesses will be crucial to enabling the steady adoption and growth of this market, and not denting public confidence in it.

Stress-testing robotics systems used in public arenas against the possibility of cyber attack is an essential requirement. Complex systems such as vehicles offer multilateral avenues of attack for hostile actors, including connected sensors, infotainment systems, GPSS and mobile networks. Investment in fully-integrated technology demonstrators that can test the robustness of the whole vehicle in computer and real-world simulations, is recommended. The involvement of stakeholders from the Future Cities community will also improve understanding of how robustness of the vehicle does not end at the edges of the chassis, but extends to the environment with which it is interacting. Finally, regulators from the relevant sectors ought also to be included in any serious technology demonstrator to develop and implement the necessary standards by which the robotic systems may be measured. For example, a fridge will require a different set of cybersecurity regulations and standards than a unmanned aerial system (a drone).

Key recommendation

Developers from different sectors should be incentivised to collaborate with regulators and certification organisations on large, complex demonstrator projects with built-in security aspects.

6 Building information management (BIM)

The listing of building assets in one holistic, overarching digital model will give those who interact with, use and manage the building more control and flexibility. Known as BIM (for building information management), this assembly of data combines product properties, geometry and visualisation data about the characteristics of the the building. BIM has the potential to deliver huge efficiency and cost savings, as well as increasing the value and lifespan of functioning buildings.

However, having such a massive mine of critical infrastructure information online represents a significant security risk. BIM already is an important cornerstone of the Government's Industrial Strategy for Construction to achieve faster delivery and lower emissions, but it is a huge challenge to ensure the data contained in BIM models is restricted to trustworthy actors. Secure authentication, encryption and identification techniques that can be deployed across this open-source cloud-based application, while retaining its inherent flexibility and accessibility, is paramount to prevent BIM being exploited for criminal gain.

Getting this right will enable the construction industry, as well as building users and custodians, facilities managers and tenants, to design, develop, manage and use advanced buildings with peace of mind.

Key recommendation

Improve ways of protecting sensitive data contained within BIM models by encouraging security to be designed in.

7 Devices used across private and professional networks

The proliferation of internet-connected devices such as mobile phones, tablets, e-readers and music players in public spaces and all connected to public networks has increased exponentially in the last few years. The growth of the IoT will only boost this growth. While this will give people even better means of communication, control and flexibility over various aspects of their lives, there are dangers in the networks we use to connect our devices.

Using personal devices on professional or corporate networks presents the danger that compromised devices – accessed by a cyber attacker over a public or even bogus open network – can infect a professional network and infrastructure through the front door. The disabling or infection of a corporate network can lead to catastrophic failure of critical systems or servers, or to data theft.

People will want to retain accessibility to their devices, apps and data when they are in corporate environments. It is practically impossible to police this without draconian and unpopular methods. However, preventing the flow and transmission of certain data – especially in highly sensitive environments, such as hospitals, Government departments, and financial institutions – is desirable to prevent malware or viruses from being deployed.

Devices are not going to go away, so imposing outmoded methods of policing personal device usage in a work or corporate environment is unlikely to be practicable or popular. Such an approach can also hinder or restrict operational tasks that require flexibility, such as social media marketing, mobile communications or collaborative working. Ensuring corporate security while enabling workers to retain their freedom, flexibility and enjoyment of communicative capability is a highly desirable outcome.

Key recommendation

Promote the adoption of best corporate practice and enshrine ownership of cybersecurity as an executive-level responsibility.

8 Increased Wi-Fi access

The proliferation of devices also goes side by side with the growing number of Wi-Fi networks, in the home as well as in public and professional environments. Again, the benefits are obvious: allowing consumers and workers greater flexibility and control without the need to eat up data allowances provided by their mobile service provider. The relative ease with which a hostile agent can set up an open-access Wi-Fi network in a public space means that anybody hopping onto the network risks their data or devices being stolen, corrupted or watched.

In extreme circumstances, workers using public Wi-Fi networks to undertake work could have sensitive corporate or even Government information that can be compromised by hostile actors, from activist hackers to nation states. Other scenarios could see unsuspecting workers take devices corrupted by bogus networks into sensitive environments such as hospitals and corporate offices, where they can hop onto the local network and deposit their hostile payloads, resulting in nuisance, damage or theft. Liability for this type of attack is also vague: employees acting as "mules" enabling this type of attack could be liable, however unwitting their participation.

Helping consumers and users differentiate between a legitimate and a bogus Wi-Fi network is the key to preventing this type of attack, and could theoretically eradicate it. The challenge will be to create a way of doing this that addresses the ease with which hostile actors can create Wi-Fi networks, while still enabling others to create networks for legitimate purposes.

Key recommendation

Work with industry, regulators and certifiers to develop kitemark standards and accreditations for public Wi-Fi networks.

9 Quantum key distribution and quantum computing

Most current cyber encryption uses Public Key Cryptography, which provides security due to the computation difficulty of factoring a very large number into two prime numbers. However, a significant potential danger associated with Public Key Cryptography is the future development of a quantum computer. These will be able to factorise large numbers in a short space of time, thereby significantly reducing the security of public key cryptography, like RSA. Although the threat of a quantum computer that can factorise numbers is still predicted to be some way off (1 in 7 by 2026 and 1 in 2 by 2031) companies such as Google, IBM and Microsoft are racing ahead with development and are speculating that they may deliver sooner than this. This risk may be relevant to current data in transit which contains long-term secrets, such as health records and company know-how. Although currently encrypted the data may be recorded now and decrypted once a quantum computer becomes available at a later date.

Two solutions are currently on offer: known as Quantum Key Distribution, and Post-quantum cryptography. Quantum key distribution (QKD) may be used to protect data from this threat by detecting the presence of evesdroppers on private channels used between two parties transmitting / receiving data between each other. Quantum cryptography services are already commercially available, at a cost. While many currently believe that QKD technology is uncrackable, there is an outstanding need for greater certification. Another potential solution is to make the encryption more resistant to attacks by a quantum computer. This may be through increasing the length of keys used, or by using alternative cryptography schemes, known as 'post-quantum' cryptography. Although these are easier to implement, and similar to existing cryptography schemes, encryption this way is likely to be more computationally intensive, and therefore slower than other solutions. The future protection that these encryption schemes offer against future, more powerful quantum computers and algorithms is also uncertain.

Laying the groundwork in preparation for these seismic shifts in computing will enable the UK to be well positioned when these technologies are adopted by the corporate and consumer markets.

Key recommendations

Build upon the existing collaboration between Innovate UK and EPSRC to identify commercial exploitation routes for quantum technologies.

Facilitate collaborations between UK quantum communications and cryptography research groups leading to joint work on QKD and post quantum cryptography as well as work on digital signatures and other uses of these technologies.

Create a pilot trial of QKD, and use this to perform conformance tests and issue accreditation certificates.

10 The human factor

While we know that much of the technology discussed in this report is potentially transformative in many sectors, what we don't know is exactly how human use, exploitation and modification will change the nature of the technology itself, and therefore change the nature of the threats and vulnerabilities presented.

With new platforms and systems being used in new ways, with ever more potential for customisation and adaptability by the user – especially with open-source code and software – it is only a matter of time until platforms develop new weaknesses or become susceptible to new types of threat or attack that have not yet been identified. But the consequences of such emerging loopholes could be highly dangerous, even lethal. If a car contains components that can be customised by users, leading to new ways in which the car is being used – for example, for online shopping, for infotainment, or communications – it could "unlock" new loopholes that can be exploited by hostile agents. We have to remember that the main threats in cybersecurity are human. Human actors are the ones seeking new ways to inflict damage, steal or cause harm, so thinking about the problem in purely technological terms will not do. We must think in human terms to understand the potential breadth of these problems.

Understanding the causes and effects of this are psychological and physiological as well as technological. The ways in which we use technology is critical to understanding new types of threat, and how users calculate and mitigate, or even ignore, risk.

A better understanding of the human factors involved in new technologies with inherent security risks could help anticipate new and emerging threats and develop countermeasures or implement best practice techniques before they become threats. Unforeseen threats, weaknesses and problems could derail projects, and dent confidence.

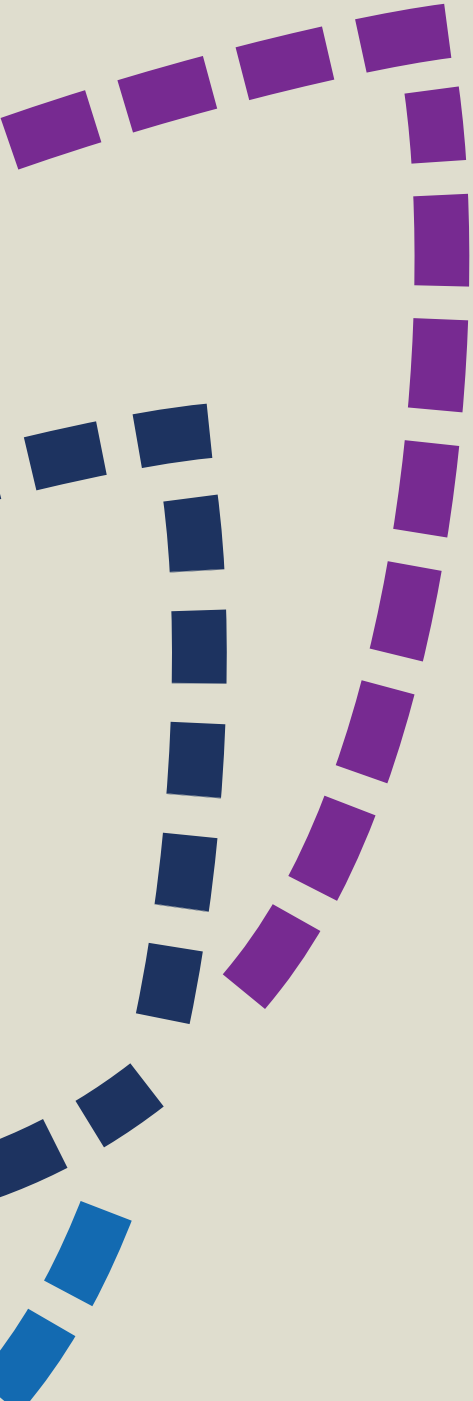
Key recommendation

Support human factors research, focusing on new, connected technologies and integrated systems. Pay particular attention to neurological, psychological and physiological effects of newly-available technology.

This report was written by Daniel Jones.

For further information please contact:

Robin Kennedy
Knowledge Transfer Manager – Cybersecurity
Telephone: 07870 899956
Email: robin.kennedy@ktn-uk.org



Head Office

Knowledge Transfer Network Ltd
Suite 218 Business Design Centre
52 Upper Street
Islington
London N1 0QH

Telephone: 03333 403251
Email: enquiries@ktn-uk.org
ktn-uk.org
@KTNUK

Innovate UK
Knowledge Transfer Network