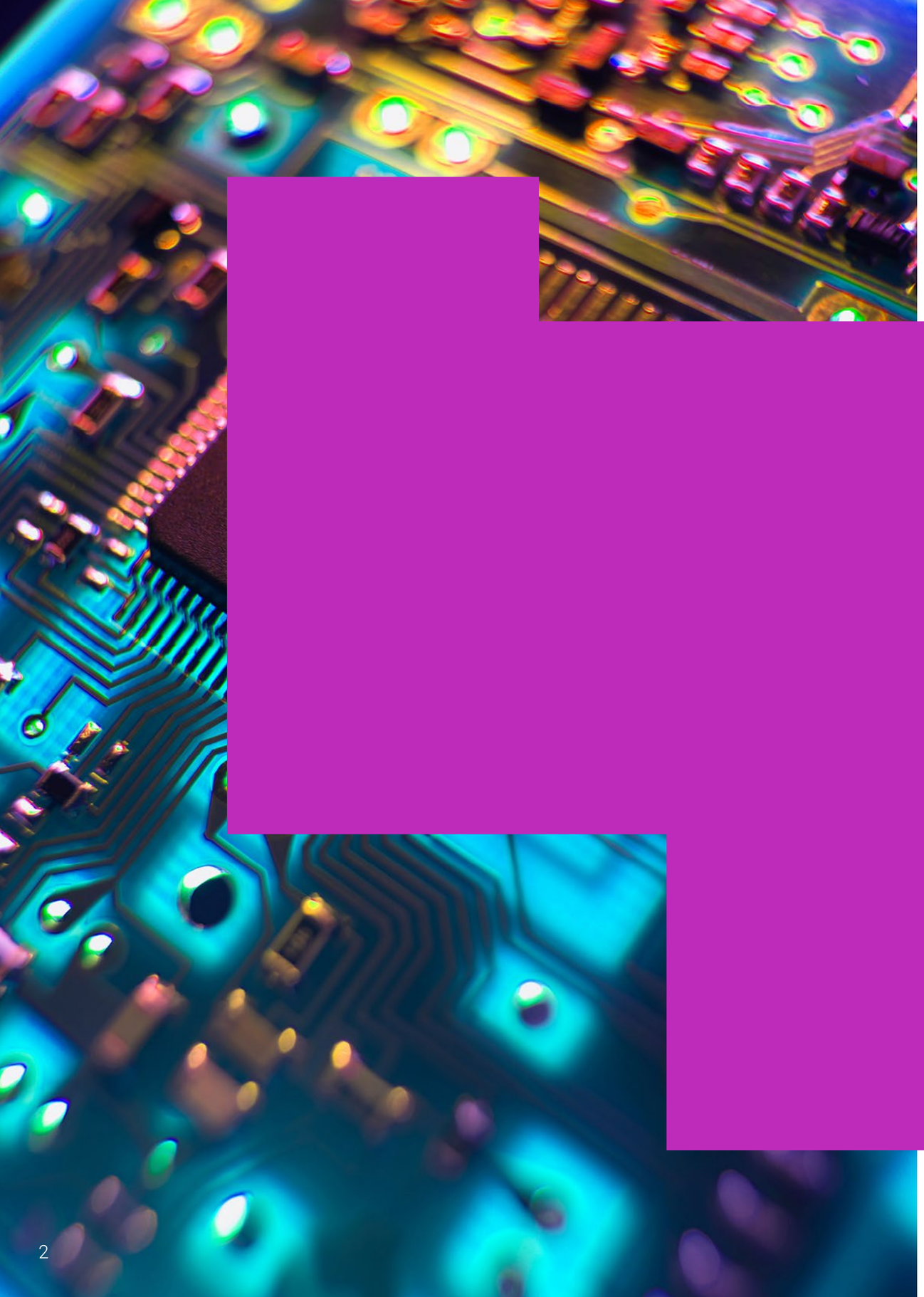
Innovate UK

Innovate UK Global Expert Mission Report

Cyber Security In Japan

June 2023

PUBLIC



Contents

01. Summary

At the end of February and early March 2023, Innovate UK through the Global Expert Mission programme visited Tokyo, Japan to gain a more in-depth understanding of the cyber security ecosystem in the country and to identify mutually beneficial opportunities for collaboration. The UK delegation consisted of representatives from Innovate UK, UK Government, academia, and industry (large and small). They met with representatives in Japan from Government, research and academia, industry bodies and companies.

The mission gave the delegates a greater understanding of the innovation landscape in Japan in the cyber security sector and how it differs from its counterpart in the UK.

Japan has a very young but evolving cyber security ecosystem which is supported by recent Government policy and funding and direct initiatives to support its development alongside the wider accelerated growth of the start-up ecosystem as a whole in Japan. There is activity both in the corporate and public sectors around cyber security and a recognition of its importance as a high priority. The drive to improve cyber security within Japan is directly related to the increased push for digital transformation and the evolution towards Society 5.0.

The start-up ecosystem has some way to go in Japan before it reaches a level of maturity that is comparable to its economic counterparts such as the United States, China, UK, Germany, and France. Recent government policy recognises that and is aimed to create more of an environment and culture that will see innovation and entrepreneurship flourish at pace within Japan. Whilst the private investment landscape is currently limited there are positive signs of change on that front and the policy that allows pension funds to play a role in this could have a significant impact.

Funding bodies and the research community in Japan already work with international partners and have the mechanisms in place to set up international collaborations to support strategic research and development between organisations in Japan and the UK. Alongside this there is also the desire to do more of this and Japan recognises that the maturity and excellence of the research activity in the UK is something they can benefit from.

The United Kingdom and Japan have been long-standing allies sharing similar values and a strong commitment to maintaining international rules-based systems. Recent agreements between UK and Japan listed below provide a framework for close and strategic collaboration.

- UK-Japan Comprehensive Economic Partnership Agreement[1]
- UK-Japan Digital Partnership - A framework for deeper UK-Japan collaboration across digital infrastructure and technologies, data, digital regulation and digital transformation. (Dec 2022)[2]
- UK-Japan Defence Agreement 2023[3]

The UK is seen as one of the world's leading hubs for cyber security and innovation. The regulatory regime is also more advanced in the UK than in many other countries. Japan has shown an interest in some of the work done in the UK around IoT security and supply chain security and is keen to understand more about the UK regulatory initiatives and also sees significant potential in working towards regulatory harmonisation which could bring about significant benefits to both countries.

The mission highlighted several opportunities for closer collaboration between the two countries. The key opportunities focussed on closer harmonisation of regulation and standards between the two countries to enhance trade and collaboration on critical technologies, IoT security and securing supply chains alongside bilateral collaboration on research and development between organisations in the two countries in areas of common strategic interest.

1 https://www.gov.uk/government/collections/uk-japan-comprehensive-economic-partnership-agreement
2 https://www.gov.uk/government/publications/uk-japan-digital-partnership
3 https://commonslibrary.parliament.uk/research-briefings/cbp-9704/

02. Acronyms

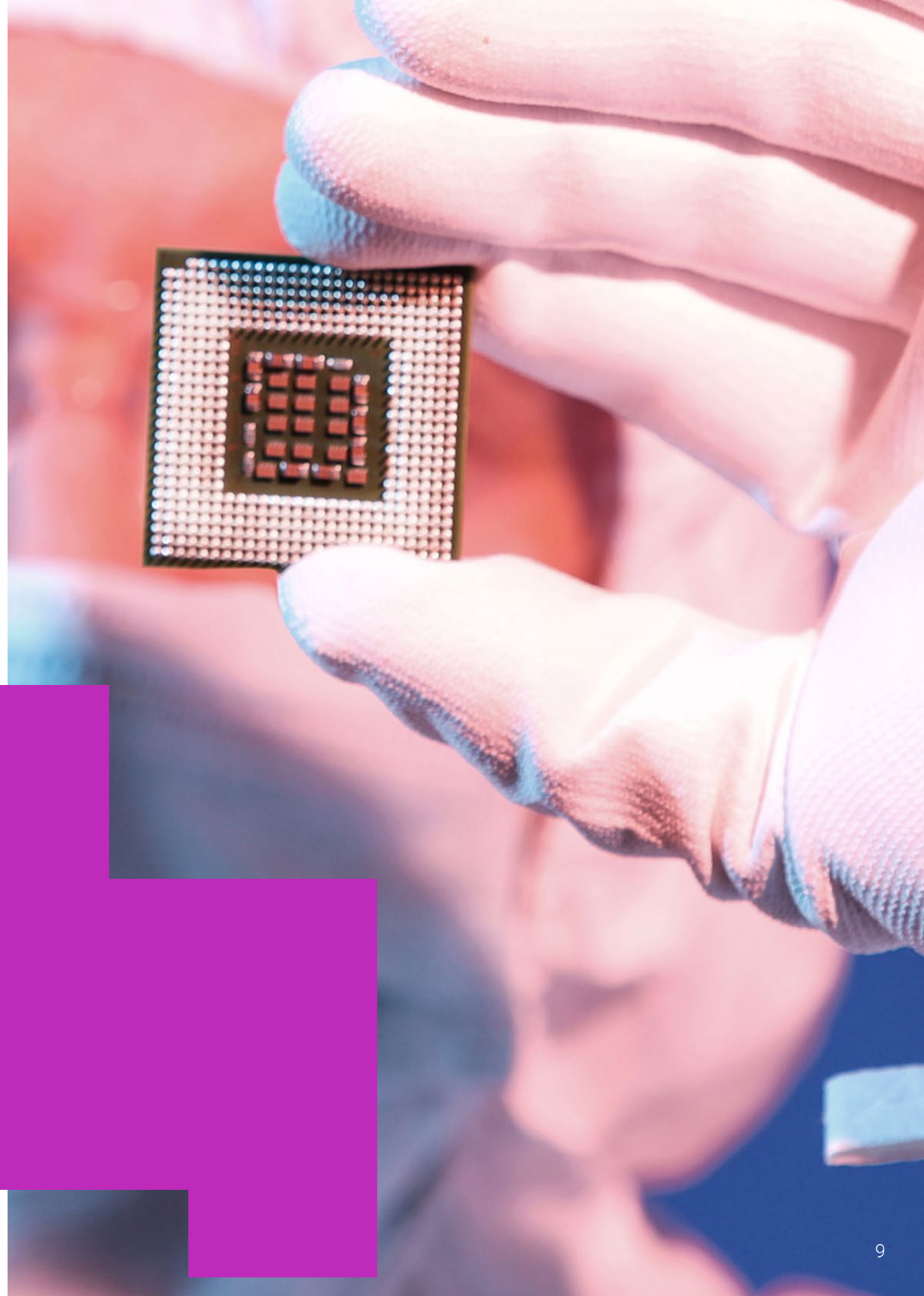
ACEA	European Automobile Manufacturers' Association
AIAG	Automotive Industry Action Group
CERT	Computer Emergency Response Team
DSIT	Department for Science, Innovation and Technology
FCDO	Foreign, Commonwealth and Development Office
GEM	Global Expert Mission
Germany VDA	German Association of the Automotive Industry
IoT	Internet of Things
SICORP	Strategic International Collaborative Research Program
SIN	Science and Innovation Network
SMEs	Small and Medium Size Enterprises
UKRI	UK Research and Innovation

03. Introduction

Innovate UK, Innovate UK KTN and the Global Expert Missions

Innovate UK supports business-led innovation and is part of UK Research and Innovation (UKRI).[4] UKRI convenes, catalyses, and invests in close collaboration with others to build a thriving, inclusive research, and innovation system. To this end, Innovate UK helps businesses to identify the commercial potential in new technologies and turn them into new products and services that will generate economic growth and increase productivity. With a strong business focus, Innovate UK drives growth by working with companies to de-risk, enable and support innovation. Innovate UK KTN exists to connect innovators with new partners and new opportunities beyond their existing thinking – accelerating ambitious ideas into real-world solutions. Innovate UK KTN is part of the Innovate UK group.

As innovation is increasingly a global endeavour and the ambition of UK businesses to become truly international enterprises is at its highest, Innovate UK established its Global Expert Mission (GEM)[5] programme in 2017. Delivered by Innovate UK KTN, in partnership with the FCDO Science and Innovation Network (SIN)[6] , GEMs help further Innovate UK's global strategy by providing the evidence base for where it should invest and by providing opportunities for UK businesses to build partnerships and collaborations with key economies.



4 https://www.ukri.org
5 https://ktn-uk.org/programme/global-expert-missions/
6 https://www.gov.uk/world/organisations/uk-science-and-innovation-network

Mission Overview and Objectives

Japan is the third largest economy in the world (by GDP) and has one of the highest R&D investment levels (R&D expenditure as a % GDP), producing some of the largest numbers of scientific publications and patents globally. The country is home to a large share of multinational corporations competing globally, with more than 200 companies on the Forbes Global 2000 list and has the third largest corporate R&D spending worldwide behind the United States and China. Foreign Direct Investment (FDI) has been increasing steadily since 2011 with inward FDI levels hitting a record high in 2020. Japan has been actively opening its doors to foreign business through new policies and enabling conditions to attract even greater FDI and talent from overseas.

The UK and Japan are close allies with shared interests and have deeply connected military alliances and defence industry supply chains. The UK's 'Integrated Review of Security, Defence, Development and Foreign Policy' (2021) highlighted the ambition of deepening the UK's engagement in the Indo-Pacific region, including its commitment to deepening its strategic partnership with Japan.

For over a decade, the UK and Japan have been producing national cyber security strategies recognising the importance of research, technology and innovation and international coordination and collaboration underpinned by common principles and values. In their latest cyber strategies, cyberspace is seen as an ever-evolving landscape with global reach and critical interdependencies that is increasingly being exposed to changing world order and a wide range of threat actors and their associated behaviours.

Following a period of pacifism, Japan is increasingly investing in its security policy, so the timing is opportune. Japan's national cyber security strategy provides a range of opportunities against which the UK's leading capabilities could play a part in addressing technology, industry, and socio-economic challenges. Prominent themes are Japan's approach to advanced digital transformation (DX), with cyber security being increasingly integrated through the concept of 'security by design'. The vision of Society 5.0, which is seen as the 'new growth engine' for Japan in which technological transformation - including the growing use of IoT, AI, 5G and cloud network services – is creating both opportunities and threats to an ever-changing cyberspace.

The purpose of this Global Expert Mission was to undertake exploration and discovery of Japan's cyber landscape in search of new partnerships and collaboration opportunities between the two countries. To this end, the UK was represented by a delegation of senior professionals from across government, academia/research, business, industry association and research & innovation investments. The UK delegation used expert-specific lenses to explore and discover the breadth of Japan's challenges, strengths, and capabilities across cyber to identify common interests and strategic opportunities for bilateral collaboration.

We engaged with key Japanese stakeholders ranging from governmental departments/ ministries, cross-departmental groups and agencies involved in cyber security strategy and associated policy development; business and industry sector leaders across the cyber security value chain; start-up innovation ecosystems and venture capital communities; academic leaders in regional and national institutes/centres of excellence in cyber security research and innovation.

Mission Scope

Innovate UK's exploration, and discovery endeavour used the following 'sector lenses' to enable bilateral discussions to share each country's individual approaches, identify joint challenges and common interests, and explore levers for collaboration across the cyber landscape.

- **Telecommunications** – the role of telecoms as an infrastructure and a system of systems of significant national importance. An increasing need to protect against the supply chain becoming more open and the target of attacks across an increasingly complex attack surface. The value of 'software-defined' against a fragile digital infrastructure.
- **Automotive** – electrification and digitalisation make the vehicle a component of a broader cyber network where distributed communication becomes vital for keeping society going with all sorts of consequences in the face of cyber threats and attacks. An industry driven by specifications and standards approaches to security that is not enough on their own to protect against attack and exploitation scenarios.
- **Smart Infrastructure** – digitally enabled infrastructures offer benefits and risks at the same time. Increasing pressures on the energy supply and the growth of cyber-attacks put energy security under increasing threat. Smart grid infrastructure manifests itself as a cyber network within which operators are equipped with the ability to control consumers / end-users and shape energy demand. Scenarios of exploiting those critical infrastructures as a potential weapon at the hands of malicious actors mandate the need for architecturally resilient digital solutions.

To summarise, this exploration and discovery endeavour emphasized the development of an understanding of the Japanese cyber ecosystem through a multi-focal approach and laying the foundation for establishing effective, long-term and trusted relationships with key stakeholders in Japan. To that end, subject to the mission's findings, Innovate UK will be exploring a reciprocal arrangement whereby key Japanese stakeholders are invited to visit the UK and experience first-hand a showcase of cyber capabilities and technology strengths with associated business meetings. This potential arrangement would align well with Japan's G7 Presidency in 2023 and ongoing dialogues at the government level.

Built around UK business, policy and research representation, the GEM aimed to:

1. Determine how Innovate UK can best support UK businesses more effectively and efficiently when considering partnerships with Japan.
2. Provide insights into synergies between the two countries in cyber security and determine whether there is an appetite for further collaboration.
3. Identify and showcase key market opportunities in Japan for innovative products and services to UK businesses that may be interested in collaborating with Japan.
4. Capture key UK R&I and market opportunities/challenges for developing innovative products and services when considering collaboration with Japan.

04. Market Overview

The Japanese cyber security market was worth USD 6.4 billion in 2021. The market is expected to grow at a CAGR of 22.6% during the years to 2030 and reach a value of USD 38.9 billion by 2030.[7]

Covid-19 seems to have led to an unprecedented spike in ransomware attacks, which suspended business operations and disabled computer and email systems just at the time when Japanese companies were shifting across to teleworking as a countermeasure against COVID-19. Businesses, especially those that own or are related to critical infrastructure, are realizing the threats posed by cyber security and are investing and working with the government to safeguard their models. All of the following are seen as contributors to the growth in the Cyber Security Market in Japan.

- The increase in cyber attacks on Japanese organizations is prompting the government to establish new legislation, strategies, and facilities.
- •According to the National Institute of Information and Communication Technology, there has been a significant increase in the number of cyberattacks on IoT devices. The ubiquitous nature of connectivity to the internet has made life more convenient for people but has as a result exposed them to a heightened risk of computer viruses and information theft.

- Japan is seeking bilateral cooperation with countries to operationalize its cybersecurity priorities, such as the agreement with the US Department of Homeland Security, to improve and collaborate on curbing cyber threats faced by the governments.[8]
- In July 2021, the Japanese government compiled a new cyber security strategy amidst a backdrop of heightened suspicion of Chinese and Russian state involvement in cyberattacks. Japan's Government believes that China is conducting cyberattacks to steal information from firms linked to the military and others with advanced technologies, while Russia is suspected of carrying them out for military and political purposes.[9]
- Additionally, a report by Japan's Ministry of Economy, Trade and Industry (METI) identified a shortage of IT professionals at 220,000, which is expected to increase to 360,000 in 2025. This shortage has led to an increase in demand for turn-key cybersecurity solutions for small and medium-sized enterprises in Japan.[10]

7 https://www.barchart.com/story/news/12289146/japan-cybersecurity-market-size-share-key-opportunities-and-future-prospect-till-2030

8 https://www.meti.go.jp/english/press/2023/0107_001.html

9 https://english.kyodonews.net/news/2021/07/d2ff7c90484a-japan-seeks-stronger-cybersecurity-amid-china-russia-threats.html

10 https://asia.nikkei.com/Spotlight/Datawatch/Low-IT-pay-stifles-Japan-s-digital-transformation

Market Trends

Solutions in the area of data security are expected to grow to a significant share of the overall market by 2030. The following are all contributors to this trend:

- The financial sector in Japan is a key adopter of regulatory frameworks implementing the appropriate information and data security standards. This allows them to ensure that there is a reliable provision of products and services, safe processing of data, and responsible use of personal data.
- Data security solutions support the mitigation of cyber risks to sensitive data and the overall management of compliance. The Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2020) ('APPI') places highly prescriptive requirements on several sectors.[11]
- As data security increasingly becomes the norm, using cybersecurity solutions and installing software, such as antivirus and antispyware programs, is expected to generate lucrative opportunities for cyber solutions in the coming years.
- Increased investment in digital transformation from both the public and private sectors, most notably, cloud adoption, Big Data analytics, and IoT enablement, are also driving interest and adoption of data security products.

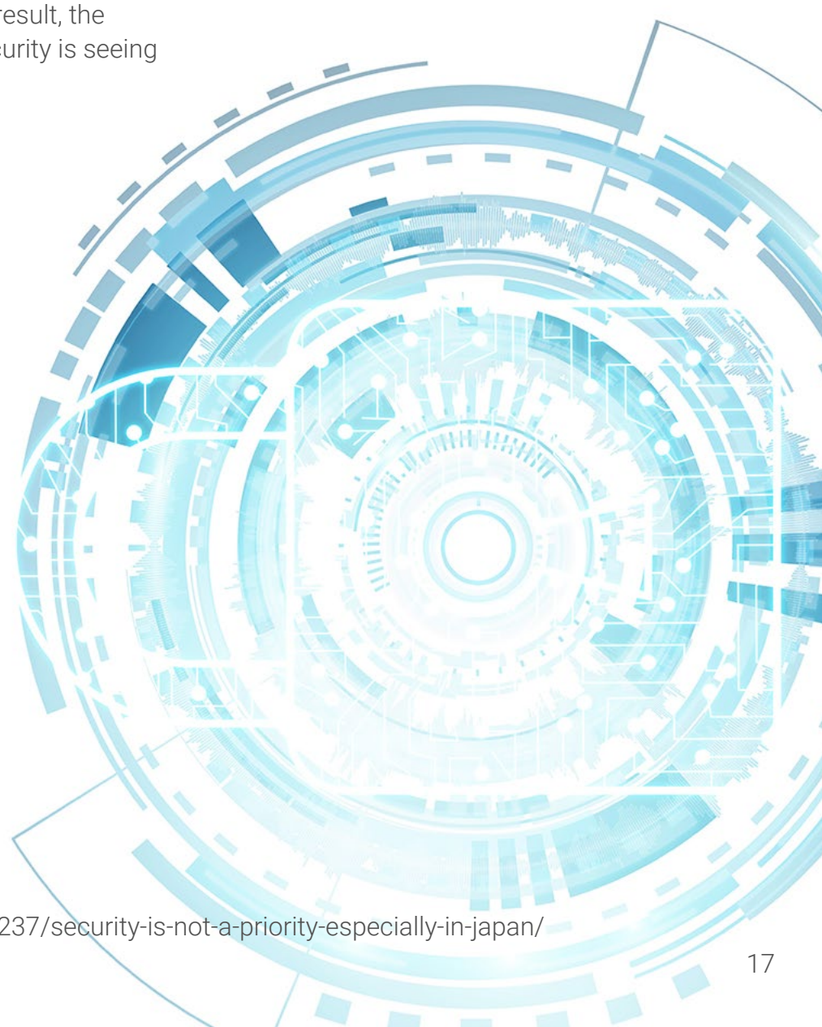
Banking, Financial Services and Insurance (BFSI) is expected to be the sector with the largest increase in spending on cyber security. These institutions are being pushed to adopt a more proactive security approach to secure critical systems and infrastructure, protect customer data and comply with an increasing plethora of regulations.

11 https://www.dataguidance.com/notes/japan-data-protection-overview

Competitive Landscape

The Japanese market is only moderately competitive as a result of the presence of various domestic and international players. Cyber security has historically been a lesser priority for Japan and that has resulted in a perception that the country is unsafe in terms of cybersecurity.[12] This has however changed as the Japanese government undertakes various stringent measures to enhance the cybersecurity capabilities of Japanese companies, as a result, the domestic market for cyber security is seeing more growth opportunities.

The key players in Japan cybersecurity market include: Caulis Inc., Trend Micro Inc., Spider AF Ltd., IBM Corporation, LAC Co. Ltd., Cyber Reason Japan Corporation, Cyber Security Cloud, Inc., Internet Initiative Japan, Inc., SCSK Corporation, Sumo Logic, Inc., Digital Arts Inc., Secureworks, Inc., Cisco Systems Inc., NEC Corporation, Underwriters Laboratories, LLC, Flatt Security, Keychain, Bankguard, GMO JapanSign, Inc



12 https://telecoms.com/487237/security-is-not-a-priority-especially-in-japan/

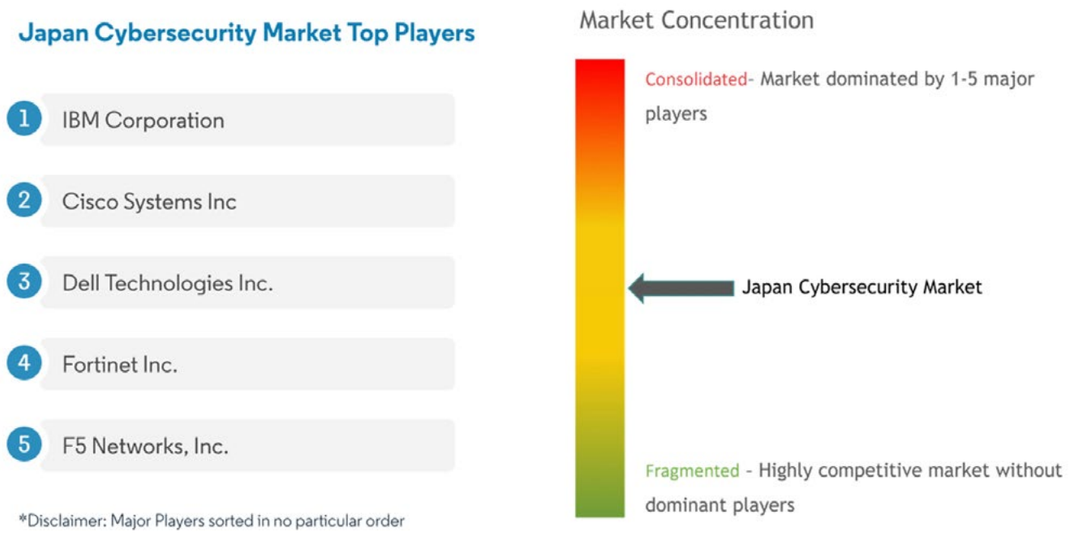


Figure 1 Japan Market Dynamics[13]

The Global Position and Japan

The global cyber security market was valued at USD 139.77 billion in 2021 and is projected to grow from USD 155.83 billion in 2022 to USD 376.32 billion by 2029, at a CAGR of 13.4% during the forecast period.[14] The United States, Israel and the United Kingdom dominate the cyber security sector in terms of global market share.

The market share of Japanese products is relatively small, lagging behind the US and Europe. Foreign companies (Figure 1) are also entering the Japanese market challenging the market share of Japanese cyber goods and services within the Japanese market.

Whilst the Asia Pacific market is expected to see exponential growth including in Japan, the view is widely held that the Japanese government is not allocating sufficient funds towards cyber security in terms of increasing local capability, skills and innovation. Experts are concerned about the country's plans, given their smaller funding and staffing levels. In contrast, North Korea's cyber security personnel number is about 6,800, which means that Japan has a long way to go to secure its data, which is a significant threat to the country.[15]

13 https://www.mordorintelligence.com/industry-reports/japan-cybersecurity-market
14 https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
15 https://www.blueweaveconsulting.com/report/japan-cyber-security-market

New companies that develop advanced technologies to tackle cyberattacks largely operate out of the US, Israel and the United Kingdom with Japanese companies playing a minor role in the cyber security sector. The government of Japan introduced policy reforms in 2013 with a three-pronged strategy that included monetary and fiscal stimulus in addition to structural reforms. The policy has not been able to successfully produce the results needed for innovation and growth in the Japanese economy.[16]

With only three Japanese organisations listed among the top 500 global cyber security companies highlights the current state of the cyber security sector in Japan. Even among the most growth-friendly cities globally for ICT/cyber security start-ups, Japanese cities are not included in the list of top 12 which includes York, Boston, Silicon Valley, Phoenix, Toronto-Waterloo, Ottawa, Hague, Frankfurt, Berlin, Prague, Tel Aviv and Be'er Sheva. The Research and Development landscape in Japan which can often be a catalyst for growth in start-ups also lags considerably behind that of the United States, Israel, the United Kingdom, and Singapore.[17]

16 https://ebrary.net/212206/computer_science/trends_outlook_global_cybersecurity_market_japan
17 https://ebrary.net/212206/computer_science/trends_outlook_global_cybersecurity_market_japan

05. Research & Innovation Landscape

Innovation Support

Japan Science and Technology Agency (JST)[18]

JST is a national research and development Agency that plays a central role in the Science, Technology and Innovation Basic Plan* and aims to promote science and technology. Its funding programmes cover:

- Strategic Basic Research which includes supporting research areas with high potential for generating the seeds of new technologies and research and development from a basic research stage to a stage where the industry can decide whether they could make a business successful.
- •International Collaboration which includes SICORP which is designed to support international bilateral R&D collaboration on an equal-partnership basis, with partner countries and regions and in research fields designated through interministerial agreement.[19]
- Industry-Academia Collaboration and Technology Transfer which includes open innovation around promoting Society 5.0 based on the UN SDGs.[20] The agency also works to promote industry-academia collaborative R&D across a wide range of phases to develop and accelerate commercial applications generated from basic research and in the creation and management of subsequent IP that is being generated.[21]

18 https://www.jst.go.jp/EN/about/overview.html
19 https://www.jst.go.jp/inter/english/index.html
20 https://www.jst.go.jp/pf/platform/file/outline_eng1.pdf
21 https://www.jst.go.jp/opera/ [no english version: use google translate]

Figure 2 NEDO's positioning

The New Energy and Industrial Technology Development Organization (NEDO)[22]

NEDO is the Japanese national research and development agency focused on creating sustainable societies by advancing transformative innovation through technology development. NEDO sees itself as an innovation accelerator leading the formulation of technology strategies and project plans. As part of its project management capabilities, the centre establishes project implementation frameworks that bring together the capabilities of industry, academia, and government in a collaborative way. NEDO also promotes technology development by carrying out, evaluating, and allocating funding to promising projects to accelerate the practical application of project results. NEDO's mission encapsulates two main objectives:

- Addressing global energy and environmental problems through the development of new energy and energy conservation technologies.
- Enhancing industrial technology by carrying out projects to explore future technology seeds as well as mid-to-long-term projects that form the basis of industrial development. It also supports research related to practical application.

The most recent funded activities in cyber security are limited to the "Cross-Ministerial Strategic Innovation Promotion Program (SIP) Phase 2: Cyber-Physical Security for IoT Society"[23] which ran from 2018 through to the end of 2022. The main research themes covered are:

- Research and development of technologies for trust creation and verification which involves working on innovations to enhance the security of individual IoT devices and services.
- Research and development of technology for building and distributing a chain of trust for IoT systems/services and procurement/construction.
- Research and development of technology for verifying and maintaining the safe operation of a chain of trust for IoT systems and services and supply chains.

22 https://www.nedo.go.jp/english/
23 https://www.nedo.go.jp/english/activities/activities_ZZJP_100156.html

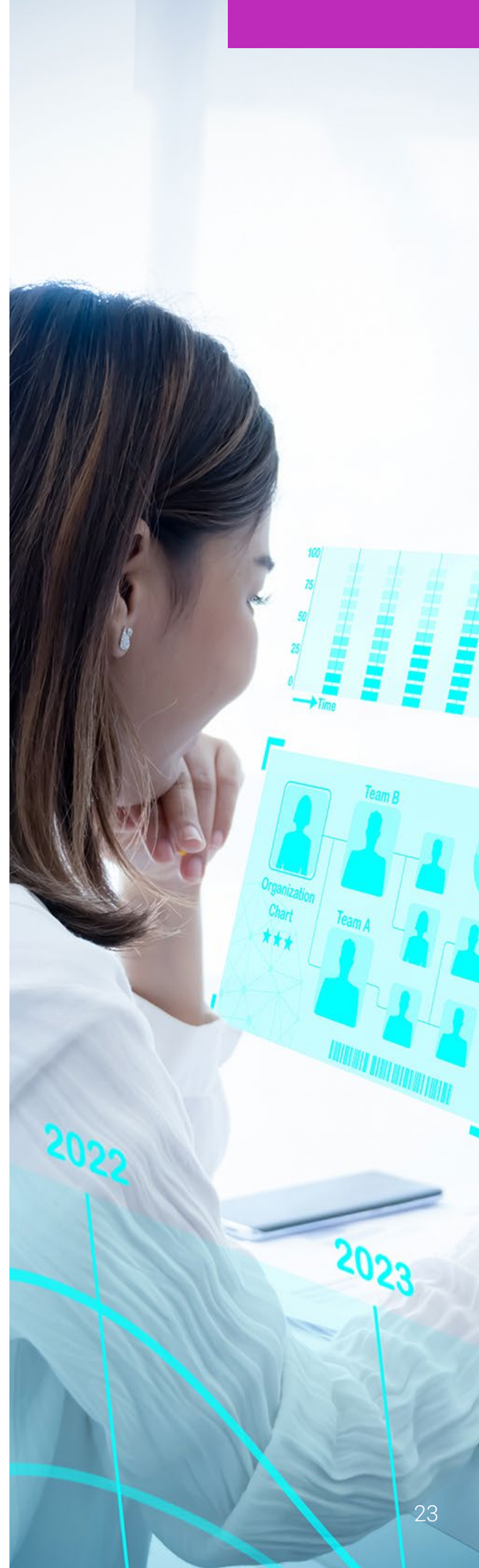
Japan Society for the Promotion of Science (JSPS)[24]

JSPS is an independent administrative institution, contributing to the advancement of science in all fields of the natural and social sciences and the humanities. Its main functions are:

- To foster young researchers,
- To promote international scientific cooperation,
- To award Grants-in-Aid for scientific research,
- To support scientific cooperation between the academic community and industry, and
- To collect and distribute information on scientific research activities.

The international collaboration is focused on forming coordinated international research support networks and providing international research training opportunities for young researchers.

24 https://www.jsps.go.jp/english/



White Papers and Policies

Japan's Cyber Security Strategy of 2021 promotes the advancement of practical research and development. This is seen as necessary to combat current issues presented in cyberspace.[25]

The areas of focus include:

- The Establishment of an all-Japan technical verification system for addressing supply chain risks including the trustworthiness of Internet of Things devices, the security of 5G components, and malicious functions of chip designs.
- Support measures for cultivating domestic cyber security capability that can improve products and services and meet the needs of SMEs.
- Strengthen Information Sharing platforms and the technology to observe, identify, and analyse cyberattacks to appropriately respond to the development of cyberattack threats.
- Advance research of cryptography with the expectation that existing encryption technologies will become compromised when practical large-scale quantum computing is realised.

Japan's Information Security Research and Development Strategy highlights all of the following areas as priorities:[26]

- New dependability of the entire information system.
- Information security infrastructure technology for next-generation networks where the real world and the virtual model in the computer are combined.
- •Technology for maintaining consistency of security configurations between layers automatically.
- •Technology for building a computer network architecture that can perform automatic recovery from failures.
- System design technology for combining biometrics information with ID management under the control of a computer.
- Zero-Day Defence based on attackers' behaviour analysis.
- Preventive base technology using attackers' behaviour analysis.
- Combination of a wide-area observation technology in a large-scale network and malware behaviour analysis technology.
- Flexible management of personal information.
- User control technology of personal information for promoting utilization.
- Data control/pursuit technology for supporting forensics.
- Systematization of theory-to-practice concerning IT risks.
- Infrastructure for stimulating research and development and systematized information security theories.
- The systematized basis for information security studies.
- Product evaluation certification technologies for ensuring the correct implementation of security components.
- Theoretically secure cryptographic technology.

Additionally, disaster-resilient technology has been especially highlighted given Japan is prone to Earthquakes - somewhat more of a nuanced issue but disaster-resilient IT Infrastructure is something that is singled out for specific focus.

25 https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf (Section 4.4.1(1) of the Cybersecurity Strategy 2021)
26 https://www.nisc.go.jp/eng/pdf/R_and_D_Strategy_eng.pdf

The Cross Ministerial Strategic Innovation Promotion Program (SIP)[27]

SIP is a national program led by the Council for Science, Technology, and Innovation (CSTI) of the Japanese Government. It addresses 23 subjects - 11 in the first phase and 12 in the second which are seen as crucial for society and that could contribute to the revival of the economy in Japan. Interdisciplinary research and development covering from fundamental study to industrial application with industry-academia-government cooperation.

This program incorporates a Research and Development Plan for Cyber-Physical Security for IoT Society.[28] The plan is primarily focused on the delivery and realisation of Society 5.0. The focus is on making sure appropriate security measures to assure safety and security are in place across the supply chain.

This means humans, organizations, products, systems, services, and data all must be considered when thinking about security. In addition, the entire IoT systems/services supply chain including manufacturing and distribution should have appropriate and effective security measures.

To realise a "cyber-physical security infrastructure" the need to develop the most advanced core technologies in the world is envisaged which will be used to assure entire supply chains (including SMEs) engaged in the procurement and construction of IoT systems/services and maintenance of security for various services.

27 https://www.jst.go.jp/sip/k03/sm4i/en/outline/about.html
28 https://www.nedo.go.jp/english/activities/ZZpage_100140.html

Bilateral Cooperation

Under the SICORP Programme, there was a Marine Sensors Proof of Concept Project between Japan and the UK. It was supported in the UK by The Natural Environment Research Council (NERC). Three projects ran from 2018 to 2021 and the collaboration was between the University of Tokyo and the National Oceanographic Centre in Southampton in the UK and The Japan Agency for Marine-Earth Science and Technology (JAMSTEC) and the University of Southampton.[29] The SICORP program is still running however there are currently no ongoing activities between the UK and Japan and there are none planned in the immediate future.

Under the JSPS International Collaboration, there have been projects between the UK and Japan in 2022 (between academia in Japan and the UK – The Royal Society and indirectly UK Universities) in the areas of Medicine and Biochemistry.[30] These sorts of collaborations between academia in Japan and the Royal Society appear to be long-standing at least as far back as 2019.[31]

Innovate UK, part of UK Research and Innovation, invested £1 million to fund UK businesses leading collaborative projects in partnership with NEDO (Japan) for research and development (R&D) under the EUREKA programme.[32]

29 https://www.jst.go.jp/inter/english/program_e/sicorp_e/uk.html
30 https://www.jsps.go.jp/file/storage/e-bilat_2022/seminar/List_of_Joint_Research_Projects_and_Seminars_FY2022_E.pdf
31 https://www.jsps.go.jp/english/e-bilat/additional.html
32 https://www.eurekanetwork.org/open-calls/globalstars-japan-2020

06. Summary of Stakeholder Meetings

Japan Automotive Manufacturing Association (JAMA)[33]

JAMA is an association representing the Automotive Sector in Japan. It has fourteen members all of whom form the core of the automotive manufacturing industry in the country. They were established in 1967 and have the objective to promote the sound development of the Japanese automobile industry and contribute to social and economic welfare. Whilst they are a body representing the industry in Japan, they have overseas offices in Washington DC, Beijing and Brussels so they are clearly aiming to represent the interests of their members globally.

They engage with counterparts internationally such as ACEA Europe, Germany VDA and North Americas AIAG.

JAMA has a Cyber Security Experts Group, and its role is to enhance coordinated cyber security measures within the automobile Industry. Their midterm policy is to promote the creation of a safe, secure and reliable cyberspace against ever-sophisticated cyberattacks in the IoT and mobility fields.

The Experts Group has three task groups:

- Supply Chain Security Task Group
- Manufacturing Plant Security Task Group
- Vulnerability and Threat Information Sharing Task Group

The discussions indicated that JAMA has strong collaborative activities focussed on promoting integrated industry measures for cyber security with the US/EU automobile industries as well. Supply chain security is amongst their key priorities and in this area, they have worked on drafting industry wide rules on enhancing the security of supply chains and the entire automobile industry, referencing METI's Cyber/Physical Security Framework.[34]

JAMA hope to collaborate with other industries and governments on the supply chain security issue and they hope to use mechanisms like the Supply Chain Cyber Security Consortium (SC3) for those sorts of collaborations.[35]

33 http://www.jama.or.jp/english/
34 https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0_eng.pdf
35 https://www.ipa.go.jp/security/sc3/about/en/

National Institute of Information and Communications Technology (NICT)[36]

NICT is Japan's sole National Research and Development Agency specializing in information and communications technology, NICT has the combined task of promoting the ICT sector in Japan as well as research and development in ICT, which drives economic growth and creates an affluent, safe, and secure society.

NICT has a Cyber Security Research Institute[37] which is one of four strategic research fields at NICT.

The institute is split up into The Cyber Security Laboratory, The Security Fundamentals Laboratory, The Cyber Security NEXUS (CYNEX), The National Cyber Training Centre and The National Cyber Observation Centre

The research and development focus areas at the Cyber Security Laboratory and The Security Fundamental Laboratory include:

- Advanced cybersecurity technologies – include research and development on cyberattack monitoring and the analysis of supporting technologies for the increasingly sophisticated and evolved cyberattacks against the government and other important infrastructure.
- Functional cryptographic technologies, provide new functionality to meet the new social needs accompanying the IoT evolution, security evaluation of cryptographic technologies contributing to the promotion and standardization of new cryptographic technologies, and constructing and maintaining safe and secure ICT systems.
- Privacy protection technologies for the practical utilization of personal data and the promotion of technical support activities for appropriate privacy measures.
- Evaluation of the security of currently used cryptographic techniques to contribute to securing ICT systems, and the security of emerging cryptographic techniques to
- Promote market deployment and standardization. Furthermore, we promote research on privacy-enhancing technologies for personal data use and support technical countermeasures to privacy threats.

The focus areas above are not dissimilar to some of the research activities in the UK and certainly provide some synergies as a basis for future collaboration.

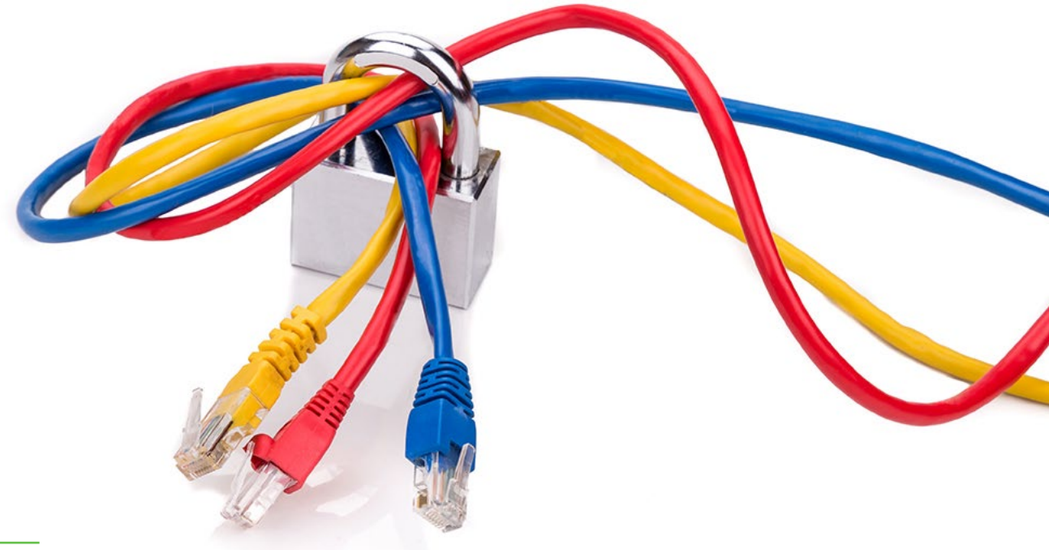
CYNEX is part of the aim of improving Japan's domestic capability and capacity concerning Cyber Security. CYNEX specifically focuses on enhancing Japan's cyber security response capabilities by collecting, accumulating, analysing, and providing cyber security information domestically and opening up a common infrastructure for developing cyber security human resources throughout Japan.[38]

NICT has international collaboration programmes aimed at supporting Japanese industry and academia in their projects that require collaborative research and exchange of personnel with overseas organizations.

International Exchange Program - international exchange of Japanese and foreign researchers in the field of advanced telecommunications and broadcasting technology.

Japan Trust International Research Cooperation Program – foreign researchers are invited to participate in the research and development of basic technologies in the areas of telecommunications and broadcasting, to Japan, in support of the research and development of private institutes.

NICT overseas centres in North America (Washington DC), Europe (France) and Asia (Thailand) - to promote global research cooperation and contribute to international standardization in an effective and efficient manner. The findings indicate a very strong desire to seek to build long-term substantive trusted relationships with government agencies, research institutes and universities internationally.[39]



36 https://www.nict.go.jp/en/index.html
37 https://csri.nict.go.jp/en/index.html
38 https://cynex.nict.go.jp/en/
39 https://www.nict.go.jp/en/global/overseas_centers/north_america/index.html

Figure 3 Activities underlying the three policy objectives

The National Center of Incident Readiness and Strategy for Cybersecurity (NISC)[40]

The National Centre of Incident Readiness and Strategy for Cybersecurity, "NISC" has been established in 2015. It plays a leading role as a focal point in coordinating intra-government collaboration and promoting partnerships between industry, academia, and public and private sectors.

NISC coordinates:

- Cybersecurity Strategy
- Cybersecurity Policy for Critical Infrastructure Protection
- Common Standard on Information Security Measures of Government Entities
- Cybersecurity Human Resource Development Plan
- Cybersecurity Research and Development Strategy etc.

NISC takes the role of a governmental CERT and in collaboration with other responsible authorities it forms the CERT covering private companies as well.

They have produced the Cyber Security Strategy in 2021 with an overarching ambition to develop and deliver "Cyber Security for all – Cyber Security which leaves no one behind". The objectives underlying this are:[41]

- To advance digital transformation (DX) and cyber security simultaneously.
- Enhancing initiatives from the perspective of national security.
- Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected, and interrelated.

The cross-cutting approaches involve the promotion of R&D which encapsulates:

- Strengthen international competitiveness by building a government-industry-academia ecosystem.
- Advance practical R&D on supply chain risks, monitoring, and analysing attacks.
- Cultivate and develop the domestic industry.

40 https://www.nisc.go.jp/eng/index.html

41 https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-gaiyou-en.pdf

Ministry of Economy, Trade, and Industry (METI)[42]

METI plays an integral part in Cyber Security policy-making within Japan. This includes:

The Cyber-Physical Security Framework – Japan is promoting Society 5.0 and the initiatives proposed in order to realise this vision requires the integration of cyberspace and physical space that create great value for citizens and companies. This however has risks that will lead to an increase in cyberattacks. The Cyber/Physical Security Framework will guide the implementation of the Connected Industries program to reduce the risk of attacks.[43]

METI is at the forefront of delivering on the policy of implementing digital transformation and cyber security in parallel whilst actively running awareness and outreach campaigns, especially to SMEs. Guidelines and standards will form a critical part of this plan. There is a challenge in persuading companies that they need to make the same investment in cyber security as they are in digital transformation.

There is significant interest in the UK Regulatory efforts on IoT security. Japan has a twofold interest in this:

- To understand what the requirements are as Japanese companies are a manufacturer of hardware devices that could be within the remit of this regulation if they are to export to the UK.
- To see what they might learn from the UK in order to enhance IoT security domestically in Japan. They are considering labelling schemes such as the one in the United States.

They are actively involved in substantive collaborations with counterparts in other countries. This includes:

A Memorandum of Cooperation between METI in Japan and the Department of Homeland Security (DHS) in the United States.[44] They will cooperate on cybersecurity in the following areas with the cooperation of related organizations.

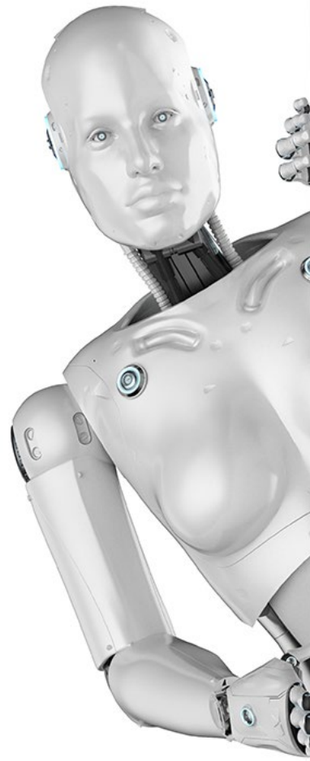
- Operational collaboration
- Enhancement of the security of industrial control systems
- Cooperation for capacity building especially for the Indo-Pacific Region
- Dialogues toward the harmonization of regulations and schemes

42 https://www.meti.go.jp/english/
43 https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0_eng.pdf
44 https://www.meti.go.jp/english/press/2023/0107_001.html

ASEAN – Japan Cybersecurity Working Group/Policy Meeting[45] which aims to promote and strengthen cyber security cooperation and collaboration between ASEAN Member States and Japan. The areas of collaboration include Cyber Exercise, CIIP Workshop, Awareness Raising, Capacity Building, Mutual Notification, Online Community, and Cybersecurity Reference. The ASEAN-Japan Cyber Security Capacity Building Centre is another activity of this ongoing partnership. The aim is to develop a cybersecurity workforce of 700+ over 4 years to enhance the capacity of cybersecurity experts and specialists in the AMS by providing training and other activities to participants from the ASEAN Member States.[46]

The meeting indicates a strong desire to work with counterparts in government in other countries and specifically with the UK in areas of common interest.

The National Institute of Advanced Industrial Science and Technology (AIST)[47]



45 https://cybilportal.org/projects/asean-japan-cybersecurity-working-group-policy-meeting/
46 https://www.ajccbc.org/about.html
47 https://www.aist.go.jp/index_en.html

Cyber-Physical Security Research Centre (CPSEC)[48]

Research is focussed on security enhancement technologies, evaluation technologies, and security assurance schemes to realize security in a society where cyber/physical space is highly integrated (**cyber-physical security**), and to contribute to economic development and the realization of solutions to social issues.

Within this, there are six research teams focussed on Cryptography, Hardware, Software, Security Assurance, Infrastructure Protection and Software Analytics

CPSEC is looking to carry out research and development towards the realisation of technologies that provide theoretically backed solutions to the security challenges faced by society today. Additionally, they are looking to anticipate future challenges and have early preparedness by carrying out research in those areas and developing the technologies to mitigate those risks.

They see some of the main security challenges around:

- Hardware security for a root of trust in supply chain integrity
- Development of advanced cryptography
- Secure multiparty computation
- Functional cryptography
- Post-Quantum cryptography (this lab briefly held the world record for the fastest
- Implementation of lattice-based cryptographic functions)

They attach considerable importance to working with academia to get cutting-edge research and results into the market to directly address the challenges industry, governments, and citizens face. AIST is expected to be a bridge in bringing academic research into practical applications.

48 https://www.cpsec.aist.go.jp/center/index_en.html

Information Technology Promotion Agency of Japan (IPA)[49]

IPA is an information technology promotion agency focused on IT Security, improving the reliability of information processing systems, and IT human resources development. IPA hosts the Industrial Cyber Security Center of Excellence (ICSCoE)[50] with the aim of developing human resources, organizations, systems, and technologies dealing with cybersecurity risks for social and industrial infrastructure. There are three main sets of activities:[51]

- Human Resource Development Program
- Risk assessment activities on the safety and reliability of actual control systems
- Investigation and analysis of cyber attacks

Within the context of human resource development, the main training program is 1 year's duration. Trainees spend the first two months learning the basics of Information Technology (IT) and Operational Technology (OT) which is followed by the basic phase where they learn more specific technologies for IT and OT which is then followed up with hands-on training so that they all the trainees get experience of real operational technologies. Finally, the advanced phase is a digital transformation focussed course that delivers awareness and understanding of International Standards. More than 300 candidates have graduated from this program.

The main international activity involves sending trainees to other countries on placements to gain insight and knowledge from how others are doing things. Such programmes exist in the UK, France, and the United States.

49 https://www.ipa.go.jp/en/index.html
50 https://www.ipa.go.jp/icscoe/english/index.html
51 https://www.ipa.go.jp/files/000092513.pdf

Japanese Cybersecurity Innovation Committee (JCIC)[52]

JCIC is the only not-for-profit cyber security think-tank. The think-tank has an emphasis on "management" and "global" perspectives. They promote their independence and neutral standpoint. Their funding comes primarily from Member companies' annual fees.

They aim to be a central hub on cyber security for every sector and stakeholder group within Japan.

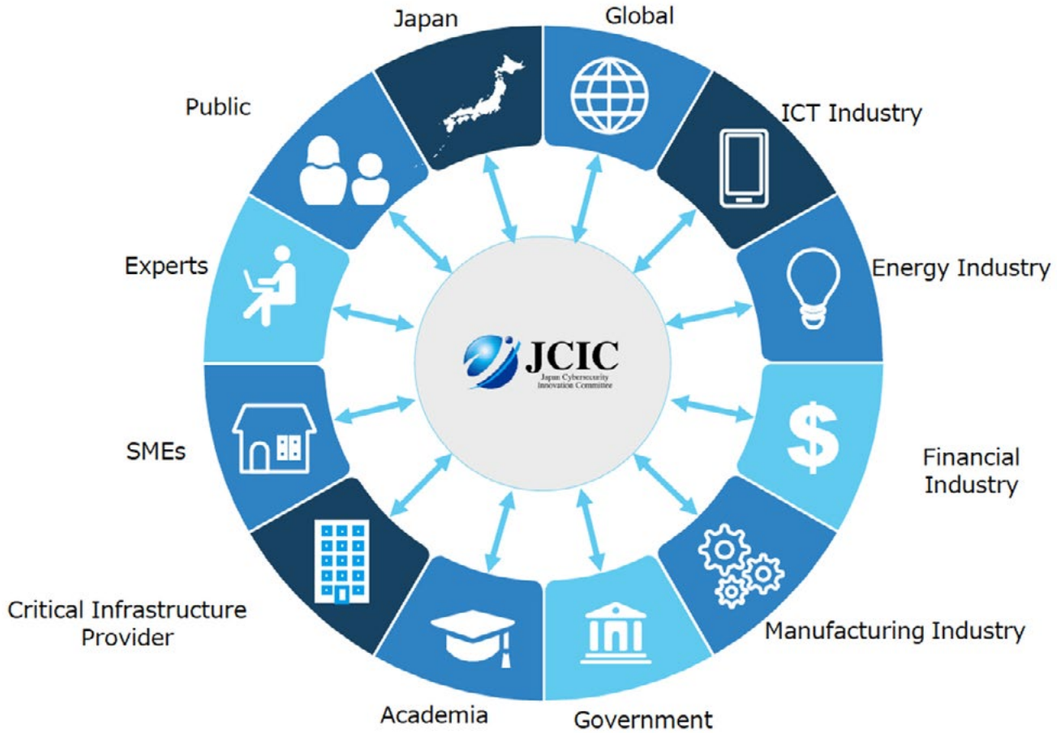


Figure 4 JCIC's position in Japan[53]

52 https://www.j-cic.com/en/about.html
53 https://www.j-cic.com/en/vision.html

They have put forward several proposals towards the realisation of a post-pandemic digital society intending to build a better Japan. These proposals include:[54]

- Proposal 1: Japan should improve an environment that allows all citizens to access the Internet.
- Proposal 2: Japan should establish a scheme for personal authentication in the digital society.
- Proposal 3: Japan should allocate sufficient human resources and budget to manage the operation of the entire digital social system.
- Proposal 4: Japan should ensure the right of all citizens to use education.
- Proposal 5: Japan should avoid the pitfalls of a pseudo-digital society.

The membership represents a broad breadth of companies across a diverse range of sectors in Japan providing the depth and breadth of coverage required to achieve policies, guidelines, and initiatives with the widest applicability across Japan.

They have identified the following as challenges against which they are conducting work in the form of publishing reports and commentaries:

- Quantifying cyber risk
- A shortfall of human resources and its solutions
- Cybersecurity KPI Model
- Corporate cyber security disclosure report
- Rebalancing convenience and security

International Dialogue has been established and so far, includes:

- Japan-Taiwan Dialogue (with ITRI [Industrial Technology Research Institute])
- Japan-Australia Dialogue (with Queensland University, Australia)

The meeting demonstrated an interest to further this international dialogue with other countries as well where the two countries share common interests and values which could provide an opportunity for further conversations to see what such a joint dialogue with appropriate counterparts in the UK could bring about.

54 https://www.j-cic.com/en/reports.html

ICT-ISAC Japan[55]

IISAC stands for Information Sharing and Analysis Centre and they first came into being under the Clinton Administration in the United States in 1998. The policy objective was to protect the important information network of the state. The establishment of ISACs was encouraged in each industry sector that constitutes important infrastructure. Each ISAC would collect, analyse, and share executable threat information to mitigate risk and increase resilience. Japan launched their first ISAC in 2002 in the telecoms sector.

The ICT ISAC has 46 member corporations that represent the telecoms, mobile operators, ISPs, broadcasters, security vendors, system integrators and 5G areas. Alongside this, there is a group of observers from government and industry associations.

The purpose of the organization is to contribute to the creation of a safe and secure “ICT society” by strengthening ties between the members and fostering a culture of information exchange to bring about an overall improvement in the ICT-related security measures and response levels.

The main activities that they undertake include:

- Collection, research, and analysis of information relating to information security.
- Promotion of information sharing (information sharing).
- Development of security personnel and education programmes on security.
- Activities to maintain security guidelines.

ICT-ISAC also has a specific concern over IoT Security. As a result, they also have three specific activities focussed on that area:

- Monitoring - monitoring and information sharing on vulnerable IoT devices.
- Notification - survey vulnerable IoT devices and alert users to the problem.
- Awareness Raising - awareness raising for corporate IoT devices.

There are currently 7 ISACs operating in Japan and there is ongoing cooperation between them. Japanese ISACs also cooperate with their counterparts in the United States and the European Union.

In 2019, ICT-ISAC was involved in establishing the International ISAC Collaboration WG to study ways to promote cooperation between ISACs in Japan and overseas (sharing and utilization of sensitive information across organizations, etc.)

55 https://www.ict-isac.jp/english/

Japan Venture Capital Association (JVCA)/ Global Hands-On VC[56] [57]

Japan Venture Capital Association was founded in 2002. It is a trade association that caters to the venture capital industry. The association conducts surveys and provides research services. It also prints publications and provides public relations services.

It also provides funding and other forms of investment as well as management support and other services to assist in the founding, growth, and development of promising start-ups not yet listed on any stock exchanges.

The association has three committees:

- the Venture Ecosystem Committee
- the Fund Ecosystem Committee
- the Open Innovation Committee

Alongside this, they have a Global Collaboration sub-committee which seeks to collaborate with VC organizations and governments outside of Japan (e.g., coordination with embassies and VC-related organizations from various countries).[58]

Global Hands-On VC is a VC fund providing Investment and hands-on support. They see themselves as different to some of the more traditional VC funds which are typically run by purely financial partners solely interested in the financial outcome. Global Hands-On VC is run by people who have been entrepreneurs themselves so they have been on the same journey that the founders they invest in are taking and can provide the support, knowledge, and insight from their experience. The fund is focused on Japan aiming to make investments to support Japanese companies' global growth. They sit alongside US funds such as Prota Ventures[59] in sharing a vision to build ventures rather than just make investments.

Japan has a rapidly maturing start-up ecosystem. In the government's June 7, 2022, announcement of its new economic strategy,[60] Kishida Fumio's administration included an aggressive vision for Japan's start-up ecosystem intending to increase the number of start-ups tenfold over the next five years.

Funding for start-ups in Japan has seen ten-fold growth since 2013 with 7% growth between 2021 and 2022. Finally, there has been a fifteen-fold increase in the number of start-ups in Japan that are successfully raising more than 10 million USD in one funding round. The gap however is still big in so far as Japan still only has 3% of the amount of funding going into start-ups in comparison to the United States. However, whilst this significant gap remains in absolute terms it may not be as relevant. Japan's start-up ecosystem as it matures is not going to play the same role in the economy as Silicon Valley has done in the United States.

In the United States, venture-capital-financed, fast-growth start-ups displaced and disrupted countless industries and incumbent large firms to become a pillar of the entire economy, venture capital became a critical component of the U.S. innovation system, and Silicon Valley produced many of the world's most highly valued and cash-rich firms. Japan's large long-standing global incumbents are unlikely to be displaced by its start-ups.

Instead, Japan's start-ups are partnering with large firms and are gaining levels of acceptance unseen in at least the past sixty years, Japan's start-up ecosystem can play a vital role in injecting flexibility, influencing the trajectory of large firms, and providing a much-needed venue for dynamism and growth.[61]

JVCA are extremely keen to learn from the UK experience and sees considerable potential in feeding through lessons learnt from countries like the UK into the policy-making activities within the Japanese Government along with input into their own planning as private investors.

56 https://jvca.jp/about/activities
57 https://www.ghovc.com/?lang=en
58 https://jvca.jp/committee
59 https://www.protaventures.com/
60 https://www.japan.go.jp/kizuna/2022/06/integrated_innovation_strategy.html

61 https://carnegieendowment.org/2022/08/09/startup-japan-series-overview-pub-87648

Institute of Information Security (IISEC)[62]

IISEC is a graduate school established in 2004 specialising in Information Security, with an aim to provide the required skills in Information Security.

Ten years ago, there was a necessity for measures to protect Information Security and that has evolved now to the need for all human resources to have training and awareness of Cyber Security.

General Studies

- Information Security Special Lectures
- Whole Class Seminar I II
- Presentation for Professional
- Critical Thinking and Innovation

Security & Risk Management

- Decision making under uncertainty
- Statistical Risk Management
- System and Security Audit
- International Standards and Guidelines
- Information Security Psychology
- Risk Management and Information Security
- Security Management and Governance
- Organisational Behaviour and Security
- Mass Media and Risk Control
- Data Science and Analytics

Mathematical Science & AI

- Crypto-Auth and Social Systems
- Cryptographic Protocol
- Algorithms
- Basic Number Theory
- Theory of Cryptography
- AI and Machine Learning
- Blockchain Theory

Cybersecurity & Governance

- Cyber Security Techniques
- Ethical Hacking/Malware Analysis
- Law & Ethics in Information Security
- Introduction to Legal Study
- Intellectual Property System
- Legal cases in Information Security
- Individual Identification & Privacy Protection

Systems Design

- Programming
- Software Design
- Operating Systems
- Information Devices Technology
- Information Systems Design
- Network Design & Security Operations
- Secure System Architecture
- Secure Programming & Secure Operating Systems
- Practical IoT Security

Hands-on Exercises

- Practical Secure Systems
- Advanced Windows Security
- Capture the Flag (CTF)
- Incident Response & CSIRT Basics
- Network Security & Web Application Inspection
- Digital Forensic

Figure 5 IISEC Graduate Programme

62 https://www2.iisec.ac.jp/english/

The programmes encompass training and education in cryptography, networks, systems technology, and organisational management, in addition to the laws and ethics related to information security.

By March 2022, the graduate school has 499 Masters graduates & 49 PhD's and these people now play an active part in the information security fields in Japan. IISEC also has a strong research and development agenda as indicated in the figure below.

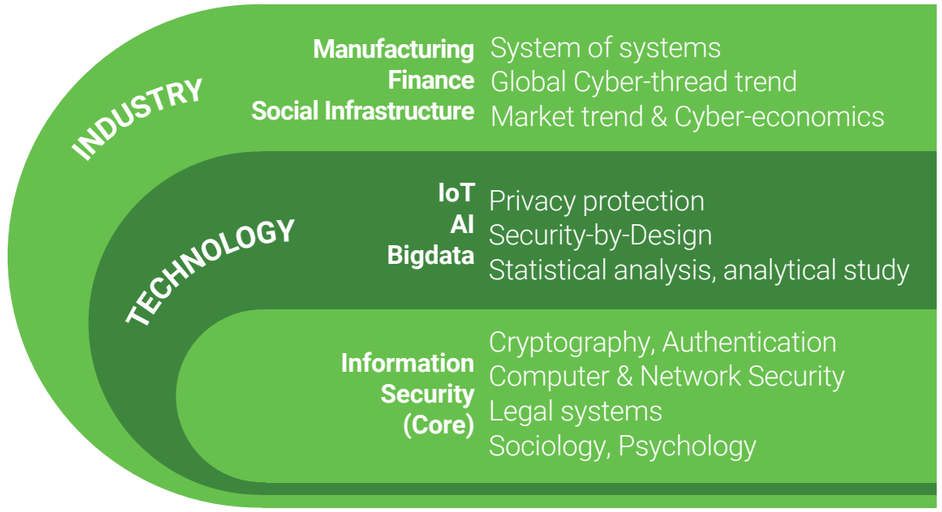


Figure 6 Cyber Security R&D at IISEC

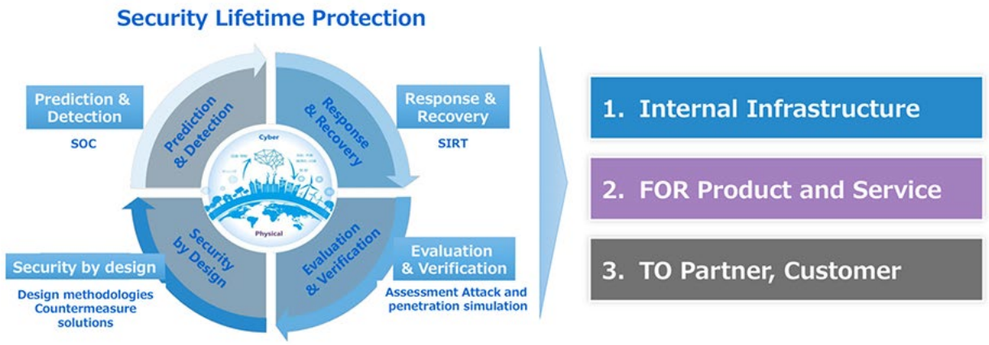


Figure 7 Security Lifetime Protection Approach

Toshiba[63]

Toshiba now primarily operates in the infrastructure sectors, developing products for customers from control systems to printers. They build Cyber-Physical Systems (CPS) to fully utilise the power of data.

They develop cyber security solutions and carry out research and development for their own products but then leverage all of that to support the cyber security needs of their customers via a dedicated cyber business as well.

With respect to the sustainable protection of Cyber-Physical Systems, they take a "Security Lifetime Approach" which involves four key steps as shown in the figure above.

They provide an Industrial Control System Security Solution & Service and this involves the provision of security services from "design and defence" to "evaluation and verification" throughout the security lifecycle

Toshiba takes a proactive approach to its own cyber security preparedness to prepare for, minimize the impact of, and recover from incidents as quickly as possible. This incorporates:

- Sustainable Hygiene - secure development and vulnerability handling, threat hunting and incident readiness.
- Minimise Impact - early detection using real-time threat information and asset information.
- Quick Response and Recover - quick and accurate forensics using threat information and log information.

The meeting indicated two key concerns/ challenges:

- There is concern about supply chain security. Toshiba has established guidelines for its partners that they use to gauge trust against the guidelines and carry out inspections and audits. This isn't seen as an adequate approach going forward as the risk of information leakage through the supply chain is increasing.
- There is an increasing challenge around being able to understand the veracity and integrity of the data that is being used which is automatically generated by devices and probes.

63 https://www.global.toshiba/ww/top.html

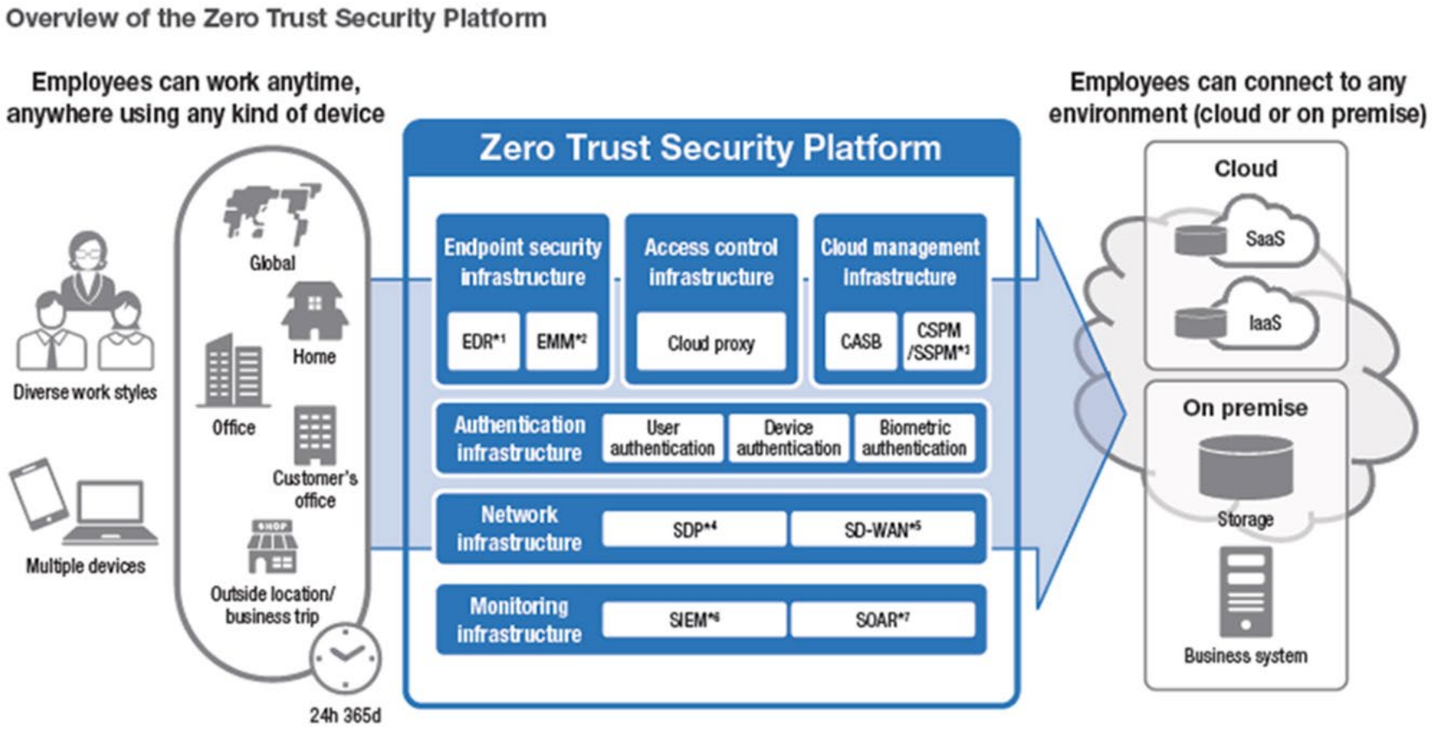


Figure 8 NEC Zero Trust Security Platform[64]

NEC Corporation[65]

The NEC Corporation is a Japanese global multinational information technology and electronics corporation. The company was known as the Nippon Electric Company, Limited, before rebranding in 1983 as NEC. NEC has 50 companies in Japan and 70 companies outside of Japan so there is a CISO for the global group and then regional CISOs.

Their Cyber Security Strategy is in essence to contribute to the realization of a safe and secure society through cybersecurity. This involves:

- Collaboration with related organizations
- Contribution to the Government's initiatives
- Framework enhancement for the provision of advanced services
- Development of in-house human resources
- Investments in the development of domestic security human resources
- Provision of education programs for customers
- Thoroughly secure development and operations
- Support for strengthening security based on in-house operational expertise

NEC has established a zero-trust security environment through their platform as shown above.

Within this Zero Trust Security environment, there is a realisation of endpoint protection and analysis. NEC is not relying on any one company instead looking to various different companies to maximise the benefits of diversity. In terms of threat intelligence gathering, they have deployed several probes to gather data aiming to move the focus away from incident response to being more proactive by using intelligence to prevent things from happening in the first place.

Internal training and skills development on cyber security incorporates specialised training for experts and a broad programme for all employees. Training for experts works towards security by design and covers risk assessment, attack simulation and training to formulate appropriate defences to differing types of attacks. NEC has developed awareness courses which are free and aimed at providing everyone with some basic knowledge and skills.[66]

The Dow Jones Sustainability Index covers cyber security and NEX rates with a score of 100 which demonstrates a degree of cyber maturity that makes them stand out amongst their counterparts.

64 https://www.nec.com/en/global/solutions/cybersecurity/
65 https://www.nec.com/
66 https://sg.nec.com/en_SG/solutions/cybersecurity/awareness/index.html

J-AUTO-ISAC[67]

J-AUTO-ISAC was established to promote the safety and security of the automobile industry. The aim is to facilitate efficient and effective information sharing and analysis of cybersecurity risks and to enhance the ability to respond to cybersecurity risks to ensure the safe and secure use of Japanese automobiles and related services.

Their principal activities include:[68]

- Collecting and analysing information concerning threats and vulnerabilities and sharing relevant information.
- Plan and provide support for cyber security measures.
- Plan and provide support for measures to develop cyber security human resources.
- Provide support for system development.
- Collaborate with external organizations.

They have three technical committees for information sharing, skill development, and promotion of solutions for specific issues.

The membership is made up of 107 companies within the automotive sector and related supply chains.

They are members of JAMA and JAPIA (Japan Automotive Parts Association)[69]

67 https://j-auto-isac.or.jp/en/
68 https://j-auto-isac.or.jp/en/about/
69 https://www.japia.or.jp/en/top/

07. Collaboration Opportunities

Whilst Japan has several initiatives underway within the context of cyber security, the domestic ecosystem is still finding its feet in establishing competitiveness across cyber security capabilities. The research and development landscape also appears to reflect this, based on the meetings held during the mission.

Bilateral agreements signed in recent years provide a promising basis for collaboration in the area of cyber security between the two countries. The UK-Japan Digital Partnership signed in 2022 provides a "framework for deeper UK-Japan collaboration across digital infrastructure and technologies, data, digital regulation and digital transformation."[70] Of the specific 14 areas where both sides have committed to working together, the following all provide opportunities for direct or indirect opportunities for specific collaborations in the cyber security area:

- telecoms diversification
- increasing cyber resilience
- semiconductors
- artificial intelligence
- championing data flows
- regulatory cooperation
- data innovation
- online safety
- digital technical standards
- internet governance
- digital identity

The UK-Japan Defence Agreement of 2023[71] outlines the rapid acceleration of cooperation between the two countries on defence and security. This also sits alongside the UK's recognition that Japan is the most important and closest security partner in Asia.[72]

70 https://www.gov.uk/government/publications/uk-japan-digital-partnership
71 https://commonslibrary.parliament.uk/research-briefings/cbp-9704/
72 https://www.gov.uk/government/publications/defence-in-a-competitive-age

Regulatory Cooperation

Japan has a substantive interest in the common challenges of IoT security and supply chain security. The UK has been one of the leaders from a regulatory and standards perspective in this area. The product security and telecommunications infrastructure Act 2022 (PSTI)[73] makes "provision about the security of internet-connectible products and products capable of connecting to such products; to make provision about electronic communications infrastructure; and for connected purposes. METI in Japan is looking to develop effective mechanisms in this area as well and regulatory harmonisation would be beneficial to both countries and would potentially improve market access for IoT device manufacturers in the United Kingdom in the future.

In 2021 the UK launched an open call for views on supply chain security, seeking insights from the industry to inform the government's understanding of supply chain cyber security.[74] The UK National Cyber Security Centre (NCSC) has also produced guidance on this area.[75] This consultation has pointed to areas in supply chain security that are not covered by the guidance. The findings also indicate that regulation would be perceived as very effective in this area as part of the need for a much more interventionist approach from the government.

Given the shared challenge and desire to find solutions, it presents a tangible opportunity for collaboration on developing common regulatory frameworks which will enhance overall cyber resilience in both countries and ensure future potential market access for the UK as regulatory harmonisation will enhance trust in secure supply chains between the two countries.

Standards

There exist areas where international consensus is important, such as deciding reasonable security criteria based on state-of-the-art technology. The Japanese International Standards Committee (JISC)[76] is contributing to consensus by providing academic results in the development of security standards for CC (Common Criteria) certification[77] within the framework of the International Standards Organisation (ISO).[78]

Collaboration between JISC and The British Standards Institute (BSI)[79] could provide a platform that could strongly influence global standards especially if wider bi-lateral and mini-lateral partnerships are leveraged by both the UK and Japan.

Participation in discussions in consensus-making organisations is an effective way to influence standards that favour strategic interests, policies, and industries

73 https://bills.parliament.uk/bills/3069
74 https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security/government-response-to-the-call-for-views-on-supply-chain-cyber-security
75 https://www.ncsc.gov.uk/collection/supply-chain-security

76 https://www.jisc.go.jp/eng/
77 https://www.iso.org/standard/72891.html
78 https://www.iso.org/home.html
79 https://www.bsigroup.com/en-GB/

Knowledge Exchange

As Japan sets out on its five-year plan to rapidly accelerate growth in its start-up ecosystem and in its desire to grow its domestic cyber security, the opportunity to share experiences from the UK is a strong one. The interactions with our Japanese counterparts during the mission suggest they are keen to learn about what we have done and how.

These mutual knowledge-sharing initiatives could form the basis for sustainable long-term collaborations and the genesis for strategic partnerships, regulatory harmonisation, collaboration in research and development, FDI from Japan to the UK and vice versa, leading to another springboard for the UK to develop wider opportunities in Asia through much closer ties with one of its leading economic powers.

Specific opportunities include:

- JVCA is keen to learn what the UK did in order to reach the sort of growth and dynamism it now has as one of the leading hubs for tech start-ups. JVCA members are keen to promote tried and tested policies to grow the start-up ecosystem and bring about the required cultural change to a more entrepreneurial mindset in Japanese communities.
- The Ministry of Education is interested in learning more from foreign programmes about entrepreneurship.
- J-AUTO ISAC could be a channel to raise awareness of DSbD among their members and encourage engagement via a working group.
- Exchanges between the UK and Japan that would support entrepreneurs from both countries spending time in each other's country to learn, understand and experience the business and innovation environment in the other country.

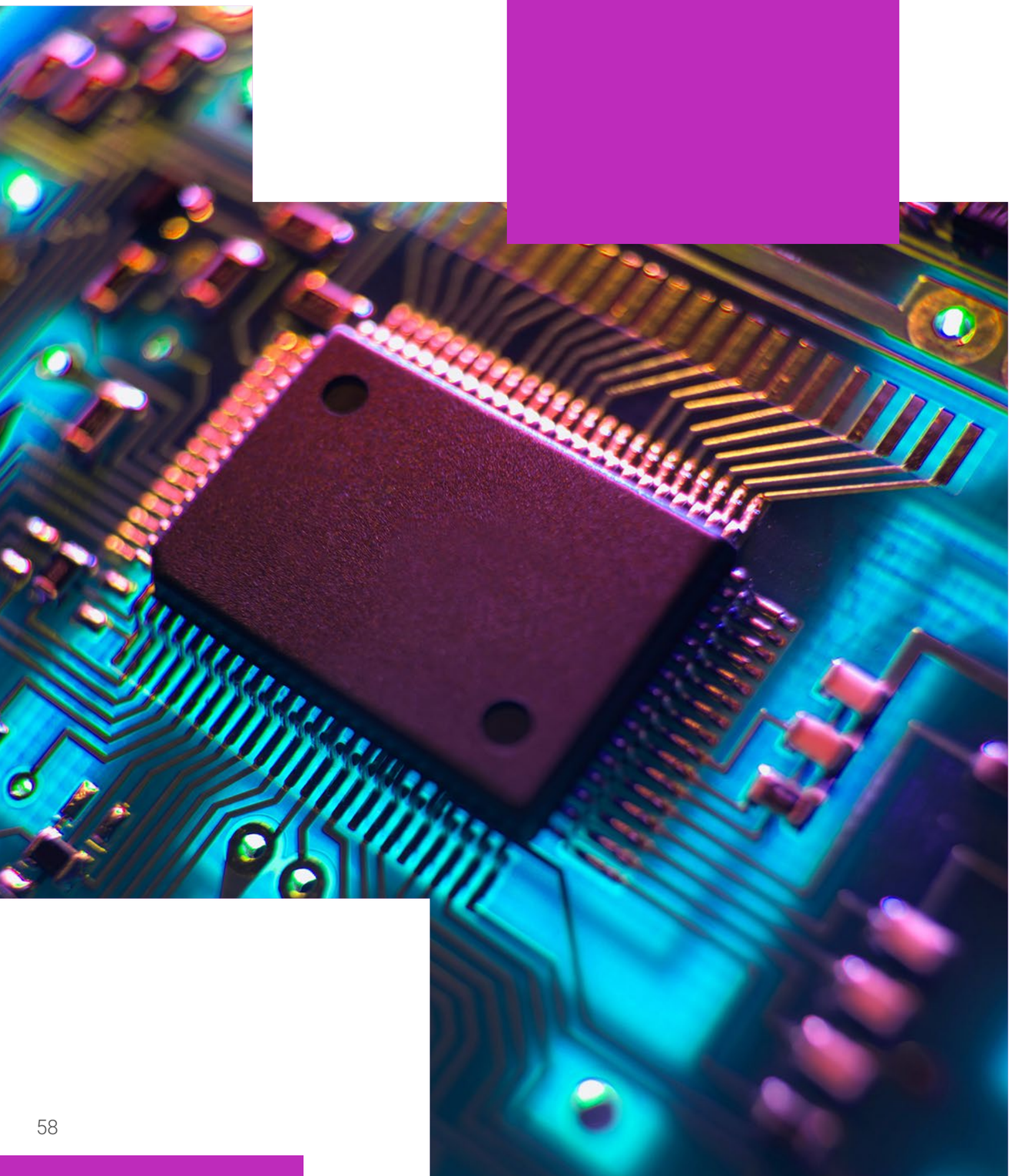
Collaborative Research and Development

Wider collaboration in research and development already goes on between the UK and Japan.

Formally this has occurred under the auspices of the SICORP programme from the Japan Science and Technology Agency (JST) and the International Collaboration programme from the Japan Society for the Promotion of Science (JSPS).

This has been bilateral between academics but to the best of our knowledge, these projects to date have not involved any activities in cyber security or even digital technologies more broadly. The projects supported under these programmes to date appear to be in areas around marine science and the medical sciences. The existence of these programmes however does mean that the mechanisms are already there for something formal in the area of cyber security.

Informal ad-hoc collaborations continue and evidence of that is in some of the joint publications from researchers at NICT and UK universities.



08. Conclusions

The Cyber Security ecosystem is evolving in Japan when compared to counterparts of esteemed status (e.g., USA, UK) and/or their neighbours in the region (Singapore, China, and Australia.) Japanese cyber security products and services do not have any significant market share in the global cyber security market and the domestic Japanese market has an increasing number of global and overseas companies which is threatening the market share held domestically by home-grown companies as well.

Digital Transformation and the vision of progressing towards Society 5.0 are both high priorities in Japan and the cyber security priorities are to a significant extent seen within that context.

The word ‘security’ carries baggage in Japan for historical reasons. There is a hesitance to talk about it. However, the Japanese government is beginning to change things with the advent of the National Security Strategy (NSS), National Defence Strategy (NDS), and Defence Build-up Program (DBP). The NSS is the principle for Japan’s national security strategy for the next 10 years, defining diplomatic and defence strategies in response to the new security environment.

Japan’s National Centre for Incident Readiness and Strategy for Cybersecurity (NISC) is the leading agency in the Central Government in forming the national cybersecurity strategy. Additionally, NISC guides all Central Government agencies in establishing and implementing cyber security policies and measures. NISC announced its National Strategy for Cyber Security 2019. The new strategy identifies an urgent need for reinforcing cybersecurity measures at all levels of Japanese society and in all aspects of technological development.

The still embryonic nature of the cyber security ecosystem and the clear indication from all the meetings and current policy positions indicates Japan is seeking to grow this ecosystem rapidly with an ambition to ‘become better than the West’. This presents the UK with a very strong opportunity to be successful in Japan from both a business and thought-leadership perspective. They are clear on their desire to learn from the UK’s success in cyber security whilst also working together in areas where there is a common strategic interest.

Japan has several agencies that are involved in funding and supporting research and development however NEDO is the one most closely comparable with Innovate UK. Mechanisms to support international collaboration with others already exist within the Japanese systems and some bilateral collaborations have occurred between the UK and Japan through those existing mechanisms.

Collaboration in cyber security research and development has primarily been much more informal between academia and research institutes between the two countries. The priority areas set out in the UK-Japan Digital Partnership provide a basis for future collaborative research and development and additionally, there is a strong interest in IoT security, supply chain security, security by design, IT-OT convergence and cyber resilience in the context of critical national infrastructure are all areas of interest and ongoing work.

METI has the equivalent responsibility for cyber security in Japan comparable to DSIT in the UK. METI has a substantive ongoing collaboration in this area with the US Department of Homeland Security and there is a desire to work with the UK in a similar way as well in areas of mutual interest. Harmonisation around regulation, standards and policy is the most likely context of any future collaboration between Japan and the UK at this level.

Industry associations like JAMA, large multinationals like Toshiba and NEC and sectoral ISACs all demonstrated that cyber security is a high priority within the private sector, and from an internal point of view, progress has been made to improve the corporate cyber security posture. The private sector is particularly open in sharing their challenges and approaches, and two (Toshiba and NEC) demonstrated real excellence in their coverage.

Operational Technologies and their impacts on CNI were a common focus theme, including the tension between OT and IT appetites for applying cybersecurity.

There are opportunities for the UK in Japan.

They can be largely set out within two categories – soft power and direct collaboration opportunities addressing an identified challenge in the private sector or through joint-funded programmes addressing strategic challenges held by both countries (preferably where there is an identified challenge owner in both countries which makes participation from innovators much more likely).

Soft power can come in the form of collaboration on policy, regulatory harmonisation, promoting standards and values, knowledge exchange and assisting with academic-industrial partnership methodologies.

The UK is a world leader in research within cyber security and the final observation would be that there is a significant opportunity to feed the results and findings from that research alongside the lessons learnt in the UK as it has grown its cyber security capability into future dialogue with stakeholders in Japan as they progress towards growing their research base and domestic capability. By doing this the UK will be able to strengthen ties, open up opportunities in the region and have long-term influence.

09. Annex 1: List of UK Participants

Department for Science Innovation and Technology (DSIT), UK Government

Assentian

PETRAS National Centre of Excellence

Internet of Things Security Foundation (IoTSF)

Siemens EDA

British Telecom (BT)

CONTACT
Veronika Barankova
Global Alliance
Innovate UK KTN
veronika.barankova@iuk.ktn-uk.org

Innovate UK drives productivity and economic growth by supporting businesses to develop and realise the potential of new ideas.

We connect businesses to the partners, customers and investors that can help them turn ideas into commercially successful products and services and business growth.

We fund business and research collaborations to accelerate innovation and drive business investment into R&D. Our support is available to businesses across all economic sectors, value chains and UK regions.

Innovate UK is part of UK Research and Innovation.

For more information visit ukri.org/councils/innovate-uk/

Follow us

Telephone: 01793 361000
Email: support@iuk.ukri.org
ukri.org/councils/innovate-uk/