plexal on behalf of Department for Science, Innovation, & Technology

SECURE CONNECTED PLACES

International Evidence Project

March 2023

A review of global policies and approaches to minimise cyber security risks in connected places

EXECUTIVE SUMMARY

Central and regional governments across the globe use a range of approaches to ensure the cyber security of their connected places (also known as smart cities). However, due to varying levels of advice, experiences and capabilities associated with specific countries, there is no standout best practice at present.

Policy to support the cyber security of connected places and smart cities (referred to in this document as secure connected places) is a new and developing field. This is evidenced by the emerging government cyber security and connected places initiatives, which highlight the need to protect connected technologies (for example, Internet-of-Things (IoT), Operational Technology (OT) and cloud) that are deployed in a place-based context. For these emerging initiatives to be successful they must be cohesive - ideally grounded in a guiding national strategy - and address a complex ecosystem of stakeholders (for example, local and national governments, citizens, technology providers and organisations).

Best practice will likely develop in the coming years, as international expertise continues to grow and countries increasingly realise the importance of cyber security to facilitate safe, efficient and secure connected places. Nevertheless, it is important to recognise that the local circumstances of connected places will mandate the need for bespoke regional cyber strategies. There is no one-size-fits-all approach.

Developed by Plexal on behalf of the Department for Science, Innovation and Technology (DSIT), this review aims to highlight the distinct approaches that countries are taking globally to mitigate cyber security risks of their connected places and promote the secure adoption of connected technologies. The review analyses a snapshot of regional, national and international initiatives in the form of policy, strategic documentation, guidelines for implementation, technical advice and international standards. Its findings will inform UK policy and further the understanding of international best practice on connected places cyber security.

National approaches

National strategies and frameworks for the cyber security of connected places represent the best practice in mitigating the cyber risks that connected technologies pose, as they take a whole-systems approach and provide a useful baseline from which further initiatives can be built. Many countries have developed a separate national cyber strategy and national

connected places strategy, demonstrating expertise and intent in both areas without a combined strategy. The review identifies the importance of a holistic approach at the national level, citing the example of Germany's Federal Office for Information Security (BSI) which has connected places cyber security guidance, regional engagement and a funding program. Further to national strategies, this review identifies a prominence of national guidance and regulation for IoT in relation to connected places. However, technology-specific guidance and regulation alone may lead to a piecemeal rather than systems approach to mitigating the cyber risks of connected places. Finally, at the time of writing, there is an identified gap in the literature regarding how new connected places deploying cutting-edge technology are being secured.

Regional approaches

While important, national frameworks are not enough to ensure the cyber security of connected places and more tailored, nuanced guidance is required to consider the specificity of each region. This review highlights the importance of place-based initiatives and regional funding. We cite the United States of America (herein the US) as a case study, who combines regional SuperClusters, with national initiatives from the National Institute of Standards and Technology (NIST) and Cybersecurity and Infrastructure Security Agency (CISA). Additionally, we also highlight Australia and Brussels as regions taking the lead to secure their local connected places. However, both top-down (US) and bottom-up (Brussels) regional initiatives need a national framework to build from. Finally, the review underscores the importance of collaboration and sharing of learnings between regions to further understanding and best practice.

International approaches

Another identified approach is the international collaboration between nations in the form of policy meetings and joint statements of cooperation. The Association of Southeast Asian Nations (ASEAN) region is cited as an area of expertise, with collaboration between member states Japan and Australia on frameworks, standards and best practice for the cyber security of their connected places. While there is no international set method for the cyber security of connected places, it is identified that the required expertise already exists in the form of international standards and international cyber security strategies.

It's clear that regional, national and international collaboration on shared learnings and expertise is the way forward for secure connected places and that future connected places currently in development have the potential to shine as examples with robust, built-in cyber security.

CONTENTS

1. INTRODUCTION

1. INTRODUCTION

1.1 Research objectives and scope

The UK National Cyber Strategy 2022 [1] outlined the UK Government's objective for to be at the forefront of the secure and sustainable adoption of connected places technology. The Department for Science, Innovation and Technology's (DSIT) work contributes to this aim by delivering policy that supports the cyber security of the UK's connected places. To do so, DSIT's Secure Connected Places team works closely with managers of connected places projects and suppliers of connected places technologies to ensure that communities across the UK can enjoy the benefits of secure connected places.

> This work has been carried out by Plexal on behalf of the Secure Connected Places team at DSIT. The Secure Connected Places team commissioned Plexal to catalogue the different approaches that countries are taking to mitigate the cyber security risks of their connected places (also known as smart cities). These initiatives could take many forms, be it policy, strategic documentation, guidelines for implementation, technical advice, or international standards. The findings of this work are intended to inform UK policy and further the understanding of international best practice to promote the secure adoption of connected places.

It is important to note that this review does not seek to evaluate or rank practices from different countries, nor is it intended as a comparison of that activity to what is undertaken currently in the UK. This research is also not a meta-analysis of international connected places literature in its entirety. Instead, it serves to highlight where interesting initiatives are being delivered in other countries to raise awareness of different approaches and share learnings.

1.2 Research methodology

Plexal has undertaken this research to understand what approaches are being taken by other countries in their efforts to secure connected places. A three-step process was used:

I. A prioritisation exercise was carried out to set the geographical scope of the research. This exercise selected several countries for inclusion in the research based on indicators or unique approaches that can be catalogued.

II. A literature review of government publications on the cyber security of connected places in the selected countries, looking at guidance and standards that have been produced, as well as academic and industry research into their approaches.

III. Creation of this findings report to summarise key findings and facilitate the international sharing of best practice in secure connected places.

A detailed description of our research methodology and its rationale is in the appendix.

1.3 Definition of terms

What is a connected place?

A connected place is defined by the UK's National Cyber Security Centre (NCSC) in the UK as:

> "A community that integrates information and communication technologies and Internet of Things (IoT) devices to collected and analyse data to deliver new services to the built environment and enhance the quality of living for citizens."[2]

Connected places use a range of technologies, both hardware and software, to collect real-time data to help improve the operation and maintenance of services and assets. Typically, the items being monitored cover areas in transportation, buildings, utilities, environment, infrastructure and other public and private services.

Many countries have carried out large deployments of connected places technology to drive benefits for the citizens who live and work in their regions. Some examples include environmental projects, progressive plans for development, citizens' abilities to live, work and use resources and services in a city, as well as an infrastructure based on technology.

Networks of IoT devices are the technology type most associated with connected places, as these are the data gathering devices which connected systems are built from. These devices could be used as sensors to monitor traffic levels, in quality measuring for clean air walking routes, or as units to support autonomous connected vehicles. However, IoT represents only a portion of technology that makes up a connected place.

> Connected places will use a digital or cyber-physical system of sensors, networks and applications to collect data that allows the improvement of operations and services, spanning several technology areas such as:
>
> - IoT devices such as sensors and actuators, in a place-based context.
> - Networks for data transmission including wireless (for example, Wi-Fi, Bluetooth, satellite), cellular (for example, 4G, NB-IoT, 5G), LPWAN (for example, LoRa-WAN, Sigfox) and wired (for example, fibre, ethernet).
> - Data aggregation for visualisation and insight.
> - Cloud computing and storage for the processing and storage of data collected from sensors and actuators.
> - Whole stack solutions (for example, across all the technologies involved in the delivery of connected places).
>
> These elements connect systems, hardware and data to facilitate interoperability and usability for the authorities or agencies who use connected places to improve services.

What is cyber security?

An extremely important, and sometimes overlooked, element of connected places is the security system. In the context of connected places, cyber security is what makes connected places a safe place to live and work. The NCSC defines cyber security as:

> "Cyber security is how individuals and organisations reduce the risk of cyber-attack. [...] Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it is difficult to imagine how we would function without them. From online banking and shopping, to email and social media, it is more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data and devices."[3]

What do we mean by secure connected places?

Throughout this report, we refer to the concept of secure connected places as the area of policy that seeks to mitigate the cyber risks of connected places and promote the secure adoption of connected technologies. It is noted that this is specifically used in UK policy, rather than globally.

Connected places cyber security threats

Having the right cyber security protocols, governance, software and hardware to protect, monitor and control the transmission of data across connected places is critical to prevent breaches, secure sensitive information and ensure the provision of services.

Connected places can be attractive targets to malicious actors due to the amount of data they process and the fact that an attack on this infrastructure could have a significant impact. As a connected place grows, and as we become more reliant on this connectedness, this risk increases. Examples of the risks include:

- A traffic light prioritisation system: if it did not authenticate emergency vehicles, it would be open to anyone changing traffic signals to green, risking lives and damage to vehicles.
- In-home health monitoring: this could be abused for criminal and commercial gain as an attacker could target victims based on their activity patterns. Protecting individuals' privacy is vital, particularly where such sensitive personal information is involved.
- Electric vehicle chargers: an attacker could sequence all chargers in the network to draw a large current simultaneously, causing a drop in voltage in an electrical power supply system.

It is also important to remember that as data collection becomes more pervasive, the right to individual privacy needs to be protected. With such widespread data collection and correlation, seemingly anonymous datasets can be aggregated and could identify individuals.

Why does the UK use the term connected places instead of 'smart cities'?

A common term for connected places globally is 'smart cities'. In many cases, the types of connected technologies which are deployed into a public environment tend to be done initially inside large urban areas. However, it is important to note that connected places technology is extremely versatile and can also be hugely beneficial in non-city environments, for example,

temperature and moisture monitoring in cliff walls to detect risks of landslides. Therefore, the UK government uses the term connected places to capture the broad range of environments and use cases that connected technology can be used in. However, smart cities are referred to throughout this document when representing the projects and initiatives from across the world that do use this term.

1.4 Report structure

The report is divided into several sections consisting of an introduction, global maturity and country prioritisation activity followed by a breakdown of national, regional and international findings. The document concludes with a summary of findings and recommendations for further research. The report is supported by an appendix with additional detail on the research design.

- Section 2. Global maturity details the findings from our country prioritisation exercise which intends to understand the maturity of connected places cyber security activity globally.
- Section 3. National approaches details initiatives localised to specific counties, sectors, or areas within the borders of a single country.
- Section 4. Regional approaches details government initiatives that address a county regardless of regional separations, but do not involve out of country stakeholders.
- Section 5. International approaches details initiatives that encapsulate multiples countries within its scope, either as stakeholders or beneficiaries, recognised by or published by international organisations, or may be an initiative by a country to develop an internationally recognised piece of literature related to secure connected places.

Spotlight case studies

The review also features four spotlight case studies that identify key examples of best practice or interesting initiatives. It should be noted that each spotlight case study is not the total of everything that a regional, national or international initiative achieves, nor does it represent the total population of all initiatives:

- Spotlight 1: Germany's Federal Office for Information Security (BSI)
- Spotlight 2: The UAE's Smart Dubai initiatives
- Spotlight 3: USA Super Clusters for regional engagement
- Spotlight 4: International collaboration in the ASEAN region

Report key:

Throughout the report, the spotlight case studies are shown in boxes like this.

Country-specific examples about sources, policies, guidance, frameworks and standards are shown in boxes like this.

And key findings are summarised in boxes like this.

2. GLOBAL MATURITY

2. GLOBAL MATURITY

2.1 Global connected places activity and cyber security maturity

> To identify countries with high connected places cyber security maturity, two global indices were used to establish a snapshot of global secure connected places maturity, correlating the findings from the National Cyber Security Index (NCSI) [4] and the Smart City Index (SCI) [5], which are presented as heatmaps in figures 1 – 4.

In this context, a country's maturity refers to how well it can implement and deliver a cyber security strategy to support and reduce risks in connected places. As cyber security for connected places should encapsulate the smart and secure implementation of connected places technologies, it was hypothesised that comparing cyber security and 'smart city' maturity would most likely find areas of best practice and dedicated initiatives. Further details and limitations of this methodology can be found in the appendix.

Figure 1: Heatmap of NCSI rank per country. Each country within the NCSI is ranked from a pool of 161 countries, considering the countries' general cyber security indicators, baseline cyber security indicators and incident and crisis management indicators. Only countries with an associated smart city within the SCI have been included; lighter colours indicate a lower NCSI rank; darker colours indicate a higher NCSI rank.

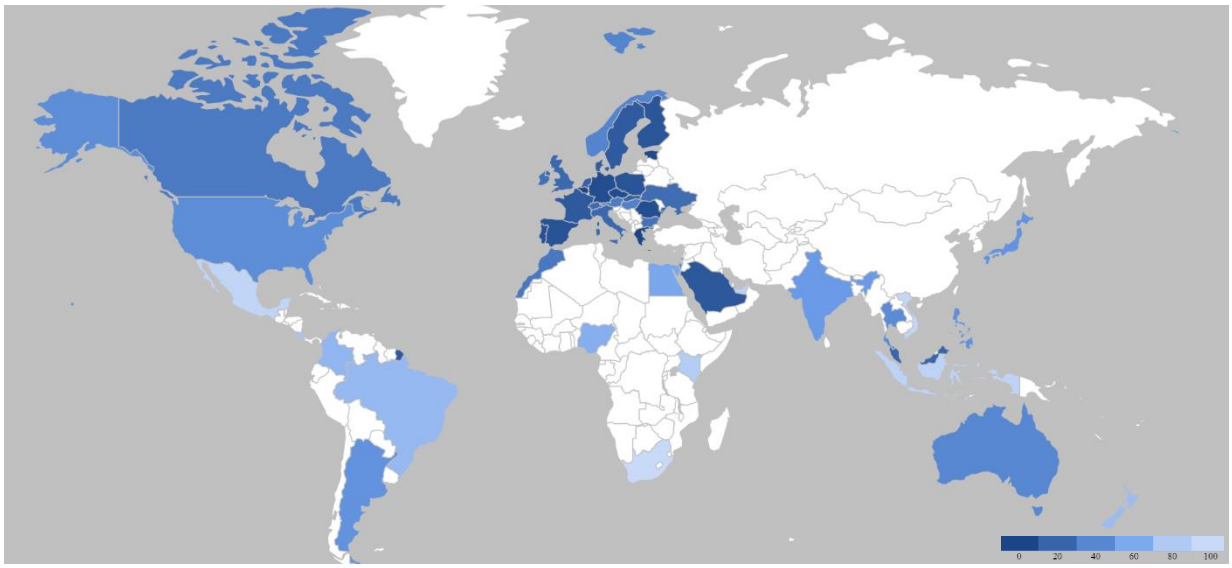


Figure 2: Heatmap of average SCI 2021 rank per country. Each country within the SCI is ranked from a pool of 118 countries, considering a specific smart city's utilisation of structure and technologies. Countries with multiple smart cities have had their SCI averaged; lighter colours indicate a lower average SCI rank; darker colours indicate a higher average SCI rank.

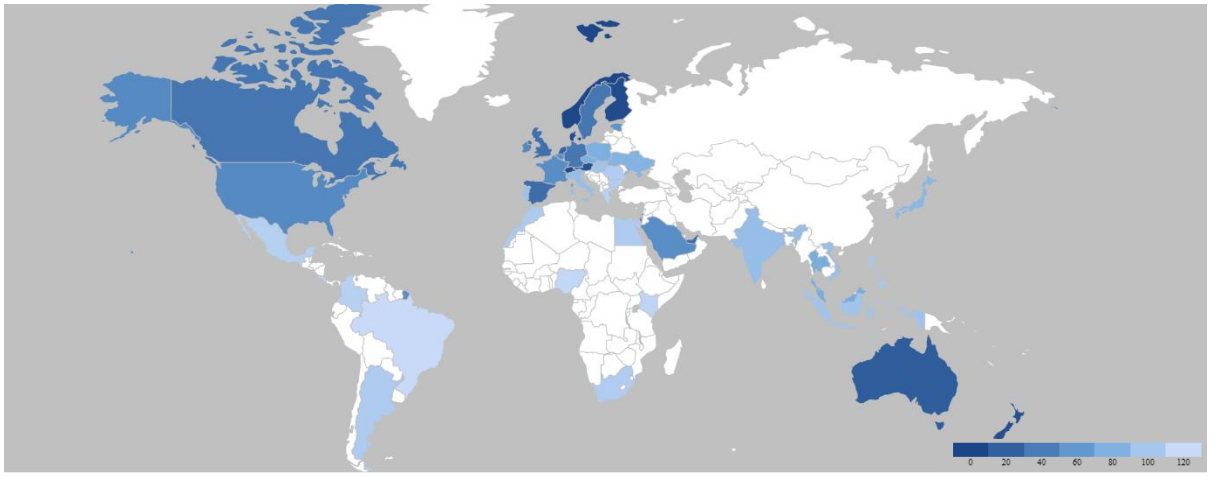


Figure 3: Heatmap of the difference between a country's security maturity versus its technology maturity. The value is generated by the country's NCSI score minus its Digital Development Level; lighter colours indicate a greater Digital Development Level to the NCSI score; darker colours indicate a greater NCSI score to the Digital Development Level. Only counties with an associated smart city within the SCI have been included.

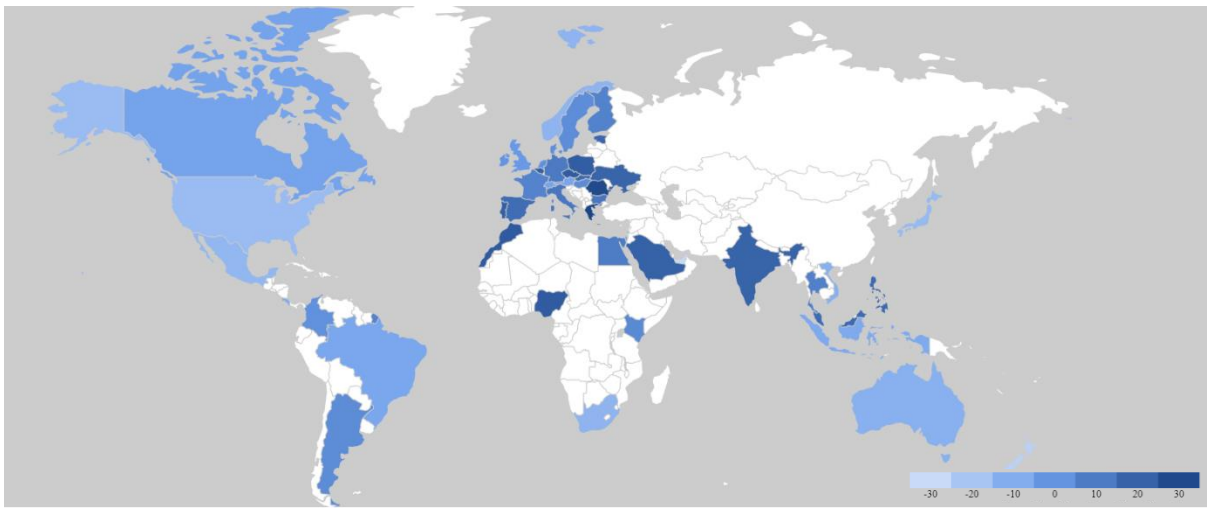
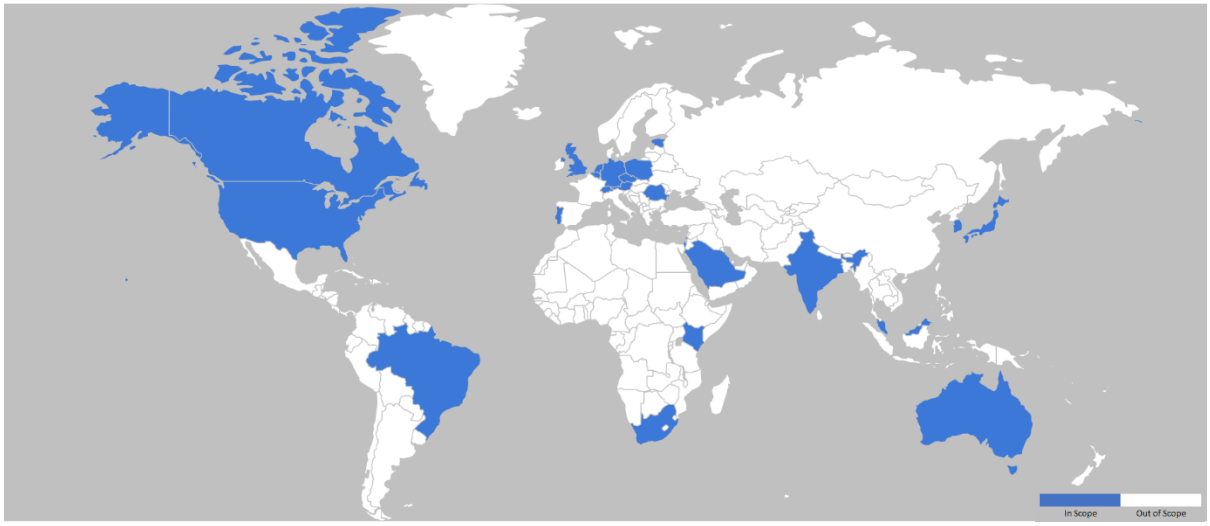


Figure 4: Depiction of countries based on the shortlisting methodology. The countries identified provide a sample from each continent. All shortlisted countries have a medium-high SCI and NCSI and are mixed representation from countries with high and low security maturity versus connected places technology maturity; blue countries indicate they are in scope; white countries indicate they are out of scope.



2.2 The UK's approach to cyber security for connected places

The UK has implemented several initiatives and protections under a broad government National Cyber Strategy [1]. The UK government has a dedicated part of its website which collates guidance for secure connected places. This includes documents on the foundations of security in smart cities technology, resilience-in-design, designing architecture, administration and data storage.

To complement the National Cyber Strategy, the UK government has also undertaken a connected places survey [6] and has developed strategies and a deeper understanding of cyber security skills within the UK. This guidance has been developed by a range of organisations and is drawn together by DSIT. It is intended to help buyers and operators of connected places technology to have greater confidence in the security and resilience of their connected places technologies and the information that those solutions generate.

The NCSC provides a single point of contact for SMEs, larger organisations, government agencies, the general public and departments for cyber security. The NCSC is responsible for understanding cyber security and distilling this knowledge into practical guidance that is made available to all. They also respond to cyber security incidents to reduce the harm caused to organisations and the UK at large. They have released several programmes, documents and guidelines including the Cyber Assessment Framework (CAF) [7] and the government-backed Cyber Essentials [8] accreditation for organisations who have taken the necessary steps to protect themselves from cyber-attacks. They have also created the Connected Places Cyber Security Principles [9] to promote the 'secure design, build and management of public realm technology, infrastructure and data-rich environments for local authorities'. The Principles cover several elements of connected places security, from engaging with stakeholders,

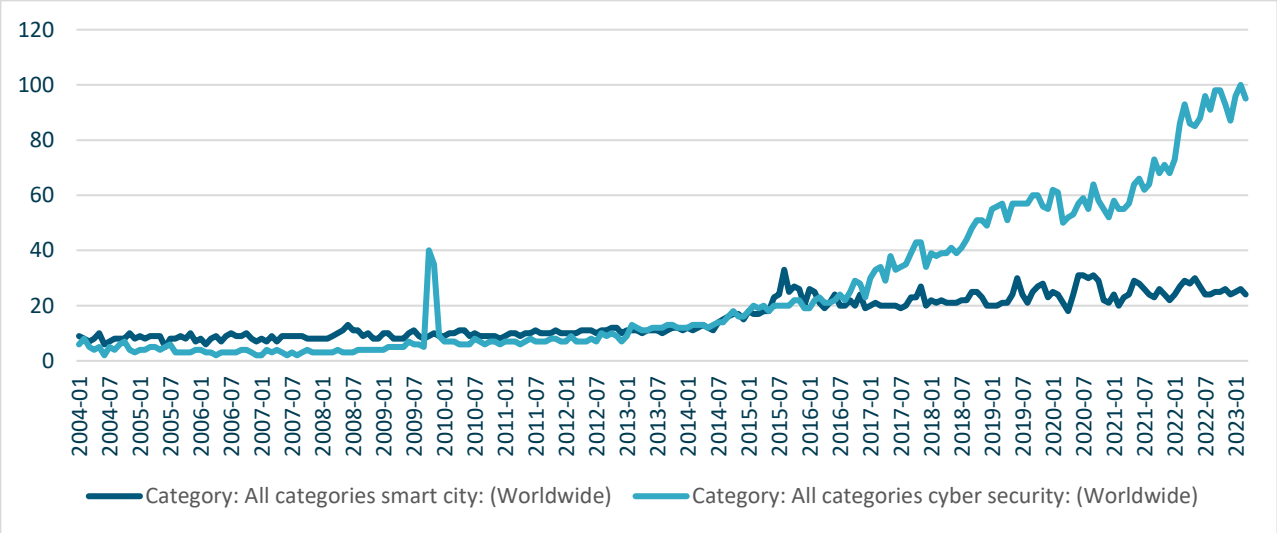
procuring technology and security within system design. DSIT has also published the Secure Connected Places Playbook - a suite of cyber security resources to support local authorities with the secure design, procurement and management of connected places projects. Together, the guidance and support aim to ensure that the UK is at the forefront of the secure and sustainable deployment of connected places projects.

2.3 Secure connected places policies over time

The concept of 'smart cities' is not a new one, however, until recently the conversation was predominantly focussed on the function of connected places, rather than their security. As society has become increasingly digitised and reliant on connected technology, the importance of cyber security has increased. Countries now need to consider how policy, guidance, regulation and standardisation can be used to prevent and mitigate connected places cyber-attacks that could impact critical services and put important data at risk.

While there are some examples of connected places documents that mention data security from over 10 years ago, such as the City of Vienna's 2013 'Smart City Wien - Framework Strategy' [10], most of the literature referenced in this review is from the year 2016 onwards. The average year for publication across all sources is 2019 and the most common year for publication is 2021. This distribution demonstrates that the cyber security of connected places is a new and emerging policy field.

Figure 5: Google Trends graph depicting mentions of the words 'cyber security' and 'smart cities' over time. Shows the rise in popularity of cyber security relative to 'smart cities' explaining the proliferation in secure connected places literature post-2016. The vertical axis represents search interest relative to the highest point on the chart for the given region and time. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. A score of 0 means there was not enough data for this term.



3. NATIONAL APPROACHES

3. NATIONAL APPROACHES

3.1 Summary

In recent years countries across the globe have recognised, and are taking concerted steps to mitigate, the cyber security risks posed by their connected places at a national level. There is no set model for securing connected places and countries are taking their approach by implementing methods to different extents. Here, we detail and categorise the approaches that central and state governments have taken to secure their connected places:

- Section 3.2: Technology-specific policy where a country has taken steps to legislate or provide guidance for a particular horizontal such as networks, data aggregation, or cloud.
- Section 3.3: Privacy and data sharing policy where a country has primarily focused on the security of data generated, stored and managed by connected places devices.
- Section 3.4: Development of new smart cities and connected places where a country has embedded cyber security into the development of a new city or region from the outset.
- Section 3.5: Separate cyber security and connected places strategies where a country references connected places and cyber security in separate documents.
- Section 3.6: National connected places cyber security strategies and frameworks where a country has directly set out their approach to secure connected places management with a dedicated strategy, framework, or principles.
- Section 3.7: Holistic national approaches to secure connected places where a country has combined many of the above measures.

Key findings:

- National connected places cyber security strategies that take a whole-systems approach to minimise cyber risks can be seen as best practice and demonstrate a country's clear intention to promote the secure adoption of connected places technologies.
- Many countries have published separate cyber security and connected places strategies, however, are yet to join the dots to publish a connected places cyber security strategy.
- These national connected places cyber security strategies range from high-level guidance and principles to specific technological approaches of a wide connected places system.
- Some countries have taken a technology-specific approach to securing connected technologies, of which IoT tends to be the focus. While national cyber authorities across the globe do also produce cyber security guidance on other connected technologies, such as cloud and networks for communication, these rarely pay reference to connected places.
- Regulations relating to connected technologies represent an attempt by national governments to enforce minimum security standards on the suppliers and manufacturers of connected technologies.

- In the absence of a specific connected places cyber security strategy, technology-specific guidance and regulations may suggest a piecemeal rather than systems approach to securing connected places.
- There is limited published evidence that new cities and places, which are currently under development and deploying state of the art connected technologies, are developing novel privacy- and secure-by-design principles. This gap in the literature is likely because the development of new cities and places, and the technologies deployed in them, are predominantly driven by industry, who are not subject to the same expectations as the government to publish their cyber security frameworks and mitigation strategies.
- Privacy is a key consideration in connected places as they generate large amounts of sensitive data. Data privacy tends to be a particular focus for European countries that recognise the importance of citizen acceptance in the adoption of secure connected places. New connected places do have a good secure-by-design mindset such as in Saudi Arabia.

3.2 Technology-specific policy

Connected places will use a digital or cyber-physical system of sensors, networks and applications to collect data that allows the improvement of operations and services, spanning several technology areas such as IoT, networks for data transmission, cloud computing and storage. Many countries have identified the risks that connected technologies pose and have taken steps, usually through their national cyber authority or equivalent, to produce guidance and regulation that is technology specific.

These technology-specific policies demonstrate countries' efforts to regulate connected technologies and disseminate information about how to mitigate their risks. However, in the absence of a specific connected places cyber security strategy, they may suggest a piecemeal rather than systems approach to securing connected places.

A global focus on IoT

As mentioned in the introduction, IoT tends to be the main technology focus of connected places cyber security attempts and this is mirrored here, where the examples of connected places technology-specific guidance and regulation focus primarily on IoT devices and networks. From our research, it was found that guidance and regulation focussed on IoT was most directly aligned with the connected places use cases, in comparison to cloud-specific cyber security guidance where use cases relating to connected places or 'smart cites' were rarely mentioned.

It is apparent that countries' early efforts to mitigate connected places cyber risks largely focus on IoT technologies. There are several other technology areas which apply to connected places (such as cloud security, network security, data management and operational technologies), however, we were unable to find mentions of connected places use cases in guidance relating specifically to these technologies.

The Netherlands' National Cyber Security Centre published a factsheet of recommendations for securely purchasing cloud services in 2020 [11]**.** While most of the guidance is relevant for private and government organisations who might be procuring cloud solutions for connected places use cases, the association with connected places has not been made.

Also published in 2020, the **US Federal Trade Commission's 'Six steps toward more secure cloud computing'** [12] includes relevant cloud cyber security advice for businesses, such as encrypting rarely used data, however, there is no mention of specific use cases for cloud computing or relevance to integration with other connected places technologies.

Technology-specific guidance

The below examples of connected places technology-specific guidance have been produced by national cyber authorities and demonstrate the varying levels of specificity and technicality present in the wider body of literature. This guidance recommends best practice and highlights key considerations but does not mandate compliance or enforce regulation.

Switzerland's National Cyber Security Centre has published a page of IoT guidance on its information pages [13]**.** The guidance outlines preventive, cyber secure measures that can be taken when purchasing, setting up and maintaining IoT devices. It also lists steps to take after a successful IoT attack has taken place. The Swiss NCSC has intended this guidance to be a high-level summary for non-specialist audiences (such as organisations, local authorities and generalist IT staff) and the article's language and length are reflective of this. This short piece of content is an example of an attempt to educate and increase understanding of the cyber security risks that IoT devices pose. Another example is the **Security of IoT devices page on the Kenya National Cyber Command Centre's website** [14] which details basic information on the risks of malware that can compromise IoT devices.

Some countries have taken a more specific approach, with security guidance for specific types of IoT devices. For example, **Israel's National Cyber Directorate's 2018 publication on best practice for reducing cyber security risks in video surveillance cameras** [15], sets out guidelines for manufacturers, installers and end-users to reduce cyber risks with a step-by-step process from procurement and installation to maintenance.

Technology-specific regulation

While guidance is necessary, it can be difficult to ensure uptake. Therefore, some countries have turned to regulation to ensure minimum security standards are met. National regulation policies in the IoT and wider connected technology space largely draw upon, and mandate adherence to, international standards (see Section 5 for further information).

The United Arab Emirates' (UAE) Telecommunications Regulatory Authority (TRA) published an IoT framework comprising regulatory policy and procedures [16]. The framework mandates that IoT devices must comply with relevant international standards and secure communication protocols, as well as setting out guidelines for IoT device manufacturers, network providers and services providers. Rather than IoT devices alone, the policy regulates the provision of 'IoT Services.' Therefore, all providers of IoT devices, functions and facilities in the UAE are required to register for a TRA Service Registrate Certificate to allow them to operate in the country. A comprehensive summary of the TRA's IoT framework can be found in source 16 [17].

A similar, example is the **Internet of Things IoT Framework in the Arab Republic of Egypt** [18] published in January 2022 by the national telecoms regulatory authority. The framework requires IoT device certification for providers to obtain licences. It also addresses networks for data transmission, by requiring licences for organisations to operate connected places networks such as LPWAN, which is a step beyond the IoT devices alone.

While national level guidance is predominantly focused on increasing education and sharing best practice amongst local governance, policy makers, the public and organisations that are procuring connected technology, regulation is used to ensure and enforce a minimum level of standard is upheld by organisations that provide connected technologies.

In some cases, countries have addressed guidance, principles and regulation measures for connected technologies in one document.

The 2020 'Roadmap for Digital Hand-and Soft-ware Security' [19]**, published by the Netherlands Ministry of Economic Affairs and Climate Policy Ministry of Justice and Security,** takes this approach. The roadmap for 'interconnected devices' outlines 'a set of measures for eliminating security gaps in hard- and software, detecting vulnerabilities and mitigating their consequences.' The measures, which span standards and certification to monitoring and statutory requirements, take a whole-lifecycle approach from design to end-of-life for IoT products. However, the document only discusses the actions that the Netherlands is taking towards setting statutory requirements, supervision and enforcement ('investigating which minimal security requirements can be made applicable to devices under the European Radio Equipment Directive' or 'organising a national dialogue session for regulators and supervisory authorities to explore their role in promoting digitally secure hard- and software') rather than setting out new regulations. Uniquely, this roadmap also mentions the balancing of public values and the suppliers, and a joint responsibility model between users, government and technology providers, which reinforces our findings that European countries place particular emphasis on citizen privacy and acceptance of connected technologies.

3.3 Privacy and data sharing policy

Data privacy is a key consideration in connected places as they generate large amounts of data that are often aggregated into large datasets. When aggregated, previously benign datasets can quickly become personally identifiable, therefore stringent data processing and storage processes are needed. It is recognised that this is especially important to gain citizen trust and acceptance towards connected places so that the technology can be successfully deployed for public benefit [20].

Connected places technologies can collect highly sensitive or personal data, such as movement in citizens' homes to assist with the care of vulnerable people, or CCTV to assist with crowd management and smart policing. While international bodies such as the European Data Protection Board (EDPB) are taking steps to regulate these sensitive areas of data collection (such as facial recognition technology) and protect personal privacy [21], countries are also implementing additional measures.

> **The German Federal Office for Information Security (BSI) has produced an 'Assessment Template'** [22] **to ensure that consumer IoT devices meet baseline security requirements** and conform to European Standards such as ETSI EN 303 645. Undergoing the assessment allows the device to gain a BSI certified security label. This policy is focussed on protecting personal privacy in the use of consumer IoT and mentions devices such as smart watches and smart washing machines.
>
> **The US has also considered the implications of connected places on privacy. In 2019, the Cybersecurity and Privacy Advisory Committee (CPAC)** – a public-private group of experts and stakeholders that advise the US Department of Commerce – published a guidebook on 'A Risk Management Approach to Smart City Cybersecurity and Privacy' [23]. Building upon the NIST Risk Management Framework, the guidebook outlines key considerations for decision makers at the municipal and community level as well as detailing privacy-focussed use cases from real-world examples.

Despite European and North American focus on data privacy, there are other instances where consent on data regulations have been relaxed to enhance the provision of services through connected places technologies.

> **Republic of Korea's Act on The Promotion of Smart City Development and Industry** [24] states in Article 37 that certain personal information acts shall not apply to the implementers and service providers for national pilot smart cities if personal information collected is used after being anonymised. This relaxation of data privacy acts specifically in national smart city pilot projects and serves to promote the experimentation and uptake of connected technologies in a sandbox environment.

3.4 Development of new smart cities and connected places

Across the globe, countries are building new spaces and environments with state-of-the-art connected technologies at their core. In these instances, it is important the cyber security is

considered at the outset and that the connected places use secure- and privacy-by-design principles to mitigate risks.

Connected places or 'smart cities' are frequently addressed in countries' digital strategies or digital visions for the future. This is common in the Middle East, where cyber security is seen as a key growth area in the diversification away from a fossil-fuel-centric economy.

> Saudi Arabia's Vision 2030 [25] sets out the country's digitisation agenda to improve infrastructure, IT and OT systems, artificial intelligence and 4th industrial revolution transformations. To support this agenda, the **Saudi National Cyber Security Authority published the 'Critical Systems Cybersecurity Controls' in 2019** [26] which details four controls: cyber security governance, cyber security defence, cyber security resilience and third-party cloud computing cyber security. The controls demonstrate Saudi Arabia's intent to set minimum cyber security requirements for critical systems. The document states that the controls were 'developed after conducting a comprehensive study of multiple national and international cybersecurity frameworks and standards, studying related national decisions, law and regulatory requirements, reviewing and leveraging cybersecurity best practice, analysing previous cybersecurity incidents and attacks on government and other critical organizations, and conducting public consultations.'

However, cyber security literature directly relating to new connected places that are currently in development, such as Saudi Arabia's NEOM project and Egypt's New Administrative Capital, is limited. Two examples from the Republic of Korea and Indonesia are listed below.

> **Republic of Korea's National Smart City projects has been developing new smart cities, with technology intrinsically part of the design of the city for many years**. They started with two pilot cities, Sejong and Busan. These were intended to be a test bed for high technologies such as AI, 5G, blockchain, autonomous vehicles and a convergence of industry, academia, smart city operations and an ecosystem for SMEs. Using private developers for each, areas of the existing city were marked out for fresh development of housing, retail and business space, with technology built as part of core public services. Sejong adopted the 'Internet of Everything' [27] principle, building cyber-physical systems that could collect, store and use data between online and offline, driving better digital healthcare, environmental protection and governance. On the other hand, Busan is being designed as an eco-smart city, with new waterways and specialist landscaping, which require innovative connected technology to sustainably filter the water. For both initiatives, cyber security was embedded into the core proposition from the start, largely due to the high amount of data that would be generated and shared by the connected assets going into these developments. The baseline for new deployments would be a solid cyber security platform in all shared ICT resources.
>
> **Another example of developing a technology-based new city is in Indonesia, where the government is moving the capital 2000km east from Jakarta to Nusantara.** They intend to develop a green city, with 70% of the land designated as green areas to ensure environmental sustainability. As part of this, new technology will be applied to make it a smart city, tying into Indonesia's 100 Smart Cities initiative [28]. There is no master plan

for information security in the new capital yet, but there are 3 principles that the government has put in place, which focus on security for critical infrastructure and liveability for citizens [29]. In practice, this means that the government is focusing on data privacy and information security and ensures compliance with the ISO 270001:2022 standard. What is unusual in the development of Nusantara is that Indonesia's National Resilience Institute, responding to global geopolitical activity, has urged the central government to develop a city-wide cyber defensive system, believing that any attack on the new capital would begin with cyber threats and involve new technologies.

Generally, despite substantial government involvement, the development of new cities and places, and the technologies deployed in them, are predominantly driven by industry. As industry is not subject to the same expectations as government to publish their cyber security frameworks and mitigation strategies, there is a notable gap in the literature on how these new connected places are being secured. This will require further research, likely using an alternative method such as engagement and interviews with key industry stakeholders.

3.5 Separate cyber security and connected places strategies

As connected places depend more frequently on advanced technologies, the need for robust cyber security measures has become more pressing. Both connected places strategies and cyber security strategies have been developed internationally, which has led many city planners and policymakers to consider the integration of cyber security strategies into their connected places strategies at a national level. However, some examples exist where national connected places and cyber security strategies exist separately. This section will provide some examples of separate connected places and cyber security strategies and guidance. It is important to note that an absence of literature does not necessarily reflect a lack of a joined-up approach, nor does it indicate that such literature may not have been produced, but rather that it may not be publicly available.

Austria highlights the importance of a comprehensive, integrated, and proactive approach to cyber security policy within its Cyber Security Strategy [30]**.** The strategy outlines goals such as guaranteeing the availability, reliability and confidentiality of data exchange, protecting the legal asset of "cyber security," and building a "culture of cyber security" through awareness measures. Austria has also published the Smart City Wien framework strategy [10], which aims to preserve and evolve Vienna as a socially inclusive and environmentally sustainable city while maintaining its high quality of life. The strategy targets all stakeholders, including citizens, enterprises, non-profit organisations and the public sector. Austria presents a mature connected places and cyber security posture based primarily on published strategy policy documents; however, a public connected places cyber security strategy was not identified as part of this research.

Within the Czech Republic, Prague is a hotspot for smart city cyber conferences with secure connected places on the agenda. **The Prague 5G Security Conference 2021** [31] **discussed the current state of cyber security on emerging and disruptive technologies.** There have also been specific technologies addressed within papers published during

these conferences, such as by Hana et al. [32]. Despite these clear initiatives within Prague centred around secure connected places, no specific policy or guidance was found as part of this research.

Several justifications could explain the lack of specific secure connected places literature in such examples. First, it may be that the link between connected places and cyber security is a relatively new concept. Second, countries may be adopting a 'service-first' approach, experimenting with the deployment of connected technology to understand the cyber security needs before a dedicated strategy can be released. Third, the existence of internationally applicable documents that already provide relevant frameworks for securing connected places, such as those by the European Network and Information Security Agency (ENISA), may negate the need for a country to publish a dedicated, country-specific strategy. Lastly, as mentioned above, the absence of said documents on open-source databases does not refute their existence.

3.6 National connected places cyber security strategies and frameworks

If a country wishes to go beyond regulating or providing guidance for one technology stream, they can create guidance that takes a systems approach to connected places cyber security, addressing the specific risks and considerations of connected places in their entirety (for examples, see connected places cyber security threats).

Countries' approaches range from high-level guidance and principles to technical approaches, such as how to create a secure systems architecture. The audiences of these documents range from technical experts to generalised; however, they tend to address local government, policymakers and those purchasing and deploying connected technologies, rather than those providing them[1]. While not exhaustive, the examples detailed below intend to reflect this range.

The Canadian Security Intelligence Service published its 'Smart Cities and National Security' guidance in 2021 [33]**.** The short document sets out the possible harmful impacts of cyber incidents on connected places and one page of key security considerations for those implementing connected places systems.

The Australian Cyber Security Centre published a similar document in November 2022 [34]**.** The document identifies that it applies to a range of use cases across cities, rural locations, manufacturing plants and critical national infrastructure, such as ports and details the security risks of 'smart places' technologies with a particular focus on IoT, supply chain, operational technology and cloud computing.

More in-depth examples of national guidance to secure connected places can be found in Japan and the US. Together, these publications from Japan and the US contain comprehensive and technically minded guidelines for a broad range of connected places stakeholders, signalling a

[1] Guidance that is aimed directly at those manufacturing connected places technology products tends to be like those covered in the **Technology-specific regulation** or **5.3 Establishment of international standards** sections.

mature approach by the central government to mitigate the risks posed by their connected places systems and technologies.

> **Japan's Smart City Security Guidelines (Ver 1.0) were published in 2020 by the Ministry of Internal Affairs and Communications** [35]. The above guideline identifies specific security considerations that should be followed regarding the cyber security of smart city developments. Smart cities are abstracted into four key areas: Governance, Service, City OS and Asset, in which each category has examples of security measures. A revised version of the guidance was released in 2021 following a consultation with experts, alongside a 'Smart City Security Guidebook' [36]. Both documents are only available in Japanese, but sources state that the 'revised guidelines outline smart city security considerations in areas such as governance, services and assets and highlight security measures relevant to smart cities including, among other things, incident response, data management and the usage of contracts.' [37].
>
> Also in 2020, **the US CISA published 'Trust in Smart City Systems'** [38] presenting a set of key trust characteristics ('an attribute or behaviour of a smart city system that the users and operators of that system need to believe the system will provide or preserve') to be considered when planning for a smart city project. The guidance is aimed at stakeholders participating in the initial design stage of connected places projects to ensure that security is embedded into connected places from the outset. The NIST has also published a key performance indicators framework for Smart Cities and Communities which uses a scientific approach which measures the effectiveness of smart city system design and assurance.

A final approach to national level guidance on connected places cyber security is the inclusion of connected places in a country's wider national cyber strategy. A country's national strategy or cyber security framework can be an indicator of its general maturity in cyber security. It is hard to define the level of maturity, given that some countries opt for providing a high-level summary of required standards, such as Canada, and some offer a much more in-depth practical guide, such as the UK's NCSC Connected Places Cyber Security Principles. But the existence of these documents shows a clear pathway for that country to deliver higher assurance on the security of connected places assets and systems.

> The **Cyber Security Strategy for Germany 2021** [39] is an example of this, where strengthening the IT security and supply chains of smart cities and IoT is detailed as a key action area. High-level documents and mentions like these, published by a national cyber authority, indicate joined-up thinking in central government on connected places cyber security and are an important first step that further frameworks, guidance and principles can build on.

3.7 Holistic national approaches to secure connected places

There are examples where a country has attempted to collate together all the techniques and models for security under one umbrella to ensure transparency and ease of use for possible stakeholders. An example of this is Germany, which has taken steps through its Federal Office for Information Security. The information for this spotlight was gathered from desk-based research.

3.7.1 Spotlight: Germany's Federal Office for Information Security (BSI) holistic approach

Background

Germany has a well-rounded approach towards cyber security. It has worked to conduct threat assessments, understand policy interventions and build trust and confidence with its citizens. This latter point is particularly important and has been the focus of several initiatives to ensure transparency and accountability in any deployment of connected technology in a public space.

The Federal Office for Information Security (BSI) was founded in 1991. It has a broad remit for supporting central government IT security, as well as providing advice to citizens, regional governments, national and local industry and academia. It has become the key point tying together a complex and comprehensive national strategy for protecting digital systems and assets.

Approach

The creation of the BSI in 1991 enabled Germany to prioritise digital security early. They set up the first Computer Emergency Response Team (CERT) in 1994, which allowed them to respond to IT security incidents rapidly at a national level. This was cemented in 2001 when the BSI was integrated as the central IT security service provider for the German federal government.

From this launch point, the BSI began to have a much broader remit in delivering information services for citizens, protecting them as they utilised the internet. Further amendments to the BSI Act in 2009 allowed for the BSI to pass on warnings about malware and vulnerabilities, taking it into an active role for the first time. In 2011, they supported the German government's push to release a Cyber Security Strategy.

In terms of connected places, this overall national focus on cyber security has meant that Germany is an early adopter of protections and guidance for connected places technology security. BSI has taken a holistic approach, ranging from standards to regional initiatives and laws, such as the German IT Security Act 2.0, all of which encourage greater thinking and analysis into the security of deployed connected places technology.

In parallel, the BSI conducted a study on the security risks of 8 German smart cities. This study identified various potential security risks associated with the implementation of smart city technology, such as data breaches, cyber-attacks and the misuse of personal

data. The study provided recommendations to local cities on how to introduce the appropriate measures to protect their networks [40].

Initiatives

- **Smart cities guidance:** the BSI has identified connected places cyber security as a priority. They have a 'smart cities' page on their website, which provides information on how to secure the connected places systems (including IoT devices, networks and data management systems including cloud storage) [41]. They also highlight the importance of security by design, providing guidelines for secure development processes for the Original Equipment Manufacturers (OEMs) of connected places technology. They have an understanding that local authorities are key stakeholders in connected places security management. For the setup of any connected places strategy or projects, local authorities can utilise BSI's guidance on the right organisational roles required, understanding what service those roles need to provide. They can also understand what makes secure architecture and what requirements they should put out to potential suppliers for device security and data management [42]. The BSI also supports understanding the lifespan of an asset. Typically, many smart city devices have a lifespan of 2-5 years, although this is getting longer as the technology develops further. Germany has understood that local authorities need to consider what to do at the end-of-life for devices, how to dispose of them safely and securely, and how to maintain network security when changes are taking place. This also requires regular security and data protection assessments to test whether the devices are maintaining their security.
- **Encouraging the Sharing of Best Practice:** The BSI has implemented a smart city platform called Smart City Dialogue [43], which acts as a forum for discussion amongst experts, local authorities and industry to exchange ideas about smart city developments, security and data ethics.
- **Laws and standards:** While not explicitly for connected places, Germany has enforced standards and laws that take active steps to ensure that public and private sector organisations are protecting their digital systems. The BSI Consumer IoT programme ensures adherence to ETSI EN 303 645 [44], which sets a baseline of security for all IoT devices in a connected home [45]. This looks to the manufacturer of the devices, ensuring that security is built-in from the source to prevent IoT devices from becoming an easy target of cyber security threats. Equally, the IT Security Act 2.0 is a legal framework pushed by BSI to enhance the cyber security resilience of critical national infrastructure in Germany. This contains several pillars of strategy: detection and defence, cyber security in mobile networks, consumer protection, security for businesses and the role of the National Cybersecurity Certification Authority (NCCA) [46]. The BSI demonstrates a strong understanding that information security and digitisation go hand in hand and that digitising public services cannot be undertaken without the proper assessments and measures to protect those digital tools.

Outcomes

The BSI has a funding programme, which involves the testing of new technology that complies with the BSI and European standards for digital security. In 2022, the programme has supported 28 smart cities model projects and has funded a total of 73 projects since its inception in 2019. These trials allow for the BSI to analyse the results of the trials and provide target group-oriented recommended actions for further work or initiatives [46].

Germany leads the way amongst other European countries in investment and growth in the cyber security sector. In 2020, German cyber security solutions accounted for around half of the 13.7bn Euro in revenues for Layer 2 Internet Services and Applications across public cloud services, particularly for infrastructure and software solutions [47]. This demonstrates that German organisations understand that secure and trustworthy data ecosystems are the foundation for successful smart city platforms and indicates that regional and local authorities are investing in these services for public infrastructure.

4. REGIONAL APPROACHES

4. REGIONAL APPROACHES

4.1 Summary

This section will detail the different approaches that are taken where central and regional governments work together to achieve higher levels of cyber security, including:

- Section 4.2: Understanding the regional context where countries have recognised that connected places are flexible concepts that require a place-based approach.
- Section 4.3: State-level cyber security initiatives where a city or region chooses to develop policy or guidance for smart cities outside of the central government's initiatives, either through a desire for speed with early-adopters of new technology, or to reflect regional nuances.
- Section 4.4: Specific smart city initiatives where a country is investing in developing a specific smart city, often a capital or regional capital, and therefore develops specific policy and guidance for that city before or separately to national guidance.
- Section 4.5: Regional initiatives by central government where a national organisational body will sponsor or purpose-build a vehicle for standardisation or governance of smart cities technology in-region, and ensure that it receives adequate engagement, before stepping away and relying on continued regional leadership of the initiative.

Key findings:

- From the evidence that we have seen in collating this research, in many cases, a national strategy does not suffice to cover all possible use cases and scenarios for securing connected places technology.
- Many cities globally have chosen to develop their own localised guidance, regulation and principles for cyber security in smart cities, to address the nuances of deploying technology in their city or region. There are multiple ways to approach this, whether it is through the selection of specific use cases that the city will focus on, and developing guidance to that, or by creating industry and academic engagement clusters that can share best practice, learning and compliance to national guidance.
- A key consideration for any regional approach would be to ensure that any activity ties into the wider national strategy for cyber security, otherwise there is a risk that policy, guidance, or regional support documentation is produced in isolation and does not correlate with national guidance. This can be avoided either with a city-wide body, such as Smart Dubai, that has a job to ensure that all the guidance produced is developed in collaboration with central government, or through a cluster structure where local government can engage with national bodies such as NIST or CISA.

4.2 Understanding the regional context

Each region will have differences and nuances in the way that they adopt and secure technology deployed in their area. This could include localised strategy, or even the range of technologies

and use cases pursued. These differences also apply from a cyber security perspective, as each connected place is uniquely complex.

> In 2019, the **Ministry of Land, Infrastructure and Transport in the Republic of Korea determined that a smart city was a flexible concept that had to vary according to the economy, society, policy and urbanization degree of the country that used it** and therefore the security had to be flexible too [27].
>
> Customization in approaches is what leads to successfully securing networks, devices and data based on what that region needs, underpinned by national guidance. That is shown clearly in the UK as it utilises the NCSC's Connected Places Cyber Security Principles for cyber security in conjunction with data hubs and localised support for authorities.

Cities or regions may also often feel that they are responsible for the ongoing maintenance of systems and therefore should be more involved with the development of policies and standards to govern them.

> **In Brussels, the regional government has put forward a strategy to develop regional cyber security, separate from the central government** [48]**.** Some connected places may feel that they have little support from the central government in developing legislation or security standards that they could implement. At the Mobile Web and Intelligent Information Systems International Conference in Rome in 2022, the delegates analysed existing security standards and felt that a methodology for comprehensively processing security standards in IoT in Smart Cities was needed [32].

But in countries where there is less of a focus on national strategic direction and policy for connected places, regions have either worked to develop their policies and standards or have collaborated with the central government to drive this change. This is the case in countries such as the UAE, where Smart Dubai is a leading organisation in developing smart cities and IoT cyber security policy.

4.3 State-level cyber security initiatives

In countries with a federalist government, such as the US, Brazil or India, there can be competing or conflicting policies and regulations developed at each level of government. This is because the regional government has the same powers to legislate and regulate as the central government, and often capitalises on this to develop policy that reflects the specific needs of their region or state. This is clear from examples in countries such as Australia, where cities such as Newcastle [49] and Sydney [50] have developed separate smart city strategic frameworks, with the same desired goals of supporting connectivity in cities and bolstering resilience, but with different nuances that better suit their regions.

In the US, the federal government demonstrates an ongoing commitment to spending more on cyber security and spends tens of billions of dollars towards securing the nation's connected systems. However, the decentralised nature of a federalist governance model can raise

significant challenges, particularly when coordinating efforts towards cyber security and making information accessible to those outside of the federal government [51]. There are more than 100 agencies responsible for their cyber security at a federal level before national cyber security agencies can begin to think of supporting regional efforts at a state or municipal level. This is by no means a problem unique to the US, as many federalist governments share similar challenges.

A decentralised model will create multiple avenues and streams of activity. Therefore, it can be hard to propagate a "single source of truth" as is possible in a unitary state without significant investment and coordination from the central government [51]. However, decentralising the ability to respond to cyber threats and challenges means that a state, city or region can develop responses more quickly than central government, and in many federalist countries, rapid steps have been taken at the local level to secure smart places technologies. As a result, many states or large cities have developed their own policy or response units.

> **In 2016, San Francisco's City and County council adopted a citywide cyber security policy** [52] which was set up to maintain and secure critical infrastructure and data systems. Whilst it does not specifically reference smart cities, it does include the key actions that staff in the council would be required to undertake protections for all systems, including IoT systems.
>
> **Equally, in 2022, the city of New York created an Office of Technology and Innovation (OTI), within which sits a Cyber Command Centre.** This centre acknowledges the growing cyber security threats against the city and its infrastructure. It works with more than 100 agencies at the state and the national level to prevent, detect, respond and recover from cyber threats [53]. They have a stream of activity dedicated to urban technology, where the centre collaborates with city agencies on smart cities projects, security 9-1-1 communications, critical infrastructure, connected vehicles, mobile phones, cloud services and secure analytics on the data generated by IoT devices.
>
> As of 2019, surveys across the 50 US states indicated that nearly half of that number do not have a separate cyber security budget, and more than a third have seen no growth or a reduction in those budgets. Despite this, IoT maturity appears to be much higher in states and at the local level than it is in the federal government [54].

This may be because industrial systems, the energy network and connected public services, such as transportation and traffic management are all managed at a municipal level, and in some cases are managed by private companies, which has required local states to become much more aware of the cyber risks to this technology. This leads federal governments largely to take a more passive role in security technology, providing high-level policy and guidance and leaves states and municipal authorities to manage incident response and active threat assessments. This is clear from advisory documents such as the Australian government's publication on securing smart places [34]. This document uses the terminology for 'smart places,' rather than smart cities to encompass 'cities, suburbs or neighbourhoods; mine sites; oil rigs; ports; manufacturing and refinery facilities.

Although the implementation of a smart place can take many forms, it will often include technologies and systems such as the following: IoT devices, operational technology, sensors

and cloud computing services'. This demonstrates that the Australian government either is looking at a broader landscape of technologies than just IoT and that it is looking to more than just cities as possible deployment locations for this technology. This broader thinking can support states and local governments in Australia, providing the right level of guidance for their specific needs. The document covers key risks that can be faced, IoT problems, sensor risks, threats to OT and cloud computing services, trying to provide a holistic view of security risks to government systems.

Therefore, it seems that in a federalist model, there will be a mixture of central and regional policy and guidance which could all apply to various connected places use cases. To ensure that the central government is supporting state or regional governments in the right way, it may be suitable for the federal government to incorporate mature regional efforts into their national strategy and documentation, ensuring that those learnings are not lost, whilst also allowing for flexibility. If the central government provides high-level support and guidance, policy and standards, this can be used by states and incorporated into their more tailored and granular risk-management strategies which consider regional requirements and nuance.

4.4 Specific smart city initiatives

In many countries, the divide between regional and national can be due to the early nature of the adoption of technology. Many cities are faster to react than national governments to the opportunities that connected places technology deployments can bring to improving public services. Private sector companies pitch their services to local governments to deploy the technology and this drives a greater imperative to secure technologies at a regional level, often before there is a national initiative to do so.

The European Cyber Security Organisation (ECSO) believes that European regions are the "laboratory for innovation and change" and that encouraging mature regional ecosystems will accelerate the development of cooperation and awareness of security within them [55]. The ECSO believes that the regions can be a catalyst for broader European cyber security and that setting up a multi-layered approach involving cyber security regional ecosystems can accelerate the creation of cyber strategies, policies and their adoption.

This is true in the Republic of Korea, where the earliest pilot smart city projects date back to 2003 [27]. However, it was not until 2008 that any national legislation was enacted when the U-City law was passed and this itself was not revised until 2017 where it became the more all-encompassing Smart City Act**. Once the Korean government was aware of the over 200 active projects across the country, they worked quickly to initiate the 4th Industrial Revolution Committee** [56], which acts as an advisory board and brings together government agencies and various innovation sub-groups to discuss deployments, security and use cases.

Then in 2020, the **Korean Internet & Security Agency (KISA) released the Smart City Security Model in partnership with the Ministry of Science and ICT** [57]. This document is broad and covers all possible threats to various services of smart cities and how they affect the lives of citizens. It calls for the strengthening of regional initiatives against

> cyber-attacks, but also for local governments to internalise security. In aid of this goal, this mode provides security frameworks, certification systems, case studies of incidents that local governments can learn from and standards for technology projects to adhere to.

Early adoption of technology by regional governments can compel the national government to create comprehensive support to drive uniformity and security across all projects and regions. An example of this is in Belgium. The city of Brussels has long had an active smart city initiative and has deployed technology to support public services. To ensure the protection of these deployments, it has concurrently developed its regional cyber security plans and has not relied on a push or strategy from the national Belgian government to do so. In this way, it has potentially informed the national strategy for securing connected places with its halo projects. Due to its large population and its concentration of businesses and public services, Brussels had to develop a tailored and immediate security plan for its technology deployments. It does not rely on government support to do so, although undoubtedly, this initiative has now fed into any national directive on connected places cyber security.

> **The Brussels city region developed the Brussels Regional Informatics Centre (BRIC) and the Brussels Prevention and Security (BPS)** as bodies which work closely with the local government to examine current cyber threats and propose methodologies to respond, as well as link into the national agencies responsible for cyber security. BRIC has developed a secure data centre to manage data generated as part of the authority's operations and ensures that all data is managed and stored per GDPR. This shows that Brussels is not just ensuring the security of IoT devices in a connected place but has also taken steps to secure and manage data properly.
>
> The same is true of Wallonia in Belgium **where, in 2019, the Walloon governmental agency for digital topics launched a dedicated cyber security mechanism called KIS: 'Keep it Secure', which is part of the Digital Wallonia programme** [58]. This regional approach was based on direct feedback from the market and from the main service providers for smart city technology. The main objective is to create a virtuous circle of trust in which companies are encouraged to invest in cyber security. The KIS regional mechanism is a framework of specific skills which assess the cyber security professionals performing through the corporate checks system. This development drew on the UK's Cyber Essentials accreditation for inspiration [55].

In Africa, multiple capital cities are pushing forwards with smart city plans, although it is not clear whether the national government or the cities themselves are pushing the national policy towards connected places deployments. This is because strategy documents are being generated by central governments in these countries, but most technology projects are being initiated at a local level.

> In Rwanda's capital Kigali, innovations such as air quality sensors and buses offering Wi-Fi connectivity are already active, with future projects in progress [59]. These future projects [60] will look at security, access control, CCTV, facial recognition, tracking vehicles and assets, water management and monitoring leaks and utility management. This rapid

adoption of connected technologies in the city requires an adequate cyber security policy to cover any potential risks.

Many governments, working closely with the Smart Africa Manifesto from 2013, have decided to push a technology and cyber security agenda in the capital city, rather than taking a nationally covered approach. Many African countries remain without a robust cyber security framework. In 2020, the ITU conducted research for their Global Cybersecurity Index and found that of the 54 countries assessed, only 19 had active Computer Emergency Response (CERT) teams and 29 had legal frameworks for cyber security [61].

As a result, some smart cities in Africa have looked to private partnerships to boost both the deployment of technologies as well as securing these networks and systems.

The municipality of Plateau in the Ivory Coast has partnered with Dassault Systems to develop a digital twin of the city, collecting thousands of data points on the city and ensuring the safety of that data's use and storage [62]. In Africa, it seems city strategies for the adoption of smart cities technology then drive a trans-continental approach to pushing for cyber security policy, such as the 2014 African Union Convention on Cyber Security and Personal Data Protection.

A clear example of where a city is leading the way at a national level is in the UAE, where Dubai has made huge strides to advance both its technology and cyber security level. With the use of the Smart Dubai initiative, housing everything in one organisation has prioritised building technology by design. Dubai is an example of where the ambition to develop a smart city has led to a concurrent stream for security adoption at the same time as deploying technologies, ensuring that all systems deployed are protected. This prevents any need for retrofitting policy to technology and given the fact that the physical cityscape itself is still growing, ties in well with Dubai's development goals.

4.4.1 Spotlight: The UAE's Smart Dubai initiatives

Background

Smart Dubai was launched in 2015 and is an initiative by the UAE government which seeks to advance Dubai's services provided to citizens through the adoption of new technology. When Dubai launched its Cyber security strategy in 2017, they highlighted that security has become an essential component of modern life, which led to the formation of the Dubai Electronic Security Centre, a facility which has manages the deployment of security policies and regulations, provides training and support, as well as incident response.

Approach

Dubai has taken the lead amongst the seven emirates of the UAE in sharing best practice regionally with its neighbours. In developing the policy and strategy that it has, it provides

an example for other regions in the Middle East to follow, as they all look to develop their smart city programmes.

Smart Dubai has four programmes that form the pillars for the next wave of Dubai's smart transformation: the Dubai Data Law, the Pulse Platform, the Blockchain Strategy and Smart Dubai Strategy. The Internet of Things strategy drives the UAE's smart transformation agenda, seeking to digitise more aspects of citizens daily life and connecting their activity to the Pulse platform, which manages all digital systems and data.

Figure 6: Smart Dubai's Strategic Initiatives

As shown in Figure 6 taken from the UAE's Internet of Things Strategy, Dubai has security, accountability and data management within each of the phases of the rollout of its IoT programme. Smart Dubai places a high value on security and wants to tie national policy and strategy into a localised strategy for the city, sharing cyber security guidance across all government organisations.

Specific initiatives

Strategy and Policy: In 2017, Dubai launched its Cyber Security Strategy, which aimed to strengthen Dubai's systems and IoT in safety and security. The strategy contained five domains:

- Cyber-smart nation – which aims to raise public awareness of the importance of cyber security and the dangers of cybercrime, as well as develop the skills required to manage cyber risks among government and private sector companies.
- Innovation - which looks to develop scientific research in the field of electronic security to support the establishment of a free, fair and secure cyberspace.

    - Cyber security – aims to build secure cyberspace by establishing controls to protect the confidentiality, credibility, availability and privacy of data.
    - Cyber resilience – which will focus on maintaining the flexibility of cyberspace and ensure the continuity and availability of IT systems in the event of any cyber-attacks.
    - National and international collaboration – which seeks to establish local and global partnerships to consolidate cooperation frameworks with different sectors to confront threats and risks.
- As noted, the government of Dubai has also developed the Dubai Electronic Security Centre, a facility and department which not only works to protect Dubai and deliver the five domains from the cyber security strategy but also sets out mandatory and recommended controls for the security of Internet of Things devices and networks. Compliance with the Dubai IoT security standard [63] is mandatory for all Dubai government and semi-government entities. The Dubai Electronic Security Centre has many other standards that overlap with connected places, including guidance for connected vehicles and operational technology, showing that Dubai is considering how connected technology can be broader than just IoT deployments into the public realm.

Data Sharing Security: In 2020, Smart Dubai partnered with Nesta to develop a data sharing toolkit that could be utilised across all public and private sector IT systems.

- The toolkit focuses on how trusted data sharing arrangements can be formed to ensure that protections for and the integrity of data are always maintained. The toolkit is designed for different levels of projects and guides the user through a process dependent on what stage or maturity of their data-protection journey is at. This means that those who are new to data sharing and need to understand fundamentals can digest the entire toolkit, whilst those more experienced can jump to areas concerned with how to best initiate projects, ensure the right governance is in place and are even provided with a decision matrix to ensure nothing is missed.
- The Smart Dubai Internet of Things Strategy covers six strategic domains: governance, management, acceleration, deployment, monetisation and security. Most importantly, the strategy governs how data enters and exits the Dubai Pulse platform, which is effectively the digital heartbeat of the city and its management systems. The strategy is being implemented between 2022-2025 and will be delivered in phases, looking at:
    - Synergising activities to implement IoT policy across government departments.
    - Integrating and converting data where necessary.
    - Optimising where Smart Dubai has a goal to translate the entire data management element of the system into a blockchain, for greater security for the data held in a distributed ledger.
- It is hoped that at this final phase, the IoT ecosystem will become self-regulating, after the full integration of IoT policies into Pulse and other platforms.

- To achieve this data harmony, the IoT Strategy has two key initiatives to facilitate the trusted sharing and exchange of information through IoT device networks with confidence in the security of valuable data.
- Public Key Infrastructure (PKI) defines the right roles, policies and procedures required to manage, store and use data effectively and the encryption certificates which safeguard that data.
- Digital Certificates, certify that the data being exchanged through IoT networks is secure and encrypted, providing higher assurance of the integrity of the data from the source.

Outcomes

Between 2019-2022, Smart Dubai has amassed new digital services that can contribute to Dubai's smart agenda. Working with more than 30 partners from the public and private sectors, spanning all industry segments, 1,129 smart services are operational over 121 initiatives, generating 200 new data sets to unlock the benefits of open and shared data for the city. All of this is strongly underpinned by the security agenda that has been incorporated into Smart Dubai by design at the point of implementation and integration.

4.5 Regional initiatives by central governments

Regions which operate closely to local industry, academia and education have an edge in elaborating on their own economic, innovation and cyber security versus central government.

The European Cyber Security Organisation (ECSO) encourages regions to develop their own Smart Specialisation Strategy [64], helping them to identify their key sectors for generating investment and the required actions to maximise their development. The European Union (EU) is encouraging more regions to do this, to understand their specialisation and identify what technology and cyber security needs to be implemented to achieve this.

The **EU through the ECSO has implemented a project called the European Cyber Valleys which hopes to deliver an inter-regional network of smart territories** which would accelerate the commercialisation of solutions that are "Made in Europe" including cyber security technology [55]. This is important because regional governments can play a key role in establishing traction between national and international institutions and local ecosystems. For example, a pilot looking at implementing a cyber security competence network called SPARTA [65], brings together 14 EU member states to test this network, using regional clusters such as the Systematic Paris Region as partners.

The EU and its member states are not the only countries looking at this hyper-localised approach to supporting awareness and the deployment of principles and support for cyber security. ECSO advocates for local authorities having a place in the governance of future European cyber security, although a precise implementation plan has not yet been put in place. This action would help to avoid overlaps in policy and standards, create closer ties between national and regional bodies and bring national priorities to a local level more clearly.

Europe is not the only global region to look at clustering regional groups to boost cyber security awareness as a national policy; the US also has a SuperCluster system which relies on regional bodies and local authorities to provide guidance and development for cyber security solutions, policy and guidance.

4.5.1 Spotlight: USA Super Clusters for regional engagement

Background

The US has had a mixture of approaches to cyber security in connected places over the past two decades. As connected technology became more prevalent, the adoption of devices and systems to deliver more efficient services became more widespread. Certain large cities like New York, Atlanta and Washington D.C. put into place smart cities strategies and rolled out thousands of devices across their networks to support services from traffic management to air quality monitoring. A federalist governance structure can result in some mis-coordination in the US, where cities and states adopt both the technology and practices to secure it and its data at different rates.

The US federal government first released a national strategy for cyber security in 2003, as a response to the 2001 terrorist attacks, followed by a full cyber security national strategy - the 'Cybersecurity Act' - in 2012. The latest version of the National Cybersecurity Strategy was released in March 2023, which has a greater focus on data security and the utilisation of federal funding to build in security at the source of technology [66].

Approach

For connected places, the US spending to boost resilience has mostly come at a state or municipal level. Cities such as Seattle have seen their budgets increased from $5.3m to $7.5m between 2020-2022. New York State has invested $60m into a "first-in-the-nation" joint operations centre for state and local cyber security needs. This centre will also serve the private sector and the state's critical national infrastructure operators such as power and transportation companies [67].

Despite these exemplary local initiatives into supporting cyber, federal government spending as of 2019 remains focused more on financial, information and communication technologies and defence industries [68]. Between 2019 and 2024, an estimated $135bn of spending would be put towards cyber in these spaces, but not focused enough on smart cities use cases, which may leave them underfunded and more vulnerable. This spending is to action EO13636, a bill passed by the US government in February 2013, which looked to improve critical infrastructure cyber security but left localised connected places cyber security requirements for the attention of local authorities.

To combat this and provide a strategic direction and support at a federal level, both NIST and the Department of Homeland Security (DHS), backed by the Department of Commerce, looked as to how they could deliver initiatives with a smart city focus. This has been sharpened with several high-profile attacks on various city Supervisory Control and Data Acquisition (SCADA) systems in cities such as Baltimore and Atlanta,

where botnet attacks on IoT devices have allowed hackers to carry out massive Distributed Denial of Service (DDoS) attacks using public hardware IP addresses.

Initiatives

- To support a greater focus on cyber security in local authorities and industry, in 2014 NIST launched an initiative called the Global City Teams Challenge (GCTC) to encourage state and regional authorities which were deploying smart city and IoT technologies to look at developing and deploying standards-based solutions.
- By encouraging the adoption of replicable, scalable interoperable and secure solutions, NIST hoped to provide benefits for cities and communities. As this programme developed over multiple years, the GCTC became a collaborative platform for cities, communities, industry, academia and federal government to meet and discuss challenges and work together on developing emerging technologies to meet their demands.
- Whilst the original purpose of these "clusters" was to encourage cross-working for efficiency and lower costs, the federal government also saw an opportunity to pursue an agenda of security across the country.
- In 2018, the US Department of Homeland Security Science and Technology Directorate (DHS S&T) joined the programme as a co-host and the GCTC was given a secondary focus on looking at smart and secure cities. This challenge, called SC3, aimed to encourage those groups who had been developing and deploying technology to consider cyber security and privacy as a core part of the development of solutions, rather than as a retrofitted aspect. Other government organisations since have also fed into the clusters, bringing challenges and considerations that improve the quality and security of any solutions deployed across the continental US.

Outcomes

In fostering collaboration and innovation across this remit, the GCTC has acted as a matchmaker and incubator, helping to form public-private partnerships, which are dubbed Action Clusters and SuperClusters. The GCTC has recruited over 200 Action Clusters, which involve over 200 cities, 500 companies, universities and non-profit organisations all looking at building secure solutions for connected places. 40% of these clusters are outside of the US, enabling innovation in Africa, Asia, and Europe and ensuring that the US is tied into the security agenda of the IoT and Smart Cities supply chain across the globe.

Given the large number of Action Clusters, NIST has divided them into SuperClusters, which look at specific aspects of technology for connected places and industry. This is so that NIST can act as a better advisor to each of these groups, which it does as a member, looking to bring cyber security and privacy across all the SuperClusters. These SuperClusters look at utilities, smart buildings, data and city platforms controlling IoT devices, wireless technologies, smart healthcare and transportation and cyber security and privacy.

Figure 7: The GCTC SuperClusters [99]

One key benefit that the amalgamation of so many organisations involved in smart city technology has had is to foster collaborative discussion on what practical things can be implemented by the federal government to support the agenda of each SuperCluster. These groups have allowed NIST to take away critical information they would not otherwise have had access to and use it to inform the development of both smart city agendas across the US and policy.

Some example documents and policies created include the IoT-Enabled Smart Cities Framework [69], a document developed by an international working group led by NIST, which provides tools to support interoperability and standards and the Municipal Internet-of-Things Blueprint [70], developed by the GCTC Wireless SuperCluster, which provides a blueprint of how IoT can affect government agencies in the future and models for engagement amongst municipal authorities looking to develop smart city technology solutions.

Responding to the need from communities across the US, in 2020 CISA also generated the Trust in Smart City Systems document [71], which provides a series of trust characteristics to authorities that helps them to adopt solutions with greater assurance towards security, reliability, privacy and integration, amongst other things.

5. INTERNATIONAL APPROACHES

5. INTERNATIONAL APPROACHES

5.1 Summary

Within this section, we focused on findings on an international level. It identifies international collaboration efforts between multiple countries and initiatives to promote international guidance or frameworks that should be utilised in the implementation of cyber security in connected places.

- Section 5.2: International activity around the globe discusses the actions that international bodies and specific countries have taken in international connected places cyber security.
- Section 5.3: Establishment of international standards discusses how specific countries have led on the establishment of new standards for the regulation of connected places cyber security.

Key findings:

- Centralised areas for international connected places cyber security policies and international standards exist but may not be fit for purpose.
- There has been a significant push to unify secure connected places policy across the globe in a centralised location, emphasising the need for a unified approach to capitalise on the wealth of guidance, principles and policy.
- Current guidance, principles and policy represent an initial push towards a specific international standard for secure connected places. Some international standards provide an overview of the considerations that should be included within a connected place, such as IoT, Cloud and Privacy considerations. There are several critiques towards these standards, including the lack of consistency between standards and organisational support in implementing security standards for connected places.
- Some international standards provide an overview of the considerations that should be included within a connected place, such as IoT, Cloud and Privacy considerations. It's currently uncertain if all material related to the international cyber security of connected places is accessible, therefore the current literature collated in this review may only represent a portion of the total relevant literature.
- Considering the wealth of technological and financial investment within areas such as ASEAN, it is evident that future collaboration regarding the cyber security of connected places will continue and become increasingly important in the years to come.

5.2 International activity around the globe

When considering international organisations that develop advice and recommendations on good practices, ENISA provides security expertise for the EU, the member states within the EU, the public sector, the private sector and European citizens. ENISA has a mission to improve the resilience of Europe's critical infrastructure and cross-border collaboration to provide security throughout the EU.

International Organisations

In 2015, **ENISA conducted a study investigating cyber security concerning Intelligent Public Transport (IPT) systems within connected places** [72]. The study highlighted the increased level of data exchange produced by these systems, as an increased amount of data provides a more in-depth visual of transportation systems and an improved level of service. The issue identified is that there was a lack of guidelines or standards to model these data exchanges. In addition, IPT operators commonly do not employ some form of cyber security policy nor define critical assets within these systems. Despite this, cyber security measures are being implemented by operators which creates further issues as solutions are not widely accepted standards, provide greater variance in technologies within an interconnected system nor are accepted as a best practice.

The approach taken to address these issues defines a high-level architecture model to understand key areas which need protection from cyber threats. Some example recommendations summarised by the report are as follows:

- Requires support to develop a cyber security framework by the involved municipalities.
- The European Commission and Member States should undergo a process of knowledge exchange related to cyber security between industry, member states and municipalities.
- IPT operators should define a clear definition of security requirements.
- Operators and municipalities should allocate higher spending on cyber security.
- Manufacturers and solution vendors should be integrating cyber security within IPT systems.

Ultimately, the study identified what the next steps should be to secure IPT systems utilised in European connected places and has contributed to the development of a framework that should be implemented to address current issues within these systems.

Another intercontinental initiative related to the cyber security of connected places was conducted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

The 2020 **NATO CCDCOE, within the horizon scanning and analysis 2030 report** [73], looks to address the landscape of cyber threats and how NATO can tackle these issues to protect its members both militarily and politically. Concerning connect places, they identify the impact of cyber warfare on smart cities and explore the relationship between cyber-attacks and how that may affect social disorder within urban spaces. Interestingly, it provides a foresight activity in which they provide a case study of a fictional but possible

> 'cyber assault' event and how it results in a serious breakdown of social, political and technical structures. It then provides an analysis of vulnerabilities associated with smart cities; looking at technological, social and governance-related risks.

The analysis concludes that significant changes are required in local governance structures and practices to mitigate these vulnerabilities. An interesting takeaway from this analysis is that there is a significant focus on the non-technical impacts of attacks on connected places technologies; smart cities now play an important role in international security as these places serve important political, economic and security functions.

These findings highlight that connected places are an international security concern, but significant effort has gone towards specifically highlighting the issues that need addressing and the mechanisms that should be put in place to mitigate them.

> An international initiative on said mechanisms can be found within the **G20 Global Smart Cities Alliance resource library** [74]. The resource library collates a foundation of multiple national policy approaches related to the cyber security of connected places to ensure that the implementation of technology has an adequate level of protection in place for privacy and security. So far there have been 25 contributing countries to the Smart Cities Alliance including at least one representative from each region, with the expectation that it will address global concerns not only with the security and resilience of connected places, but also the inclusivity, privacy and transparency, openness and operational and financial sustainability. It represents an international effort to actively address the need for implementable policies in a single location.

Specific Cross-Country Collaboration

Cross-County Collaboration specifically refers to initiatives that include two or more countries looking to work together on the topic of secure connected places.

> An example of Cross-Country Collaboration can be seen in the **Smart Africa & Smart Cities Initiative** [75], which recognises 24 African member states including Egypt, Kenya, and South Africa to put ICT development, accessibility, efficiency and sustainability at the forefront of their country's socioeconomic agenda.

According to the initiative, Africa is seeing an exponential increase in urban population, with the total population expected to exceed the total rural population in 2030-2040. Within this strategy it identifies the desire to develop 1,000 smart city initiatives, tackling issues such as transportation, energy, water and safety in addition to the development of 50 Security Operation Centres (SOCs) to protect critical infrastructure. The initiative indicates an international desire to develop secure connected places throughout the African continent and has developed a set of blueprints and resources to support connected places development [76].

> We can also see Singapore collaborating with the UK on the **Secure by Design - UK-Singapore IoT Statement** [77]. Singapore and 52 other nations, through the Commonwealth Cyber Declaration, agreed to work towards the development and

> convergence of approaches for internet-connected devices and associated services to promote user security by default.

As part of the Singapore-UK Strategic Partnership, the two countries agreed to work together on greater cooperation and alignment to support a global consensus for 'secure by design'. They aim to take a leading role in driving improvements in the security of smart consumer products while ensuring that the IoT industry can continue to grow and innovate. The UK and Singapore recommend that manufacturers implement industry best practice to ensure the safety and security of citizens and the wider economy while using their products. Both nations will adopt a multilateral approach by working with their partners, both internationally and regionally, to promote the implementation of good practice as set out in relevant industry global standards. They also committed to strengthening their dynamic partnership for the 21st century through the sharing of best practice.

5.3 Establishment of international standards

The purpose of published international standards is to establish guidelines of best practice through the utilisation of a standardised language and create a demonstratable certification that provides confidence in an organisation's ability to adhere to the standard's recommendations.

> **Commonly used examples of international standards are the ISO/IEC 27001** [78] which focuses on Information Security Management Systems and encapsulates aspects of risk management and security. **Other examples of international standards that have been published related to the cyber security of connected places include**:
>
> - ISO/IEC 30145: Smart cities ICT reference framework – Focuses on smart city-specific processes, including common processes between a smart city and commercial organisations [79].
> - ISO/IEC 37156: Guidelines on data exchange and sharing for smart community infrastructures – Framework for data exchange and sharing between entities and an authority to develop and operate community infrastructure [80].
> - ISO/IEC 30141 and ISO/IEC 27400: IoT standards – Specific technology standards utilised in connected places, focused on reference architecture [81] and security and privacy guidelines for IoT [82].
> - ISO/IEC 17789 and 27018: Cloud computing standards – Specific technology standards utilised in connected places, focused on reference architecture [83] and codes of practice for protecting Personally Identifiable Information (PII) [84].
> - These international standards have been used to create the ISO/IEC 27570, which has created privacy guidelines for smart cities [85].

However, it is important to highlight that specific countries may push for specific international standards to be developed. The reasons for this may be due to the need to address specific needs, promote industry competitiveness or establish leadership in a specific field. An example concerning connected places can be seen in the development of ISO/IEC 37155 which was proposed by Japan and looks at building a 'framework for integration and operation of smart

community infrastructures' [86][87]; as stated by the Ministry of Economy, Trade and Industry, the purpose of the international standard was to encourage more Japanese companies to enter international smart city markets.

Although standards related to secure connected places have been published, there have been **critiques in the form of Sveccova** [32] in which they surmised that the current 'legal norms of international standards have been developed inconsistently' and that 'cities, municipalities, regional self-governments or state security forces have no support in legislation or international standards in the form of security standards that they could implement in connection with the integration of the Smart Cities concept'. This implies that an international standard for secure connected places does not currently exist.

A good example of international cyber security of connected places and collaboration can be seen throughout the ASEAN region.

5.3.1 Spotlight: International collaboration in the ASEAN region

Background

The ASEAN is an intergovernmental organisation founded in 1967 and is comprised of 10 countries within Southeast Asia: Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam [88]. It is currently one of the fastest growing economic regions in the world [89]. The region provides a significant case study that encapsulates both internal international collaboration between member countries to tackle the challenge of the cyber security of connected places and external collaboration with other international organisations such as the EU and countries such as the Republic of Korea, Australia and Japan.

Related to the cyber security of connected places, Singapore chaired the ASEAN in 2017 in which the region published the Cybersecurity Cooperation Strategy 2017-2020 intending to provide a roadmap for regional cooperation and strengthen information and communication technology security. Interestingly, the Singapore Cybersecurity Strategy 2021 [90] highlights the ASEAN CERT and ASEAN Information Exchange Mechanism in addition to the importance of cyber security. Although multiple member states may have contributed to the development of the Cybersecurity Cooperation Strategy, Singapore had a good level of cyber security maturity during this time and could have been driving the adoption of such a strategy.

Approach

The region has seen the development of the ASEAN Regional Forum with the purpose to foster constructive conversations on political and security issues [91] and the ASEAN Consultative Committee for Standards and Quality (ACCSQ) which had released a strategic plan for 2016–2025 [92].

The ACCSQ has published several cooperation initiatives with countries outside of the ASEAN region. Examples include [92]:

- ASEAN, Australia, New Zealand Free Trade Area and the ASEAN Australia Development Cooperation Programme.
- ASEAN-Japan Comprehensive Economic Partnership Agreement.
- ASEAN-Korea Free Trade Agreement.
- Regional Comprehensive Economic Partnership Agreement.

Initiatives

Cross-Country Guidelines: one of the key cross-county guidelines related to secure connected places is the ASEAN Cybersecurity Cooperation Strategy [93].

- The 2021-2025 Strategy aims to establish a rules-based multilateral order for cyberspace and enhance cooperation within ASEAN and with dialogue partners to build a secure, interoperable and resilient cyberspace. This will support ASEAN's digital ambitions and initiatives such as the ASEAN Smart Cities Network (ASCN) and the ASEAN Declaration on Industrial Transformation to Industry 4.0.
- Specific to connected places is the development of the ASEAN Smart Cities Network during the 32nd ASEAN Summit in 2018 [94] to develop smart and sustainable urban development using 26 pilot smart city action plans. From the initiative, the ASEAN Smart Cities Framework [95] emphasises three interdependent objectives for smart cities: competitive economy, sustainable environment and high quality of life. Two key urban systems that are essential to achieving these objectives are integrated master planning and development, and dynamic and adaptive urban governance. The article also highlights three focus areas for smart city projects: civic and social, health and well-being, and safety and security.

International Collaboration: concerning connected places, two key examples of international collaboration efforts exist between ASEAN:

- Japan in the form of connected technology and cyber security collaboration and Australia in the form of a trust fund specifically for ASEAN connected places.
- In 2022, ASEAN-Japan held its 15th Cybersecurity Policy Meeting [96], held annually since 2009 to enhance collaboration on cyber security with the ASEAN member states and Japan. The meeting focused on exchanging views on cyber security policies over the past year and confirming and evaluating collaborative activities, such as critical information infrastructure protection workshops, joint awareness raising, capacity building, joint government-industry-academia and cyber exercises. The meeting confirmed progress and agreed to continue implementing collaborative activities. From the 15th annual meeting, the collaboration has established 9 key Collaborative Activities including 3 specific themes relevant to connected places:
    1. **Protecting Critical Information Infrastructure:** The Critical Information Infrastructure Protection Workshop took place with a focus on critical infrastructure and data protection. Attendees shared information about legal

efforts and measures in their respective countries to address cyber-attacks and discussed plans for next year's workshop.

2. **Capability building and awareness raising:** Reports were provided on the implementation status of Japan's capacity building projects in cyber security and awareness-raising activities. These included plans for the ASEAN-Japan Cybersecurity Capacity Building Centre to hold training courses, workshops and online events such as the JP-US-EU Industrial Control System Cybersecurity Week for the Indo-Pacific Region, which offered hands-on training and workshops related to industrial control systems [97].
3. **Remote cyber exercises and mutual notification of incidents:** the outcomes of two exercises were reported: a remote cyber exercise and a tabletop exercise. The remote exercise involved a scenario of cyber-attacks on government organisations and critical infrastructure and utilised an online chat tool for communication, which was praised for its utility. The tabletop exercise focused on upgrading ransomware countermeasures and promoting the digitalization of government organisations, with participants exchanging views on challenges and knowledge. Additionally, a report was provided on initiatives to reconfirm and address the framework for mutual notification in the event of an incident in another country, with participants evaluating and discussing further improvements.

- ASEAN also collaborates with Australia in the form of the ASEAN-Australia Strategic Partnership, ASEAN-Australian Development Cooperation Programme (AADCP) and regarding connected places, the ASEAN Australia Smart Cities Trust Fund (AASCTF).
- The ASEAN-Australia Strategic Partnership has established a plan of action which aims to guide the implementation of goals and objectives from 2020 to 2024. It builds on the history of cooperation and partnership between ASEAN and Australia, reaffirming their partnership and outlining priority actions to intensify engagement to shape a peaceful, prosperous and rules-based region with ASEAN at its centre, including the promotion of cooperation, an integration process and addressing emerging regional and global challenges over the next five years.
- The ASEAN-Australian Development Cooperation Program aimed to promote sustainable economic and social development and integration within the ASEAN region over six years. The program was comprised of 3 components: Program Stream, Regional Partnerships Scheme and Regional Economic Policy Support Facility. The ASEAN-Australian Development Cooperation Program Independent Completion Report assesses the program's design and objectives, effectiveness, efficiency and impact. It was deemed relevant and important but lacked an overarching design and coordination mechanism. Its ambitious and vague goals and objectives made it difficult to evaluate success and there was no results framework to assess outcomes.
- The ASEAN Australia Smart Cities Trust Fund was a single-donor trust fund established in April 2019, supported by the Government of Australia, and managed by the Asian Development Bank. Its goal is to assist ASEAN cities in

enhancing their planning systems, service delivery and financial management by developing and testing appropriate digital urban solutions and systems. The trust fund aims to facilitate the transformation of cities to become more liveable, resilient and inclusive while identifying scalable best practice to be replicated across cities in Asia and the Pacific.

Outcomes

ASEAN has a cyber security and smart city strategy that recognises the need to protect connected place technologies and critical infrastructure. While a framework specifically discussing secure connected places has not been published, contributing countries within and collaborating with ASEAN has established a baseline of knowledge addressing aspects of secure connected places, therefore indicating that the expertise exists internationally. ASEAN is collaborating with Japan and Australia on connected technology, cyber security and smart city development. The ASEAN-Japan collaboration has established 9 key collaborative activities, including protecting critical information infrastructure and mutual notification of incidents. ASEAN's collaboration with the ASEAN-Australian Development Cooperation Program lacks an overarching design, but the ASEAN Australia Smart Cities Trust Fund aims to enhance planning systems, service delivery and financial management through digital urban solutions.

As international collaboration efforts on connected places, cyber security and investment continue within the ASEAN region, there might be evidence for a unilateral increase in secure connected places maturity as countries invested in the region continue to collaborate. This could be considered a potential avenue for research in the future.

6. CONCLUSION

6. CONCLUSION

6.1 Summary of findings

Connected places technology has the potential to improve the quality of life for citizens and generate significant economic development. However, with this deployment comes the need for strong cyber security policies and practices, as any connected places system includes a wide variety of hardware and software that makes it vulnerable to attack.

There is no one pathway to take to ensure effective cyber security across connected places systems, assets and technology. Countries take different approaches to how they provide guidance and best practice to public and private organisations. There are nuances to reflect, not just from country-to-country, but also within each country, at a regional and city level, that require specific guidance and possibly legislation, to ensure that the solution is fit for the problem. As a result, we have seen many cities such as Brussels develop their own localised guidance, regulation and principles for cyber security, addressing their needs outside of Belgian or even EU guidance.

Countries must ensure that organisations comply with any guidance generated by the national and regional governments. Most guidance, standards or principles documents are produced for local governments, policymakers and connected technology procurers, however, they do not always reach their intended audience or get different stakeholder groups talking to one another. A way to potentially combat this is to develop technology-specific regulation and standardisation such as the Swiss NCSC and the UAE's IoT Security Frameworks, which educate potential users of that technology about the risks and make sure they understand how to work closely with the manufacturers.

There are of course also ethical concerns on top of the specific cyber security threats which connected places technology can prompt, particularly when using technologies for surveillance. However benign the purpose, public perception of these types of technologies can be negative and this can open the system up to attacks from people wishing to disable them. It's important that countries and authorities deploying technology understand where the threat to their infrastructure comes from and take the right steps to prevent them as well as engage with citizens to help increase trust in and use of connected places technologies.

It is also key to share best practice in-country, as well as globally, wherever possible. Singapore City is one of the most advanced smart cities in the world. Part of the reason is its leading role in developing national cyber security labs, policies and strategies to protect connected places digital infrastructure, and for its founding role in the ASEAN Smart Cities Network. This is also apparent from the success of the US SuperClusters, where the US government sponsored the development of groups of organisations, focused on different technology verticals, to come together to discuss opportunities, deployments and security risks. That structure has now been owned regionally, showing that with the right stimulus, regional bodies can take responsibility for security in their area and make sure that those nuanced requirements are addressed.

The pinnacle of international best practice sharing is when countries can come together to develop cross-border standards. This is a big driver for the manufacturers of connected technologies to bring their solutions in line with what those governments expect, as their

addressable market now all require the same level of security built into the hardware or software by design. It's key to avoid specifics that favour just one country, but if done correctly, these sorts of standards could be extremely effective.

There are many strong initiatives to grow the cyber security resilience of connected places globally, and from this research, we can determine that a combination of methodologies needs to be employed to ensure a robust, holistic security landscape in any given country.

6.2 Recommendations for further research

While our research has shed light on global policy and literature, there are still many factors that should be considered when exploring secure connected places. In this section, we will discuss avenues for future exploration into the space of secure connected places and areas which were considered out of scope for the undertaking of this study.

- **Comparing a country's technological and cyber security maturity with its Gross Domestic Product (GDP), population density and total population**. A hypothesis to test could be whether countries with a higher GDP are more likely to invest in connected places technologies, which creates a greater incentive to protect these technologies by adopting cyber security measures. Countries with a lower GDP may still invest in connected places technology to promote economic or domestic growth but may lack the resource to ensure that those technologies are kept secure. In addition, a country with a greater population density may have the incentive to implement connected places technologies to provide essential services to a concentration of citizens. Alternatively, a country with a low population density may find that implementing connected places technologies does not support enough concentration of its citizens to make it worth investing in; this point may apply to both population density and total population.

- **Investigate private companies that deliver connected places technologies and analyse their approach to cyber security**. The issues with this undertaking were that there was not enough visibility or published material that provided insight into how a private supplier provides secure connected places technologies. A potential viewpoint to justify this may be due to the desire to maintain a competitive edge over other suppliers, or the associated risks with publishing information about the security of technologies.

- **Emerging connected places that are currently being developed.** Most of the literature surrounding these initiatives focuses on the social and economic benefits rather than providing any strategy regarding the implementation of a secure connected place. Further research should be conducted when these new connected places become operational.

APPENDIX

A. Research design, methodology and limitations

A1. Country prioritisation exercise

To narrow the focus of this work, and to provide an initial avenue for research, a country prioritisation exercise was undertaken to identify in scope countries.

The process utilised two key resources which provided a method of scanning indices to quickly identify countries with significant connected places activity:

- **The National Cyber Security Index (NSCI)** [4]: Developed by the e-Governance Academy Foundation, the NCSI was created to act as an accurate, up-to-date, uniform benchmark for cyber security maturity. It is a global live index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents, in addition to hosting a database with publicly available evidence materials and a tool for national cyber security capacity building.
- **Smart City Index (SCI)** [5]: The SCI ranks 118 of the world's most advanced smart cities and we have used this as a measure of connected places maturity. Each country's ratings are calculated by canvassing citizens on their perceptions of their city's infrastructure and technological provisions evaluated over five key areas: health and safety, mobility, activities, opportunities and governance.

Correlating these two indices was used to identify places of both cyber security and connected places of significance to provide a method to collate potential countries for the literature review. From this process, 162 countries identified within the NCSI were correlated with 118 cities identified in the SCI.

The following process was then used to identify in scope countries:

1. **Countries that did not have a smart city in the SCI 2021 were discounted.** Countries without a mature smart city offering have been deemed out of scope as we expect their connected places maturity and technology advancement to be low. Therefore, they are less likely to have connected technologies and a lower need for policy work in this area.
2. **Automatically count in scope any country that has a city in the top 25% of the SCI 2021.** Countries in the top 25% of the SCI 2021 have been automatically deemed in scope, regardless of their NCSI score, as there are likely to be interesting examples of connected technology deployment. Where their corresponding NCSI is low, this presents an interesting juxtaposition that will require further investigation.
3. **The remaining countries were categorised by region to ensure global representation in the research.** We split the remaining countries out by the following regions: Africa, Europe, the Middle East, North America, South America, Asia and Oceania.
4. **Within each region, the countries were ordered by their NCSI rank and the top 25% per region were selected as in scope.** This allowed us to consider best in class for cyber security per region, rather than globally where some countries would have struggled to be represented. It also allows us to take a proportional view of countries so that the number of in scope countries corresponds to the number of countries in the region.

This process identified 40 countries as in scope for research and analysis.

To determine whether our criteria for prioritising countries was comprehensive enough to cover a wide range of the international region, we conducted a test between the SCI and the Economist's Digital Cities Index 2022 [98]. The findings were that certain regions such as Africa, the Middle East and the UAE did not have representation in the DCI, however, included European countries such as France. It was decided that the SCI provided a greater pool of international countries to focus the literature review.

A shortlisting process was then undertaken to understand which countries had a significant amount of literature that contributes to the discussion of secure connected places. The process involved studying publicly available literature using search engines, academic databases, news sources, government departments and interviews conducted with associated companies involved in connected places to highlight regional, national and international literature related to secure connected places.

A2. Stakeholder interviews

To validate and stress test our findings from desk-based, open-source research. We conducted interviews with experts from the following organisations: Resecurity, Crypto Quantique and Business Information Systems department at Central Michigan University.

A3. Limitations

A limitation identified was the use of only the NCSI and the SCI to scan indices for relevant countries that may contain information regarding secure connected places initiatives. Using multiple resources may provide a better method of understanding the areas of potential for secure connected places. In addition, the SCI used for this report is not the only resource discussing connected places; another example of a connected places study could be the Digital Cities Index 2022 [98]. These limitations are valid in the case of this report, as it is difficult to understand the entire population of secure connected places activity from these two resources. In addition, each resource selected has a disconnected methodology to rank each country regarding cyber security and connected places activity.

However, as of the time of writing there currently exist no approved method for recording and comparing secure connected places activity; there exists no recommendations nor dedicated resource that can effectively collate what is required for the literature review. Although there are valid critiques for the methods used in this report, it is the start of a new process that ultimately engages the need for future literature related to secure connected places.

Another limitation of the report is that it does not have optimal access to specific resources and guidance, such as the cyber security policy of companies providing connected places technology. This means that the report only contains a portion of the assumed international findings related to the cyber security of connected places. As further collaboration on cyber security for connected places continues, more resources should emerge.

A final limitation is the stakeholder interviews used to supplement desk-based research. Given the tight timelines that this work was performed, it was not possible to meet with key government stakeholders to validate all the report's findings. We would recommend future work to conduct additional stakeholder interviews to further supplement the key points set out here.

A4. Ethical Considerations

The report ensured that any information included that was procured from an interview was given with the consent of the individual interviewed and that they had prior notice that the interviews could be used within the report. DSIT and Plexal privacy notices were shared with all individuals invited to interview.

B. Glossary of terms

Term	Definition
AADCP	ASEAN-Australian Development Cooperation Programme
AASCTF	ASEAN Australia Smart Cities Trust Fund
ACCSQ	ASEAN Consultative Committee for Standards and Quality
Architecture	The designed structuring of something e.g., an agreed set of components for IT systems
ASEAN	Association of Southeast Asian Nations
ASCN	ASEAN Smart Cities Network
BPS	Brussels Prevention and Security
BRIC	Brussels Regional Informatics Centre
BSI	Germany's 'Federal Office for Information Security'
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CISA	The US 'Cybersecurity and Infrastructure Security Agency'
CAF	Cyber Assessment Framework
CERT	Computer Emergency Response Team
Connected places	Connected places are communities that integrate information and communication technologies and Internet of Things devices to collect and analyse data to deliver new services to the built environment and enhance the quality of living for citizens. Connected places will use a system of sensors, networks and applications to collect data to improve their operation, including transportation, buildings, utilities, environment, infrastructure and public services
Connected technologies	Products with technology built in that allow them to connect with their environment and other products, for instance, internet of things devices
CPAC	The US 'Cybersecurity and Privacy Advisory Committee'
Cyber-physical systems	Systems have physical inputs and/or outputs which are controlled by computers. At one extreme this means industrial control systems and some critical infrastructure, like power generation and distribution. At a smaller scale, many IoT devices are also cyber-physical systems.
Cyber security	The practice of protecting computer systems from attack
DDos	Distributed Denial of Service (DDos) describes the goal of a class of cyber-attacks designed to render a service inaccessible
DHS	The US Department of Homeland Security

DHS S&T	US Department of Homeland Security Science and Technology Directorate
DSIT	Department for Science, Innovation & Technology
ECSO	European Cyber Security Organisation
EDPB	European Data Protection Board
ENISA	European Union Agency for Cybersecurity
GDP	Gross Domestic Product
IoT	The Internet of Things describes physical objects with sensors, processing ability and software that connect and exchange data with other devices and systems over the Internet or other communications networks
IPT	Intelligent Public Transport
KISA	Korean Internet & Security Agency
NCCA	Germany's 'National Cybersecurity Certification Authority'
NCSC	The UK's 'National Cyber Security Centre'
NCSI	National Cyber Security Index
NIST	The US 'National Institute of Standards and Technology'
OEMs	Original Equipment Manufacturers
OT	Operational Technology (OT) is defined as technology that interfaces with the physical world and includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS)
OTI	New York's 'Office of Technology and Innovation'
Personally Identifiable Information (PII)	Information that relates to an identified or identifiable person. This can be name, phone number, IP address etc. If it is possible to identify an individual from the information, then it may be personal information
PKI	A Public Key Infrastructure (PKI) is used to confirm identity. It does this by proving ownership of a private key. It is a 'trust service' which can be used to verify that a sender or receiver of data is exactly who they claim to be.
SCADA	Supervisory control and data acquisition is a control system architecture (SCADA) that comprises computers, networked data communications and graphical user interfaces for high-level supervision of machines and processes
SCI	Smart City Index
Secure connected places	The area of policy seeking to mitigate the cyber risks of connected places and promote the secure adoption of connected technologies. It is noted that this is specifically used in UK policy, rather than globally

SOCs	Security Operation Centres
Supply chain	The system of people and things that are involved in getting a product from production to the buyer
System	A group of people, processes and technologies that conform to a policy to achieve a desired objective
System approach	A philosophy that considers a problem as the result of (or to be solved by) a system
TRA	UAE Telecommunications Regulatory Authority
UAE	United Arab Emirates
US	United States of America

C. Figures

D. Bibliography

[1] 'National Cyber Strategy 2022 - GOV.UK'. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 (accessed Mar. 21, 2023).

[2] 'Secure connected places - GOV.UK', 2022. https://www.gov.uk/guidance/secure-connected-places (accessed Mar. 22, 2023).

[3] 'What is cyber security? - NCSC.GOV.UK'. https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security (accessed Mar. 20, 2023).

[4] E-Governance Academy, 'National Cyber Security Index', 2021. https://ncsi.ega.ee/ (accessed Feb. 13, 2023).

[5] International Institute for Management Development, 'Smart City Index 2021', 2021. Accessed: Feb. 13, 2023. [Online]. Available: https://www.imd.org/smart-city-observatory/home/

[6] 'UK connected places survey - GOV.UK', 2022. https://www.gov.uk/government/publications/uk-connected-places-survey (accessed Mar. 22, 2023).

[7] 'Cyber Assessment Framework - NCSC.GOV.UK'. https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework (accessed Mar. 22, 2023).

[8] 'About Cyber Essentials - NCSC.GOV.UK'. https://www.ncsc.gov.uk/cyberessentials/overview (accessed Mar. 22, 2023).

[9] 'Connected Places Cyber Security Principles - NCSC.GOV.UK'. https://www.ncsc.gov.uk/collection/connected-places-security-principles (accessed Mar. 22, 2023).

[10] City of Vienna, 'Smart City Wien - Framework Strategy', 2013. Accessed: Mar. 28, 2023. [Online]. Available: https://www.wien.gv.at/stadtentwicklung/studien/pdf/b008384b.pdf

[11] '5 recommendations for securely purchasing cloud services | Factsheet | National Cyber Security Centre'. https://english.ncsc.nl/publications/factsheets/2020/december/31/factsheet-5-recommendations-for-securely-purchasing-cloud-services (accessed Mar. 20, 2023).

[12] 'Six steps toward more secure cloud computing | Federal Trade Commission'. https://www.ftc.gov/business-guidance/blog/2020/06/six-steps-toward-more-secure-cloud-computing (accessed Mar. 20, 2023).

[13] 'Security in the Internet of Things (IoT)'. https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-behoerden/aktuelle-themen/massnahmen-schutz-iot.html (accessed Feb. 13, 2023).

[14] 'Security of IoT devices – NC3'. https://nc3.go.ke/resources/security-of-iot-devices/ (accessed Feb. 13, 2023).

[15] 'Best Practice Reducing cyber security risks in video surveillance cameras | Israel National Cyber Directorate'. https://www.gov.il/en/departments/policies/iotcameras (accessed Feb. 20, 2023).

[16] 'Regulatory Policy Internet of Things IoT', Accessed: Mar. 28, 2023. [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwic9N-Krf79AhWNRsAKHXZQBzcQFnoECBAQAQ&url=https%3A%2F%2Ftdra.gov.ae%2F-%2Fmedia%2FAbout%2Fregulations-and-ruling%2FEN%2FRegulatory-Policy---Internet-of-Things--IoT--pdf.ashx&usg=AOvVaw3BHGXXjkcrjMryvwXRwluA

[17] 'Regulating the Internet of Things in the UAE - PwC Middle East'. https://www.pwc.com/m1/en/publications/regulating-the-internet-of-things-in-the-uae.html (accessed Feb. 16, 2023).

[18] 'IoT Regulatory Framework - National Telecom Regulatory Authority'. https://www.tra.gov.eg/en/regulations/regulatory-framework/iot-regulatory-framework/ (accessed Mar. 07, 2023).

[19] 'Roadmap for Digital Hard- and Software Security | Publication | The Netherlands at International Organisations'. https://www.permanentrepresentations.nl/documents/publications/2020/01/06/roadmap-for-digital-hard--and-software-security (accessed Feb. 13, 2023).

[20] A. van Twist, E. Ruijer, and A. Meijer, 'Smart cities & citizen discontent: A systematic review of the literature', *Government Information Quarterly*. Elsevier Ltd, 2023. doi: 10.1016/j.giq.2022.101799.

[21] 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement | European Data Protection Board'. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en (accessed Mar. 08, 2023).

[22] 'BSI - Consumer IoT - Consumer IoT'. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Consumer-IoT/Consumer-IoT.html (accessed Feb. 27, 2023).

[23] 'SMART AND SECURE CITIES AND COMMUNITIES CHALLENGE (SC3) A Risk Management Approach to Smart City Cybersecurity and Privacy A Guidebook from the Cybersecurity and Privacy Advisory Committee (CPAC) Public Working Group', 2019.

[24] Korea Legislation Research Institute, 'Statutes of the Republic of Korea', 2018. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=50634&lang=ENG (accessed Mar. 28, 2023).

[25] 'Homepage: The Progress & Achievements of Saudi Arabia - Vision 2030'. https://www.vision2030.gov.sa/ (accessed Feb. 20, 2023).

[26] National Cybersecurity Authority, 'Critical Systems Cybersecurity Controls', 2019. Accessed: Mar. 28, 2023. [Online]. Available: https://nca.gov.sa/files/cscc-en.pdf

[27] J. Lim, 'Korea's Smart City Policy & Strategies', 2019, Accessed: Feb. 15, 2023. [Online]. Available: https://www.cica.net/wp-content/uploads/2019/06/Korea_s-smart-city-policy-and-strategies-1.pdf

[28] 'Building a Green and Smart City in Indonesia's New Capital | SEADS'. https://seads.adb.org/news/building-green-and-smart-city-indonesias-new-capital (accessed Mar. 22, 2023).

[29] D. I. Sensuse, P. A. W. Putro, R. Rachmawati, and W. D. Sunindyo, 'Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology', *Information 2022, Vol. 13, Page 580*, vol. 13, no. 12, p. 580, Dec. 2022, doi: 10.3390/INFO13120580.

[30] 'Austrian Strategy for Cybersecurity 2021', 2021. Accessed: Mar. 28, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

[31] 'The Prague Proposals The Chairman Statement on Cyber Security of Emerging and Disruptive Technologies Prague 5G Security Conference 2021'.

[32] H. Svecova, 'Design of a Method for Setting IoT Security Standards in Smart Cities', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13475 LNCS, pp. 118–128, 2022, doi: 10.1007/978-3-031-14391-5_9.

[33] Canadian Security Intelligence Service, 'Smart Cities and National Security', Accessed: Feb. 20, 2023. [Online]. Available: https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/Canadian_Smart%20Cities_EN_Digital_ISBN_A.pdf

[34] 'An Introduction to Securing Smart Places | Cyber.gov.au'. https://www.cyber.gov.au/acsc/view-all-content/publications/introduction-securing-smart-places (accessed Feb. 20, 2023).

[35] Ministry of Internal Affiars and Communications, 'Smart City Security Guideline (Ver 1.0)', 2020, Accessed: Feb. 15, 2023. [Online]. Available: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Smart_City_Security_Guideline_ver1.0.pdf

[36] Ministry of Internal Affiars and Communications, 'Smart City Security Guidelines v 2.0', 2021. Accessed: Mar. 28, 2023. [Online]. Available: https://www.soumu.go.jp/main_content/000757799.pdf

[37] 'Japan: MIC publishes revised Smart City Security Guidelines | News post | DataGuidance'.

https://www.dataguidance.com/news/japan-mic-publishes-revised-smart-city-security (accessed Mar. 08, 2023).

[38] Cybersecurity & Infrastructure Security Agency, 'Trust in Smart City Systems: Characteristics and Key Considerations', 2020, Accessed: Feb. 13, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Trust%20in%20Smart%20City%20Systems%20Report_0.pdf

[39] B. and C. Federal Ministry of the Interior, 'Cyber Security Strategy for Germany 2021', 2021, Accessed: Feb. 27, 2023. [Online]. Available: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf?__blob=publicationFile&v=4

[40] 'BSI - Bundesamt für Sicherheit in der Informationstechnik - Große Smart-City-Studie zu IoT-Infrastrukturen in acht deutschen Städten (archiviert)'. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/Smart-City-Studie_140720.html (accessed Mar. 22, 2023).

[41] 'BSI - Smart City - Smart City'. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Smart-City/smart-city.html (accessed Mar. 22, 2023).

[42] 'BSI - Smart City - Smart City'. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Smart-City/smart-city.html (accessed Mar. 28, 2023).

[43] 'Smart City Dialog - Herzlich Willkommen!' https://www.smart-city-dialog.de/en/startseite-en (accessed Mar. 22, 2023).

[44] 'Cybersecurity testing and certification for consumer IoT products | BSI'. https://www.bsigroup.com/en-GB/industries-and-sectors/internet-of-things/IoT-Assurance-Services/consumer-iot-verification/ (accessed Mar. 21, 2023).

[45] 'BSI - Consumer IoT - Consumer IoT'. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Consumer-IoT/Consumer-IoT.html (accessed Mar. 22, 2023).

[46] 'BSI - The German IT Security Act 2.0 - Second act on increasing the security of IT systems (German IT Security Act 2.0)'. https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig_2-0.html (accessed Mar. 22, 2023).

[47] 'Cybersecurity is a Key Driver of Smart City Markets - The Security Imperative - Issues - dotmagazine'. https://www.dotmagazine.online/issues/the-security-imperative/cybersecurity-smart-city (accessed Mar. 22, 2023).

[48] BRIC, 'Towards a Regional Cybersecurity Plan'. https://paradigm.brussels/en/news_publications/publications/papers/towards-a-regional-cybersecurity-plan-september-2018 (accessed Mar. 22, 2023).

[49] 'Newcastle City Council Smart City Strategy', 2017, Accessed: Mar. 22, 2023. [Online]. Available: www.newcastle.nsw.gov.au

[50] 'Smart city strategic framework - City of Sydney'. https://www.cityofsydney.nsw.gov.au/strategies-action-plans/smart-city-strategic-framework (accessed Mar. 22, 2023).

[51] 'Inside the Government Cybersecurity Landscape: Federal vs. State Level Challenges | Tripwire'. https://www.tripwire.com/state-of-security/government-cybersecurity-federal-state (accessed Mar. 22, 2023).

[52] City and County of San Francisco, 'Citywide Cybersecurity Policy Committee on Information Technology COIT Policy Dates', 2019, Accessed: Mar. 22, 2023. [Online]. Available: https://sf.gov/sites/default/files/2021-05/CCSF%20Cybersecurity%20Policy%20Final_2.pdf

[53] 'Cybersecurity - NYC Office of Technology and Innovation - OTI'. https://www.nyc.gov/content/oti/pages/cybersecurity (accessed Mar. 22, 2023).

[54] 'How "smart cities" push IoT cybersecurity for state and local IT | CSO Online'. https://www.csoonline.com/article/3196989/how-smart-cities-push-iot-cybersecurity-for-state-and-local-it.html (accessed Mar. 22, 2023).

[55] A. Audic, 'The Role of the Regions in strengthening the European Union's cyber security Position Paper', Accessed: Mar. 22, 2023. [Online]. Available: https://www.eurobits.de/wp-content/uploads/20190320_Regions_Position_Paper_approved.pdf

[56] 'The Presidential Committee on the 4th Industrial Revolution | STIP Compass'. https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2021%2Fdata%2FpolicyInitiatives%2F16688 (accessed Mar. 28, 2023).

[57] Korea Internet & Security Agency, 'Smart City Security Model', 2020. https://www.kisa.or.kr/EN/302/form?postSeq=62&page=1#fnPostAttachDownload (accessed Feb. 15, 2023).

[58] 'Keep It Secure | Infopole'. https://clusters-wallonie-be.translate.goog/infopole/fr/projets/keep-it-secure?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-GBhttps://clusters-wallonie-be.translate.goog/infopole/fr/projets/keep-it-secure?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-GB (accessed Mar. 28, 2023).

[59] 'Test bed: Turning Kigali into Africa's smart cities hub - edie'. https://www.edie.net/test-bed-turning-kigali-into-africas-smart-cities-hub/ (accessed Mar. 22, 2023).

[60] Rich Rafi, Westerberg Pontus, and Torner Javier, 'Smart City Rwanda Masterplan', Accessed: Mar. 28, 2023. [Online]. Available: https://unhabitat.org/sites/default/files/documents/2019-05/rwanda_smart_city-master_plan.pdf

[61] 'Global Cybersecurity Index'. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed Mar. 22, 2023).

[62] 'IVORY COAST: Dassault prepares the transformation of Plateau into a smart city | Afrik 21'. https://www.afrik21.africa/en/ivory-

coast-dassault-prepares-the-transformation-of-plateau-into-a-smart-city/ (accessed Mar. 22, 2023).

[63] 'Standards & Policies - DESC'. https://www.desc.gov.ae/regulations/standards-policies/ (accessed Mar. 22, 2023).

[64] 'Smart Specialisation Strategy (S3)', 2020, Accessed: Mar. 28, 2023. [Online]. Available: https://www.interregeurope.eu/sites/default/files/inline/Smart_Specialisation_Strategy__S3__-_Policy_Brief.pdf

[65] 'SPARTA'. https://www.sparta.eu/about/#SPARTA (accessed Mar. 28, 2023).

[66] The White House, 'National Cybersecurity Strategy', 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (accessed Mar. 22, 2023).

[67] 'New York opens joint cybersecurity center to serve state and city needs | StateScoop'. https://statescoop.com/new-york-opens-joint-cybersecurity-center-state-local/ (accessed Mar. 22, 2023).

[68] 'Cybersecurity Clinic | Social Cyberdefense of Critical Urban Infrastructure'. http://urbancyberdefense.mit.edu/cybersecurityclinic (accessed Mar. 22, 2023).

[69] 'A Consensus Framework for Smart City Architectures IES-City Framework (Internet-of-Things-Enabled Smart City Framework) Release v1.0 20180930', 2018.

[70] W. Barkis, 'The Municipal IoT Blueprint. The Municipal Internet of Things (IoT) Blueprint', 2019, Accessed: Mar. 22, 2023. [Online]. Available: https://pages.nist.gov/GCTC/super-clusters/

[71] CISA, 'Trust in Smart City Systems: Characteristics and Key Considerations', 2020, Accessed: Mar. 22, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Trust%20in%20Smart%20City%20Systems%20Report_0.pdf

[72] C. Lévy-Bencheton, Eleni. Darra, and European Union. European Network and Information Security Agency., *Cyber security for smart cities : an architecture model for public transport*. ENISA, 2015.

[73] A. Ertan, K. Floyd, P. Pernik, and T. Stevens, 'Cyber Threats and NATO 2030: Horizon Scanning and Analysis', 2020, Accessed: Mar. 08, 2023. [Online]. Available: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

[74] G20 Smart Cities Alliance, 'Resource Library'. https://www.globalsmartcitiesalliance.org/resources# (accessed Mar. 08, 2023).

[75] D. Nikurikiyimfura, 'Smart Africa & Smart Cities Initiative'. http://media.firabcn.es/content/S078018/download/14NOV_GF_EGOV_KN2.pdf (accessed Mar. 10, 2023).

[76] 'Blueprints – Smart Africa'. https://smartafrica.org/blueprint/ (accessed Mar. 10, 2023).

[77] 'Secure by Design - UK-Singapore IoT Statement - GOV.UK'. https://www.gov.uk/government/news/secure-by-design-uk-singapore-iot-statement (accessed Mar. 07, 2023).

[78] 'ISO - ISO/IEC 27001 and related standards — Information security management'. https://www.iso.org/isoiec-27001-information-security.html (accessed Mar. 08, 2023).

[79] 'ISO/IEC 30145-1:2021(en), Information technology — Smart City ICT reference framework — Part 1: Smart city business process framework'. https://www.iso.org/obp/ui/#iso:std:iso-iec:30145:-1:ed-1:v1:en (accessed Mar. 09, 2023).

[80] 'ISO - ISO 37156:2020 - Smart community infrastructures — Guidelines on data exchange and sharing for smart community infrastructures'. https://www.iso.org/standard/69242.html (accessed Mar. 09, 2023).

[81] 'ISO - ISO/IEC 30141:2018 - Internet of Things (IoT) — Reference Architecture'. https://www.iso.org/standard/65695.html (accessed Mar. 09, 2023).

[82] 'ISO - ISO/IEC 27400:2022 - Cybersecurity — IoT security and privacy — Guidelines'. https://www.iso.org/standard/44373.html (accessed Mar. 09, 2023).

[83] 'ISO - ISO/IEC 17789:2014 - Information technology — Cloud computing — Reference architecture'. https://www.iso.org/standard/60545.html (accessed Mar. 09, 2023).

[84] 'ISO - ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors'. https://www.iso.org/standard/76559.html (accessed Mar. 09, 2023).

[85] 'ISO/IEC TS 27570:2021(en), Privacy protection — Privacy guidelines for smart cities'. https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27570:ed-1:v1:en (accessed Mar. 09, 2023).

[86] 'ISO - ISO 37155-1:2020 - Framework for integration and operation of smart community infrastructures — Part 1: Recommendations for considering opportunities and challenges from interactions in smart community infrastructures from relevant aspects through the life cycle'. https://www.iso.org/standard/69241.html (accessed Mar. 08, 2023).

[87] T. and I. Ministry of Economy, 'New International Standards for Framework for Development and Operation of Smart City Infrastructures Issued', 2021. https://www.meti.go.jp/english/press/2021/0708_002.html (accessed Feb. 15, 2023).

[88] 'About ASEAN - ASEAN Main Portal'. https://asean.org/about-asean (accessed Mar. 09, 2023).

[89] 'Industries to Watch Out for Growth in Southeast Asia in 2023'. https://www.aseanbriefing.com/news/industries-to-watch-out-for-growth-in-southeast-asia-in-2023/ (accessed Mar. 09, 2023).

[90] Cyber Security Agency of Singapore, *The Singapore cybersecurity strategy 2021*. Accessed: Mar. 27, 2023. [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjk0bHQl_z9AhXWiVwKHa6kCMgQFnoECAoQAQ&url=https%3A%2F%2Fwww.csa.gov.sg%2FTips-Resource%2Fpublications%2F2021%2Fsingapore-cybersecurity-strategy-2021&usg=AOvVaw2pWuZqZP5cBXhniVD-vgF7

[91] 'ASEAN Regional Forum'. https://aseanregionalforum.asean.org/about-arf/ (accessed Mar. 09, 2023).

[92] 'Strategic Plan 2016-2025 - ASEAN Main Portal'. https://asean.org/our-communities/economic-community/standard-and-conformance/strategic-plan-2016-2025/ (accessed Mar. 09, 2023).

[93] 'ASEAN Cybersecurity Cooperation Strategy', 2021. Accessed: Mar. 28, 2023. [Online]. Available: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

[94] '32nd ASEAN Summit - ASEAN Main Portal'. https://asean.org/32nd-asean-summit/ (accessed Mar. 10, 2023).

[95] ASEAN Smart Cities Network, 'ASEAN Smart Cities Framework', 2018, Accessed: Mar. 10, 2023. [Online]. Available: https://asean.org/wp-content/uploads/2019/02/ASCN-ASEAN-Smart-Cities-Framework.pdf

[96] 'Outcomes of the 15th ASEAN-Japan Cybersecurity Policy Meeting'. https://www.meti.go.jp/english/press/2022/1006_002.html (accessed Mar. 07, 2023).

[97] '"JP-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region" was Held'. https://www.meti.go.jp/english/press/2022/1031_001.html (accessed Mar. 21, 2023).

[98] 'Digital Cities Index 2022 – Homepage – Economist Impact'. https://impact.economist.com/projects/digital-cities/?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18156330227&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclid=CjwKCAjwiOCgBhAgEiwAjv5whEQ5_GTbKvxmImy73ECaauKEUE84ZKab8sgTSIAkazQOsztrIoho0xoCE-cQAvD_BwE&gclsrc=aw.ds (accessed Mar. 20, 2023).

[99] NIST, 'Global City Teams Challenge', 2021. https://www.nist.gov/ctl/smart-connected-systems-division/iot-devices-and-infrastructure-group/smart-americaglobal-0 (accessed Mar. 28, 2023).

E. About Plexal

Plexal is the innovation company solving society's challenges through collaboration with government, startups and industry. The business is closing the gap between organisations – small and large, local and global, private and public – and working towards a common goal: using science and technology to deliver national security and prosperity. It was founded in 2017 as the innovation centre at Here East and is owned by clients of specialist real estate investment advisory company Delancey.

Providing bespoke consultancy services and state-of-the-art workspaces for over 1,000 innovators, Plexal sources the right partners from our ecosystem of 15,000 connections. It supports entrepreneurs, startups and scaleups building emerging technologies and operates across multiple sectors including cyber, healthcare, intelligence and defence, government, public safety, financial services and telecoms.

Expanding on its existing presence in London and Manchester, Plexal acquired a majority shareholding in Hub8 – the Cheltenham network of co-working spaces for cyber-tech, digital and creative startups and SMEs. This is part of an ongoing mission to build the UK's most connected cyber ecosystem, with GCHQ's more than 70-year heritage in Cheltenham.

Plexal delivers projects for key government departments and global tech companies including the National Cyber Security Centre, Department for Science, Innovation and Technology, Foreign, Commonwealth and Development Office, Amazon Web Services and IBM. The NCSC For Startups alumni of over 60 companies has collectively raised over £430m and created over 700 jobs, while 72 cyber startups that have gone through Plexal's LORCA accelerators have collectively raised over £300m, generated more than £68m in revenue and hired over 800 people.

plexal on behalf of Department for Science, Innovation, & Technology

www.plexal.com
Registered address: c/o Delancey, 6th Floor, Lansdowne House, Berkeley Square, London, W1J 6ER
Trading Address: 14 East Bay Lane, The Press Centre, Here East, Queen Elizabeth Olympic Park, London, E15 2GW
Company Number: 10012478 © 2023.
All rights reserved.