Submodule C:
Internet of Things
Frontier ICTs for Sustainable Development for Digital Leaders

Submodule C: Internet of Things
Academy of ICT Essentials for Government Leaders

Frontier ICTs for Sustainable Development for Digital Leaders

This work is available open access by complying with the Creative Commons license created for inter-governmental organizations, available at:

http://creativecommons.org/licenses/by/3.0/igo/

Publishers must remove the United Nations emblem from their edition and create a new cover design. Translations must bear the following disclaimers: “The present work is an unofficial translation for which the publisher accepts full responsibility.” Publishers should email the file of their edition to apcict@un.org

Photocopies and reproductions of excerpts are allowed with proper credits.

Disclaimers: The views expressed herein are those of the authors, and do not necessarily reflect the views of the United Nations. This publication has been issued without formal editing, and the designations employed, and material presented do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Mention of firm names and commercial products does not imply the endorsement of the United Nations.

Correspondence concerning this report should be addressed to the email: apcict@un.org

Copyright © United Nations 2022
All right reserved
Printed in Republic of Korea
ST/ESCAP/3045

Cover design: Barbara Kempton and Zihao Zhen

Contact:
Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT/ESCAP)
5th Floor G-Tower, 175 Art Center Daero
Yeonsu-gu, Incheon, Republic of Korea
Tel +82 32 458 6650
Email: apcict@un.org
ACKNOWLEDGEMENT

The Academy of ICT Essentials for Government Leaders: Frontier ICTs for Sustainable Development for Digital Leaders was developed under the overall guidance of Kiyoung Ko, Director of Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT). Module development was coordinated by Hyangsk Seong.

The module was written by Sukkyoung Kim. Rashad Aliyev Abulfazan-khva and Ronny Estrella Conza provided substantive assistance. The publication benefited from valuable advice and comments provided by experts during the review meeting of the draft module, held virtually on 1 April 2022: Asomiddin Atoev, Rustam Gadzhiev, Sang-yirl Nam, Yudho Sucahyo, and Saleem Zougbi. Suggestions were also received from national partners from Armenia, Lao People’s Democratic Republic, and Turkmenistan.

The following ESCAP staff members contributed with substantive inputs and suggestions: Jonathan Tsuen Yip Wong and Tengfei Wang of the Trade, Investment and Innovation Division, Tae Hyung Kim and Chang Yong Son of the ICT and Disaster Risk Reduction Division.

Cover design was created by Barbara Kempton and Zihao Zhen. Publication layout and proofreading was provided by Sara Bennouna and Amal Kadir. Joo-Eun Chung and Ho-Din Ligay undertook administrative processing necessary for the issuance of the module.
Submodule Overview:

The purpose of the whole module is to provide the technological overview and considerations, potential policy recommendations, and international cooperation agenda for the adoption of frontier ICTs for digital leaders in developing countries to unlock the full potential of frontier ICTs.

In this purpose, the entire module consists of an overview of Frontier ICTs and three submodules. In the future, new submodules can be added as needed to cover new emerging technologies.

The overview module covers the definition, scope, and common features of frontier ICTs, as well as barriers and risks of scaling frontier ICTs. It also covers the key areas for policymaking and international cooperation that policymakers should consider from a national perspective for the promotion and development of frontier ICTs.

The submodules address three technologies, i.e. Artificial intelligence, Blockchain, and the Internet of Things, respectively. Each submodule provides an overview of the technology, the impact of the technology on the Sustainable Development Goals, challenges and risks, the status of the technology-related policies. Cases are also reviewed, drawing on policy recommendations and international cooperation agenda for maximizing the development and utilization of the technology.

This submodule covers IoT which is recognized as an important means of achieving the 2030 Sustainable Development Goals (SDGs) agenda. However, the use, adoption, and adaptation of the technology are not the same in all countries around the world.

IoT is expected to have a greater impact on sustainable development and is also recognized as an important source of concerns for socio-economic development (especially policymaking) in developing countries.

Therefore, this submodule provides fundamental information, challenges/risks, best practices, policy recommendations, and international cooperation agendas related to IoT that policymakers in developing countries should consider when developing and applying IoT to enable sustainable development through innovation in their public sector and society.

Objectives

The main objective of the submodule is to provide relevant information, cases, policy recommendations, and international cooperation agenda(s) to enable national policymakers to properly apply IoT in achieving the SDGs.

Specifically, this module aims to:

1. Introduce the definition, scope, and features of IoT.
2. Examine the role and importance of IoT in achieving the SDGs.
3. Provide major challenges, barriers, and risks to be considered in developing and introducing IoT.
4. Provide the current status of policies related to IoT and global cases applied in the public sector.
5. Suggest policy recommendations and international cooperation measures for effective and efficient development and application of IoT. This promotes a better understanding of the goals and direction for government policymakers to pursue.

**Learning outcomes**

After working on this submodule, readers should be able to:

1. Promote a better understanding of IoT as well as an overall understanding of frontier ICTs.
2. Provide a rationale for the use of IoT to achieve the SDGs.
3. Understand challenges and risks in the effective and efficient application of IoT for sustainable development and measures to address it.
4. Promote a better understanding of where IoT can be applied and the conditions and methods for success.
5. Identify key policy directions and measures to consider in the development, application, and deployment of IoT for sustainable development.
6. Provide the ideas for international/regional cooperation to accelerate the application of IoT to countries.

**Target Audience**

This submodule was developed for digital leaders in developing countries interested in IoT. This submodule provides digital leaders the general and comprehensive knowledge they need to understand from a technical and policy perspective for the use, adoption, and application of IoT. The target audience of this submodule can include people who wish to solve problems facing the country by utilizing IoT, establish related strategies or plans to maximize the use of IoT, or have a holistic view of IoT at the government level.

**Analytical Framework**

In order for policymakers to clearly understand the various issues surrounding the development, application, and deployment of frontier ICTs, this module examines the issues in technological, economic, social, and environmental dimensions, and
suggests policy recommendations to address the issues. These four dimensions reflect the technical features of frontier ICTs and three pillars of SDGs.

- **Technical features of frontier ICTs:** Although there are common characteristics that penetrate frontier ICTs, each technology has distinctive features. Therefore, it is necessary to examine technical issues related to the inherent nature of each frontier ICT such as AI, blockchain, and IoT.

- **Three pillars of SDGs:** As shown in Figure 1, the 17 goals of the SDG are broadly divided into three main categories or pillars: Society, Economy, and Environment. Although frontier ICTs are expected to have significant positive impacts on the SDGs, they are expected to have negative impacts on some SDGs depending on the technical features and readiness. Therefore, it is necessary to examine issues and considerations for each domain to ensure balanced and sustainable development at the social, economic, and environmental levels.

**Figure 1 Categorization of the SDGs into the Society, Economy, and Environment groups**


Following the description above, this module suggests and uses a TESE (Technological, Economic, Social, Environmental) framework that synthesizes the technical features of frontier ICTs and the three main pillars of SDGs so that digital leaders can identify considerations and potential policy recommendations related to frontier ICTs in a systematic way. Based on the policy recommendations derived in this way, digital leaders can establish policies, plans, and regulations related to frontier ICTs that are suitable for the environment and situation of the country.
**Table 1 TESE (Technological, Economic, Social, Environmental) framework**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Considerations</th>
<th>Policy Directions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technological</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**A Suggestion for Learners**

Each technology (AI, blockchain, IoT) is covered in a structured manner with an intentional order. This order and structure are intended to help and direct the learner not only to absorb the material, but also to practice a sequence of practical steps leading to drafting a policy recommendation agenda which can then be helpful in guiding policy development planning. In each part, a sequence of five preparatory steps (Technology overview, Opportunities for sustainable development, Considerations, Policy, Case studies) lead toward two steps of forming corresponding recommendations (Policy recommendations, International cooperation opportunities). Therefore, it would be most beneficial if readers, after each step, reproduce a similar process and results within the context of their own country.

Because this submodule is not intended for any specific region, digital leaders should consider their country's social and economic context when formulating policies related to frontier ICTs.
TABLE OF CONTENTS

Submodule Overview: .................................................................................................................. ii

Objectives .................................................................................................................................................. ii

Learning outcomes ............................................................................................................................... iii

Target Audience ....................................................................................................................................... iii

Analytical Framework ............................................................................................................................. iii

A Suggestion for Learners ....................................................................................................................... v

LIST OF FIGURES ................................................................................................................................. vii

LIST OF TABLES ....................................................................................................................................... vii

ABBREVIATIONS AND ACRONYMS ................................................................................................... ix

1. IoT overview .......................................................................................................................................... 1
   1.1. Internet of Things defined ....................................................................................................... 1
   1.2. Key characteristics & main technologies .................................................................................. 6
   1.3. Current status ............................................................................................................................ 7
   1.4. IoT in government ...................................................................................................................... 11

2. Opportunities for sustainable development ....................................................................................... 15
   2.1. IoT and societal outcomes ...................................................................................................... 15
   2.2. IoT and economic outcomes ................................................................................................... 15
   2.3. IoT and environmental outcomes ............................................................................................ 15

3. Considerations for using IoT ............................................................................................................... 17
   3.1. Taxonomy of challenges in IoT adoption .................................................................................. 17
   3.2. Risks inherent to IoT ................................................................................................................ 18
   3.3. Common challenges in IoT adoption ....................................................................................... 20
   3.4. Challenges for IoT adoption in developing countries ............................................................... 22
   3.5. Stages of IoT development ....................................................................................................... 24

4. IoT-related policy ................................................................................................................................. 26
   4.1. Global IoT policy highlights .................................................................................................... 26
   4.2. National IoT policies & strategies: current status ................................................................. 29
   4.3. National IoT policies & strategies: examples ......................................................................... 30

5. Case studies in the public sector ....................................................................................................... 39
   5.1. IoT usage and typical IoT application in the public sector ..................................................... 39
5.2. Case studies in the public sector from OECD OPSI ............................................ 40

6. Policy recommendations ................................................................................................. 41
   6.1. Mapping of IoT considerations to policy directions .................................................. 42
   6.2. Policy implications from national IoT strategy analysis ......................................... 43
   6.3. Policy implications from IoT use-case analysis ...................................................... 45
   6.4. Recommended policy directions .............................................................................. 45

7. International cooperation opportunities .......................................................................... 51

Annex 1. Examples of IoT and sustainable development .................................................... 54
   1. Opportunities for sustainable development ................................................................. 54
   2. Potential for a negative impact on sustainable development ........................................ 58

Annex 2. Case Studies of IoT based on OECD OPSI ........................................................ 60

LIST OF FIGURES

Figure 1 Categorization of the SDGs into the Society, Economy, and Environment groups ........................................................................................................ iv
Figure 2 The Internet of Things from connecting devices to human value ................................. 2
Figure 3 IoT Architecture .................................................................................................. 5
Figure 4 Top 10 IoT application areas 2020 ........................................................................ 8
Figure 5 Internet of Things (IoT) market - growth rate by region ......................................... 8
Figure 6 The market concentration of IoT ........................................................................ 10
Figure 7 The framework of IoT integrated into the government ........................................... 12
Figure 8 Key differences between IoT and traditional digital systems ................................. 19
Figure 9 The level of IoT risk within the three main domains ............................................ 22
Figure 10 IoT risk level by region, domain, and impact ....................................................... 24
Figure 11 Process map for IoT project initiation ................................................................ 25
Figure 12 IoT governance level by region, domain, and impact area .................................. 28
Figure 13 The gap between IoT risks and the governance ................................................... 38
Figure 14 The gap scores of IoT governance within the three main domains ....................... 42
Figure 15 Collaborating for IoT safety and security ............................................................... 47

LIST OF TABLES

Table 1 TESE (Technological, Economic, Social, Environmental) framework ..................... v
Table 2 Summary of IoT-related policy initiatives in China ................................................... 31
Table 3 Summary of IoT-related policy initiatives in Japan .................................................. 33
Table 4 Summary of IoT-related policy initiatives in the Republic of Korea ....................... 35
Table 5 Summary of IoT-related policy initiatives in Singapore ......................................... 37
Table 6 Examples of IoT applications .................................................................................. 39
Table 7 IoT applications in the public sector ....................................................................... 40
Table 8 IoT adoption cases in the public sector from OECD OPSI .......................... 40
Table 9 Summary of IoT considerations and policy directions using TESE framework.
........................................................................................................................................... 42
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4S</td>
<td>Safematics Smart Safety System</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AR</td>
<td>Augmented Reality</td>
</tr>
<tr>
<td>BFSI</td>
<td>Banking, Financial Services, and Insurance</td>
</tr>
<tr>
<td>CIFAR</td>
<td>Canadian Institute for Advanced Research</td>
</tr>
<tr>
<td>dapps</td>
<td>decentralized applications</td>
</tr>
<tr>
<td>DPOS</td>
<td>Delegated Proof of Stake</td>
</tr>
<tr>
<td>ESCAP</td>
<td>Economic and Social Commission for Asia and the Pacific</td>
</tr>
<tr>
<td>ETDA</td>
<td>Electronic Transactions Development Agency</td>
</tr>
<tr>
<td>FTS</td>
<td>Federal Tax Service</td>
</tr>
<tr>
<td>GDP</td>
<td>Gross Domestic Product</td>
</tr>
<tr>
<td>GPT</td>
<td>General-Purpose Technologies</td>
</tr>
<tr>
<td>HIAS</td>
<td>Hebrew Immigrant Aid Society</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technologies</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Intellectual Property</td>
</tr>
<tr>
<td>IPGAIN</td>
<td>IP Global Artificial Intelligence Network</td>
</tr>
<tr>
<td>MIT</td>
<td>Massachusetts Institute of Technology</td>
</tr>
<tr>
<td>ML</td>
<td>Machine Learning</td>
</tr>
<tr>
<td>MOORE</td>
<td>Matching for Outcome Optimization and Refugee Empowerment</td>
</tr>
<tr>
<td>MSIT</td>
<td>Ministry of Science and ICT</td>
</tr>
<tr>
<td>MUAS</td>
<td>Munich University of Applied Sciences</td>
</tr>
<tr>
<td>NITI</td>
<td>National Institution for Transforming India</td>
</tr>
<tr>
<td>NLP</td>
<td>Natural language processing</td>
</tr>
<tr>
<td>OAI</td>
<td>Office for Artificial Intelligence</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OPSI</td>
<td>Observatory of Public Sector Innovation</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-Peer</td>
</tr>
<tr>
<td>PoS</td>
<td>Proof of Space</td>
</tr>
<tr>
<td>PoS</td>
<td>Proof of Stake</td>
</tr>
<tr>
<td>PoW</td>
<td>Proof of Work</td>
</tr>
<tr>
<td>QLUMP</td>
<td>The Queensland Land Use Mapping Program</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>RFIT</td>
<td>Reducing Friction in Trade</td>
</tr>
<tr>
<td>RL</td>
<td>Reinforcement Learning</td>
</tr>
<tr>
<td>RPA</td>
<td>Robotic Process Automation</td>
</tr>
<tr>
<td>SDGs</td>
<td>Sustainable Development Goals</td>
</tr>
<tr>
<td>SMEs</td>
<td>Small Medium Enterprises</td>
</tr>
<tr>
<td>STEM</td>
<td>Science, Technology, Engineering, and Mathematics</td>
</tr>
<tr>
<td>STI</td>
<td>Science, Technology, and Innovation</td>
</tr>
<tr>
<td>UK</td>
<td>The United Kingdom</td>
</tr>
<tr>
<td>UN</td>
<td>The United Nations</td>
</tr>
<tr>
<td>UNCTAD</td>
<td>The United Nations Conference on Trade and Development</td>
</tr>
<tr>
<td>UNESCO</td>
<td>The United Nations Educational, Scientific and Cultural Organization</td>
</tr>
<tr>
<td>UNICEF</td>
<td>United Nations Children's Fund</td>
</tr>
<tr>
<td>USA</td>
<td>The United States of America</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>USD</td>
<td>US Dollar</td>
</tr>
<tr>
<td>VR</td>
<td>Virtual Reality</td>
</tr>
<tr>
<td>WEF</td>
<td>The World Economic Forum</td>
</tr>
<tr>
<td>WFP</td>
<td>World Food Programme</td>
</tr>
<tr>
<td>XAI</td>
<td>Explainable AI</td>
</tr>
<tr>
<td>XR</td>
<td>Mixed Reality</td>
</tr>
</tbody>
</table>
1. IoT overview

Around the world, there are 7.6 billion active IoT devices, and this number is expected to grow to 24.1 billion by 2030\(^1\). IoT is an emerging technology and offers several benefits to the global society. It allows dynamic data gathering, analytics-based decisions, and automatic actions in the physical world. IoT works in combination with other technologies such as Cloud Computing, Big Data, and Artificial Intelligence\(^2\). The integration of IoT and other technologies enables the creation of applications relevant to major economic sectors like health, education, agriculture, transportation, manufacturing, energy, and others. IoT also contributes to the improvement of citizens’ quality of life and industry competitiveness. Therefore, IoT can work in favor of sustainable development and help countries accelerate their actions towards achieving the SDGs. However, to reach the true potential of IoT, it is essential to be aware of the various threats, technical and ethical issues surrounding this technology. These devices require a network connection that can be local to a specific area, an organization, or globally connected to the Internet.

This chapter is organized as follows:

- Chapter 1 covers an overview of IoT, key characteristics, current status, and potential government applications.
- Chapter 2 discusses the effects of IoT and its contribution to the SDGs.
- Considerations behind IoT adoption or development can be found in Chapter 3.
- Chapter 4 addresses the status of current policies and regulations relative to IoT.
- Use cases of IoT implementations are developed in Chapter 5.
- Recommendations of policy relative to IoT can be found in Chapter 6, and international opportunities for collaboration are explained in Chapter 7.

1.1. Internet of Things defined

Definition of IoT

The idea behind an intelligent communication object is not new. In the early 1990s, Xerox PARC proposed ideas about ubiquitous computing; they imagined the possibility of interconnecting specialized hardware and software elements through wires, radio waves, or infrared frequencies. Elements of communication were predicted to be ubiquitous, so people would not notice their presence\(^3\).

From a technical perspective, IoT is defined as a network of devices that communicate

\(^1\)Transforma Insights (2020, May 19). Global IoT market to grow to 24.1 billion devices in 2030, generating $1.5 trillion annual revenue. Available from https://transformainsights.com/iot-market-24-billion-usd15-trillion-revenue-2030

\(^2\)OECD (2016). The Internet of Things Seizing the Benefits and Addressing the Challenges (OECD DIGITAL ECONOMY PAPERS).

using a wireless or wired network. These devices can be connected and combined with cloud services to allow remote interaction and operation of different applications. However, since 2011, IoT has been used to describe different applications and developments where a “thing” is connected to the Internet. These days, almost everything can be connected to the Internet. IoT devices have micro-sensors or controllers that make them “smart.” This allows everyday devices to share data and communicate.

The main elements that allow IoT interaction are Cloud Computing, Big Data, machine-to-machine communications, sensors, and actuators. If we consider the different elements or impacts of IoT, the definition becomes complex. IoT can also be considered as a platform where different smart devices interact with each other. At the same time, IoT is a collective term referring to connected things, how these things communicate and spread data, the technologies behind them, and the goals to do that. Figure 2 shows how the interaction of IoT elements generates value to people through data collection and analysis.

Figure 2 The Internet of Things from connecting devices to human value


The International Telecommunications Union (ITU) defines IoT as a “global infrastructure for the information society that enables advanced services working as a link to connect physical and virtual world things based on existing and evolving,

---

interoperable information and communication technologies." The interoperability of multiple technologies (sensors, actuators, etc.) has allowed IoT to evolve and be defined as the Internet of Everything. This term refers to things connected to the internet and incorporates the possibility of monitoring environments, humans, animals, food, and much else that is not considered as a thing. Smart things have the ability to sense, record, interpret, communicate, process and act based on the data collected in the physical world.

This module will refer to IoT as the ecosystem that allows the interconnectivity and interoperability of devices that gather data on the internet or local networks to generate decisions or responses based on data. The next part of this chapter describes the key characteristics of IoT.

**Architecture and main technologies of IoT**

IoT is composed of different layers that form IoT architecture. These layers can be divided into four as shown in Figure 3, smart device/sensor, network/communication, service support and application support, and application layers.

**Smart Device/Sensor Layer**

This is a physical layer which provides IoT solutions with devices and sensors that allow the sensing and gathering of information from the environment.

- **Sensors:** In general terms, a sensor is an electronic device that generates data. In the case of IoT sensors, these devices sense changes in the physical environment and produce valuable data that will be transferred using the internet or network technologies. Sensors convert and process signals into understandable data. These days, most physical objects can have a sensor embedded in them. In the era of intelligent manufacturing or autonomous driving, different types and low-cost sensors are needed.

**Network/communication Layer**

The second layer is responsible for the interconnectivity of things, devices, and servers. The protocols in this layer allow the transmission and procession of data.

- **Network:** Network plays an essential role in IoT. It enables sensors to transmit or receive data over a network or the Internet. The network provides sensors with the ability to communicate with objects, machines, or things. Networks are categorized in terms of coverage, distance, range that a communication device...
can share with others. In addition, there are several communication protocols used for IoT communications (e.g. Wi-Fi, Bluetooth, Z-wave, Lora, NFC, others). In this category, it is also essential to consider additional infrastructure elements like datacenters, security protocols, services layers, and high-capacity computers (servers).

- **Cloud Computing:** Cloud computing comprises different features that provide flexible access to information and data from anywhere. It offers computational power, memory, and storage without the requirement for physical hardware. These features are delivered over the Internet using transmission control and Internet protocols (TCP/IP). The main objective is to allow IoT devices to interconnect and transmit data more efficiently.

**Service Support and Application support layer**

This layer is in charge of the analysis and knowledge generation. It comprises different ways to analyze, manage, secure, and store data. In this layer, there are other technologies that can allow encryption, access control, statistical analysis, predictive analysis, data mining, and others.

- **Data Analytics:** Every day, billions of IoT devices connected through the Internet generate a massive amount of data. This data is stored using cloud computing services and analyzed to create new information and decision knowledge using advanced analytics programs. Industries, policymakers, and governments can utilize IoT data to predict, optimize, and improve operations and business.

**Application Layer**

The last layer is responsible for delivering different application services to the end-user. It defines how IoT can be deployed to provide different smart solutions (e.g. farming, healthcare, transportation, agriculture, others). Some examples of smart applications are provided below.

- **Smart House:** Several devices interconnected provide intelligent and automated services to users. They help in energy conservation and provide security to house owners. For example, light systems can be automated to follow daily routines in the house.

- **Smart Transportation:** It allows the management of daily traffic in cities by using sensors and devices to collect information on the roads of the city.

---

12Ibid.
main goal is to minimize traffic congestion, avoid incidents, and law enforcement\textsuperscript{18}.

- **Smart Water Systems**: The management of water resources is a concern for every city. Smart solutions help to measure the degree of the water inflow, outflow, and possible leakages\textsuperscript{17}.

The integration of these layers allows the interaction between the physical and virtual world. Sensors provide the notion of environment sensing and interaction\textsuperscript{18}. The networks allow bidirectional communication with cloud computing services for data transmission. Data analytics give sense to the data and enable automatization. With the essential characteristics of IoT and main technologies that compose the different layers, it is also possible to create big data ecosystems and integrate machine learning applications. These ecosystems and integrations allow the sensing, analytics, and automated control of the smart application offered by IoT.

**Figure 3 IoT Architecture**


\textsuperscript{16}Ibid.
\textsuperscript{17}Ibid.
1.2. Key characteristics & main technologies

IoT’s fundamental characteristics include interconnectivity and heterogeneity, accessibility, things-related services, dynamic changes, enormous scale, safety, and connectivity.

**Interconnectivity and heterogeneity:** Interconnectivity plays an essential role. It allows us to interconnect and communicate with different IoT devices to gather or send information through communication infrastructure. At the same time, it enables different devices from different brands to share each other data to create intelligent environments. Therefore, manufacturers need to provide heterogeneity during the manufacturing process of IoT solutions. This, in combination with open standards and protocols, will allow the interoperability of IoT solutions independent of the hardware or network, while enabling additional interactions with other devices or services platforms that use local or Internet connections.

**Accessibility:** IoT requires constant communication of data to provide services or smart solutions. Accessibility is an essential characteristic that allows IoT to interconnect to consume and provide data. It also enables access to services, devices, and data generated in an IoT solution to provide services or execute automatic tasks. This accessibility is through IoT devices that are connected using local area networks or the Internet.

**Things-related services:** IoT enables things-related services. Things can provide services to individuals in real-time using a virtual clone of a physical thing in a virtual environment. These services (e.g. activity trackers to transmit key health indicators, home security surveillance systems, digital twins) can be automatically executed or controlled manually via the Internet.

**Dynamic changes:** IoT solutions need to use different states for memory and proper function. These states change dynamically depending on the need or the task within the day (e.g. sleep, wake-up, connect, active, disconnect). Depending on the location and data transmission speed, the number of IoT devices can dynamically change. In some cases, an increase in the number of devices allows better coverage or increases data processing capacity. Therefore, IoT solutions need to be ready to adopt an increase in the number of devices without affecting the overall performance of the solution.
Enormous scale: Every day, more and more devices are communicated and managed through the Internet. IoT requires multiple interconnected devices to generate data that will be used to provide services. Therefore, IoT network implies a large scale of interlinked devices requiring network capacity and efficient methods for data handling\textsuperscript{26}.

Safety: It is an important characteristic that needs to be considered when implementing IoT. Personal data, endpoints, and transmission channels must be protected against bad actors. Therefore, IoT solutions need to consider encryption, data integrity, and other security mechanisms to protect IoT solutions\textsuperscript{27}.

1.3. Current status

In 2020, the global IoT market size was USD 308.97 billion, and it is expected that the market reaches USD 1,854.76 billion by 2028\textsuperscript{28}. IoT is a keystone for the digital transformation and foundation for the operational efficiency of various areas. The constant adoption of IoT across manufacturing, government, transportation, and healthcare areas has increased the number of IoT projects as well. Figure 4 shows the growing trend in the adoption of IoT by application areas in 2020. IoT projects are more common in the Manufacturing/Industry (22 per cent), Transportation/Mobility (15 per cent), and Energy (14 per cent) sectors.

The IoT market has expanded significantly in 2019 and 2020. Companies are working to provide more innovative solutions that include IoT as the main core. For example, retailers are using IoT to improve customers' experience and increase their operational efficiency\textsuperscript{29}; companies are launching a dedicated satellite based IoT connectivity service\textsuperscript{30}; manufacturing companies are adopting sensors and robots to become smarter through IoT\textsuperscript{31}; and cloud environments are evolving to allow the building and deployment of IoT solutions as well. In terms of global market growth, Figure 5 shows the comparison of market growth by region. North America and Europe present a middle-market growth rate. The Middle East, North, Sub-Saharan Africa, Latin America, and Caribbean regions present the lowest market growth rates. In case of the Asia-Pacific region, the market growth is the highest. This market growth is due to the large consumer base, advanced network infrastructure, investment in Industry 4.0,

and the construction of smart cities.

**Figure 4 Top 10 IoT application areas 2020**


**Figure 5 Internet of Things (IoT) market - growth rate by region**


With regards to network infrastructure, the Asian-Pacific region is spreading 5G networks adoption. For instance, the Republic of Korea became the first country to deploy 5G networks in 2019\(^{32}\). 5G Technology plays an essential role to provide mass

---

IoT connections, higher speed, reliability, broader coverage, and higher bandwidth. In terms of investment, IoT is attracting the attention of enterprises and multinational companies that are constantly investing in IoT startups. Startups are working to provide innovative solutions for different industries such as vehicle telematics, driver safety, mobile workflow and compliance, asset tracking\(^{33}\), home security solutions and the alarm industry\(^{34}\), machine learning solutions to improve rail travel\(^{35}\) or provide IoT as a platform for smart packing for pet food, rice, or detergent products\(^{36}\).

The IoT market is highly competitive, most of it is composed of large enterprises and specific small players that operate in domestic and international markets. Currently, some of the major players are Cisco Systems, Inc., Google, Inc., IBM Corporation, Microsoft Corporation, and Huawei Technologies\(^{37}\). In the case of small players, some innovative companies of 2021 are Farmer’s Fridge (IoT solution for Food), Enovo (IoT for waste management), Inspire (Smart energy IoT Solutions), Cooler Screens (IoT for retail coolers), and ClearBlade (IoT platform for smart buildings). Figure 6 shows the level of consolidation of the market, which remains competitive, major players opt for mergers and acquisitions to keep innovating in IoT markets.

As mentioned before, Figure 4 shows that the major application areas of IoT are manufacturing/industry, transportation/mobility, energy, agriculture, and others.

Examples of IoT applicability by key industry sectors are provided below.

**Manufacturing industry:** IoT represents a game-changer to industrial applications. It provides the opportunity to allow real-time tracking of inventory and yields or monitoring downtimes. To do that, IoT is integrated into other technologies such as robotics and software for industrial use. If sensors are merged into the machinery, it will allow predicting maintenance, and data will be delivered from the machinery to staff in the industry. This data will help reduce potential issues and downtime that can represent an economic loss. IoT enables the predictive maintenance analysis that helps create strategies and mitigation plans\(^{38}\).

**Healthcare:** In the case of healthcare, IoT helps to create smart care. Hospitals are adopting IoT healthcare solutions to assist hospital procedures with robot

---


surgeons. IoT sensors allow personalized patient treatment and care with more precise data. IoT wearables help to prevent illnesses such as heart disease or diabetes by warning in advance before any serious damage is done. That, combined with mobile applications, sends automatic reminders to users to take their medication, check their blood pressure and collect medical data in real-time. IoT medical devices have been used in airports and ports to screen body temperature during the COVID-19 pandemic.39

Figure 6 The market concentration of IoT

![Market Concentration of IoT](image)

Source: Mordor Intelligence (2021).

**Automotive:** IoT technologies integrated into vehicles allow continuous real-time communication with real environments. In addition, it permits autonomous driving technology, the interconnectivity of vehicles, and sensors on roads and highways. High-speed mobile networks allow the connectivity to transport infrastructure that creates a smoother driving experience. The current technology provides driving-assistance systems (ADAS) and V2X (vehicle to everything).40

**Aerospace:** The integration of IoT into aerospace allows a better flight experience. Maintenance of airplanes in time, spot potential problems or engine issues. IoT will enable engineers to build smart airplane components. The data collected by aerospace companies or airlines can provide more safety, efficiency and reduce flight costs. IoT can provide real-time data to simulate and review flights.41

**Smart Houses:** IoT provides a way to create a better way to consume energy in houses. IoT enables intelligent lights, cooling, and heating systems. It creates automatic reports and informs of potential operability issues. IoT applications create smart homes that allow housewares to automate lighting, heating, cooling, and security systems based on patterns or times of the day.42

**Agriculture:** IoT technologies integrated into agriculture allow farmers to measure

---

41 Ibid.
soil conditions and control environmental elements such as temperature, humidity, and light. IoT improves agricultural yields, increases the efficiency of harvesting and allows a better monitoring of the entire farming process.\textsuperscript{43}

**Logistics:** IoT ecosystems allow better data transmission between different logistics, shipping, and transportation ecosystems. Integrating into cloud computing, satellite, and GPS technologies enables businesses to monitor assets in real-time independent of the transportation medium. The integration with network communications allows the centralized data and the automatization or remote execution of tasks.\textsuperscript{44}

The next chapter explores the current status of IoT in government.

1.4. **IoT in government**

One of the possible application domains of IoT is government. The connectivity of sensors creates a digital world that allows services and applications to collect citizens' data, public infrastructure data, and environmental data. IoT can develop insights and build knowledge. This assists in solving problems and automating the process without the intervention of a human actor. The integration of IoT with AI enables the creation of a smart government.\textsuperscript{45} That can help achieve better citizen engagement, interoperability with e-government applications, and accountability. As a result, IoT improves the efficiency of governance and citizens' quality of life. Figure 7 provides a framework for the interoperability of IoT integration to the government.

The framework is primarily composed of four parts and the interactions between them. The first is the domains to which IoT can be applied in the government sector. This domain provides different input data generated by different government domains (e.g. social and cultural, public safety and defense, energy and utilities, trade and industry, infrastructure, education, healthcare, and transportation). The collected data is fed to an IoT solution that combines with Artificial Intelligence to create a smart government.

The second part is composed of IoT-enabled systems. IoT will enable the collection of different types of data that can influence the decision-making process and outcomes of the smart government. This section presents all the technical requirements needed for the correct IoT deployment. At the same time, different stakeholders govern and participate in the IoT solution to provide regulations, policies, and principles. In return, the smart government solution supports the activities of the different stakeholders and benefits in various public services across domains of the government. The third part is IoT principles, regulations, and policies for effective and efficient use of IoT at the government level. Governments should aim for a transparent, accountable, ethical, and fair use of IoT and ensure data privacy and security, sustainability, and interoperability. In addition, data collected can be shared to promote transparency and awareness and to stimulate citizen participation in public domains. The last


component is multi-stakeholder partnerships: in order to succeed in the implementation of IoT projects, it is important to promote the involvement of different sectors such as academia, industry, and public organization.

Consequently, data can be exchanged for public, government, academic, and industrial purposes. In this sense, the government should provide warranties to address data privacy and security, sustainability, and interoperability. Therefore, smart nations and smart cities are a composition between IoT-enabled solutions, government sectors, regulations and policies, and stakeholders.

Figure 7 The framework of IoT integrated into the government

IoT solutions can contribute to different areas of the government such as city planning and management, job creation, public safety and defense, infrastructure monitoring, law enforcement, and others.\(^4^6\)

City planning and management: IoT solutions can be implemented to analyze different city planning and management aspects. Factors such as population growth, mapping, water consumption and supply, transportation patterns, traffic volume, social services, and land use can be monitored by IoT. Detailed data can be

\(^4^6\)Mohapatra, Dr. A. K. M., Mr Ashis Kumar Mishra, Prof Yogomaya. (2020). Introduction to Internet of Things (Basic Concept, Challenges, Security Issues, Applications & Architecture). Nitya Publications.
gathered using a combination of IoT solutions. Each factor can be analyzed and the data can produce value. In the case of management, it allows the government to actually "live" with its citizens, give primary support services, and infrastructure relative to transportation, water control, waste management, emergency services, and healthcare. It provides detailed real-time data that support decision-makers to take fast actions to address citizens' issues or needs, optimize cities' operations, and automate processes to cut down unnecessary state expenses. For example, intelligent trash bins installed in New York inform waste management companies when they need to be emptied.

**Job creation:** Data collection from different government sectors provides a better economic analysis. IoT can help disclose possible blind spots and support better economic modeling. Industries and markets can be analyzed to allocate economic resources and create new job opportunities. In addition, the government can allocate funding to create initiatives for IoT startups creation.

**Public safety and defense:** IoT solutions can provide armed forces with tools and sophistication to manage public safety and national defense. Borders can be monitored and controlled with high-performance IoT devices. The protection task can be automated through IoT, reducing the number of individuals in charge of the safety and defense, improving accuracy and speed.

**Law enforcement:** IoT can improve the justice system. With IoT solutions, the government can boost transparency, critical data distribution and reduce human intervention. Automation through IoT can provide better data sharing and reduce human labor. IoT can help control traffic violations, emit electronic violation ticketing, share logged footage of violations, and remote observation. With the reduction of human interventions, corruption is reduced as well. For example, patrol control can use IoT devices for a dart. The device is implanted in the infraction vehicle, and data is transmitted to a central system to locate the vehicle and avoid accidents during the chase.

**Infrastructure management:** Every year, the government invests tremendous amounts in building and maintaining public infrastructure (e.g. roads, bridges, power grids, water supply, gas supply, rail lines, airports, and others). If damage to these infrastructures is not detected on time, major disruptions can be caused to civilian activities. IoT can enable governments to maintain and monitor public infrastructure. Sensors can be used to monitor railway lines, regulate power supply, and help identify potential threats. Data collected can help to estimate costs and make decisions in new infrastructure projects.

**Disaster management:** Every country is exposed to natural disasters, and governments must preserve human life during an emergency disaster. In this sense, IoT can help detect forest fires, and early stages of areas prone to flooding by

---


monitoring water levels. It can also prevent human-induced disasters by helping emergency teams respond with a constant monitoring solution.
2. Opportunities for sustainable development

As a disruptive technology, IoT has a key role in global sustainable development. IoT's positive effect can help address sustainability and development challenges. This chapter provides an overview of the positive impacts of IoT adoption on the Sustainable Development Goals proposed in the 2030 Agenda for sustainable development. IoT characteristics allow its applicability to different SDGs. At the same time, this adoption can benefit the SDGs as well. With the collection of significant amounts of data per different sectors, IoT can enable a correct follow-up of the status of the SDGs. It can also foster smart and big data ecosystems that integrate different technologies to help achieve SDGs. Case in point, countries could leverage IoT's potential, by collecting and distributing reliable data, increasing productivity, and monitoring health and water quality.

As mentioned in the previous chapters, the SDGs can be divided into three main components (Society, Economy, and Environment). The next chapter provides a broad explanation of the positive effects per goal and showcases real use examples in which IoT solutions are implemented.

2.1. IoT and societal outcomes

Goals in the pillar of society provide ways to contribute to the growth of communities, families, and individuals. The main characteristic of this pillar is to address issues relative to the quality of life, city development, and the correct allocation of natural resources. IoT plays an important role in enabling data collection from different sectors. The data collected can be used at a later stage to generate knowledge to track the progress of the SDGs in different countries. Annex 1 provides a list of examples of how IoT positively impacts the goals related to society.

2.2. IoT and economic outcomes

The SDGs' economic component allows the identification of potential solutions that have implications from trade and investment to employment growth and private sector development. Thereby, IoT solutions can help provide better resource allocation, increase profit, track systems that allow reduced losses, control of supplies, and initiatives to use data in favor of development. Annex 1 provides specific examples of the use of IoT to support SDG goals relative to economic outcomes.

2.3. IoT and environmental outcomes

Biological diversity is at risk worldwide. Land degradation, deforestation, and desertification affect food security and water availability. Environmental degradation affects terrestrial and aquatic ecosystems, which reduce access to natural resources and ecological services. IoT can contribute to water management, agriculture, wildlife monitoring, and waste and wastewater management, which can contribute to solving these environmental challenges. The Internet of Things cannot stop disasters, but it can help identify, alert, and assist. Considering the different approaches in which IoT
can contribute to environmental outcomes, Annex 1 provides examples for each specific SDG related to the environment component.

Besides positive impacts, the adoption of IoT causes risks and challenges. For instance, the larger number of devices used to implement a specific innovative solution increases the chances and vulnerability of IoT to attacks by bad actors. Current research in IoT reports that the limitations of IoT are manifold and include, but are not limited to: integration, usability, security, interoperability, and user safety\textsuperscript{49}. Therefore, challenges and issues in the context of IoT must be further explored. This will be discussed in detail in Chapter 3.

3. Considerations for using IoT

All kinds of innovation bring new challenges and unexpected effects upon economies, society, and culture. Despite the remarkable economic and social benefits, technological innovation can also have negative impacts. IoT is no different. IoT promises many advantages and improvements to technology and life overall. Nevertheless, when it comes to real implementation and adoption, it is faced with significant technical and nontechnical challenges. The most important challenges found in current literature are presented in this chapter.

As it was presented in Chapter 1.1, IoT Architecture has four layers (Device and sensor layer, Network & communication layer, Service support and application support layer, and Application layer). The two upper layers (Service support and application support layer, and Application layer) have similarities with AI technology. In fact, in a broad sense, AI is the driving technology for these layers because the same processes of data storage, processing, analysis, machine learning, Big Data, and others are a part of the IoT ecosystem. Naturally, the challenges and problems that occur within these two upper layers are very similar to those discussed in Chapter 3.3. The technology elements of IoT systems such as data aggregation, data processing, analytics, and AI algorithms lead to an overlap of many challenges such as accountability, transparency, ethics, fairness, privacy and security, sustainability, interoperability, and others. To avoid repetition in this chapter, the focus will be on challenges that are unique to the IoT context and different from challenges that are already elaborated in the context of AI.

The risks and challenges associated with IoT could potentially have unintended negative consequences for the SDGs. Therefore, in order to effectively utilize IoT for the SDGs, it is necessary to be aware of the negative impact of IoT on the SDGs. For more information on the SDGs, please refer to Annex 1.

3.1. Taxonomy of challenges in IoT adoption

Because IoT systems are complex and have many layers, requiring interaction and communication of various stakeholders and tech systems, the value chain for IoT services is unclear and hard to trust. Accordingly, the types of challenges are diverse. The importance and significance of different challenges changes depending on stakeholders and domain of application. Moreover, some challenges are more severe in developing countries. Therefore, geographical, and economic factors matter too. Thus, it is necessary to classify challenges in IoT in a way that allows for a clear understanding and categorization. This module adopts a taxonomy of challenges presented by the World Economic Forum in collaboration with the Global Internet of Things Council and PWC in their “State of the Connect World 2020 Edition” white paper.

Application domains: There are three primary domains: Consumer IoT (e.g. smart

---

51Ibid.
home devices, internet-connected home appliances, wearables, etc.); Enterprise IoT (e.g. smart factories, internet-enabled machinery, intelligent building management systems, precision agriculture, etc.); Public spaces IoT (e.g. smart city tech for traffic and lighting management, public safety systems, emergency notifications, waste management, fleet management, etc.).

**Impact areas:** To summarize various challenges in a manner that is suitable for IoT technology, five main areas of impact are identified:

- **Safety and security:** The ability of IoT devices and systems to maintain a safe and secure development, deployment, and operational environment.
- **Privacy and trust:** The ability of IoT devices and systems to safeguard the privacy of users and generate trust that personal information will be collected, stored, and used for agreed purposes in an ethical and responsible manner.
- **Interoperability and system architecture:** The ability of IoT devices and systems to interact effectively with each other to execute tasks in an efficient and cost-effective manner.
- **Societal benefits and equity:** The ability of IoT devices and systems to fairly benefit and protect societal stakeholders irrespective of geographic, socioeconomic, or other factors.
- **Economic viability:** The ability of IoT devices and systems to be financially and operationally sustainable throughout their life cycles in the context of rapid technological and social changes.

The next session introduces the risks which are inherent to IoT and caused by the nature of the technology. Afterwards, common challenges that are not strongly associated with the nature of IoT technology are presented. Finally, challenges that are important in the context of developing countries will be developed.

### 3.2. Risks inherent to IoT

**Safety and security:** IoT consists of millions of data-collecting sensors that are using wireless networks. The nature of IoT creates an ever-expanding collection of targets that are attractive and vulnerable to bad actors (Figure 8). Hackers attempt to penetrate home security systems, automotive driver assistance systems, large-scale energy grids, etc. At large companies, the cost of IoT hacker attacks can be measured in tens of millions of US dollars\(^{52}\). One of the best-known IoT hacks is the Mirai Botnet attack. Malware, called Mirai, turned networked CCTV cameras into remotely controlled bots and initiated distributed denial of service (DDoS) attacks. In October 2016, it almost brought down the entire internet on the east coast of the US\(^{53}\). Even if security designs are revised or updated after devices are installed, systems can still face security threats if users or companies decide that it is too complicated, confusing,


or expensive to continue to update them.

Overall, IoT solutions are unique in that the safety and security problems are compounded because IoT systems comprise a very large number of interconnected IoT devices and network devices such as routers may have their own vulnerabilities as security features of various providers are different.\(^{54}\)

**Figure 8 Key differences between IoT and traditional digital systems**


**Privacy and trust:** Due to the complex nature of IoT solutions, consumers have no proper understanding of how, where, and when sensors and various other IoT devices collect their personal data. According to NCTA – the Internet and Television Association, there were about eight networked devices per person in the United States of America in 2018, and the number was projected to climb to 13.6 per person by 2022.\(^{55}\) Deployment of IoT sensors in public spaces is also growing quickly and invisibly, with little understanding of what they are used for or why they are in use.\(^{56}\) In the United States of America, more than 20 per cent of the population uses smart wearables.\(^{57}\) The global smart wearable market is projected to grow at a compound annual growth rate of 19 per cent from 2020 to 2025.\(^{58}\) With smart speakers and home security cameras being widely adopted, very few aspects of our lives are not monitored. Another inherent feature of IoT is that the data captured by IoT devices is transmitted and analyzed in real-time, which means that there is no time to review and ensure the privacy of consumers. Academic literature shows that in a study, the manufacturers of 72 out of a total of 81 studied consumer IoT devices shared the data they collected with third parties, and the data shared went far beyond basic information about the physical device being used.\(^{59}\)

**Interoperability and system architecture:** IoT is a rapid-growing, multi-layered, and enormously complex set of technologies. In contrast to the Internet, which is built on a single set of internet protocol technologies, every IoT system has its own data,  

---

56 Ibid.
57 Wurmser, Y. (2019). Wearables 2019: advanced wearables pick up pace as fitness trackers slow.
communications, and platform standards\textsuperscript{60}. The lack of interoperability makes it difficult for end-users in every domain to streamline their operations and protect their investments in the technology or move among providers\textsuperscript{61}. This leads to high switching costs for consumers of all types. Interoperability issues and the lack of global standards are undermining progress and creating barriers for the further development of IoT. IoT solution providers have to create, test, and support multiple versions of the same device in order to ensure interoperability across different communications protocols and platforms. The lack of interoperability makes it far more complicated and expensive to replace legacy IoT systems or build new capabilities onto older ones creating problems for maintenance and scalability\textsuperscript{62}. The interoperability of existing standards is still not proven in the context of wide practical adoption or is still being formulated, making it difficult for IoT devices to function across ecosystems\textsuperscript{63}.

**Spectrum resources:** With the multitude of devices and layers of IoT, different parts of the IoT ecosystem need a variety of spectrum resources. The electromagnetic spectrum is used up in most countries around the world. Therefore, IoT providers find it challenging to obtain a spectrum that meets their requirements. Globally, regulators are aware of the general scarcity of spectrum supply for all uses and endeavor to make spectrum available, but existing users often have valid objections to vacating or sharing spectrum\textsuperscript{64}.

**Economic viability.** The cost of maintenance for IoT solutions is often underestimated. Securing the funding and resources needed to maintain long-term financial sustainability and viability is critical. There are examples of smart city systems that have been abandoned after initial deployments due to the lack of maintenance funding and resources\textsuperscript{65}.

### 3.3. Common challenges in IoT adoption

**Safety and security in governance:** The general public is largely unaware of security risks and doesn’t know how to adhere to security design and processes. The majority of attacks occur due to lack of information, lack of provider-driven security updates, lack of experience, and unsafe user behavior\textsuperscript{66}. This points to a lack of governance. Governments at the regional, country, and state levels are beginning to address the need for better IoT security governance, but efforts so far have been patchy and


\textsuperscript{64}Organization for Economic Co-operation and Development. (2016). The Internet of Things: Seizing the benefits and addressing the challenges. OECD Publishing.


\textsuperscript{66}Ibid.
globally fragmented, making compliance both confusing and costly for companies. Industrial players have made some early attempts to establish IoT security frameworks. The industry-driven C2 Consensus on IoT Security Baseline Capabilities and the Cloud Security Alliance\(^{67}\) (CSA)’s IoT Security Controls Framework\(^{68}\) contain guidelines to refer to. However, these are only guidelines, discretionary and non-binding, with no uniform global baseline for all to follow. Few regional efforts, such as the ioXt security certification program\(^{69}\) have been initiated, but there is still no globally recognized IoT security certification program.

**Transparency:** Due to the lack of regulation of IoT, under most state laws in the United States of America, breaches exposing records containing users’ names and associated biometric or sensor data do not trigger notification requirements\(^{70}\). Research by Consumers International illustrates that only 50 per cent of IoT consumers are aware of the settings on their IoT devices that control data collection\(^{71}\). Finding out what data is being collected in public on a ubiquitous IoT network is practically impossible. Companies and governments alike are already using facial-recognition technologies to collect and store the faceprints of millions of people. The devices or sensors, such as cameras on the street, or motion sensors under a patient’s bed, may collect peoples’ data without their consent. Lack of transparency in IoT has already led many consumers to view public IoT systems as “creepy” and “untrustworthy”.

**Societal benefits and equity:** For the advantages and beneficial outcomes of IoT projects to be used and experienced by societies as a whole in any given nation, the know-how, best practices, standards, and other important information must be shared. In reality, however, information sharing between regions and authorities is often limited with little communication of either best practices, or challenges that were encountered\(^{72}\). Another issue is that the applications and services could benefit the economy overall (e.g. through better planning), but not show direct benefits to citizens or asset owners. In this sense, there could be significant tensions between stakeholders\(^{73}\).

As seen in Figure 9, the highest risk levels are experienced in the consumer IoT domain, followed by the public space IoT domain, and the enterprise IoT domain.


\(^{69}\)ioXt Alliance. ioXt Certification Program., Available from https://www.ioxtalliance.org/get-ioxt-certified


having the least amount of risk concerns. “Safety and security” together with “privacy and trust” appear to be the areas of greatest impact in terms of risk. These two impact areas are important throughout all three domains.

**Figure 9 The level of IoT risk within the three main domains**

![Figure 9](image)


### 3.4. Challenges for IoT adoption in developing countries

**Awareness of privacy and trust:** One of the main problems in developing countries is the lack of awareness about privacy and trust risks. The key reason for this is the relatively low penetration of IoT solutions on a mass scale. For example, African experts generally perceive the risks from consumer IoT applications to be lower than respondents from other regions. Since Africa is still lagging behind the rest of the world in internet penetration\(^74\), it may take longer for the general public to get access to IoT applications and have the appropriate experience to assess their associated risks.

**Interoperability and system architecture issues due to digital divide:** There can be further interoperability issues for the developing economies because information requirements in developing countries differ from those in advanced countries\(^75\). Consequently, IoT systems generally have different design requirements and technological frameworks for developing countries. Furthermore, developing countries lack modern infrastructure\(^76\) and have a limited stable and reliable power supply. The same is true in terms of the availability of data centers.

**Societal benefits and equity issues due to the digital divide:** In 2020, only 54 per

---


cent of the global population was connected\textsuperscript{77}, and people in poorer regions are far less likely to be online, especially women, elderly people, and those living in remote and rural areas\textsuperscript{78}. In developing countries, the differences between rural and urban areas are vast: 85 per cent of poor people live in rural areas\textsuperscript{79}. As a combination of various kinds of digital technologies, IoT is very likely to exacerbate the digital divide between digitally advanced and connected populations and those without digital access. An IoT application as straightforward as water-quality monitoring, for example, might be made available only in developed areas where it is most economically efficient, even though underdeveloped areas are in far greater need. In addition, consumer IoT applications such as smart homes and connected cars have not been widely adopted in most developing countries\textsuperscript{80}. In developing countries, another main challenge is the lack of technically knowledgeable personnel\textsuperscript{81} required for regular maintenance, updates, and function testing of IoT systems.

**Funding and inequalities:** Implementing enterprise IoT solutions is usually complex and costly. Larger companies have the knowledge and capital available to implement advanced IoT projects. According to the World Economic Forum’s research, larger businesses (those with more than 500 employees) are six times more likely to use industrial IoT than small and medium-sized businesses\textsuperscript{82}. This could further widen the gap between large incumbents and small, local, and minority-owned businesses. Naturally, this is a threat for developing economies because most large businesses are located in advanced countries.

Figure 10 summarizes risk levels across different regions and three main domains. It is important to observe that risks in the consumer IoT domain are relatively high all over the world. In contrast, the level of risk in enterprise IoT and public spaces IoT is less noticeable for developing regions (Latin America, Africa, the Middle East). This can be explained by the much weaker penetration of enterprise and public space IoT solutions in developing countries, while consumer devices such as wearables and smart speakers are relatively well penetrated across all regions. Moreover, “safety and security”, as well as “privacy and trust” impact areas are more strongly highlighted.

than the other three impact areas in the developed regions. The reason for this is that IoT overall is much more developed and adoption is much higher within developed countries, naturally leading to more attacks and vulnerabilities.

**Figure 10 IoT risk level by region, domain, and impact**


### 3.5. Stages of IoT development

The various challenges and issues that may occur when deploying IoT solutions require continuous monitoring and checks throughout various stages of IoT project development.
IoT projects follow a phase-based process with iterative elements. Such strategy is proposed in Figure 11. It allows enterprises to consider various challenges at different stages of implementation by identifying and matching processes with business goals. After the identification of a business, the next step is the development of a use case that allows us to verify the technical requirements for the solution. A description of the stages considered during the process is given below:

- Identification of Business Goals
- Development of IoT Use Cases
- Creation of IoT Vision and Roadmap
- Launch IoT Pilot or Proof of Concept
- Update the IoT Vision and Roadmap
- Implement and deploy the initiative

It is also important to remember the constant iteration, validation, and verification of internal support processes allow us to create cycles between the stages. In the long term also, it is necessary to constantly evaluate the project to verify if the solution still delivers the business goals.

**Figure 11 Process map for IoT project initiation**

4. IoT-related policy

The Internet of Things is still a global phenomenon in development. Nevertheless, it is widely used in many areas of life. Connected sensors have become a new normal for most big cities around the globe. IoT integrated within the infrastructure allows governments to face problems such as traffic management, crime prevention, reduction of pollution, environmental monitoring, disaster prediction, and more. By 2025, IoT is expected to contribute an additional value of USD 11 trillion to the world economy\textsuperscript{83}.

Due to the inherent nature of IoT, devices such as network-connected sensors are used in the public sensor in a ubiquitous way, more often deployed in public spaces. Although it is accepted as beneficial in general, as it was mentioned in Chapter 5.3, such an intermix of technologies presents some serious challenges for governance\textsuperscript{84}. Being smart about public policymaking in a proactive manner of supporting innovation and preventing any harm that may come from excessive regulation has been proven as an efficient and effective way for the successful development of technologies such as the Internet, GPS, and many others\textsuperscript{85}. IoT is no different in this regard.

One of the best ways to reap the benefits and avoid pitfalls with IoT adoption and development is to look at what the leading countries have done. Therefore, this chapter reviews the global status of IoT regulation and policy. Next, examples of specific policy initiatives are presented and discussed.

4.1. Global IoT policy highlights

It is very important to note that the IoT is often addressed indirectly within national or any other kind of policy. This is due to the fact that IoT has within itself many other kinds of technologies in an interconnected manner. It seems that with the current level of development and policy maturity, initiatives address the IoT by focusing on complementary technologies\textsuperscript{86} which include connectivity, AI, smart cities, robotics, etc.

For the same reason of the complexity of IoT, policy initiatives addressing interoperability are of major importance. Having multiple key stakeholders (e.g.

hardware manufacturers, software platform providers, communication service providers, application developers, etc.) throughout various sectors of the society and the industry (e.g. healthcare, lifestyle, connected homes, transportation, etc.), the development of IoT interoperability standards is still far from mature\(^{87}\). This is despite the fact that global organizations such as the International Telecommunication Union (ITU), the European Telecommunication Standards Institute (ETSI), the American National Standards Institute (ANSI), the Telecommunications Industry Association (TIA), the International Standards Organization (ISO) and the International Engineering Consortium (IEC) as well as the World Wide Web Consortium (W3C), the Institute of Electrical and Electronic Engineers (IEEE), the Industrial Internet Consortium (IIC) and the Internet Engineering Task Force (IETF) are all involved in the efforts towards standardization of the IoT.

Remembering the two big issues mentioned here (i.e. the complexity of IoT and involved technologies, and interoperability issues) is very important for a proper understanding of the multitude of various IoT policy initiations. First, as it shall be seen in the rest of this section, the complexity of IoT is the key reason for governments to address it through different initiatives that may not be targeting IoT in a very direct way. Second, interoperability is probably the number one reason why it is difficult to address IoT as a whole in a single overarching policy document.

Before reviewing IoT policy initiatives on a level of national strategies, it is important to understand the level of governance on a regional scope (Figure 12).

The first thing to note is that the global level of IoT governance is relatively low. This confirms that IoT governance and regulation are still in their early stages. The Asia-Pacific region seems to have the highest levels of IoT governance overall. The Asia-Pacific region is quite heterogeneous with countries of various levels of technical development. It is important to note that some of the most technologically advanced nations are within this region (e.g. China, Japan, Republic of Korea, Singapore). Although North America is a region that is known for being highly developed in terms of technology maturity, the level of governance is observed to be significantly lower than elsewhere around the world. The most plausible explanation is that the leader of the regions, the United States of America, is made up of states each having different sets of laws and regulations. Moreover, in the United States of America, IoT is largely driven by the industry, rather than the government. This makes issues around IoT complexity and interoperability play out even more. Even with national cybersecurity regulations and enterprise security policies in place in North America, enterprises there still consider the current governance level as unsatisfactory\(^{88}\).

---

\(^{87}\)Organization for Economic Co-operation and Development. (2016). The Internet of Things: Seizing the benefits and addressing the challenges. OECD Publishing.

Figure 12 IoT governance level by region, domain, and impact area

<table>
<thead>
<tr>
<th>Governance</th>
<th>Respondent region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Global</td>
</tr>
<tr>
<td>Safety and security</td>
<td>Light blue</td>
</tr>
<tr>
<td>Privacy and trust</td>
<td>Light blue</td>
</tr>
<tr>
<td>Interoperability and system architecture</td>
<td>Light blue</td>
</tr>
<tr>
<td>Societal benefit and equity</td>
<td>Light blue</td>
</tr>
<tr>
<td>Economic viability</td>
<td>Light blue</td>
</tr>
</tbody>
</table>

4.2. National IoT policies & strategies: current status

The potential benefits of IoT adoption are clear to most governments. As a result, governments have initiated a variety of policies to enable existing goals or conduct research\(^9\). There is no general or uniform approach towards IoT policies. Thus, it is helpful to present existing initiatives from across the globe.

In the United States of America, a 2016 survey of 125 state and local government decision-makers conducted by the Center for Digital Government (CDG) showed that governments are investing in evaluations of their current needs and future plans with a special focus on the IoT\(^{90}\). The report indicates that 52 per cent of respondents have been evaluating their network needs and future plans, and half of them stated that this activity is triggered by new technologies like the IoT\(^{91}\).

In Europe, the European Union has included IoT as a crucial part of the Digital Agenda for Europe 2020 which focuses on applications, research and innovation, as well as the policy environment. In the European Union, special attention is given to promoting research and innovation\(^{92}\).

Encouragement and support of investments into IoT is another important type of policy many countries around the world engage in. Companies that invest in IoT in Saudi Arabia, are given tax breaks and grants to inspire further commitment\(^{93}\). In Brazil, parliament members have come forward with legislation\(^{94}\) targeting abolishing taxation on IoT products.

Cross-border cooperation and facilitation of conversations around IoT on a global scale are also happening. In January 2019, Japan’s former prime minister, Shinzo Abe, announced the launch of the “Osaka Track” as a part of the G20 summit. The goal was to promote an overarching “Data Free Flow with Trust” framework\(^{95}\). In practice, significant progress is yet to be seen.

Although most nations have accepted the IoT as a high priority for the government,

---


\(^{92}\)Organization for Economic Co-operation and Development. (2016). The Internet of Things: Seizing the benefits and addressing the challenges. OECD Publishing.


\(^{95}\)Shinzo Abe, Prime Minister of Japan, Office of the Prime Minister of Japan, Davos Speech, 23 January 2019, Available from https://www.weforum.org/agenda/2019/01/abe-speech-transcript/
with some countries having developed national strategies to support the technology, there still are not many well-known examples of a fully developed and implemented IoT strategy that is comprehensive\textsuperscript{96}.

Therefore, rather than focusing on geographical diversity or economies of different size, it is important to review countries that have started first and have gone the farthest on the way towards a successful national IoT strategy and policy.

4.3. National IoT policies & strategies: examples

China, Japan, the Republic of Korea, and Singapore are early adopters of IoT and related technologies. All four countries also have already established policies relating to artificial intelligence and the fourth industrial revolution\textsuperscript{97}. Over the past few years, the governments of China, Japan, the Republic of Korea, and Singapore have formulated a wide range of policies to facilitate the development and adoption of frontier technologies. Even though it is too early to measure the impact of these policies, different global indices (e.g. automation readiness, autonomous vehicles readiness, global innovation index, digital evolution index) are already measuring the capabilities of these countries. Each of them is among the top performers and is developing competencies in specific areas related to IoT and frontier technologies. This subchapter contains a discussion of the policies implemented by the four countries related to IoT.

China

China has introduced a wide range of policies\textsuperscript{98} and strategies to support the development and adoption of frontier technologies, including IoT. It has both sector-specific policies and technology-specific policies. Sector-specific policies are directed towards smart manufacturing, smart cities, and intelligent vehicles (Table 2). For example, the smart manufacturing (10-year Made in China 2025) policy, is aimed at transforming China into a leading, high-end manufacturing power through the integration of IoT in manufacturing, the enforcement of green manufacturing, strengthening quality management, and globalization of Chinese manufacturing brands\textsuperscript{99}.


\textsuperscript{97}ESCAP, U. (2018). Evolution of science, technology and innovation policies for sustainable development: the experience of China, Japan, the Republic of Korea and Singapore.

\textsuperscript{98}Ibid.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Policy Instrument</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT</td>
<td>National center devoted to IoT R&amp;D&lt;sup&gt;100&lt;/sup&gt; (2010)</td>
<td>The Chinese central government committed USD 117.2 million to boost national competitiveness&lt;sup&gt;101&lt;/sup&gt;.</td>
</tr>
<tr>
<td>IoT</td>
<td>Five-Year Plan for the Development of the IoT by China’s Ministry of Industry and Information Technology (MIIT) (2011)</td>
<td>Governments’ intentions to support the technology, such as by setting standards and demonstrating real-world applications were outlined. The plan called for creating an IoT “Special Fund” to support R&amp;D with investments totaling USD 774 million for the period of 2011 to 2015&lt;sup&gt;102&lt;/sup&gt;.</td>
</tr>
<tr>
<td>IoT</td>
<td>Inter-agency council to guide national policy on the IoT and issued guidance to support the technology (2013)</td>
<td>Fostered industry development, workforce training, and R&amp;D targets&lt;sup&gt;103&lt;/sup&gt;.</td>
</tr>
<tr>
<td>Smart City</td>
<td>Guidance to support smart city pilot programs by China’s State Council (2013)</td>
<td>Focus was on smart utilities and transportation, and the Chinese Development Bank agreed to establish financing programs for smart city pilots&lt;sup&gt;104&lt;/sup&gt;.</td>
</tr>
<tr>
<td>IoT</td>
<td>Notice on Printing and Distributing the Information and Communication Industry Development Plan 2016-2020 by the MIIT (2017)&lt;sup&gt;105&lt;/sup&gt;</td>
<td>Outlines steps for creating an IoT society, with a strong emphasis on industrial aspects, security, and trade.</td>
</tr>
<tr>
<td>IoT &amp; Manufacturing</td>
<td>A plan to promote 5G and industrial internet by the MIIT (2019)</td>
<td>Make key 5G breakthroughs to meet the requirements of industrial internet by 2022.</td>
</tr>
</tbody>
</table>


Note: The latest information has been updated based on the contents of this source.


Japan

In June 2013, Japan declared\textsuperscript{106} it would strive to make the country the “world’s most advanced IT nation,” and adopt consistent measures to develop IoT solutions in the areas of healthcare, disaster resilience, public safety, and infrastructure planning, as well as encourage sensor technology R&D\textsuperscript{107}.

The Government of Japan also has specific policies\textsuperscript{108} to invest in the fourth industrial revolution (Table 3). For example, the “Future Vision towards 2030s” was introduced in May 2017 to promote growth through solving problems in mobility, supply chains, health care and lifestyle by leveraging IoT and other frontier technologies.

Japan collaborates\textsuperscript{109} with other leading countries, such as Germany and the United States of America, to strengthen its competitiveness. In April 2016, the Ministry of Economy, Trade and Industry and the Federal Ministry for Economic Affairs and Energy of Germany signed a joint statement\textsuperscript{110} regarding Japan-Germany cooperation on the Internet of Things/Industries 4.0.

\footnotesize
\textsuperscript{108} ESCAP, U. (2018). Evolution of science, technology and innovation policies for sustainable development: the experience of China, Japan, the Republic of Korea and Singapore.
\textsuperscript{109} Ibid.
### Table 3 Summary of IoT-related policy initiatives in Japan

<table>
<thead>
<tr>
<th>Domain</th>
<th>Policy Instrument</th>
<th>Objectives</th>
</tr>
</thead>
</table>
| Fourth Industrial Revolution (IoT, Smart City, Manufacturing, etc.) | Fifth Science and Technology Basic Plan (2016-2020) | • Optimizing the energy value chain; building a global environment information platform; maintaining and upgrading of an efficient and effective infrastructure; attaining a resilient society against natural disasters;  
  • Creating intelligent transport systems; developing new manufacturing systems; building integrated material development systems; promoting integrated community care systems; developing hospitality systems;  
  • Creating smart food chain systems; and constructing smart production systems. |
| Facilitate the fourth industrial revolution (2016) |                                                         | • Establish a public-private council to lead the fourth industrial revolution  
  • Implement regulatory reforms to simplify administrative procedures and utilize information technology  
  • Promote business streamlining and restructuring of SMEs via the use of data and technologies such as fintech, robots, and sensor technologies  
  • Triple the investment from corporations in universities and research institutes by 2025 and establish five world-class R&D centers  
  • Strengthen human resources capacity by providing IT in schools and recruiting highly skilled foreign professionals through a green card system |
| Connected Industries Policy (March 2017)          |                                                         | • Identify five priority areas: automated driving and mobility service; biotechnologies and materials; Smart Life; plant/infrastructure safety management; and manufacturing and robotics  
  • Become competitive in global “real data” |
| Future Vision towards 2030s (May 2017)            |                                                         | • Develop the New Industrial Structure Vision to leverage the Internet of Things, big data, AI, and robots to solve problems in the fields of mobility, supply chains, health care, and lifestyle;  
  • Develop approaches in each field to gain global markets and generate economic growth in the short, medium and long term |


**Republic of Korea**

In October 2014, the Ministry of Science and ICT of the Republic of Korea released a roadmap for IoT to guide government actions to develop cybersecurity standards and best practices.\(^{111}\) The Republic of Korea has also allocated government funding that has contributed to the building of the Songdo International Business District, the

---

world's first purpose-built smart city\textsuperscript{112}. In May 2014, the Korean government published\textsuperscript{113} its plan for building the IoT with the aim of a hyper-connected, "digital revolution". The commercialization of 5G mobile communications by 2020 and for Gigabit Internet to achieve 90 per cent of national coverage by 2017 were the main goals.

The Republic of Korea has joint research projects with the European Union on the Internet of Things, cloud computing, and 5G networks\textsuperscript{114}. There is also strong policy cooperation with leading economies in 5G (China, Japan, the European Union, and the United States of America) to create an ecosystem that integrates 5G and other industries, such as automobile, manufacturing, and medicine\textsuperscript{115}.

\begin{footnotesize}
\begin{enumerate}
\item Organization for Economic Co-operation and Development. (2016). The Internet of Things: Seizing the benefits and addressing the challenges. OECD Publishing.
\end{enumerate}
\end{footnotesize}
<table>
<thead>
<tr>
<th>Domain</th>
<th>Policy Instrument</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT &amp; Manufacturing</td>
<td>Manufacturing Industry Innovation 3.0 strategy (2014)</td>
<td>Promote smart factories through: &lt;br&gt;• Creation of new manufacturing featuring industrial convergence;  &lt;br&gt;• Enhancement of the major segments; &lt;br&gt;• Advancement of industrial infrastructure for innovation; &lt;br&gt;• Set up 10,000 smart factories by 2020 to facilitate convergence between software and hardware technologies with an investment of USD 972 million.</td>
</tr>
<tr>
<td>IoT</td>
<td>Master Plan for Building the Internet of Things (2014)</td>
<td>Foster the development and use IoT services through: &lt;br&gt;• Developing an open platform for IoT in collaboration with the private sector;  &lt;br&gt;• Promoting open innovation  &lt;br&gt;• Developing and expanding products and services through collaboration with global businesses;  &lt;br&gt;• Developing customized strategies for start-ups, SMEs, and large businesses</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things Information Security RoadMap (2014)</td>
<td>To guide government actions in developing cybersecurity standards and best practices: &lt;br&gt;• Security would be embedded in seven IoT application categories  &lt;br&gt;• The Secure Dome project would develop nine core security technologies aligned with IoT characteristics;  &lt;br&gt;• IoT convergence security, proof-of-concept projects.</td>
</tr>
<tr>
<td>IoT</td>
<td>K-ICT Strategy (2015)</td>
<td>Include IoT-related objectives, such as: &lt;br&gt;• Establishing large-sized IoT test complex (healthcare, smart city);  &lt;br&gt;• Developing the &quot;sensor industry&quot;;  &lt;br&gt;• Cultivating domestic IoT start-ups and ventures to become global enterprises.</td>
</tr>
<tr>
<td>Fourth Industrial Revolution (IoT, Cloud, Big Data, Mobile)</td>
<td>Strategy for the Fourth industrial revolution “I-Korea 4.0” (2018)</td>
<td>Realization of People-Centered Fourth Industrial Revolution: &lt;br&gt;• Create diverse new industries through intelligent technology innovation and strengthen major industries;  &lt;br&gt;• Improve people’s quality of life by resolving chronic social problems; &lt;br&gt;• Create high-quality jobs and strengthen the social security net in preparation for changes in the job market;  &lt;br&gt;• Secure world-class intelligent technologies, data, and networks accessible to all.</td>
</tr>
</tbody>
</table>

Source: ESCAP (2018). Evolution of science, technology and innovation policies for sustainable development: the experience of China, Japan, the Republic of Korea and Singapore.  
Note: The latest information has been updated based on the contents of this source.
Singapore

In May 2005, Singapore unveiled\textsuperscript{116} its “Intelligent Nation 2015” 10-year plan to support the growth of the information and communications technology industry. Supporting the development and deployment of sensor networks and developing the communication infrastructure necessary to support ubiquitous connectivity is one of the main focus points\textsuperscript{117}. In November 2014, Singapore also launched its Smart Nation initiative to secure economic and social benefits through greater adoption and cohesive use of technology, particularly the Internet of Things\textsuperscript{118}. In August 2015, a group of government agencies began to work on guidance to define standards for the Internet of Things, such as sensor network standards and domain-specific standards, to support the Smart Nation initiative and private-sector deployment of the technology\textsuperscript{119}. Singapore works in collaboration with other ASEAN countries on smart cities promotion and with Australia on research and innovation.


Table 5 Summary of IoT-related policy initiatives in Singapore

<table>
<thead>
<tr>
<th>Domain</th>
<th>Policy Instrument</th>
<th>Objectives</th>
</tr>
</thead>
</table>
| ICT in general           | Smart Nation initiatives (2014)          | To harness digital technologies to improve living, create more job opportunities, foster innovation and growth and build a stronger community; Five key strategic national projects were identified:  
  • National Digital Identity framework,  
  • e-Payments,  
  • Smart Nation Sensor Platform to deploy sensors,  
  • Smart Urban Mobility to improve public transport through autonomous vehicles. |
| ICT in general           | Infocomm Media 2025 (2015)               | To guide the development of Infocomm media (ICM) over the next decade:  
  • Data, advanced communications, and computational technologies  
  • Nurture an ICM ecosystem to develop Singapore-made products  
  • Connect people through ICM  
  • Priority development was given to six technology areas: big data and analytics; IoT; future comms; cybersecurity; cognitive computing/advanced robotics; and immersive Infocomm media. |
| Infocomm Media Industry  | Infocomm Media Industry Transformation Map (2017) | To develop the digital economy through  
  • Building capabilities in four frontier technologies (i.e. AI and data analytics, IoT, immersive media, and cybersecurity);  
  • Strengthening the core of the ICM sector;  
  • Guiding SMEs and the workforce to adopt digital technologies to improve efficiency and productivity |
| Research, Innovation     | Research, Innovation and Enterprise 2020 | To grow industry R&D and innovation capabilities and their innovative capacities by prioritizing public funding in  
  • Advanced manufacturing and engineering,  
  • Health and biomedical sciences,  
  • Urban solutions and sustainability (e.g. self-driving vehicles),  
  • Services and digital economy (e.g. autonomous technologies, real-time analytics, IoT healthcare devices, and data mining). |

Source: ESCAP (2018). Evolution of science, technology and innovation policies for sustainable development: the experience of China, Japan, the Republic of Korea and Singapore.  
Note: The latest information has been updated based on the contents of this source.

Governments in these four countries are vision setters. They set out the overarching framework for developing and applying different types of frontier technologies (e.g. AI and the Internet of Things), or for developing specific sectors (e.g. smart manufacturing) or employing holistic approaches (e.g. Japan’s Fifth Science and

---

120 ESCAP (2018). Evolution of science, technology and innovation policies for sustainable development: the experience of China, Japan, the Republic of Korea and Singapore.
Technology Basic Plan, or STBP).

As with emerging technologies, the rapid pace of IoT innovation and deployment has left the effort to govern and regulate it far behind\textsuperscript{121} (Figure 13).

**Figure 13 The gap between IoT risks and the governance**


5. Case studies in the public sector

5.1. IoT usage and typical IoT application in the public sector

IoT is an increasingly important technological paradigm that is considered to be a key enabler of public sector smartness\textsuperscript{122}. It is predicted that IoT technologies can affect almost every public service and significantly improve processes and human efficiencies\textsuperscript{123}.

### Table 6 Examples of IoT applications

<table>
<thead>
<tr>
<th>Area</th>
<th>Examples of IoT applications</th>
<th>Area</th>
<th>Examples of IoT applications</th>
</tr>
</thead>
</table>
| Transportation and logistics | • Logistics  
• Assisted driving  
• Mobile ticketing  
• Environmental monitoring | • Augmented maps  
• Emergency services  
• Traffic and highways | Health care                    | • Tracking  
• Identification, authentication | • Data collection  
• Sensing |
| Health care                    | • Tracking  
• Identification, authentication | | Smart environment                    | • Comfortable homes/offices  
• Industrial plants  
• Smart museums and gyms | • Retail  
• Surveillance  
• Smart metering |
| Smart environment                    | • Comfortable homes/offices  
• Industrial plants  
• Smart museums and gyms | | Personal and social                    | • Social networking  
• Historical queries  
• Losses | • Thefts  
• Home utilities and appliances |
| Personal and social                    | • Social networking  
• Historical queries  
• Losses | | Futuristic                    | • Self-driving taxi  
• City information model | • Enhanced game room |


Note: They suggested examples of IoT applications based on Atzori et al. (2010), with additional examples from Lakshmi (2018), Miorandi et al. (2012), and Whitmore et al. (2015).

Applications that are expected to create value by utilizing IoT in the public sector can be divided into public services, response, cost efficiency, and proximity to citizens. Although IoT is being used in a variety of ways in different fields, the uses are oriented towards a set of common goals including (1) connected physical safety and security, (2) cost savings through increased efficiency and employee productivity, (3) automating decision-making, and (4) applying the IoT to long-standing practices to achieve additional benefits\textsuperscript{124}.

\textsuperscript{123}Tomar, P., & Kaur, G., Green and smart technologies for smart cities. CRC Press, 2019.
Table 7 IoT applications in the public sector

<table>
<thead>
<tr>
<th>Area</th>
<th>Examples of IoT applications</th>
</tr>
</thead>
</table>
| Services              | • Safety and traffic management  
• Water quality, usage and distribution  
• Better time estimates for public transportation  
• Public health  
• Integrated services of education technology |
| Response              | • Awareness and response for flooding conditions  
• Built-in sensors for emergencies  
• Air pollution monitoring and response  
• Data collection for better decision-making |
| Cost efficiency       | • Solar powered trash compactors  
• Personnel monitoring  
• Use of public spaces  
• Waste management  
• Electric grid management |
| Proximity to citizen   | • Interaction between citizens and public agencies evolve  
• Direct and timely communication |


5.2. Case studies in the public sector from OECD OPSI

A total of five cases of IoT application in the public sector since 2016 were identified in the OECD OPSI. Three are examples in the field of environment and two are examples in the field of safety. There is a summary of the identified cases in Table 8. Since there are two cases of waste management in the environment sector, four cases except for one duplicate case of waste will be described in detail in Annex 2.

Table 8 IoT adoption cases in the public sector from OECD OPSI

<table>
<thead>
<tr>
<th>No</th>
<th>Sector</th>
<th>Country</th>
<th>Year</th>
<th>The name of project</th>
<th>Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Environment</td>
<td>Colombia</td>
<td>2018</td>
<td>SIGAB – Information System for New Waste Management Model in Bogotá</td>
<td>Implementation</td>
</tr>
<tr>
<td>2</td>
<td>Environment</td>
<td>Finland</td>
<td>2019</td>
<td>Healthy Outdoor Premises for Everyone HOPE-project</td>
<td>Implementation</td>
</tr>
<tr>
<td>3</td>
<td>Environment</td>
<td>Turkey</td>
<td>2016</td>
<td>SMART RUBBISH COLLECTION</td>
<td>Implementation</td>
</tr>
<tr>
<td>4</td>
<td>Safety</td>
<td>Hong Kong, China</td>
<td>2018</td>
<td>Safematics Smart Safety System – 4S Solution</td>
<td>Developing Proposals, Implementation</td>
</tr>
<tr>
<td>5</td>
<td>Safety</td>
<td>Ireland</td>
<td>2018</td>
<td>Aeolus – Mid-altitude maritime monitoring platform for security, search &amp; rescue and environmental monitoring</td>
<td>Implementation</td>
</tr>
</tbody>
</table>
6. Policy recommendations

IoT promises solutions to major social problems, but this vision of a fully connected world will not be achieved without strong leadership from policymakers to promote its deployment and avoid potential risks along the way.

From Subchapter 1.4 it can be concluded that the current state of governance in IoT is far from satisfactory. Also, potential risks were reviewed in Subchapter 1.3. Based on the information reported so far, a governance gap can be defined as the difference between the potential risks posed by a technology and society’s efforts to safeguard itself against these risks through laws, industry standards, and self-governance approaches designed to achieve the greatest potential benefit of IoT\textsuperscript{125}. Effective technology governance minimizes risks while maximizing the technology’s positive impacts. Making sure IoT is used in a way that benefits everyone equally and reduces inequalities seems to be the largest governance gap (Figure 14).

Ensuring economic viability, and interoperability seems to be the other two areas of governance that pose a great challenge to policymakers.

Whether society will be able to benefit from IoT largely depends on how policymakers handle the potential risks. Overall, there are four general approaches policymakers can take regarding IoT\textsuperscript{126}: 1) Precautionary regulation, 2) No intervention, 3) Indigenous innovation, and 4) Technology champions.


It is up to the representative policymakers of each country to decide what approach best suits their needs and national interests. To reach sound decisions, a policy framework that promotes the benefits and responsibly protects against potential dangers of IoT is necessary. Therefore, the rest of this subchapter is dedicated to identifying appropriate policy directions for each type of challenges, identifying policy implications, and suggesting the best ways of tackling the issues by providing policy recommendations.

### 6.1. Mapping of IoT considerations to policy directions

<table>
<thead>
<tr>
<th>Domain</th>
<th>Considerations</th>
<th>Policy Directions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technological</td>
<td><strong>T1.</strong> Multi-layer, multi-device nature of IoT makes it vulnerable to bad actors.</td>
<td><strong>TP1.</strong> Promote the security of the whole ecosystem, not just IoT devices.</td>
</tr>
<tr>
<td></td>
<td><strong>T2.</strong> There is little understanding of how sensors collect data.</td>
<td><strong>TP2.</strong> Invest in education and awareness.</td>
</tr>
<tr>
<td></td>
<td><strong>T3.</strong> Every IoT system has its own technical standards.</td>
<td><strong>TP3&amp;4.</strong> Ensure interoperability &amp; standardization on an international scale.</td>
</tr>
<tr>
<td></td>
<td><strong>T4.</strong> Lack of interoperability makes switching costs very high for consumers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>T5.</strong> There is no globally recognized IoT security certification.</td>
<td><strong>TP5.</strong> Ensure cross-border cooperation on interoperability &amp; standardization.</td>
</tr>
<tr>
<td></td>
<td><strong>T6.</strong> IoT amplifies the already existing lack of spectrum resources.</td>
<td><strong>TP6.</strong> Reevaluate spectrum management policy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain</th>
<th>Considerations</th>
<th>Policy Directions</th>
</tr>
</thead>
</table>
| **Economic** | **EC1.** IoT leads to a waste of energy.  
**EC2.** The IoT value chain is unclear and hard to trust.  
**EC3.** The cost of maintenance for IoT is often underestimated.  
**EC4.** Developing countries have weak tech infrastructure. | **ECP1.** Promote green IoT & renewable energy.  
**ECP2.** Promote transparency.  
**ECP3.** Ensure investment in IoT.  
**ECP4.** Adjust policy to attract investments. |
| **Social** | **S1.** It is hard to opt-out from data collection by IoT in public spaces.  
**S2.** IoT hardware is ubiquitous and hard to notice.  
**S3.** The general public is unaware of security risks.  
**S4.** IoT is viewed as creepy and untrustworthy.  
**S5.** Information sharing between regions is limited.  
**S6.** IoT amplifies the Digital Divide. | **SP1&2.** Ensure consumer awareness and participation.  
**SP3.** Invest in education and awareness.  
**SP4.** Regulate privacy issues in IoT.  
**SP5.** Promote the exchange of information locally and cross-border cooperation.  
**SP6.** Attract investment from developed countries in exchange for data access. |
| **Environmental** | **EN1.** IoT leads to an increase of e-waste.  
**EN2.** IoT systems produce a lot of untapped heat into the environment. | **ENP1.** Require waste-management & recycling.  
**ENP2.** Promote green IoT. |

Note: Considerations in Subchapter 1.3 were categorized by using TESE framework and policy directions were drawn by authors to match with every consideration.

As in the previous chapter the TESE framework is used as a reference to match policy directions against the main challenges of IoT that were identified in Subchapter 1.3 (Table 9). Next, key insights extracted by analyzing IoT policy instruments around the globe are given.

### 6.2. Policy implications from national IoT strategy analysis

The global level of IoT governance is still relatively low. IoT policymaking is still in the early stages of maturity. One of the main reasons for the low level of maturity is that IoT is often addressed indirectly in policy documents. This happens because there already exist a number of policy initiatives and mechanisms of regulation that apply to the many complementary technologies within IoT (e.g. AI, networks, robotics, etc.).

Although global organizations like ITU, ETSI, ISO, IEEE, and others are involved in efforts towards policymaking and standardization of IoT, there are remaining challenges, with interoperability being the number one reason why it is difficult to
address IoT as a whole in a single extensive policy document.

Technologically advanced nations share several common characteristics such as:

- Government sponsoring R&D efforts in IoT;
- Using tax breaks and other incentives for IoT promotion; and
- Country leaders recognize and actively advocate the need for cross-border cooperation.

Some countries have already achieved significant progress in IoT adoption and policymaking. Therefore, rather than working alone in a slow manner, it makes more sense to attempt leapfrogging by adopting the lessons learned by IoT leaders. For this purpose, a summary of the main policy implications derived from subchapters 4.2 and 4.3 are listed below:

It is important to apply both sector-specific and technology-specific policies. Sector-specific policies can take the form of policy instruments supporting smart manufacturing, smart cities, or other specific adoptions of IoT. At the same time, long-term national policy should be developed as well.

- Governments should take on the responsibility for heavy investments into R&D.
- It is best to have a government body, or an independent organization with strong contacts with the government that is dedicated to IoT policy development.
- Even though international standardization is hard to achieve, it is important to kick off internal efforts for standardization in a given country.
- Fostering inter-agency cooperation for information sharing for IoT is a must.
- Technologically advanced nations focus on their local strengths and use IoT to interconnect existing traditional industries for technology-enabled manufacturing.
- Establish strong partnerships in the field of technology and knowledge sharing.
- Establish policy instruments to foster public-private-partnerships for industry 4.0.
- Reform and change existing government administrative procedures in a way that makes it easy to adopt IoT solutions.
- Find ways to convince corporations to invest in local universities for partnership in IoT research.
- Attract top foreign talent through various incentives (e.g. green card systems).
- Build policy with a vision for short, medium, and long-term perspectives.
- Establish special zones where business players can experiment with IoT (e.g. Songdo in the Republic of Korea).
- Use government funds to support entrepreneurship and SMEs that engage in IoT-enabled business.
- Develop policy initiatives that support and promote the whole ICT ecosystem.
6.3. Policy implications from IoT use-case analysis

Despite the fact that there are very few countries with advanced levels of IoT development, there are many successful use cases globally. A brief list of implications from the analysis of Subchapter 1.5 is given below:

- The key success factor for IoT pilot projects is to ensure inter-agency cooperation.
- Design projects that provide direct benefits to the citizens are needed to ensure the highest rates of approval and effective promotion of IoT.
- Demonstrating political willingness and technological leadership is necessary.
- Crowdsourcing is an important source of input for IoT projects for the public good. Therefore, policy instruments that provide the basis for crowdfunding should be developed.
- To secure continuous benefits from IoT projects, it is necessary to make sure the data and results generated can be shared and reused for other projects. Thus, foundations for an open data policy must be established.

A more detailed view of policy recommendations is provided in the next section. It is well-known that AI is a key component of IoT solutions. As a result, several similar challenges can be observed. Accordingly, policy recommendations could also turn out to be somewhat similar. The next subchapter aims to avoid duplication and focus on issues that are relevant and more specific to the IoT context and different from the AI context analyzed in earlier chapters.

6.4. Recommended policy directions

To stimulate economic growth through IoT and mitigate security, safety and privacy risks, governments can take the following policymaking actions:

1. Develop a national IoT strategy

As underlined in the module, there are a number of challenges and risks that, if left unaddressed, can slow the technological progress at the national level. Thus, there is a compelling case for countries to craft comprehensive strategies for IoT\textsuperscript{127}. National governments should create comprehensive national IoT strategies to ensure that the technology develops cohesively and rapidly, that consumers and businesses do not face barriers to adoption, and both the private and public sectors take full advantage of the coming wave of smart devices.

A clear government vision can help businesses to anticipate possible changes and

adjust investments accordingly\textsuperscript{128}. Governments must take on a leading role as well as be a strategic customer of IoT innovations. Overall, developing a national strategy can ensure a country is positioned to take full advantage of the Internet of Things\textsuperscript{129}.

2. Establish a government body dedicated to IoT

Academic literature suggests that there should be one body that is responsible for creating an IoT technology vision and coordinating its implementation. This suggestion does not imply the creation of a new body of governance that is independent of other institutions, but rather points towards the necessity of having a government body that is a “go-to” for most if not all IoT matters. This government body can then coordinate the activities within and among other existing institutions.

If companies face multiple regulators, a confusing and disjointed set of regulations will prevent any substantial progress. If a company making a device for a car may have previously worked with a single government agency, a company developing connected devices for cars today could be subject to overlapping or inconsistent rules from a consumer protection regulator, a transportation safety regulator, and a spectrum regulator, among others\textsuperscript{130}. A government body dedicated to IoT should be set up to prevent these negative consequences.

3. Ensure the security and safety of IoT through effective policy

It is critical for safety and security measures to be included throughout the life cycle of IoT projects, from procurement to deployment to post-deployment operations and maintenance\textsuperscript{131}. To achieve this, funding should be secured not only for the deployment of IoT applications but also for their long-term maintenance.

To reward companies for investing in cybersecurity or to help more secure products gain market share, policymakers should require companies to publish their security policies. That would force a competitive interest in describing the types of security measures they have in place with greater specificity than vaguely claiming “we take security seriously.”

Safety and security measures should be implemented through the joint efforts of all stakeholders - governments, industry, enterprises, and individuals alike (see Figure 15).

4. Ensure equality and social benefits for all

The Internet of Things can be a valuable tool to help meet the needs of underserved populations, but adoption will be uneven without appropriate public policies such as ensuring that smart city technologies serve all cities and neighborhoods rather than just affluent ones. For example, smart city technology that police departments use to reduce crime would be substantially less effective if they could only analyze data from certain neighborhoods.

Currently, there are no formal overarching governance mechanisms for reducing the risk of the unfair or unequal distribution of societal benefits through IoT. Therefore, it is crucial to take this point under consideration when developing an IoT policy. Policymakers must ensure that citizens are not discriminated against based on their economic limitations or issues of identity (i.e. race, religion, ethnicity, gender).

Low-cost sensor technologies and networked services empower underserved populations to more easily provide data that is useful for improving their quality of life. This can only happen if governments invest in and deploy these technologies equitably. The public sector must take this into account to avoid amplification of existing inequalities by ensuring that the benefits of data-driven decision-making are not provided only to a selected few, placing already underserved communities at an even greater disadvantage.

---

5. Close the digital gender gap

The best way of closing the digital gender gap is to make sure more women participate in IoT technology development and policymaking. This would require finding the necessary talent, which can be difficult. Therefore, to address the root cause of this problem, education policy should be updated to provide more chances for educating women on IoT and ICTs in general. An efficient way of attracting more female students is to establish scholarships and other support systems allowing more women to start a career in technology.

Another important issue is to make sure women can express their needs as consumers of IoT services. Due to male dominance in tech industries, it could be easy to ignore or be unaware of the needs and wants of female consumers.

6. Reduce the data divide

Policymakers should encourage widespread adoption of connected devices, from wearable fitness trackers to sensors on street corners, to close the “data divide” which refers to the social and economic inequalities that may result from a lack of collection and use of data about an individual or community. The goal of policymakers should be to ensure that all groups are systematically included in data collection activities so that all individuals can obtain the social and economic benefits of data. Policymakers should work to develop programs to enable communities to benefit from IoT. For instance, funding for smart city infrastructure should be made available to a diverse set of neighborhoods, including low-income ones.\textsuperscript{135}

7. Build trust and demonstrate transparency

Because IoT represents an emerging set of technologies, many potential users, including companies and local governments, will disregard the benefits it promises and delay adoption until the technology is proven.

For a successful adoption of IoT, transparency and communication must be regarded as critical priorities for policy.\textsuperscript{136} People need to be informed about deployments as they occur, and any associated risks. The information must be intelligible and comprehensible to a wide range of stakeholders.

8. Provide a mechanism for data sharing and reusing

IoT will generate an unprecedented quantity of data, and policymakers should be careful not to equate simple data sharing with harmful misuse. Data collected from connected devices offer a myriad of potential benefits to consumers, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians, clinicians.


researchers, government agencies, and commercial entities, and if these datasets are shared, their benefits are multiplied\textsuperscript{137}. There may be one primary reason to collect data, but beyond its initial purpose serves a multitude of good applications of this data. To maximize the social and economic benefits of information, data users of all kinds acting in good faith must be able to share and reuse data with ease.

The full potential benefits of IoT will not be realized until data from interconnected technology are widely used. Therefore, it is crucial for policymakers to incentivize both individuals and the private sector to share data\textsuperscript{138}.

9. **Governments must become early adopters**

Governments must realize their potential as demand enablers, and, where possible, migrate towards utilizing IoT-enabled solutions for public services\textsuperscript{139}. Given the efficiency and productivity gains IoT technology can offer to the private sector, countries that readily adopt and implement IoT solutions will gain a competitive edge over those that do not\textsuperscript{140}.

10. **Embed support for interoperability and standardization within IoT policy**

While local governments should be encouraged to experiment with the Internet of Things, national governments have an important coordinating role to play in developing large-scale deployments of sensor networks and smart infrastructure that spans multiple jurisdictions\textsuperscript{141}. Doing so requires interoperability and standardization across jurisdictions and national borders. Currently, the effort to design governance mechanisms and standards to promote IoT interoperability are fragmented and largely regional in nature\textsuperscript{142}.

IoT policy must promote the use of global technical standards for the IoT developed by standards-setting bodies or industry consortia\textsuperscript{143}. Standardization plays a key role in the development of an interoperable IoT ecosystem and is essential for stimulating the emergence of new systems, boosting innovation, and reinforcing competitiveness.


\textsuperscript{138}Ibid.


\textsuperscript{141}Ibid.


\textsuperscript{143}Organization for Economic Co-operation and Development. (2016). The Internet of Things: Seizing the benefits and addressing the challenges. OECD Publishing.
11. **Address radio spectrum scarcity**

Billions of connected devices communicating with one another within IoT are creating demands for spectrum frequency space that many national spectrum licensing regimes will likely be unable to support. If too many transmitting devices compete for spectrum, they will be unable to share data with each other or operate effectively.

Spectrum resources management must be addressed in policy to satisfy IoT needs, both current and future. Different elements of the IoT, from machines to sensors, need a variety of spectrum resources that are fit for purpose. Relevant authorities should assess future demands for spectrum and review the mechanisms by which spectrum could be made available for a range of uses\(^\text{144}\).

12. **IoT R&D and education should be included within policy**

As IoT technologies and applications continue to evolve at an accelerated pace, the need for education to equip the next generation of experts with critical skills to fill the talent gap becomes paramount. It is critical for policymakers to understand the emerging technology trends and how they may affect society\(^\text{145}\).

Governments must engage and partner with local communities through education and outreach. They also need to be able to raise awareness, build capacities and engage all stakeholders, identifying their individual roles and responsibilities in the overall management of risks from IoT deployments, while clearly communicating the broad-ranging benefits of the technology\(^\text{146}\).

13. **Provide incentives to engage in IoT initiatives**

Governments may slow down innovation in the use of IoT by not providing incentives such as funding for pilots and exemptions from regulatory requirements during experimentation and pilot studies. They could consider incentivizing businesses that use IoT applications to generate and share real-time data demonstrating compliances\(^\text{147}\). Incentives may include reduced inspections, fees, or recognition. In addition, the government can influence companies’ incentives through their own purchasing policies. Thereby, the government can fulfill an exemplary role as a launching customer\(^\text{148}\).

---


\(^{147}\) Ibid.

7. International cooperation opportunities

Policymakers should work together to find efficient mechanisms for developing mutually compatible IoT policies. While reaching full alignment across the globe could be extremely challenging, better mechanisms can be put in place for the policy and technical communities to discuss issues in a constructive way. It is important to note that since AI is a key component and tool within IoT infrastructures, reviewing and applying the recommendations for international cooperation in AI mentioned in Submodule A is extremely important. In addition to those mentioned in the Submodule A, some policy directions that would benefit from international collaboration are mentioned below.

1. e-Waste management

Governments need to cooperate together to convince device manufacturers to adopt design approaches for making IoT devices more sustainable, with design-for-life principles to enable users to effectively repair, upgrade, customize and recycle IoT devices. For example, The World Economic Forum has started an initiative for reducing e-waste, with the goal of enabling a circular economy for electronic devices in China through public-private cooperation. The initiative supports the work of the E-Waste Coalition, a group of seven United Nations entities that have come together to increase cooperation and provide more efficient support to the United Nation’s member States to address the e-waste challenge. The Forum hopes to end electronic waste, which is the fastest growing waste stream in the world, while also promoting the use of 25 per cent recycled content in new IoT and electronics products manufactured in China.

2. IoT security

As the number of IoT devices is increasing, the security risk is amplified as well. Consumers have a hard time to judge the security of IoT products they purchase. Therefore, the multitude of IoT devices that are inter-connected and share data, present a significant vulnerability and are posing a serious threat to cyber security. Consumers purchase devices and use software from different countries, different manufacturers. Thus, to guarantee security, nations and corporations must cooperate for the purpose of establishing IoT infrastructures that are secure for all. The key idea in this regard is that of “Secure by Design.” As mentioned earlier, security should be built into a product before devices are purchased and installed.

Nations can collaborate together by joining international organizations such as the Global Forum on Cyber Expertise (GFCE). GFCE has an “International IoT Security Initiative” that aims to provide policymakers, regulators, executives, chief Information Security Officers (CISOs) with understanding and guidance in order to

achieve a more secure IoT environment. This initiative intends to leverage successful policies, good practices and practical solutions to solve the cross-domain and cross-functional challenges of IoT security.

Another important instrument that countries across the globe must utilize is to have bilateral commitments to security in IoT. “Security by Design – UK-Singapore IoT Statement\textsuperscript{151},” a joint statement on cooperation between Singapore and the United Kingdom on the Internet of Things is a great example and reference of the kind of collaborations that are needed to make the IoT infrastructure secure. At the Commonwealth Heads of Government Meeting in April 2018, Singapore, along with 52 nations, through the Commonwealth Cyber Declaration agreed to commit to work towards the development and convergence of approaches for internet-connected devices and associated services, in order to promote user security by default.

As part of the Singapore-United Kingdom Strategic Partnership, it was agreed that the two countries would work together on areas of common interest, including greater cooperation, alignment and coordination to support a global consensus for "secure by default”.

3. IoT standardization

IoT and its associated technological innovations are still an evolving field. While numerous exciting and innovative devices, technological systems and infrastructure have been developed recently, their dependability (reliability, availability, resilience, maintainability, and use) is often questionable in the absence of uniform standards. It is important for governments, especially those in developing countries, to actively participate in the development of such standards to ensure that their needs and constraints are expressed and addressed.

Some leading examples of global standards efforts with broad private sector membership include the Industrial Internet Consortium (IIC), Open Connectivity Foundation (OCF), OpenFog Consortium (OpenFog), and GSMA’s initiative on IoT device self-certification:

- Industrial Internet Consortium (IIC): Launched in March 2014, the IIC is a global, member-supported organization that promotes the accelerated growth of the Industrial IoT by coordinating ecosystem initiatives to securely connect, control, and integrate assets and systems of assets with people, processes, and data using common architectures, interoperability, and open standards to deliver transformational business and societal outcomes across industries and public infrastructure.

- Open Connectivity Foundation (OCF): Launched in February 2016 to bring together the competing Open Internet Consortium and AllSeen Alliance, the OCF is defining connectivity requirements to improve interoperability between the billions of devices making up the IoT. OCF will deliver a specification, an open-source implementation, and a certification program ensuring

interoperability regardless of manufacturer, form factor, operating system, service provider, or physical transport technology.

- **OpenFog Consortium (OpenFog):** Launched in November 2015, Open Fog is driving industry and academic leadership in fog computing architecture, testbed development, and a variety of interoperability and composability deliverables that seamlessly leverage cloud and edge architectures to enable end-to-end IoT scenarios\(^{152}\).

\(^{152}\)For more information, see OpenFog Consortium, https://www.openfogconsortium.org/about-us/
Annex 1. Examples of IoT and sustainable development

1. Opportunities for sustainable development

Societal impacts of IoT

SDG 1 (No poverty): Under this goal, there is the target of reducing exposure to climate-related extreme events, and other economic, social, and environmental shocks and disasters. IoT has the high potential to contribute to adding value through the use of sensors that collect and distribute reliable data on weather conditions. This can allow the prediction and quick reaction to environmental events\(^\text{153}\).

SDG 2 (Zero hunger). Among the targets of this goal, there is the need to double agricultural productivity. If IoT is used to increase precision, agricultural sectors can have a positive impact. For example, Smart Farming solutions can increase food production by providing innovative ways that are more profitable, resilient, and greener agri-food systems\(^\text{154}\). Greece applied IoT solutions using very high satellite imagery and field spectrometer technology to identify crop disease risk levels in asparagus farms\(^\text{155}\).

SDG 3 (Good health and well-being): This goal proposes to reduce by one-third premature mortality from non-communicable diseases through prevention and treatment and promote mental health and well-being by 2030. In this case, IoT can potentially contribute to the goal through the implementation of smart health solutions. That allows the use of health devices interconnected to monitor, analyze and treat diseases in some cases (automatic medicine dosage). Case in point, Chiuchisan proposes the use of smart medical devices to assess the physical conditions of older adults. Devices collect information to measure physical activity in the living environment and self-monitored older adults' living conditions\(^\text{156}\). The main goal of the project is to promote IoT as a solution to monitor elderly patients' health at home.

SDG 6 (Water and sanitation for all): Freshwater is an important natural resource. This Sustainable Development Goal proposes to achieve universal and equitable access to safe and affordable drinking water for all. However, drinking water facilities face problems like limited water resources, difficulty to acquire equipment due to high cost, growing population, the difficulty of access to rural areas, and

excessive use of sea resources (salt extraction) that affect the quality of water available for human consumption. IoT can play an important role. Omar Faruq proposes using an IoT-based solution to create a water quality monitoring system for people living in Bangladesh’s outskirts. The solution allows the recollection of several water parameters such as temperature, turbidity, and hydrogen potential to assess water quality.\textsuperscript{157}

**SDG 7 (Affordable and clean energy):** It is important to double the global rate of improvement in energy efficiency. Therefore, IoT sensors can highly contribute to improving the understanding of the energy demand, load predictions, and energy consumption which can lead to an increase in energy efficiency. Electricity supply networks that interconnect sensors with digital communications to detect and react to changes in demand (Smart grids) can use IoT to collect data and automatically provide energy. The use of IoT devices allows rerouting power to prevent cascade outages. Smart grids can prioritize energy services. For example, it can bring emergency services first during disasters. IoT makes homes, buildings, and public facilities more efficient by automatizing everyday power-consume devices (e.g. lightbulbs, fans, air conditioning) to reduce unnecessary use.\textsuperscript{158}

**SDG 11 (Sustainable cities and communities):** Reduce the adverse per capita environmental impact of cities by paying special attention to air quality and other waste management. IoT solutions can contribute to achieving this goal by allowing data collection of different environmental indicators. Smart devices in buildings, parks, public infrastructure, and homes can help to control and monitor air quality, thermal information, and visual comfort. In India, the city of Agra has implemented smart city air quality monitoring systems that allow the control of PM10 and PM2.5 levels. Authorities use this IoT solution to check the city’s environmental health in real-time. The data collected is used to act for the benefit of the citizens.\textsuperscript{160}

**Economic impact of IoT**

**SDG 8 (Decent work and economic growth):** Achieving higher levels of economic productivity through diversification, technological upgrading, and innovation through a focus on high-value-added and labor-intensive sectors is important for the promotion of decent work and economic growth. IoT can highly contribute to increasing efficiency in agriculture and manufacturing services through data collection and processing. For example, strawberry production is highly competitive in China. Therefore, IoT solutions allow the data collection of growth environments.


\textsuperscript{158}IoT For All (2019, April 24). How to Use IoT to Protect Our Homes and Cities from Climate Change. Available from https://www.iotforall.com/how-to-use-iot-protect-homes-cities-climate-change


A project conducted by China Mobile and LinkDotter proposes a mobile network environment. Cloud-based solution gives strawberry farmers the ability to control air, soil conditions, light, water, CO2, and other nutrient levels using the Internet. This IoT solution optimized the production and harvesting of strawberries, which helped farmers increase their profits\(^\text{161}\).

**SDG 9 (Industry, innovation, and infrastructure):** In order to contribute with innovation, it is essential to upgrade infrastructure and retrofit industries to make them sustainable, taking into consideration the creation of networks that can interact with new technology in which IoT can be the leading player of this digital infrastructure. It allows innovation and automatization of the industry which contributes in a positive way to the SDG 9 targets. For example, Australian industrial businesses lose approximately USD 4.3 billion in physical assets, shipping equipment, and mobile storage every year. IoT solutions provide companies with networks and analytics solutions that help logistics companies control assets. Telstra’s Track and Monitoring is a solution that combines IoT technologies to cover almost 4 million square kilometers. STC Logistics, an Australian company, uses this solution to track non-powered assets across Australia. The use of the solution represents savings of AUD 3.8 million a year to the company\(^\text{162}\).

**SDG 12 (Responsible consumption and production):** It is important to halve per capita global food waste and reduce food losses in the production and supply chains. IoT can contribute positively by allowing the track of food waste and data provision about food production. For example, Eseye company proposes the use of IoT circuits onto flexible labels. These labels can be placed on food items and provide complete real-time visibility of the entire supply chain. As a consequence, producers can have more awareness and data to reduce oversupply\(^\text{163}\).

**SDG 17 (Partnerships for the goals):** Global collaboration promotes countries’ growth and the constant production of different technologies and research related to IoT. It is essential to define ways and processes that allow technology commercialization. The export of IoT solutions can enhance North-South, South-South, and triangular regional and international cooperation on access to science, technology, and innovation. For example, the United Nations Global Pulse partners with the global mobile telecommunications industry association to create an initiative to leverage mobile operators’ big data capacities. This action can enable governments to respond more efficiently and effectively to world problems in the context of health, humanitarian, and environmental causes. IoT data-driven solutions can strengthen governments’ capacity to plan and mitigate solutions


through data collection for prediction\textsuperscript{164}.

**Environmental impacts of IoT**

**SDG 13 (Climate action):** All countries need to strengthen resilience and adaptive capacity to climate-related hazards and natural disasters. IoT can help countries build early warning and predictive systems against natural disasters. Volcanic eruptions are a well-known type of natural disasters. The research introduced by Awadallah, Moure, and Torres-Gonzales in 2019 shows the possibility of using long-range (LoRa) technology for volcanic monitoring. Researchers propose the use of an IoT solution in the form of a low-power and low-cost wireless sensor network. IoT can help measure groundwater levels and heat abnormality in volcanic areas. A run test was deployed on the Teide volcano in Tenerife\textsuperscript{165}.

**SDG 14 (Below water):** Minimizing and addressing the impacts of ocean acidification is important to prolong the life of the oceans. IoT solutions can be implemented to measure the pH levels and provide data to monitor ocean acidification. An initiative in the Agua Hedionda Lagoon in Carlsbad, CA, the NOAA-facilitated project was proposed by researchers from Scripps institution of oceanography and industry. The project intends to address an oceanic data shortage issue in the west coast shellfisheries. The research team developed a multiparameter oceanographic sensor package to measure pH, dissolved oxygen, salinity, temperature, and water depth through IoT. The data collected is sent in real-time using a 3G network and collected in an online spreadsheet stored on the Internet\textsuperscript{166}.

**SDG 15 (Life on land):** It is essential for humanity to ensure the conservation, restoration, and sustainable use of terrestrial and inland freshwater ecosystems and their services, particularly forests, wetlands, mountains, and drylands. IoT can play an essential role in combating forest fires. The use of remote sensors and satellite communications to measure forest areas can help to promote the conservation of terrestrial ecosystems and prevent forest fires. In 2018, Kalatzis et al. proposed using a hierarchical architecture that combines a three-stage ecosystem that combines cloud computing, fog computing, and unmanned aerial vehicle (UAV) sensing capabilities. The system automatically activates every time fire occurs, and alerts are sent through a mobile application. The concept of smart forest is presented as an IoT solution that provides remote sensing and collects

---


environmental data\textsuperscript{167}.

2. Potential for a negative impact on sustainable development

Just like any other technology, IoT can also lead to negative impacts. It is important to note that the potential negative effects of AI on sustainable development listed in Annex 1 of Submodule B, are also valid for IoT. Therefore, it is important for readers to review the material in Annex 1 of Submodule B for a better understanding. Additional detrimental effects of IoT on the Sustainable Development Goals are mentioned below:

SDG 7 (Affordable and clean energy), SDG 13 (Climate action): The number of IoT devices has increased tremendously, leading to a rapid surge of demand for energy. IoT systems were not designed with energy efficiency in mind. As a result, devices are enabled and active even when it is not required. This, in turn, leads to a waste of energy and to the production of unnecessary heat which is not utilized for beneficial purposes. Such waste of energy threatens the global economic and environmental safety\textsuperscript{168}.

SDG 10 (Reduced inequalities), SDG 16 (Peace, justice and strong institutions): IoT initiatives often come with promises of enhanced democracy and openness, increased efficiency for overworked infrastructure, economic benefits for citizens and users, stimulation and vitalization of new markets, and the positive social impact of digitally led innovations on the community\textsuperscript{169}. Whether these positive impacts are to be experienced by all members of the society (directly and indirectly) at all levels, and not just those who are leaders and initiators is under question. Indeed, when IoT devices are deployed in public places, they gather data from all people who happen to be on the premises without the possibility of opting out of such systems. This is especially true if IoT devices are deployed within a public space through which individuals frequently move. Moreover, even if it was possible to opt-out, people are not even aware of IoT devices without appropriate signage and notifications\textsuperscript{170}.

SDG 11 (Sustainable cities and communities), SDG 12 (Responsible consumption and production): IoT systems involve several hardware components (e.g. sensors, actuators, etc.) that are ubiquitous, hard to notice, expensive, and hard to upgrade and replace. These will ultimately become outdated. Accordingly, IoT has


a heavy environmental burden due to outdated hardware and generated e-waste\textsuperscript{171}. It is not just sensors, actuators, and other IoT components, but also the plugs, electric cables, and batteries that keep IoT applications running\textsuperscript{172}.


Annex 2. Case Studies of IoT based on OECD OPSI

1) SIGAB – Information System for New Waste Management Model in Bogotá (Colombia, 2018)\(^{173}\)

Case summary

In 2018, the city of Bogotá, Colombia, developed SIGAB, a waste management information system that utilizes new digital technologies to solve the difficulties of waste management and meet the needs of citizens. SIGAB is a Colombian abbreviation for Bogota Waste Management Information System. Under the leadership of the UAESP, the Special Administrative Unit for Colombian Public Services, and the Mayor of Bogotá, the UAESP, city officials and local agencies, and service providers worked together to promote the SIGAB project.

New waste management mechanisms and solutions have been developed by combining big data, IoT, and cloud computing. IoT was particularly applied to real-time vehicle monitoring and data collection in Bogotá City to optimize routes for garbage collection companies. Through the new mobile app, citizens can track the vehicles that will collect garbage from their homes and, if needed, upload a photo to request a collection service.

By enhancing the efficiency of waste management, this project can contribute to improving city-wide environment.

Challenges

- Technological architecture: SIGAB requires the creation of a standardized and robust technical architecture that guarantees availability, security, and interoperability between the information systems of the actors involved.
- Actors’ articulation: SIGAB requires the articulation of all actors involved in waste management. Permanent information exchange and active use of information technologies have allowed UAESP and concessionaires to be articulated for guaranteeing continuous improvement and higher quality in the city public waste service.
- Go to the public: SIGAB requires the empowerment of citizens. Different services have been enabled so that citizens can be informed, interact and be part of the solution of the new city waste management system. However, without proper offering and guidance of citizens in using these services, it is not possible to ensure correct appropriation.

Conditions for success

- UAESP’s expertise, the leadership of the mayor of Bogota, and well roles specialization and game rules so that everyone does their part, wins, and contributes were very critical to succeed in this project.

2) Healthy Outdoor Premises for Everyone HOPE-project (Finland, 2019)\(^{174}\)

Case summary

Since 2019, Finland has been promoting the HOPE (Healthy Outdoor Premises for Everyone) project that monitors air quality in high-resolution ultra-regional areas through a portable mobile sensor based on citizen participation to improve air quality in Helsinki.

With the participation of citizens carrying mobile sensor devices, ultra-regional real-time air quality data is collected, and is transmitted to the University of Helsinki’s Internet of Things (IoT) data platform. The collected data is calibrated and processed using AI algorithms, machine learning, and edge computing.

Based on this processed data, the government has developed the My Air Quality application to provide local residents with various ways to improve air quality and to share their air quality status and action efforts. It launched the Green Paths service to provide healthier and more comfortable biking and walking paths based on real-time air quality and noise information.

This project contributes to collecting new and accurate air quality information and developing the best air quality improvement solutions for local residents through the expansion of local residents’ participation and industry-university-research cooperation.

Challenges

- Citizen engagement: Engaging with citizens has proved to be even more labor-intensive than initially anticipated.

Conditions for success

- An active local civil society, transparency, engagement of public policy and governance, human and financial resources, effective policy for open data and innovation, state-of-the-art technology, and scientific excellence are needed for success.
- Collaboration in universities and the related parties is important.

\(^{174}\) Sources: 1. OECD OPSI (Observatory of Public Sector Innovation), Healthy Outdoor Premises for Everyone HOPE-project, https://oecd-opsi.org/innovations/hope-project/
2. HOPE Website, https://ilmanlaatu.eu/
3) Safematics Smart Safety System – 4S Solution (Hongkong, China, 2018)\textsuperscript{175}

Case summary

The Hong Kong, China local government piloted smart safety systems such as 4S (Safematic, Smart, Safety, System) and Advanced Driver Assistance Systems (ADAS) to public sector vehicles in 2018. This project aims to investigate how to improve driver behavior for safe driving by collecting various data generated by driver, car, road, etc. during driving. This project is expected to verify the usefulness of the driver's driving safety issues and contribute to improving the efficiency and effectiveness of related policies such as universal standards for safe driving.

Challenges

- Competitor: The competitors of Safematics Solution and ADAS System are black boxes, car cameras, or automobile data recorders which may apply in public widely. In comparison with competitors, this approach is more precise in data collection and analytics.

Conditions for success

- To be successful in this project, the cooperation between specific government departments and civil experts is crucial. Their advice, suggestions, and feedback were critical in successfully developing the pilot project.

4) Aeolus – Mid-altitude maritime monitoring platform for security, search & rescue and environmental monitoring (Ireland, 2018)\textsuperscript{176}

Case summary

In 2018, Ireland developed Aeolus, a new medium-altitude maritime monitoring platform that dramatically increased the monitoring range to overcome the limitations

\textsuperscript{175} Sources: 1. OECD OPSI (Observatory of Public Sector Innovation), Safematics Smart Safety System – 4S Solution, https://oecd-opsi.org/innovations/safematics-smart-safety-system-4s-solution/

\textsuperscript{176} Sources: 1. OECD OPSI(Observatory of Public Sector Innovation), Aeolus – Mid-altitude maritime monitoring platform for security, search & rescue and environmental monitoring, https://oecd-opsi.org/innovations/aeolus-mid-altitude-maritime-monitoring-platform-for-security-search-rescue-and-environmental-monitoring/
of existing monitoring systems installed on ships. Existing systems can only monitor up to 14 nm (about 25 km), so there were many limitations in object detection due to the curvature of the earth. However, Aeolus can significantly increase the operational monitoring range by raising the altitude of the monitoring system based on sensor technology and AI systems that support object identification.

Testing of the Aeolus prototype showed that it could operate effectively 450m above the ship and increased the surveillance area by more than 11 times what the existing solution could monitor. It can also be used with multiple lifting systems, and its integrated power management and wireless communications capabilities allow it to operate for extended periods of time while continuously sending real-time data to the bridge.

The platform was prototyped on a public-private partnership basis and is currently testing version 3.5 with the Irish Navy and developing version 4.0. To extend this platform to search and rescue, naval, and customs services across Europe, the actors in this project have worked with partners in several key sectors in Europe.

**Challenges**

- Funding: To secure continuous project funding, the actors of this project worked closely with key advocates of innovative change in these organizations.
- Resources: There is a significant shortage of experienced personnel in the market, it took persistence to attract and keep the right people for the job.
- Weather: Weather in Ireland off the Atlantic coast is a challenge and disrupted the onshore and offshore trialing schedule.

**Conditions for success**

- Sponsorship at the top of the key organizations such as the Defense Forces, Enterprise Ireland, and the SEA was essential.
- Establishment of a governance model which included the right people/organizations to underpin decisions and provide guidance allowed to build teams and collaborate with key organizations.
APCICT

The Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT) was inaugurated on 16 June 2006 as a regional institute of Economic and Social Commission for Asia and the Pacific (ESCAP), and is located in Incheon, Republic of Korea. Guided by the 2030 Agenda for Sustainable Development and other internationally agreed development goals, the Centre’s objective is to build and strengthen the capacity of members and associate members of ESCAP to leverage information and communication (ICT) for the purpose of socio-economic development. APCICT’s work is focused on training, knowledge sharing, and multi-stakeholder dialogue and partnership.

APCICT is located in Incheon, Republic of Korea.

http://www.unapcict.org

ESCAP

The Economic and Social Commission for Asia and the Pacific (ESCAP) is the most inclusive intergovernmental platform in the Asia-Pacific region. The Commission promotes cooperation among its 53-member States and 9 associate members in pursuit of solutions to sustainable development challenges. ESCAP is one of the five regional commissions of the United Nations.

The ESCAP secretariat supports inclusive, resilient and sustainable development in the region by generating action-oriented knowledge, and by providing technical assistance and capacity-building services in support of national development objectives, regional agreements and the implementation of the 2030 Agenda for Sustainable Development.

https://www.unescap.org