Issue Paper: Asia-Pacific Bureau

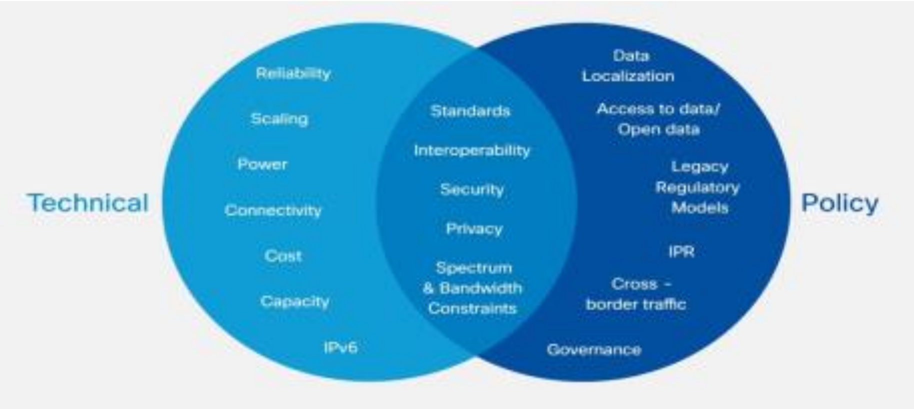
Internet of Things

November 2017

Building on the framework and concepts presented in the ***Internet Society Policy Brief on the Internet of Things***,[1] this issues paper focuses on concerns and good practices related to the Internet of Things in the Asia-Pacific region. Please refer to the policy brief for an introduction to the topic.

The Issues

It is estimated that there will be 8.6 billion "things" connected in the Asia-Pacific region (excluding Japan) by 2020, accounting for 29% of the world's connected devices, 1 out of 5 of which will be in China.[2]



The Internet of Things (IoT) has been widely recognised as an important tool for sustainable development.[3] Yet, many issues need to be addressed before its benefits can be fully leveraged. The International

[1] Internet Society, "The Internet of Things: An Internet Society Public Policy Briefing," 2 August 2016, https://www.internetsociety.org/policybriefs/iot. See also Internet Society, "The Internet of Things: An Overview," October 2015, http://www.internetsociety.org/doc/iot-overview.

[2] Glen Burrows, "Rounding out the IoT ecosystem in 2016," CIO Asia, 5 February 2016, https://www.cio-asia.com/print-article/92587/; and IDC, "Asia-Pacific Internet of Things Market Forecast," April 2015, http://infographics.idc.asia/Iot/ap-frontline-for-iot.asp.

[3] ITU, Harnessing the Internet of Things for Global Development (Geneva, 2016), http://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf.

Telecommunication Union (ITU) provides a summary of challenges related to IoT.

Source: ITU, Harnessing the Internet of Things for Global Development (Geneva, 2016)

IDC's 2016 Global IoT Decision Maker Survey, which polled 200 organisations in Australia had the following key findings:[4]

- 72% feel that IoT is very important or extremely important.
- 60% see IoT as strategic to their business and a means to compete more effectively.
- 38% have launched IoT solutions, with an additional 46% looking to roll them out in the next 12 months.
- Security and privacy, as well as upfront/ongoing costs are top concerns for decision makers, who likewise worry about the lack of relevant skills to design and deploy IoT systems.

Data privacy and protection challenges

Through IoT, data, a substantial portion of which is personal information, can be collected by devices across networks without the user's knowledge, intervention or control. Moreover, IoT devices frequently have no user interface to configure privacy preferences.[5]

Data protection authorities in 26 countries coming together as part of the Global Privacy Enforcement Network that includes Australia, China, Japan, Republic of Korea, New Zealand and Singapore, found, by investigating IoT technologies in 2016, that over 60% of them were not fully privacy compliant. Out of 300 reviewed devices:[6]

- 59% did not provide adequate information on how personal data is collected, used and communicated to third parties.
- 68% did not provide appropriate information on the modalities of data storage.
- 72% did not explain to users how their data can be deleted from the device.
- 38% did not guarantee easy-to-use modalities of contact for those wanting to obtain clarifications on privacy compliance.
- Some health-related devices triggered security issues as they transmitted data to medical practitioners without encryption.

Enforcing privacy compliance on IoT is complex: the type of data collected by a device may change over time, and providing notice and obtaining consent at each juncture are in many cases impracticable. Issues also arise when data sets that do not initially contain personal or sensitive information are, over time or in combination with other data sets, able to reveal an individual's personal details. A good example is the location data generated by mobile and wearable devices.

As nations develop and scale IoT-based initiatives such as smart cities and smart grid, there will be a blurring of roles and responsibilities between the public and private sectors, including in the collection, storage and use of personal data. For these IoT initiatives, it will be a complex challenge to figure out which data protection rules would apply, who owns the data, and who bears the liability for any damage or harm caused to the user of an IoT technology.

[4] IDC, "Press Release: IDC's 2016 Global IoT Decision Maker Survey Finds Australian Organizations Moving Past Pilot Projects and Toward Scalable Deployments," 4 October 2016, https://www.idc.com/getdoc.jsp?containerId=prAP41841816.

[5] See Issues Paper on Online Privacy.

[6] Giulio Coraggio, "Global: Large number of Internet of Things devices are not privacy compliant," *DLA Piper*, 4 October 2016, http://blogs.dlapiper.com/privacymatters/internet-of-things-devices-are-not-privacy-compliant/.

IoT security challenges

The security vulnerabilities of IoT caught the public's attention in 2016 when devices in Singapore and the US were compromised, harnessed as botnets, and used as launching points for malware propagation, distributed denial of service (DDoS) attacks and anonymising malicious activities.

In October 2016, StarHub–a large Singapore telecommunications company and Internet service provider–was hit by a DDoS attack, caused by a botnet of vulnerable IoT devices. Internet-connected DVR players, Wi-Fi cameras, music systems and routers, installed in the homes of StarHub customers (and made by a variety of manufacturers) were compromised. The devices came with default credentials that were not changed upon installation on the customers' premises, allowing remote attackers to gain access and control the devices.[7]

This and a larger attack in the US that targeted systems operated by the domain name service provider–Dyn, demonstrate the vast number of insecure IoT devices that can be used to attack third parties.

It brings up the issue of the lifecycle of an IoT system and how it is maintained after deployment. How do you keep the system secure, especially after it gets out of date?

Once devices are in the market, it becomes almost impossible to fix the issue without recalling them or issuing security updates and/or having physical access to the devices as they may not necessarily support remote updates, particularly if they have already been compromised. Moreover, when updates are received, it is essential that they can be validated to ensure they are legitimately issued by an authorised entity (usually the manufacturer) and have not been tampered with in transit. This can be difficult for devices with limited processing power and storage, and thus limited ability to perform these types of checks.

In addition, IoT products may not be engineered to protect data as they are often created by consumer goods producers with limited experience and capability with network security practices, rather than computer software or hardware firms. It is essential that security and privacy be part of the design process at every step of the design and development process, rather than being viewed as something that can be "bolted on" at the end (if at all).

Relevant government regulations and standards are currently lacking. Neither is there sufficient awareness among consumers to demand privacy and security solutions.[8] Nonetheless, the IDC predicts that by 2019, over 75% of IoT device manufacturers will use security and privacy as competitive positioning.[9]

The Online Trust Alliance, an Internet Society initiative, has developed a number of very useful resources, including an IoT Trust Framework and a white paper–*Securing the Internet of Things; A Collaborative & Shared Responsibility*.[10] The GSMA has developed a set of IoT Security Guidelines and an IoT Security Self-Assessment to promote best practice for the secure development, design and deployment of IoT services on a mobile network.[11]

[7] Amit Roy Choudhury, "IoT devices become new targets for cybercriminals (amended)," *The Business Times*, 28 December 2016, http://www.businesstimes.com.sg/technology/iot-devices-become-new-targets-for-cybercriminalsamended; and Fadli Sidek and Jamie Rubbi-Clarke, "The Top Cyber Security Risks in Asia-Pacific in 2017," *Control Risks*, January 2017, https://www.controlrisks.com/en/our-thinking/cyber-security-academy/top-cyber-security-risks-in-asia-pacific.

[8] Conventus Law, "Asia Pacific - 2017 Predictions: Criminals Harness IoT Devices as Botnets to Attack Infrastructure," 9 January 2017, http://www.conventuslaw.com/report/asia-pacific-2017-predictions-criminals-harness/.

[9] IDC, "IoT is Strategic to Organizations," http://www.idc.com/promo/thirdplatform/innovationaccelerators/iot.

[10] Online Trust Alliance, "Internet of Things," https://otalliance.org/iot.

[11] GSMA, "IoT Security & Connection Efficiency," http://www.gsma.com/connectedliving/future-iot-networks/.

In Japan, the National Center of Incident Readiness and Strategy for Cybersecurity released the General Framework for Secured IoT Systems.[12] It encourages security-by-design for IoT networks and platforms, as well as devices, and adopts a multi-stakeholder approach that includes manufacturers.[13]

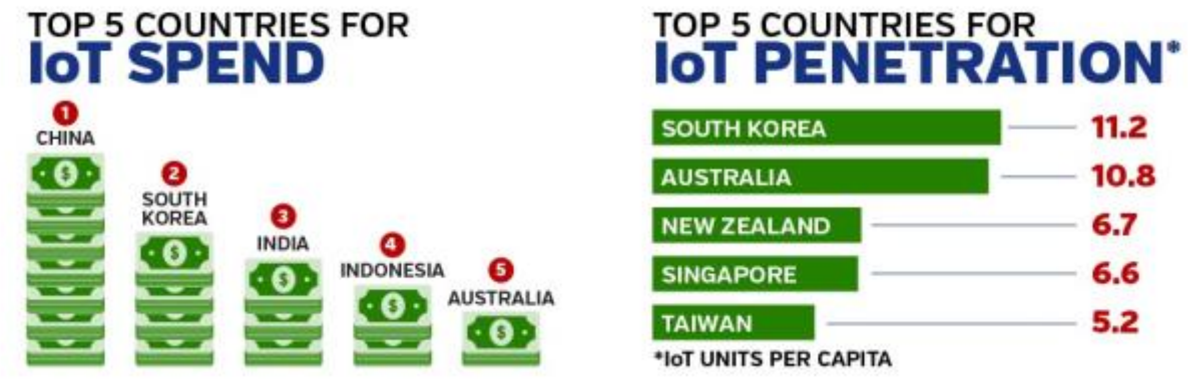
In Australia, an IoT Alliance was established in 2016 that brings together industry, government, academia, startups and investors to accelerate IoT innovation and adoption. One of its key priorities is to develop security and data protection guidelines for IoT services.[14]

The Opportunities

Advanced and large economies in the Asia-Pacific region are taking the lead in IoT development

The Republic of Korea, Australia and Japan are in the top five countries of IDC's G20 IoT Development Opportunity Index Ranking, indicating that these countries are most ready to generate and benefit from IoT.[15]

Countries that are leading in IoT development in the Asia-Pacific region include: Australia, China, India, Indonesia, Japan, Republic of Korea, New Zealand, Singapore and Taiwan.



Source: IDC, "Asia-Pacific Internet of Things Market Forecast," April 2015.

[12] See http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf.

[13] Mihoko Matsubara, "Assessing Japan's Internet of Things (IoT) Security Strategy for Tokyo 2020," *Paloalto Networks*, 19 September 2016, http://researchcenter.paloaltonetworks.com/2016/09/cso-assessing-japans-internet-of-things-iot-security-strategy-for-tokyo-2020/.

[14] IoT Alliance Australia, "What We Do," http://www.iot.org.au/what-we-do/.

[15] IDC, "IDC Launches Updated G20 Internet of Things Development Opportunity Index Ranking," 2 November 2016, http://www.idc.com/getdoc.jsp?containerId=prUS41888616.

A lot of hype around IoT comes from the consumer segment–connected baby monitors, refrigerators and cars. However, governments and businesses are starting to focus on developing and scaling IoT use cases in different sectors.[16]

TOP IoT USE CASES
1
SMART GRID
2
MANUFACTURING OPERATIONS
3
ASSET/FLEET MANAGEMENT
4
SMART BUILDINGS
5
PUBLIC SAFETY/ EMERGENCY SERVICES
6
DIGITAL SIGNAGE

An IDC survey of the Asia-Pacific region in 2015 identified the top six IoT use cases (left).

Another poll in 2016 revealed that 41% of the healthcare organisations in the Asia-Pacific region (excluding Japan) plan to launch at least one IoT solution in the next two years, focusing on remote patient monitoring, resource utilisation and tracking.[17] Over 63% believe it to be the central theme for driving digital transformation in health. them deal with the various dangers they face online.[18]

Source: IDC, "Asia-Pacific Internet of Things Market Forecast," April 2015.

Countries in the Asia-Pacific region are developing IoT roadmaps, plans and standards

These include:

- The ASEAN ICT Masterplan 2020 and ASEAN Smart Network Initiative - One of five outcomes of the Masterplan focuses on "Sustainable Development through Smart City Technologies," which includes the deployment of IoT technologies.[19]
- Australian authorities freed up additional spectrum bands dedicated to the use of IoT in December 2015.[20]
- China's 10-Year "Made in China 2025" IoT Roadmap.[21]
- India's IoT Draft Policy, 2015.[22]
- Japan's General Framework for Secured IoT Systems, 2016.[23]
- Republic of Korea's Master Plan for Building the Internet of Things, 2014.[24]
- Malaysia's National IoT Strategic Roadmap, 2014.[25]

[16] Glenn Burrows, "A Look into the IoT Crystal Ball," *Asia Outlook Magazine*, 23 February 2017, http://www.asiaoutlookmag.com/news/a-look-into-the-iot-crystal-ball.

[17] Enterprise IT World, "41% Healthcare organizations in APeJ to launch IoT solutions by 2019: IDC," 31 March 2017, http://www.enterpriseitworld.com/index.php/41-healthcare-organizations-in-apej-to-launch-iot-solutions-by-2019-idc/.

[18] Internet Matters, "E-safety app for parents and children," 4 August 2016, https://www.internetmatters.org/hub/esafety-news/new-e-safety-app-for-parents-and-children/.

[19] ASEAN, "The ASEAN ICT Masterplan 2020," https://www.trc.gov.kh/wp-content/uploads/2016/10/1.pdf.

[20] ITU, *Harnessing the Internet of Things for Global Development* (Geneva, 2016), http://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf.

[21] See https://community.iotone.com/t/report-made-in-china-2025-the-10-year-industrial-iot-roadmap-in-china/109.

[22] See http://meity.gov.in/writereaddata/files/Revised-Draft-IoT-Policy_0.pdf.

[23] See http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf.

[24] See http://karus.or.kr/uploadFiles/board/KOREA-IoT%20Master%20Plan.pdf.

[25] See http://mimos.my/iot/National_IoT_Strategic_Roadmap_Book.pdf; and for Executive Summary see http://mimos.my/iot/National_IoT_Strategic_Roadmap_Summary.pdf.

- New Zealand's Business Growth Agenda, 2017 includes initiatives to accelerate the adoption of IoT technologies through market research and the establishment of an IoT Alliance, a collaboration between industry and government.[26]
- Singapore's IoT Standards Outline in Support of the Smart Nation Initiative, 2015.[27]

In India, the government is driving IoT adoption by investing in smart cities and promoting startups. In collaboration with the private sector, it established a Centre of Excellence for IoT[28] that aims to support and nurture local talent to create enterprises that will drive the IoT market in the country.

Other emerging economies are exploring the use of IoT at a local scale and for more specific issues. For example, to reduce traffic congestion in the city of Makassar, in Indonesia, CCTVs provide a live video feed of traffic at highways and roads that tend to get congested.[29] In Thailand, the Provincial Electricity Authority is planning to roll out a smart grid pilot project in Pattaya by early 2018, including the installation of 120,000 smart meters in homes and the construction of a data centre for data processing.[30] The Philippines and Viet Nam are also planning smart city initiatives.[31]

These IoT initiatives are playing a role in providing new opportunities to innovate, producing some exciting startups in the region, and supporting the revival of small and medium enterprises.[32]

Furthermore, IoT is being used to combat climate change in the Asia-Pacific region, with national climate change plans incorporating the use of IoT to enhance energy efficiency and the uptake of renewable energy.[33]

Asia-Pacific countries are active in developing interoperability standards

Advanced economies such as Japan, Republic of Korea and Singapore are driving interoperability in the region. Singapore, for example, is trialling a new standard for over-the-air subscription management to enable SIM chips embedded in IoT devices to switch between different mobile operators.[34]

GSMA together with the mobile industry has been developing and standardising IoT technologies, such as low-power wide-area (LPWA) networks. Compared to other wireless systems, LPWA offers a longer range of connectivity and battery life at lower costs. They are suited to applications such

[26] Government of New Zealand, "The Business Growth Agenda: Building a Digital Nation," March 2017, http://www.mbie.govt.nz/info-services/science-innovation/digital-economy/building-a-digital-nation.pdf; and Stuart Corner, "New Zealand IoT Industry Alliance Formed," *IoT Australia*, 31 March 2017, https://www.iotaustralia.org.au/2017/03/31/iotnewanz/new-zealand-iot-industry-alliance-formed/.

[27] Spring Singapore, "Internet of Things (IoT) Standards Outline to Support Smart Nation Initiative Unveiled," 12 August 2015, https://www.spring.gov.sg/NewsEvents/PR/Pages/Internet-of-Things-(IoT)-Standards-Outline-to-Support-Smart-Nation-Initiative-Unveiled-20150812.aspx.

[28] See http://coe-iot.com.

[29] Tan Wee Kwang, "Driving IoT Growth in Asia," *eGov Innovation*, 1 November 2016, http://www.enterpriseinnovation.net/article/driving-iot-growth-asia-1907449576.

[30] GSMA, "The Mobile Economy: Asia Pacific 2016," 2016, https://www.gsmaintelligence.com/research/?file=5369cb14451e0db728bd266c7657a251&download.

[31] Asia IoT Business Platform, http://iotbusiness-platform.com/iot-philippines/ and http://iotbusiness-platform.com/iot-vietnam/.

[32] For examples of Asian IoT startups see: Shona, "Internet of Things (IoT) Startups in Asia," Demystify Asia, 10 August 2016, http://www.demystifyasia.com/internet-things-iot-startups-asia/; and Joe Liebkind, "7 Asian IoT startups set to change the way you live," TechInAsia, 21 January 2016, https://www.techinasia.com/talk/7-asian-iot-startups-set-change-live.

[33] See Issues Paper on Climate Change.

[34] Infocomm Media Development Authority, "Leading the Charge for Open IoT Standards," 28 November 2016, https://www.imda.gov.sg/infocomm-and-media-news/whats-trending/2016/1/leading-the-charge-for-open-iot-standards.

as environmental sensors, energy meters, logistics tracking, and animal and crop monitoring that require large numbers of widely dispersed devices to send occasional status updates.[35]

In 2016, Korea Telecom, which has been taking the lead in IoT development in the Republic of Korea[36], established a nationwide IoT network based on the 3GPP network standard, LTE-M. This is the first LPWA network to serve IoT devices and services. It also set up IoT Makers–an open platform for developers to design and test IoT solutions with ease, thus reducing costs and time-to-market. In 2016, about 1,000 new services were created on the platform with 100,000 devices connected.[37]

GSMA together with China Mobile, China Unicom, Korea Telecom, KDDI and NTT DOCOMO in Japan, along with other telcos are also looking to establish an IoT Big Data Ecosystem that will deliver harmonised data sets and application programming interfaces (APIs),[38] thus enabling easy adaptation and deployment of IoT solutions in multiple locations.

Furthermore, IoT-conscious Asia-Pacific countries are working with the ITU to enable the coordinated development of IoT, particularly in smart cities.[39] Other international standards bodies like the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF) have IoT-related activities. Industries in the region are likewise part of a number of IoT-specific standardisation groups, including OneM2M,[40] the Industrial Internet Consortium[41] and the AllSeen Alliance.[42]

Alignment with the SDGs

The SDGs do not specifically mention IoT, but refer to ICT and various technologies and innovations as a means to achieve the SDGs. The relevant targets include:

- Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020 (SDG9c).
- Fully operationalise the technology bank and science, technology and innovation capacity-building mechanism for least developed countries by 2017 and enhance the use of enabling technology, in particular information and communications technology (SDG17.8).

The ITU has produced a report documenting examples of how IoT is being used to help realise the SDGs.[43]

[35] GSMA, "Mobile Internet of Things Low Power Wide Area Connectivity - Industry Paper," 2016, http://www.gsma.com/connectedliving/wp-content/uploads/2016/03/Mobile-IoT-Low-Power-Wide-Area-Connectivity-GSMA-Industry-Paper.pdf.

[36] GSMA, "The Connected Living Programme," http://www.gsma.com/connectedliving/connected-living-mobilising-the-internet-of-things/.

[37] Broadband Commission, "The State of Broadband 2016," September 2016, http://broadbandcommission.org/Documents/reports/bb-annualreport2016.pdf.

[38] GSMA, "IoT Big Data," http://www.gsma.com/connectedliving/iot-big-data/.

[39] ITU, "ITU-T, Smart Sustainable Cities," http://www.itu.int/en/ITU-T/ssc/Pages/default.aspx; and Marco Carugi, "Overview of Internet of THings Standardization Activities in ITU (ITU-T SG20)," presentation made at the ISO/IEC/ITU Internet of Things Workshop, Berlin, Germany, 13 May 2016, https://www.din.de/blob/160428/5120ec266254d2f46773497219f7ba2f/itu-data.pdf.

[40] See http://www.onem2m.org/.

[41] See http://www.iiconsortium.org/.

[42] See https://allseenalliance.org/.

[43] ITU, *Harnessing the Internet of Things for Global Development* (Geneva, 2016), http://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf.

Questions to Think About

- What regional or national approaches can be adopted to leverage IoT to achieve the SDGs, particularly through the development of innovative IoT solutions by local researchers and industries?
- What is the best way to ensure that IoT device manufacturers integrate privacy-by design and security-by-design principles, as well as interoperability standards into their core values?
- What steps can industry take to develop a “code of practice” that helps improve overall IoT security and privacy? Which other stakeholders should be a part of such an initiative?
- How can we ensure the user (and not the manufacturer or service provider) has full control over data generated by their IoT device? What process should be in place to seek user consent when accessing or using the data?
- What is the impact of IoT development and deployment on gender relations, on people with disabilities and on other marginalised groups? What strategies need to be in place to ensure that IoT development and deployment are gender sensitive and inclusive?
- Are there regional or national platforms for multiple stakeholders to engage in meaningful dialogue on the wide-ranging IoT challenges?

cc BY SA