International Journal of

IoT Law & Public Policy

FEATURED ARTICLES:

Government Action on IoT Security

Expediting Trade: Smart Technologies and Cross Border Commerce

VOLUME 1 • ISSUE 1

2018

Table of Contents

IoT M2M Council (IMC), 16 Sussex Street London SW1V 4 RW, United Kingdom
Tel: +44 20.7596.8777 - info@iotm2mcouncil.org
http://www.iotm2mcouncil.org/

©Copyright 2018 IMC. All rights reserved.

Government Action on IoT Security

Peter F Stone,
Counsel, Hopkins Carley, Palo Alto

1 Introduction

High profile cyberattacks effected through IoT devices have drawn the attention of media and the public worldwide. Headlines were made by recent revelations that foreign governments may have achieved the ability to gain control of critical US infrastructure through attacks on networked nodes within the utility grid.

Governments at all levels in the US and abroad are responding with a variety of initiatives ranging from public education and best practices advisories to formulation of new prescriptive and prohibitive regulations and application of prior laws and regulations to address IoT security concerns. Congress, executive branch departments, independent regulatory agencies and state governments are all in the early stages of formulating responses to the vulnerabilities that security incidents have exposed.

This article highlights key arenas of government action that are addressing IoT security. Our intent is to encourage IMC members and the IoT industry as a whole to focus attention on government initiatives that are of increasing importance to the industry.

2 Consumer Devices

The FTC is the lead agency regulating commercial practices affecting consumers. The Commission has been the forum in which consumer groups have launched litigation directed at a class of IoT consumer devices – connected children's toys – that are charged with significant breaches of data privacy regulations.

- 2.1 United States v. VTech Electronics

  In January of this year, the FTC settled a complaint against electronic toy manufacturer VTech Electronics Limited that alleged violations of the Children's Online Privacy Protection Act (COPPA). According to the complaint, VTech collected personal information from parents on its Learning Lodge Navigator online platform, where the Kid Connect app was available for download. Parents were required to register and provide personal information including their names, email addresses, their children's names, dates of birth and gender. VTech also collected personal information from children when they used the Kid Connect app.

  The violation charged was the collection of personal information on millions of children without providing direct notice and obtaining parental consent. The company was also charged with failing to take reasonable steps to secure the data it collected. The FTC further charged that the company violated the COPPA Rule by failing to post a privacy policy for their Kid Connect online service providing clear, understandable, and complete notice of their information practices; failing to provide direct notice of their information practices to parents; failing to obtain verifiable parental consent prior to collecting, using, and/or disclosing personal information from children; and failing to establish and maintain

©Copyright 2018 IMC. All rights reserved

reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. [1]The FTC further charged that the company violated the COPPA Rule by failing to post a privacy policy for their Kid Connect online service providing clear, understandable, and complete notice of their information practices; failing to provide direct notice of their information practices to parents; failing to obtain verifiable parental consent prior to collecting, using, and/or disclosing personal information from children; and failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. [2]

As part of the settlement, VTech agreed to pay a penalty of $650,000 and agreed to independent audits of its ongoing compliance with COPPA for a period of 20 years. While some observers characterized the settlement as a slap on the wrist given the magnitude of the breach, the FTC noted in its release that this was first time that the agency had brought a privacy and security case involving connected toys.

- 2.2 Connected Consumer Devices and DDOS Attacks

Consumer devices have been prominent in many of the highly publicized distributed denial of service (DDoS) attacks of recent years such as the 2016 Dyn cyberattack. That attack took down a who's who of famous websites including Etsy, Netflix, Spotify, and Twitter. It utilized a botnet of connected consumer devices, including video cameras, printers and baby monitors, to generate millions of domain name lookup requests that clogged the Internet for hours at a time.

These consumer devices typically contained well recognized security vulnerabilities such as uniform and commonly utilized default passwords with no instructions to consumers as to how or why to change them. Many of these devices do not have the processing capability to accept updates, leaving no alternative to complete recall in order to eliminate the vulnerability that could otherwise be exploited.

The Department of Homeland Security and the FBI launched investigations into the attacks on Dyn. [3] The FTC has not formally investigated the role of these connected consumer devices in DDoS attacks, nor has it issued any regulations directed at reducing or eliminating the vulnerabilities that the attackers exploited.

However, the FTC has issued guidance for manufacturers who wish to strengthen their products' ability to withstand cyberattacks. In February 2018, the FTC released a report with recommendations on ways to improve the security of mobile devices. The FTC's recommendations center around the need to incorporate the capability to patch vulnerabilities. In a possible precursor to potential prescriptive regulation, the FTC suggested that manufacturers could require purchasers of connected products to change default passwords as part of the installation or activation of the device.

Other regulatory agencies and executive branch departments are likely to proceed along a similar path. Agencies are in no hurry to adopt new regulations. They are afraid of getting it wrong. But they will continue to encourage the industry to upgrade its designs and practices around cybersecurity.

- 2.3 Potential for Private Litigation

[1] UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF ILLINOIS EASTERN DIVISION Case No : 1:18-cv-114 United States of America vs VTECH Electronics Ltd & VTECH Electronics North America LLC, 8th January 2018, https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_stip_order_1-8-18.pdf

[2] ibid

[3] Finkle, Jim, Volz, Dustin, Homeland Security Is 'Investigating All Potential Causes' of Internet Disruptions, Time, 21 October 2016, http://time.com/4540921/internet-dyn-outage-homeland-security/

©Copyright 2018 IMC. All rights reserved

Not to be overlooked as a motivator to improving security practices is the likelihood of class action lawsuits on behalf of consumers injured by security breaches. As certain basic security practices, such as the ability to remotely update IoT devices, become entrenched, failure to adhere to these practices is likely to result in manufacturers being found liable under negligence or product liability theories.

3 Legislative Initiatives

Congressional initiatives to date are focused on using market mechanisms to motivate industry to adopt security best practices.

- 3.1 Warner-Gardner Bill

  The piece of legislation most frequently cited is the Internet of Things (IoT) Cybersecurity Improvement Act of 2017, sponsored by Senator Mark Warner (D-VA) and co-sponsored by Senators Cory Gardner (R-CO), Ron Wyden (D-OR); Steve Daines (R-MT); and Margaret Wood Hassan (D-NH). The bill was introduced in the Senate August 1, 2017 and has been referred to the Committee on Homeland Security and Governmental Affairs. The bill is intended to "provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal Agencies." The sponsors aim to put the full weight of government procurement and the huge market that it represents behind the push for IoT device adherence to cybersecurity standards.

  Government suppliers and contractors would be required to provide written certification that devices supplied to the government (i) do not contain any known security vulnerabilities, (ii) rely on software or firmware that is capable of accepting properly authenticated updates from the vendor, (iii) use only non-deprecated industry-standard protocols and technologies for communications, encryption, and interconnection with other devices; and (iv) do not include any fixed or hard-coded credentials for remote administration, delivery of updates or communication. [4]

  The bill would also require vendors to notify the purchasing agency of any security vulnerability subsequently disclosed to or discovered by the vendor. Government contracts for Internet-connected devices would need to require that such devices be updated to allow any future security vulnerability to be patched in order to fix the vulnerability. [5]

  The bill does allow purchasing federal agencies to side-step its requirements on the grounds of compliance being either technically or economically unfeasible. In such a case, the agency can petition the Office of Management and Budget for a waiver. [6]

  Non-compliant devices under the bill may be considered for use by federal agencies if the Office of Management and Budget and NIST agree to their use when combined with network security measures such as network segmentation or micro-segmentation, system level security controls, including containers or microservices, multi-factor authentication, or intelligent network or edge systems that can isolate, disable or remediate connected services. [7]

  Criticism of the bill might include some ambiguity in defining the devices covered by the proposed legislation. The bill defines its scope as covering any device that is 'capable of

[4] Internet of Things Cybersecurity Improvement Act of 2017, https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017

[5] ibid

[6] ibid

[7] ibid

©Copyright 2018 IMC. All rights reserved

connecting to … the Internet' and that can 'collect, send or receive data.' [8] This is a broad definition. It encompasses not only devices that are conventionally described as belonging to the Internet of Things category, but other devices such as servers, desktop computers, laptops and phones. It is unclear if the bill intends to cover every class of computer as well as such recognised IoT devices as Internet enabled printers and webcams.

The Cybersecurity Improvement bill has been read twice and is currently referred to the Committee on Homeland Security and Governmental Affairs.

- 3.2 Markey-Lieu Bill*

  In 2017, a bill was introduced in the Senate that took a different, albeit not conflicting, approach, the Cyber Shield Act of 2017, sponsored by Senator Edward Markey (D-MA) and Representative. Ted Lieu (D-CA).

  The bill aims to use yet another voluntary, market-based set of incentives – consumer purchasing power - to influence the design of IoT products in a more security-conscious direction. The Markey bill would establish an advisory committee to create a security seal of approval program based on IoT products' security standards compliance. Presumably, consumers would prefer to purchase products that are less hackable and would rely on seals of approval to guide their purchasing decisions.

  The scheme is voluntary. It permits vendors to submit their products for review and certification and places a duty on the advisory committee to create and maintain cybersecurity and data security benchmarks for devices within the scope of the bill. [9]

  This duty would apply, according to the bill, to any 'consumer-facing physical object that can – connect to the Internet; and collect, send, or receive data.' [10] Such a definition would cover phones and laptops, and possibly desktop computers as well as conventionally termed Internet of Things objects. However, it would not cover many Internet of Things devices embedded into infrastructure or used in a business environment, as these are not 'consumer-facing'.

  sThe bill is ambiguous as to whether it is intended to cover embedded IoT devices that are part of a building, energy, or transport infrastructure that are operated by a business, but are part of infrastructure used by consumers. With some devices, it might be clear as to which ones are 'consumer-facing'. However, there are other such devices where the level of being 'consumer-facing' may be a point of contention.

- 3.3 Current Status of Legislation

  Neither bill has received a hearing yet, although the Warner bill is almost two years beyond its initial introduction. While commentaries on the Warner bill from people who follow the space have been generally favorable, Congress has no great sense of urgency to act, preferring to let others – particularly industry – take the lead.

4 Regulation Outside the U.S.

The climate is different in other countries – notably Europe and China. Government regulation of IoT is a much hotter topic outside the US. China has adopted its first cybersecurity law, which will apply to all companies doing business in China. It carries the potential for large fines for non-compliance.

[8] Ibid
[9] Cyber Shield Act of 2017, https://lieu.house.gov/sites/lieu.house.gov/files/CyberShield.pdf
[10] ibid

©Copyright 2018 IMC. All rights reserved

In September 2017 the European Commission issued a proposal for a unified certification framework for cybersecurity in ICT products. Under the EC proposals, the EU Network and Information Security Agency, ENISA, would be tasked with ‘proactively' contributing to the development of policy in the area of network information security, as well as to other policy initiatives with cybersecurity elements in different sectors (e.g. energy, transport, finance).

ENISA would also support the EU policy and law in the areas of electronic communications, electronic identity and trust services, with a view to promoting an enhanced level of cybersecurity. The agency would be required to contribute to the establishment of Information Sharing and Analysis Centres (ISACS) in various sectors by providing best practices and guidance on available tools and procedures. [11]

The EC proposals have however been trenchantly criticised for failing to emphasise the role of risk-based management, blurring the separation of standards, legislation and conformity assessment, and downgrading the role of cybersecurity standards in ensuring device security. [12]

5. Standards-Based Regulation

In the US, regulators seem to be content to issue advisories and guidelines on the grounds that it is too early in the development of IoT for adoption of hard and fast regulations. Like legislators, they are calling on industry to take the lead.

- 5.1 Industry-Favored Deliberate Approach

  Many industry voices echo the sentiment that the government should proceed very deliberately on IoT regulation, because the technology is evolving rapidly. Premature regulation could have the unintended result of freezing development of new technologies that have the potential to actually raise the bar of best practices around security. However, there is the risk that developments outside the US will generate that freezing effect for US products that need to have the availability of all major markets. In that view, the US had better get into the act with a more proactive stance toward regulation so as to influence the development of international cybersecurity standards.

  Evolution of industry standards – typically the outcome of a voluntary government-industry collaboration – can help to drive state-of-the-art security practices into product development of IoT devices – security by design. Eventually, regulation will catch up. As an example, the security standards set out in the Warner bill, which, as noted, is far from actual adoption, already reflect the input of industry and academic experts and represent a fair approximation of what is already an informal industry standard approach.

  Companies making IoT products will find it difficult to ignore emerging standards, even though these standards will undoubtedly raise costs and even threaten the viability of some ultra-low cost products. From an industry standpoint, however, a collaborative standards-making approach in which industry has a strong voice is likely the best path for sensible regulation.

- 5.2 NIST Report

  In an example of public-private collaboration, NIST has just released for public comment (comment period ends April 18, 2018) - with significant industry input - a draft of its

[11] Cybersecurity Package – European Commission, https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

[12] OpenForum Europe Feedback to the European Commission – EC, https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477/feedback/F8002_en

©Copyright 2018 IMC. All rights reserved

Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT). This Report seems destined to become a major reference point in the discussion of IoT security. Annex D to the report is a compendium of IoT standards that includes a characterization of the state of maturity of each standard. Some have gained much greater adherence than others. The standards are broken down into 11 areas of cybersecurity concern: cryptographic techniques; cyber incident management; hardware assurance; identity and access management; information security management; IT system security evaluation; network security; security automation and continuous monitoring; software assurance; supply chain risk management; and system security engineering.

The report also highlights security issues specific to five major IoT verticals – connected vehicles, consumer IoT, health IoT and medical devices, smart buildings and smart manufacturing.

6 Summary

Given the scary headlines and the scary realities underneath the headlines, the rapid march of technology aimed at addressing IoT security issues may be matched by unusually rapid standards adoption. The next stage will be government regulatory and legislative action, hopefully based on standards supported by industry. IoT companies will no doubt move aggressively to adopt best security practices throughout their businesses.

©Copyright 2018 IMC. All rights reserved

Expediting Trade: Smart Technologies and Cross Border Commerce

William Payne

Introduction

Cross border trade accounts for over half of global trade. About 77% ($32.18 trillion) of that trade is made up of goods – the rest is services.[13] Yet global cross border trade is falling in relative terms. The fall has become so marked and long-standing that economists at the World Bank and the International Monetary Fund have coined the term 'Peak Trade', suggesting that cross border trade has now embarked on a course of irretrievable long term decline.[14]

At the same time, concerns over international terrorism, mass migration and international criminal activities, such as drug smuggling, have led governments in every part of the world to strengthen existing borders.

In order to accelerate cross border trade, a number of governments are investigating the use of cross border technologies. These countries include China, Japan, Singapore, Australia, Republic of Korea, New Zealand, Canada, and the United Kingdom. All these countries have embarked, or are preparing to embark, on extensive plans to implement new technologies to accelerate and simplify cross border trade while maintaining or improving border counter terrorism and criminal justice systems.

The core technology that countries are highlighting in their strategies are variants of Internet of Things (IoT). This is frequently coupled with blockchain, upgraded telecommunications infrastructures, artificial intelligence (AI), and real-time analytics.

This article examines the approaches to cross border technology and the initiatives being put in place by governments in three separate regions.

China provides the example of a consolidated grand strategy approach involving up to $8 trillion dollars of investment[15] spread over a decade or more of planned infrastructure development, coordination with 62 nations involved, and invested with the prestige of President Xi.

The six Asia Pac advanced economies of Japan, Australia, Korea, Taiwan, New Zealand, and Singapore are adopting a collaborative approach among themselves. They are sharing technology, developing joint projects, with pilots to test new technology and logistical models.

In Europe, the European Union initiated a smart borders programme in 2015 under the aegis of the eu-Lisa Security and Justice Technology Agency. A pilot was carried out involving 12 countries across the Union. The pilot was found, according to the eu-Lisa Agency, to prove the technology as both operationally and technically feasible, and that use of it did not infringe fundamental rights.

[13] World Trade Organisation; World Trade Statistical Review 2016; https://www.wto.org/english/res_e/statis_e/wts2016_e/wts2016_e.pdf

[14] A troubling trajectory, Dec 11th 2014, The Economist, https://www.economist.com/news/finance-and-economics/21636089-fears-are-growing-trades-share-worlds-gdp-has-peaked-far

[15] Bruce-Lockhart, Anna, China's $900 Billion New Silk Road Explained, CW Magazine, 27 October 2017, https://english.cw.com.tw/article/article.action?id=1703

©Copyright 2018 IMC. All rights reserved

The United Kingdom is confronting the need to maintain trade and free movement of people over its land border with the Republic of Ireland, even as it becomes a 'third country' in regard to the European Union. It is investigating the adoption of smart border technology in order to allow rapid transit of goods through both its land border and its east coast ports.

An EU appointed expert who has drafted the European Parliament report on the subject, former director of the World Customs Organisation Lars Karlsson, has said that the UK's adoption of smart border technology will give it extra advantages over EU countries in trade.[16]

Peak Trade

Cross border trade accounts for a significant proportion of global GDP. Yet its share of global GDP has been falling year on year for nearly a decade - hurting especially those developed economies whose success depends on exports. Traditional regional strategies of expanding cross border trade by reducing or removing border impediments to trade and movement are increasingly facing resistance as a result of security concerns and political pressures.

In 2016, according to the World Bank, cross border trade accounted for 56.40% of global GDP, amounting to $42.78 trillion out of total world GDP of $75.85 trillion.[17] ,[18]

However, that figure is falling. In 2014, the proportion of global cross border trade to global GDP was 57.91%, while in 2011, the figure had been 60.56% of global GDP.[18]

This diminution in share of GDP is a result of a slow down in growth of cross border trade. In the two decades before the global financial crisis, cross border trade grew at 7% a year on average, outpacing the overall rate of global GDP. But since 2011, cross border trade has faltered, falling behind the overall pace of GDP growth.[14]

Some economists have invented the term 'Peak Trade', seeing a parallel with 'Peak Oil'. 'Peak Trade' suggests that the world has reached the maximal point of global trade, and that it is now in inevitable and unstoppable decline. Economists Cristina Constantinescu and Michele Ruta of the International Monetary Fund and Aaditya Mattoo of the World Bank have argued that the slowdown in cross border trade is the result of a maturing of established supply chains and associated supporting technologies.[19] The three economists also argue that the establishment of the World Trade Organisation and the completion of the Uruguay Round of trade talks in 1994 gave a decades long boost to global cross border trade the began to peter out in the early 2010s.[19]

This IMF/World Bank analysis argues that, starting in 2011, there were three factors leading to a slowing of world cross border trade: a stagnation in logistics and supply chain technologies; non-innovation in supply chain business models; and an absence of major global or regional initiatives to stimulate cross border trade, as there had been in the early 1990s with the Uruguay Round.

China: One Belt, One Road

China and the EU are two of the world's three largest trading blocs. The EU is China's largest trading partner and China is now the EU's second-biggest trading partner, behind the United

[16] Malnick, Edward, Smart borders after Brexit will give Britain 'extra advantage', EU-commissioned expert says, The Daily Telegraph, 24 February 2017, https://www.telegraph.co.uk/politics/2018/02/24/smart-borders-brexit-will-give-britain-extra-advantage-eu-commissioned/

[17] Global GDP figures 2016, The World Bank, https://databank.worldbank.org/data/download/GDP.pdf

[18] Trade (% of GDP), Data - World Bank, https://data.worldbank.org/indicator/NE.TRD.GNFS.ZS

[19] Constantinescu, Cristina; Mattoo, Aaditya; Ruta, Michele; Global Trade Slowdown, Cyclical or Structural?; IMF/World Bank/World Trade Organisation; 6 November 2014; https://www.imf.org/external/np/seminars/eng/2014/trade/pdf/constantinescu.pdf

©Copyright 2018 IMC. All rights reserved

States.[20]

Almost all goods (99%)[21] traded between the two regions are transported by sea. Land corridors through Central Asia have rarely been used.

China's One Belt, One Road (Yi dai, Yi lu) is an effort to boost trade between China and Europe, as well as other destinations, including Africa, South East Asia, and the Gulf region. The aim is to modernise and build rail and road infrastructure on overland routes between China and Europe, spanning a number of Central Asian and East European states. In addition, the strategy also calls for the modernisation and creation of large scale port facilities along maritime routes from the East China Sea and South China Sea through to the Mediterranean via the Indian Ocean, Red Sea and Suez Canal.

In addition to modernising and building new transport infrastructure and port facilities, China is embarking on a programme of cargo tracking and environmental monitoring and integrated supply chain management over the multiple stages and facilities of both the overland and maritime routes. This is requiring the construction of high speed networks, IoT services, and satellite services on both the six trans-Asia overland routes and the maritime routes.

The One Belt, One Road strategy is not focused solely on China - Europe trade. The initiative is equally about improving access and infrastructure throughout Central Asia, including Pakistan, the Central Asian states, and Russia, as well as along the maritime route, including Singapore, Kolkata in India, Gwador in Pakistan, Djibouti on the Horn of Africa, as well as Piraeus in Greece. Developing deeper trading links with the Gulf region and with East Africa is also a goal. With the development of Piraeus Harbour in Attica, Greece, and mooted acquisition of port facilities in Hamburg[22], as well as direct rail connections from China to deep harbour facilities in Rotterdam and London Gateway, the western end of the One Belt, One Road could serve as a future transhipment point onwards to western Africa and the eastern seaboards of the United States and South America.

The Information Silk Road

The One Belt, One Road initiative (OBOR) also incorporates telecommunications infrastructure, under the title of the Information Silk Road, which has the aim of complementing rail, road, maritime and port infrastructure with a global network of high speed, land-based optical cables, transcontinental submarine cables and improved satellite networks spanning the entire distance of the multiple overland and sea routes.[23]

Chinese telecom operators China Telecom, China Unicom and China Mobile have already embarked on OBOR-related projects. These include projects across the Central Asia region, South East Asia, and the India Ocean littoral. This includes improving infrastructure in eastern Africa, which is part of the maritime OBOR route and an intended destination point.[24]

[20] China - Trade - European Commission, http://ec.europa.eu/trade/policy/countries-and-regions/countries/china/

[21] Potential for Eurasia Land Bridge Corridors, EC DG TREN 6FP, https://www.tno.nl/media/2825/report_potential_eurasia_land_bridge_rail-corridors_final_25042012.pdf

[22] Eldering, Paul, Chinese opmars bedreiging haven - Rotterdam dreigt slag te verliezen, De Telegraaf, https://www.telegraaf.nl/financieel/268209/rotterdam-dreigt-slag-te-verliezen

[23] Beijing's Silk Road Goes Digital, Council on Foreign Relations, June 6, 2017, https://www.cfr.org/blog/beijings-silk-road-goes-digital

[24] Key connectivity improvements along the Belt and Road in telecommunications & aviation sectors, Ernst & Young, September 2016, http://www.ey.com/Publication/vwLUAssets/ey-china-go-abroad-4th-issue-2016-en/$FILE/ey-china-go-abroad-4th-issue-2016-en.pdf

©Copyright 2018 IMC. All rights reserved

The Space Based Silk Road

In addition to the overland and submarine optical cable networks, China is embarking on a Silk Road in Space, a chain of satellites from the North Sea to the East China Sea based on the Beidou satellite network. Using China's own version of GPS, this is designed to support telecommunications and IoT services across the length of both overland and maritime routes. Basic services are designed to be active along both routes during the course of 2018. Limited satellite network services supporting the route infrastructure were already in operation along parts of the Indian Ocean littoral in Summer 2017.[23]

Chinese telecommunications operators are targeting Gulf region and Middle Eastern markets for IoT services, remote sensing and telecommunications requirements through the China based International Alliance of Satellite Application Service (ASAS).[25]

Chinese Telecoms Restructuring

The Chinese Government has also embarked on a restructuring of the country's telecoms industry, with the government shifting the major operators towards mixed ownership models.[26]

The reforms of the Chinese telecoms sector are implicitly connected with the One Belt, One Road strategy.[24] The aim of the structuring is to encourage greater innovation and investment in the One Belt, One Road telecoms initiatives, and also allow corporations and governments in regions being modernised through upgraded telecoms infrastructure to invest in the entities carrying out the programme.

Smart Cities

The One Belt, One Road initiative also includes the development of Smart Cities. Both ZTE and Huawei are focusing Smart City development efforts on cities that lie along the demarcated overland and maritime OBOR routes. These include developments in Singapore, the Philippines, Kenya, Malaysia, Germany and within China. China's model smarty city, Yinchuan, is an ancient Silk Road city that is now poised to play a pivotal role in the New Silk Road.[23]

IoT and One Belt, One Road

The Chinese Government sees IoT as a key enabling technology of the One Belt, One Road programme.[27]

As part of the strategy, China Telecom and Ericsson have launched the China Telecom IoT Open Platform, which has been designed to interconnect and interoperate with different IoT technologies across the sixty different countries in Asia, Europe and Africa that are taking part in the OBOR initiative. The China IoT Open Platform enables a common unified overview of devices and access networks, and will be available across the six separate overland routes being developed from China to Europe, as well as the maritime route through the Indian Ocean to Africa and through the Suez Canal, to Europe.

French company Actility has also been engaged to build low bandwidth IoT networks along the

[25] Jiang Jie, Nation considers space-based ‘Silk Road of satellites’ to provide data services, Global Times, 31 May 2015, http://www.globaltimes.cn/content/924600.shtml

[26] China state-owned telecom privatisation seen as too timid, Financial Times, 21 August 2017, https://www.ft.com/content/0dd0b152-8659-11e7-bf50-e1c239b45787

[27] Daniels, Guy, IoT to play a key role in China's "One Belt One Road" economic strategy, Telecom TV, 6 July 2017, http://www.telecomtv.com/articles/iot/iot-to-play-a-key-role-in-china-s-one-belt-one-road-economic-strategy-15789/

©Copyright 2018 IMC. All rights reserved

OBOR land routes to track cargo, monitor environmental conditions and provide cargo tracking intelligence.

The build out of the cargo tracking LoRa network will begin in the city of Xi'an, considered as a principal starting point in China for the overland OBOR routes westwards.[28]

Asia Pac Advanced Economies

Just behind the world's three largest trading blocs of the United States, the EU and China, there is a fourth grouping defined by the IMF and the World Bank: the Asia Pac Advanced Economies.[29] With a cumulative GDP of $9.66 trillion, just behind China's $11.2 trillion, the Asia Pac Advanced Economies form a geographic and economic cluster with close trading, political and military ties. There are six countries in this grouping: the economic giant of Japan, followed by Australia, Republic of Korea, Taiwan, Singapore, and New Zealand.

All six countries trade closely with each other. However, unlike a grouping such as the European Union, which aims at the removal of international borders within the bloc, the Asia Pac Advanced Economies wish to maintain and strengthen their existing borders.

As each of the six wishes simultaneously to strengthen its borders and accelerate and simplify the flow of trade between each of the six as well as other neighbouring countries, developing and implementing smart border logistics and management systems is a key concern to each of them.

Japan

Japan is currently conducting two pilots aimed at accelerating cross border trade. A collaboration between Misui OSK Lines (MOL), the Sumitomo Mitsui Financial Group (SMFG), the Sumitomo Mitsui Banking Corporation (SMBC), the Japan Research Institute (JRI), and IBM Japan is trialling a pilot employing blockchain to streamline cross border logistics and goods handling.[30]

A second pilot is aimed at accelerating trade between Japan and Singapore, and is being undertaken by Japanese bank MUFG and Japanese telecoms operator NTT. This pilot is also utilising blockchain and is aiming to integrate Japanese trading systems with Singapore's recently developed National Trade Platform (NTP). According to participants, the goal is to 'help lay the foundation for a regional digitalised trade and supply chain platform in Asia'.[31]

Singapore Customs is collaborating with NTT and MUFG in integrating and developing the system.[32]

Singapore

In addition to working with Japan on the NTT - MUFG cross border trading pilot, Singapore has also initiated a cross border trade platform with Hong Kong. The Global Trade Connectivity Network (GTCN) is described as a platform for 'seamless transfer of digital documents and data

[28] IoT to help turn the Silk Road into a modern-day transport corridor, International Telecommunication Union, 2 August 2017, http://news.itu.int/iot-to-help-turn-the-silk-road-into-a-modern-day-transport-corridor/

[29] Regional Economic Outlook: Asia Pacific, October 2017: Making the Most of the Upswing, 9 October 2017, IMF, https://www.imf.org/en/Publications/REO/APAC/Issues/2017/10/09/areo1013

[30] Demonstration Test of Blockchain Technology in Cross-Border Trade Operations, Mitsui O.S.K. Lines, 12 December 2017, http://www.mol.co.jp/en/pr/2017/17090.html

[31] Bermingham, Finbarr, Blockchain pilot to boost Singapore-Japan trade ties, Global Trade Review, 7 December 2017, https://www.gtreview.com/news/fintech/blockchain-pilot-boost-singapore-japan-trade-ties/

[32] Antonovici, Anatol, Japan, Singapore Start Blockchain Pilot to Improve Trade Links, Cryptovest, 7 December 2017, https://cryptovest.com/news/japan-singapore-start-blockchain-pilot-to-improve-trade-links/

©Copyright 2018 IMC. All rights reserved

across borders, starting with the Singapore - Hong Kong trade corridor'.[33]

Australia

Second largest of the Asia Pac Advanced Economies, Australia is developing a strategy to create a single digital platform for all the country's international trade. The strategy has been developed by Australia's Home Affairs Agency.

In a report to the Australian Parliament, the Home Affairs Agency submitted that it is examining technology options to provide visibility of goods as they move through global supply chains outside the country's borders, in order to expedite cross border trade and ensure greater security at the border. Among the technologies the Home Affairs Agency is reviewing is blockchain and artificial intelligence.[34]

Republic of Korea

The Republic of Korea operates a mature, paperless trading system, KTNET. The platform was established by the Ministry of the Knowledge Economy (MKE). It is underpinned by a series of laws that include the e-Trade Facilitation Act (2005), The Commercial Law Act (2007), the Electronic Transactions Act, and the Digital Signature Act.[35]

According to KTNET, the platform has cut Samsung's lead time by 67% and processing time by 80%.[35]

Korea has cross border electronic initiatives based on the KTNET platform with Japan, China, Taiwan, Hong Kong, Macau, Australia, and New Zealand. The Korean Government is working on developing further initiatives through the Association of Southeast Asian Nations (ASEAN).[35]

The European Union

The European Union has a smart borders development programme under the eu-Lisa Security and Justice Technology Agency. It ran a major pilot study involving 18 countries in 2015.

Other countries within Europe already operate smart borders, notably Norway along its land border with Sweden.

The United Kingdom is investigating the use of smart technologies for port based goods clearance and for its land border with the Republic of Ireland following its departure from the European Union. The UK Government has made achieving 'friction-less trade' a key priority,[36] and is looking at smart technologies as part of a composite approach to achieving this.

The eu-Lisa Smart Borders project

The European Union has the goal of establishing smart borders at the external boundaries of the

[33] Bermingham, Finbarr, Hong Kong-Singapore blockchain trade platform to go live in 2019, Global Trade Review, 15 November 2017, https://www.gtreview.com/news/asia/hong-kong-singapore-blockchain-project-to-go-live-in-2019/

[34] Coyne, Allie, Home Affairs plots a 'single digital window' for Australia's international trade, itnews, 6 February 2018, https://www.itnews.com.au/news/home-affairs-plots-a-single-digital-window-for-australias-international-trade-484531

[35] Korea's experience in cross-border paperless trade facilitation, United Nations ESCAP, 14 February 2017, http://www.unescap.org/sites/default/files/11_Korea%27s%20experience%20in%20CBPT%20Facilitation%20v1.0.pdf

[36] Future customs arrangements - a future partnership paper, UK HM Treasury, 15 August 2017, https://www.gov.uk/government/publications/future-customs-arrangements-a-future-partnership-paper

©Copyright 2018 IMC. All rights reserved

Union.

The EU has established a smart borders programme within the eu-Lisa Agency. In 2015, eu-Lisa ran a pilot that involved some 12 countries across the EU.[37]

Operational tests were run at 18 different border crossing points in 12 European countries from March to September 2015 in order to assess the feasibility of using some technologies and technological approaches for European border checks and generally to support the decision making process going forward.

More than 58,000 volunteering third country nationals participated in the pilot, providing qualitative and quantitative information on the quality of data, particularly biometric data, that could be enrolled at the border, the durations of various proposed processes and traveller and border guard perspectives on the tests.

According to eu-Lisa, the pilot increased confidence that the proposed processes are operationally and technically feasible, as well as respecting fundamental rights.[38]

United Kingdom

The United Kingdom has made achieving 'friction-less trade' with the European Union a key priority when it leaves the EU in 2019.[36]

The UK's trade in goods with the rest of the EU amounts to £236 billion, while EU exports to the UK amount to £318 billion. The share of UK exports accounted for by the EU has fallen over time from 54% in 2006 to 43% in 2016, the year of the referendum to leave the European Union.[39]

With Britain's exit from the EU, it will become a 'third country' and is likely to trade outside both the EU Single Market and the EU Customs Union, although negotiations are still in progress and the final trading arrangement is currently unknown.

Most of Britain's trade with the EU is conducted through a series of ports in the south east and eastern coasts of the country, including London, Felixstowe, Grimsby, Immingham, Southampton, Dover, Tees, and Forth.[40]

The UK also shares a land border with the Republic of Ireland. The UK is a principal destination for Irish exports, with 44% of all exports by Irish owned firms going to the UK. In some sectors, such as agriculture, up to 90% of exports go to the UK.[41] Since the UK referendum, Ireland has increased the volume of exports to the UK, despite a depreciation in Sterling caused by the referendum result. In 2017, the Republic of Ireland's exports to the UK increased by 8.21%, strengthening the importance of the UK as an export destination for Ireland.

While the shape of the final Brexit trade settlement is currently unknown, the UK Government has introduced a bill into Parliament to address any possible outcome: the UK Cross Border Trade Bill. It is also looking at the potential of smart border technology to expedite trade both at the UK - Republic of Ireland land border, and at UK ports, where the majority of UK trade in goods with the

[37] The future tested: Towards a Smart Borders reality, eu-Lisa, 8 October 2015, https://www.eulisa.europa.eu/Publications/Reports/2015%20eu-LISA%20Annual%20Conference%20Report.pdf

[38] eu-Lisa, https://www.eulisa.europa.eu/AboutUs/SmartBorders/Pages/default.aspx

[39] Statistics on UK-EU trade - House of Commons Library - Briefing Paper No 7851, 19 December 2017; https://researchbriefings.files.parliament.uk/documents/CBP-7851/CBP-7851.pdf

[40] UK Dept for Transport - UK Port Freight Statistics, 1 September 2017 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/646188/port-freight-statistics-2016-revised.pdf

[41] Majority of EU goods most exposed to UK are Irish; Reuters; 13 September 2017; https://www.rte.ie/news/business/2017/0913/904427-irish-exports-to-uk/

©Copyright 2018 IMC. All rights reserved

rest of the EU is conducted.

- The UK Cross Border Trade Bill

  The UK Cross Border Trade Bill (CBT), which received its first reading in the House of Commons at the end of November 2017, will be a key piece of legislation regulating EU-UK cross border trade following Brexit.

  At present there is no UK import duty regime and a limited excise duty regime for UK-EU cross border trade. CBT sets out to expand both to a fully free standing system post-Brexit, with alterations also to the VAT system.[42] The bill is generally short on detail but sets out a range of options that allow for a 'Hard Brexit' without any free trade agreement, right through to the option that nothing in the trading arrangements will change, and the UK will continue as a member of the Single Market and the Customs Union. As such, the bill does not attempt to predict the outcome of current negotiations between the EU and the UK.

- UK Smart Borders

  The UK has signalled a strong interest in employing smart border and trading technology to expedite flow of goods following its exit from the EU in 2019.

  A report by a former director of the World Customs Organisation, Lars Karlsson, for the European Parliament in November 2017, laid out suggestions for how smart border technology might be deployed at the Ireland - Northern Ireland land border.[43]

  Karlsson suggested that to allow the continued operation of the UK-Ireland Common Travel Area, under which citizens of both countries can travel freely between them, while each country bars individuals from entering that are banned by either country's security or immigration statutes (CTA does however allow visitors to both countries who are not covered by CTA rights), the use of automatic number plate recognition (ANPR) should be adopted at both manned and unmanned border crossings. He suggested that there should be a single check on visitors at the jurisdiction of entry, with the creation of a frequent traveller programme for visitors who are not eligible for free movement under the CTA agreement.[43]

  Mr Karlsson also suggested that Ireland and the UK have a formal agreement for collaboration and data exchange.[43]

  At the moment, the number of ineligible visitors is relatively small, since it covers mostly visitors from certain Commonwealth countries. However, after Britain's exit from the EU, it could cover all non-Irish EU citizens.

  In 1997, the Republic of Ireland changed its immigration rules in a move that effectively required all UK citizens to show identity documents, despite the existence of both the EU and the Common Travel Area. In a legal opinion, Irish High Court Judge Mr Justice Gerard Hogan opined that the change in Irish immigration rules effectively nullified the Common Travel Area. [44],[45]

  In addition, to facilitate accelerated trade across the Ireland - UK land border, Karlsson recommended a bilateral EU-UK agreement regulating an advanced Customs cooperation that would avoid duplication and where UK and Irish Customs can undertake inspections on

[42] The Cross Border Trade Bill; Slaughter and May; December 2017; https://www.slaughterandmay.com/media/2536626/the-cross-border-trade-bill.pdf

[43] - Smart Border 2.0 Avoiding a hard border on the island of Ireland for Customs control and the free movement of persons http://www.europarl.europa.eu/RegData/etudes/STUD/2017/596828/IPOL_STU(2017)596828$_{EN}$.pdf

[44] Pachero v. Minister for Justice 2011 IEHC 491 at para. 18, 2011 4 IR 698 (29 December 2011)

[45] Butler, Graham (November 2015). "Not a "real" Common Travel Area: Pachero v Minister for Justice and Equality". Irish Jurist Volume 54

©Copyright 2018 IMC. All rights reserved

behalf of each other; mutual recognition of Authorised Economic Operators (AEO); a Customs-to-Customs technical agreement on exchange of risk data; pre-registration of operators (AEO) and people (Commercial Travellers programme in combination with a Certified Taxable Person programme); identification system by the border; a Single Window with one-stop-shop-element [46]; a Unique Consignment reference number (UCR); a simplified Customs declaration system (100% electronic) with re-use of export data for imports; Mobile Control and Inspection Units; Technical surveillance of border (CCTV, ANPR etc).[43]

The UK Government has signalled caution over Mr Karlsson's recommendations. The UK Government believes that more extensive technology measures as well as greater political cooperation is required to deliver 'friction-less' trade and free movement of persons, according to a statement by UK minister Suella Fernandes to the British House of Commons, 16th March 2018.[47]

Summary

The growing need in the world's most advanced economies to boost cross border trade as an engine of GDP growth while maintaining or increasing border security means that development and uptake of cross border logistics, expedited trading, and smart border technologies by governments across the globe is only likely to grow.

Each of the three approaches and contexts outlined in this article are different.

China provides an example of a grand strategy involving some 62 countries across three continents, with $900 billion of earmarked expenditure, and an anticipated further $7 trillion of funding over the course of the next decade.

The six Asia Pac advanced economies are collaborating on pilot projects, sharing technologies and approaches. Each is building or planning consolidated trade platforms and are looking to IoT, AI and blockchain to expedite logistics. One of the most ambitious of these projects is Australia's, which envisages global maritime supply chain visibility coupled with AI to anticipate and clear goods through its ports automatically.

The UK is looking to smart border, logistics, supply chain, and AI technologies to help it maintain free movement and rapid transit of goods through both its ports and its land border with the EU. Achieving success in this is a high political priority for the UK Government.

The EU itself has its own smart borders programme under the auspices of the eu-Lisa Security and Justice IT agency. It is likely to look at developments in the UK, as well as other projects such as those being operated by Japan and Australia with interest.

Other countries around the world are similarly interested in adopting advances in smart technologies with a view to accelerating trade as well as ensuring management and security of their borders. These countries include Canada, the United States and Mexico.

[46] This would appear to be similar to the planned system by the Australian Home Affairs Agency

[47] UK backs away from tech solutions touted in Irish border report, mlex Market Insight, 16 March 2018, https://mlexmarketinsight.com/insights-center/editors-picks/brexit/europe/uk-backs-away-from-tech-solutions-touted-in-irish-border-report

©Copyright 2018 IMC. All rights reserved

Reference Tool

Global Listing of Government Action Affecting IoT

(click here for a spreadsheet PDF of current, major government initiatives from around the world)

North American News

NIST Releases Draft Report on IoT Cybersecurity Standards

The US National Institute of Standards and Technology (NIST) has released a draft report (NISTIR 8200) that is intended to inform policy and standards makers in developing cybersecurity standards for IoT devices and systems.

The report has been prepared by the Interagency International Cybersecurity Standardisation Working Group (IICS WG).

The draft report examines cybersecurity in five IoT application areas. These are:

- Connected Vehicles, including vehicles, infrastructure
- Consumer IoT, including home devices, wearables, and mobile devices
- Health, including hospital connected systems such as EHR as well as patient health data
- Smart Buildings, including building control systems, energy monitoring, lighting systems, HVAC, etc
- Smart Manufacturing, enterprise IoT systems and cloud based IoT data systems.

An analysis of the risks and threats in each of the application areas is presented, broken down into eleven cybersecurity technology areas.

The report also reviews existing standards that might apply to IoT devices and technology. It maps each of the identified standards onto one of the eleven outlined IoT technology areas, with an assessment of the applicability of the standard, and gaps that might remain in cybersecurity standardisation.

The 8200 report calls for federal agencies to work closely with private companies, and that close collaboration between the two will be essential to developing effective cybersecurity standards.

It notes however that the IoT environment is fast moving and evolving rapidly, which makes standardisation more difficult. It also notes that technologies can be applied differently, with different policies and risk management, across the different application areas.

Cybersecurity efforts have to recognise this difference in application area functionality and risk applying potentially to identical technology.

An example might be technology developed and applied for consumer devices might be applied to patient data gathering, which might necessitate a different cybersecurity risk profile than a

©Copyright 2018 IMC. All rights reserved

consumer device app. If that same technology is then utilised interconnected with a hospital electronic health record system, the corresponding level of cybersecurity risk might alter again, and quite significantly.

- Links:

  Draft Interagency Report, NISTIR 8200, Summarizes International | CSRC

Chao holds listening sessions on self-driving car regulations

The US Department of Transportation has held a 'listening session' that brought industry players together with federal and state regulators to discuss regulation of self driving cars.

US Secretary of Transportation, Elaine Chao, said "We are not on the business, we don't know how, to pick the best technology or to pick the winners. We're not in the business of picking winners or losers. The market will decide what is the most effective solution."

Chao issued guidance in September 2017 on self driving vehicles that updates that issued under President Obama.

The September guidance largely continues the policy set out before under the previous administration of voluntary rules. Ms Chao referred to the guidance document as 'Version 2.0' in reference to the Obama era rules.

Ms. Chao said that 'Version 3.0' of the guidance will be issued during the course of 2018.

The Department of Transportation and administration approach may be at odds with Congress. The House of Representatives has passed the Self Drive Act, which requires the federal government to develop regulations for self driving, rather than encourage industry to develop its own regulations.

A proposal in Congress to increase the number of exempted self driving vehicles allowed on public roads from the 2,500 currently provided for to 100,000, is currently stalled due to increasing uncertainty among lawmakers about self driving safety following a number of accidents. The death of a woman hit by an Uber vehicle on an almost empty road recently will increase that uncertainty further.

During the department's listening session, DOT general counsel Steven Bradbury said "We as regulators have to realise that the AVs are coming. I don't share some of the scepticism in terms of timing. I think it's coming really fast … and it's going to be upon us in the very near term, whether we're ready or not."

- Links:

  Self-driving cars continue to face little resistance from the federal government - The Verge

  U.S. DOT releases new Automated Driving Systems guidance | NHTSA

DHS launches smart city challenge for first responders

The Department of Homeland Security is offering $150,000 to entrepreneurs and companies that can deliver IoT solutions to first responders by 2020.

The DHS Science and Technology Directorate (S&T) has launched a smart city grant, entitled 'Request for Innovators', that promises the funding to ventures and companies that can develop new tools to help first responders in navigation, sensors, and indoor building sensors.

It is also including the funding for the development of a 'Smart Hub' that can manage data between

©Copyright 2018 IMC. All rights reserved

wearable devices from devices such as cameras and radios, and data from infrastructure mounted devices such as building sensors, mounted cameras and other IoT devices.

The DHS is working with the Smart Cities Internet of Things Innovation Labs (SCITTI) and with the First Responders Group in running the programme.

- Links:

  DHS launches smart city challenge for first responders | Government Innovators Network

Two Fed Circuit judgments loosen Alice tech restrictions

The Alice judgment, which is held to have weakened the position of software patents in US courts, has been dealt a double blow in a series of judgments by Federal Circuit judges. The decisions will reinforce federal protection of software patents and provide greater security for technology investments.

In the 2014 Alice judgment, the Supreme Court established a series of tests to determine if a software patent was eligible. The first of these determined whether the claimed patent was applied to an ineligible category for patents, such as a natural phenomenon or a law of nature, or an abstract idea.

If the claimed patent did fall into such a category, a second test was established to determine if the patent contained an 'inventive concept' that established a concrete and distinct technology process that was different from established or conventional methods.

The result of the Alice judgment is that lower courts have been invalidating software patents in large numbers at the pleadings stage, before proceeding even to trial.

The recent Berkheimer v HP Inc case however established that determining software patent eligibility required determining questions of fact. This effectively bars lower courts from invalidating software patents on the basis of legal arguments at pleading stages or by summary judgments.

The Berkheimer judgment also raised the bar on the second test, stating that proof of prior practice did not imply that a concept was conventional, established or well understood. A software patent incorporating an approach that had been practised prior could still be unconventional, and hence valid under the Alice tests.

In a subsequent Federal Circuit judgment in Aatrix Software v Green Shades Software, the court held that arguments that a claimed invention improved technical systems should be accepted as plausible at a pleadings stage and not dismissed without hearing.

The consequence of the two judgments is that it should make it easier to validate software patents. The judgments will certainly make it easier for patent defenders to achieve hearings and not have their claims summarily dismissed.

- Links:

  Federal Circuit Decisions Raise Bar for Invalidating Patents on Section 101 Grounds Before Trial - Lexology

Congressional Smart Cities Caucus launched

A bi-partisan Congressional Caucus on Smart Cities has been launched to help develop legislation

©Copyright 2018 IMC. All rights reserved

and initiatives to help the development of American smart cities.

The caucus will host a series of round-tables throughout the spring of 2018 on issues facing smart cities.

The round-tables will focus on: connectivity; mobility; workforce; and sustainability, and provide an opportunity for business leaders to inform Congressional policy and law-making.

A bill is currently before Congress to expand the Smart Cities Council's Readiness Challenge Grants scheme.

The Trump administration has proposed granting $200 billion to states to spend on infrastructure, with $50 billion allocated for rural broadband improvements.

The Democrat grouping in Congress has proposed $1 trillion in infrastructure spending, with a large proportion allocated to rebuilding and improving urban infrastructure.

Neither the Trump nor minority Democrat budget proposals are considered likely to be implemented as neither would be likely to pass through Congress before the mid term elections in autumn.

- Links:

  Smart Cities Caucus Regional Smart Cities Initiative

California passes tough net neutrality law

California's state legislature has approved a net neutrality bill that will impose tough restrictions on Internet service providers. The act has however been criticised by some of its proponents, arguing that the legislation passed by the State Senate is vulnerable to legal challenge in the courts.

The Federal Communications Commission has repealed net neutrality rules at the federal level. The FCC repeal included a provision preventing states from enforcing their own net neutrality laws.

As a response to the FCC decision, and despite its provision, New York and Montana have enacted decrees enforcing net neutrality.

The California bill prohibits home and mobile Internet providers from blocking lawful content, applications, services or non-harmful devices, except for reasonable network management.

The bill outlaws throttling, paid prioritisation, or preferential treatment.

The Electronic Freedom Frontier, a proponent of software and Internet freedom and access, has warned that the California legislation is vulnerable to being nullified by the courts.

The EFF said that by not restricting the legislation strictly to within the boundaries of California, it could be construed as intruding on inter-state communications, which is the domain of federal government oversight and regulation.

The EFF said that California should rewrite its bill to explicitly limit it to intra-state communications – that is, Internet services and communications that occur solely within the state, and exclude any communications that are inter-state.

- Links:

  California bill would restore, strengthen net neutrality protections The Mercury News

©Copyright 2018 IMC. All rights reserved

TCJ Act challenges smart city funding

The US Tax Cuts and Jobs Act 2017 could make funding smart city and energy programmes more difficult, according to municipal finance specialists. They claim that the Trump administration law hits cities twice over, making municipal bonds less attractive, and reduces the tax that cities can raise. Faced with reductions in income, and in the ability to borrow money, US cities will find it more difficult to fund ambitious smart city programmes.

President Trump signed the Tax Cuts and Jobs Act into law in December. A major provision of the law is cutting corporate tax rates. Municipal finance specialists say that this has made municipal bonds, which are federal-tax-free, less attractive as investment options. Municipal bonds are a principal means by which cities raise money for large capital projects.

According to Bloomberg Intelligence, banks and insurance companies hold nearly 29% of municipal bonds.

To counter a decline in investment, cities will probably be forced to raise their interest rates, reducing the funds they have to plough into capital projects.

The Act also caps the amount of local and state taxes that taxpayers can write off against their federal tax bills.

While this doesn't affect current local and state taxes directly, it will make it politically more difficult for cities and states to raise taxes in future, as non-federal taxes will bite deeper into voters' pockets. It may also increase demand to reduce the level of current state and local taxes.

According to Moody's, the Act will cut city and state income from taxes by an average of 1% even in 2018. That impact on city tax revenue could well grow over time.

- Links:

  Tax Law Complicates Smart City Financing Plans | Bloomberg Law

European News

France considers IoT manufacturer liability

The French Government is considering making IoT device manufacturers liable for security of their devices as long as they are on the market. And to require IoT device manufacturers to open source their software code once the products are withdrawn from the market.

The proposal is contained in the French Government's Rue Strategique de Cyberdefense

The measures are seen as a governmental response to a series of leaks that are damaging the reputation of France's President, the Macron email leaks. These leaks have been made through the use of bots and smpanners. The Government has accused Russia's Government of being responsible. The emails have been published on the WikiLeaks website as well as Twitter, Facebook and 4chan.

The proposals have been construed by some in the industry as enforcing unlimited liability on device manufacturers.

©Copyright 2018 IMC. All rights reserved

The French Government also, unusually, identified a number of 'key players' in cyberspace, and advocates having 'open channels' to these players, identified as the UK, China, Russia and the USA, in order to help it minimise or prevent attacks on French Government and corporate bodies.

- Links:

  France mulls manufacturer liability & open-sourcing, IoT industry on edge

EU voluntary IoT cybersecurity framework

The European Union is proposing a voluntary IoT cybersecurity framework that would supersede member states' own certification schemes. The proposed framework, if accepted, would come into force in late 2019.

The framework would be overseen by the EU Agency for Network and Information Security (ENISA).

The proposal must be considered by the European Parliament and by the European Council, which represents the 28 member Governments of the EU. Both institutions could alter the proposals or reject them outright.

The proposal could also be adopted by EEA members such as Norway and Iceland, although they could vote to reject it in the EEA Council.

- Links:

  Cybersecurity Package | European Commission

Berlin Working Group calls for mandatory security updates for IoT devices

The Berlin based International Working Group on Data Protection within Telecommunications have called for IoT device manufacturers to be made liable for the security of their devices and be required to update software to ensure the highest level of security throughout the working life of the product.

The report, published in German, calls for legislators to: "establish requirements for the safety of IoT devices that are sold to private individuals, including the obligation to provide information about the installed firmware over the period and to provide updates to the firmware of the devices for known vulnerabilities. Also to provide a procedure so that consumer products can be updated with the latest available security updates to known threats."

The Working Group advocates that manufacturers should be required to support devices with security updates over the entire supported life of a product. Once a product is withdrawn from the market, manufacturers should be obliged to make their code open source.

The Working Group is made up of representatives of data protection agencies, government bodies, and research scientists.

- Links:

  Datenschützer fordern verpflichtende Updates für das Internet der Dinge – netzpolitik.org
  Internetauftritt der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

©Copyright 2018 IMC. All rights reserved

Dutch Government passes Internet surveillance bill

The Dutch Government has ignored the results of a referendum it called to gain popular approval for its Intelligence and Security bill, which grants the Netherlands Government wide-ranging powers to surveil Dutch citizens' through the Internet and connected devices.

Although forecast to win a handsome majority in favour of the Internet surveillance law, the Government was taken aback by a surprise defeat as the no camp gained a significant majority rejecting the Government's surveillance bill.

Analysis by pollsters showed that despite a larger than expected turn-out among older people, young people had not gone to the polls in any significant numbers. Pollsters said that rejection of the bill was high among young people, and that if they had participated, two thirds of the vote would have gone against the Government.

However, after consultations with other parties in the Dutch Parliament, the Dutch Government decided to proceed with the bill. It justified its action by arguing that the referendum was 'consultative' and non-binding, and that the Government had noted the results of the referendum.

The new law will give the Dutch intelligence services, the foreign intelligence service the AIVD, and the security service the MIVD, the power to collect and analyse large amounts of internet data.

Dutch civil rights associations, Amnesty International, the Council for the Judiciary, the Dutch Association for Journalists, the Scientific Council for Government Policy, and the Council of State, the Netherlands constitutional advisory body and supreme constitutional court, have all criticised the bill and called for it to be dropped. The Dutch government has been determined however to proceed with the legislation.

- Links:

  Dutch pass 'tapping' law, intelligence agencies may gather data en masse | Reuters

UK IoT security code of practice

The UK Government has unveiled a new code practice for manufacturers to tighten IoT device security. The code of practice follows a security review into IoT device security that included input from GCHQ, the UK's communications intelligence agency.

Companies making IoT devices will have to implement admin passwords, generate vulnerability policies, encrypt data and issue automatic updates.

The Government's review into IoT devices, Security by Design, concluded that manufacturers of consumer IoT devices had made connecting their devices quickly and easily to the Internet their top priority, and in some cases had allowed device security to be compromised as a result.

- Links:

  New measures to boost cyber security in millions of internet-connected devices - GOV.UK

©Copyright 2018 IMC. All rights reserved

Asia-Pac News

China publishes National Standard for Personal Data Protection

China has published a new set of standards on personal information and data security. The National Standards on Information Security Technology - Personal Information Security Specifications GB/T 35273-2017 will come into force on May 1.

The new regulations complement and clarify existing Chinese legislation in the area, including the Cybersecurity Law and the Consumer Protection Law.

The regulations also outline compliance requirements.

The new regulations make plain a requirement for explicit consent for data collection of sensitive personal data, or use of personal data for new purposes.

The new standard sets out requirements for personal information security impact assessments.

There is a provision for forwarding information to off-shore parties, with yet to be published procedures for how this shall be conducted.

Personal information of minors, defined as those below the age of 14, is considered a special case under the regulations.

Organisations are required to establish data protection departments and appoint a data protection officer to ensure the requirements of the regulations are carried out, and to be directly responsible for the protection and security of personal data held or processed by the organisation.

Enforcement actions against organisations has already begun. Wider investigations are considered likely to begin in the second quarter of 2018.

- Links:

  China Publishes National Standard for Personal Data Protection - Lexology

Japan to begin Vietnam smart city construction

A Japanese Government led effort to construct a smart city on the outskirts of Vietnam's capital, Hanoi, will begin construction in autumn, according to reports. The $37 billion programme is part of the Japanese Government's effort to promote, fund and build advanced technology infrastructure in emerging countries. The effort is a cornerstone of Japanese Prime Minister Shinzo Abe's foreign policy.

The programme is said to be the largest Japanese overseas project to date, according to Japanese officials.

The smart city will be constructed to the north of Hanoi. The drive to the centre of the capital from the new smart city will be 15 minutes.

The project is being led by Japan's Ministry of Economy, Trade and Industry. Japan's International Cooperation Agency is also involved. Companies taking part include Sumitomo, Mitsubishi Heavy Industries, Panasonic, KDDI, Daikin Industries, ODA and the Tokyo Metro.

The new smart city will feature self driving buses, an electric vehicle network (EVN), both of which

©Copyright 2018 IMC. All rights reserved

will be produced by Mitsubishi Heavy Industries.

The smart city will also have a smart energy system, with technology from Panasonic, KDDI and Daikin. It will also include renewable energy and waste recycling plant.

The consortium of companies constructing the smart city is being led by Sumitomo Corporation.

- Links:

  Hanoi s $4b smart city project begins in 2018 - News VietNamNet

Singapore to set standards for IoT deployment

The Government of Singapore is to demand open standards for IoT deployments in the state, the Government Minister for the Smart Nation initiative, Dr Vivian Balakrishnan, told delegates at the IoT Asia 2018 Conference.

According to Dr Balakrishnan, closed IoT standards and technologies are an impediment to developing complex, large scale development programmes. The Singapore Government, he said, is determined to oppose proprietary technologies, and will insist on the use of open technology standards in Singapore.

Dr Balakrishnan said that this approach necessitated the Government providing manufacturers with the necessary infrastructure and framework so that companies could comply with the Government's requirements and standards.

Part of this framework is a requirement for security to be built-in to the device, Dr Balakrishnan said.

International News

Saudi Arabia begins $500 billion smart city

The Government of Saudi Arabia has begun to award contracts for the construction of a $500 billion, 10,230 square mile mega smart city that will also straddle Jordanian and Egyptian territory. The new smart city is planned to be 33 times larger than the land area of New York City.

The new city, called Neom, is a key part of the Saudi Government's ambitions to diversify away from a reliance on oil revenues.

Neom will be powered completely by renewable energy.

The Government aims for the city to become a hub for developing energy and water technologies, biotechnology, food, advanced manufacturing and media.

The city will be located in Saudi Arabia's north-west corner, by the border with Jordan, and a short distance across the Gulf of Aqaba from the north-east corner of Egypt.

Former Siemens chief executive Klaus Kleinfeld has been appointed to manage the project.

The Government has been in talks with British firm ARM Holdings about using its technology to help develop robotics and artificial intelligence applications.

©Copyright 2018 IMC. All rights reserved

The Egyptian and Saudi Governments have set up an initial $10 billion fund to begin construction of the city.

Saudi Arabia will sell 5% of its stake in oil giant Saudi Aramco, as take other measures, to raise $300 billion for the main phase of city construction.

- Links:

  British chip designer in talks to build $500bn smart city on Red Sea - Business - The Times

  Saudi Arabia announces $500B plan to build a new megacity - Smart Cities Dive

India releases $1.5 billion for smart cities

The Government of India has released $1.5 billion of funding for smart cities so far, according to spending figures from the Government.

The Indian Government has made building 99 smart cities across the subcontinent a flagship policy. The Government has proposed spending 2.03 lakh crore ($30 billion) on the programme in total. To date, $1.5 billion has been allocated to the Indian states to fund initial developments.

The funding is aimed at a number of 'smart projects', including roads, water modernisation, education, skills and training, health and urban infrastructure.

Critics of the Government's programme have claimed that the states have been underfunded, and many of the 99 demarcated cities do not have adequate funds to implement smart city projects.

- Links:

  Smart Cities Mission: Government releases Rs 9,940 crore to states for Smart Cities Mission - The Economic Times

©Copyright 2018 IMC. All rights reserved