United Nations ECE/TRADE/C/CEFACT/2022/13

Economic and Social Council

Distr.: General
19 July 2022

Original: English

Economic Commission for Europe

Executive Committee

Centre for Trade Facilitation and Electronic Business

Twenty-eighth session
Geneva, 10-11 (am) October 2022
Item 5 (d) of the provisional agenda
Recommendations and standards:
Implementation support material

Report of eDATA Management Domain on Internet of Things Standards for Trade Facilitation

Submitted by the Bureau

Summary

The Internet of Things (IoT) facilitates trade by enabling the collection and exchange of cross-border electronic information without human interference and, thus, it is more secure, effective and economical. Given the widespread use of IoT, this report highlights the role that United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) standards can play in defining data and process flows between IoT devices operated by various parties as part of an international supply chain and how this data can be integrated into existing supply chain automation processes in an interoperable manner. The report provides examples of IoT data, process and information exchange standards and identifies data needs for the wider adoption of IoT in trade facilitation applications.

Document ECE/TRADE/C/CEFACT/2022/13 is submitted to the twenty-eighth session by the Bureau for noting.

I. Introduction

1. The Internet of Things (IoT) is a network that connects uniquely identifiable "things" or devices to the Internet. These devices have sensing capabilities and can, potentially, be programmed. Through the exploitation of their unique identification and sensing capabilities, information about these devices can be collected and the state of these devices can be changed.

2. Some of the key features of an IoT ecosystem include the following:

- Interconnections with and between devices;
- Uniquely identifiable devices;
- Sensing capabilities;
- Embedded intelligence;
- Communication capabilities; and
- Programmability.

3. These IoT ecosystems have the potential to make novel applications possible that facilitate cross-border paperless trade through the use of connected devices that sense, collect, process, share and act on data. Data such as temperature, humidity and location can be collected from IoT devices and can be used to power a number of applications ranging from the ability to ensure freshness of produce across a supply chain, to asset location tracking, to detecting equipment failure in logistics and transportation.

4. IoT devices also have the ability to capture and record data in real time and in a continuous manner and to associate this data with unique IDs. Therefore, they can be used to trace the origin of data from basic sensor readings even as this data is used by software applications to create complex derived information. This real-time data can be fed into decision systems, that are part of an international supply chain, for further action and automation as documented by the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) Smart Container Project.

5. IoT creates interesting opportunities for trade facilitation by providing the ability to create and exchange cross-border electronic information without human interference, thus, in a more secure, effective and economical manner. IoT systems can also be designed to ensure the integrity of data about the physical condition of things such as packaging, vehicles, and containers.

6. In combination with other emerging technologies such as blockchains, 5G networks, application programming interfaces (APIs) and cloud platforms, IoT could have a huge impact on the drive toward significant automation of international supply chains and the facilitation of cross-border paperless trade.

7. There are already many projects around the globe trying to revolutionize supply chains using the operational efficiencies created by IoT for better asset tracking, inventory management and the predictive maintenance of equipment. An interesting example of this is documented in the UN/CEFACT Smart Containers Project which looks at how smart containers (standardized seagoing containers fitted with sensors) are enabling door-to-door tracking and monitoring. Smart containers have the potential to drive end-to-end visibility and transparency throughout the entire supply chain.

8. Given the widespread use of IoT within a wide range of systems, and its potential to enhance existing communication channels and create new channels, this paper seeks to highlight the role of standards and how UN/CEFACT can play a role in developing or

extending existing technical specifications to maximize this technology's value to the UN/CEFACT constituency.

9. This paper, therefore, focuses on the role that UN/CEFACT standards can play in defining data and process flows between IoT devices operated by various parties as part of an international supply chain and how this data can be integrated into existing supply chain automation processes in an interoperable manner.

II. Data standards

10. IoT can make sense of what is happening in the physical world by gathering data derived from physical movements and environmental changes. This process begins with sensor devices recording the physical movements of people, animals, automobiles, parcels etc., and/or environmental changes such as temperature and humidity. This raw data is then pushed to a gateway device which converts the raw data into a transmittable Internet Protocol (IP) compliant data format and sends it to servers, which are either on premises or in the cloud, for storage and computation purposes. Data is then, once again, reformatted into a standardized format so that its content can be understood and used to derive optimum desired outcomes.

11. An example of an IoT project that has leveraged and built upon the UN/CEFACT core component library is the UN/CEFACT Smart Container Project. This project forms an important part of the development of international multimodal standards to support the future of global trade. A smart container is a marine shipping container that is fitted with a permanently installed smart monitoring device. The smart device has a set of sensors embedded within the container enabling it to measure real-time information such as location, door opening and closing, vibrations, temperature, humidity and other measurable physical parameters of the environment surrounding the assets within the container, as well as the container itself. It also has communication capabilities (used to send the measured data to a collection centre) and it can be paired with extra remote sensors to address the specific needs of a given cargo consignment.

12. As part of the data modelling process, the Smart Container Project added new items to the Core Component Library (CCL) and Multi Modal Transport (MMT) Reference Data Model to capture

- Sensor-related data elements and classes;
- Geographical information data elements and classes; and
- The linking MMT entities like consignment and transport equipment.

13. While smart containers present an interesting example of the use of UN/CEFACT standards in IoT, as IoT usage expands across transport and trade, there is scope for enhancing the CCL data model to better meet the changing business requirements created by the growing number of IoT applications.

III. Process standards

14. Various technologies can make supply chains more efficient through appropriate information sharing across different stages in supply chains. IoT is one such technology that can enable smooth data exchange with the help of numerous sensors by providing information such as atmospheric conditions, temperature, shocks and vibrations, GPS position, etc. This data, once obtained via an IoT device, can be used as input to programmes that remotely change settings, control the environment and provide the right atmosphere for

maintaining the quality of goods. They can also be used as input to other processes such as those for insurance claims.

15. There are multiple opportunities for IoT-compliant process standards from UN/CEFACT to enhance efficient cross-border, paperless trade. One of the main obstacles to the smooth adoption of IoT systems lies in authorities being reluctant to surrender control of their data and processes to shared platforms that are outside their jurisdictions[1]. To overcome this reluctance, processes need to be established that will allow the recorded data to be appropriately shared across borders and on different platforms without violating privacy and regulatory norms.

16. The Smart Container Project is an excellent example of how IoT can be leveraged in the supply chain. UN/CEFACT has established Business Requirements Specifications (BRSs) for smart containers which are the first formal standards detailing the data elements used by smart container applications. It is important to adhere to these standards, as the widespread adoption of smart containers is very much needed by different stakeholders, and IoT systems based on standards have a greater potential to increase adoption of smart containers. Standardization of smart containers is important as it will reduce the deployment and development costs of IoT solutions[2], which are needed to reduce shipment times and risks for all parties.

17. The UN/CEFACT Buy-Ship-Pay model's business process standards[3] have served as a reference for the application of the UN/CEFACT BRSs.[4] This model describes the main parties and processes involved in the international supply chain and establishes a relationship between the data entities used in different parts of the supply chain, ranging from transport contracts to international sales contracts. These business processes are interrelated within the Buy-Ship-Pay model's scope, which includes operational transport and logistics, commercial transport contracts, border clearance, regulatory and financial processes and provides a way to exchange information both within business areas and between them.

18. The Buy-Ship-Pay model can be applied by any region, industry, or country for developing electronic transport and trade-related data exchange documents that are further integrated into software solutions for carriers, agents, traders, customs, freight forwarders, etc. The model is also helpful in supporting and growing single window implementations as it provides the basis for data harmonization and for globally aligned data exchange specifications in the international supply chain. IoT systems can further enhance the capabilities of the buy-ship-pay model by leveraging the existing, established standards for Buy-Ship-Pay processes and developing them further to be compatible with information received through IoT systems.

19. The owners of data feeds generated by IoT devices are usually specific platforms, infrastructure operators or value-added service providers, and the data is made available through platform APIs or message-based approaches. If process standards are established within the Buy-Ship-Pay business process standards for managing the data gathered through IoT, this will support significant growth in international trade due to improved timeliness, quality, volumes of supply chain data, and it will also increase adoption of the Buy-Ship-Pay model.

[1] UN/CEFACT, 'White Paper: Technical Applications of Blockchain to UN/CEFACT Deliverables, version 2", (2019) available at https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain_TechApplication.pdf

[2] UN/CEFACT, 'Business Requirements Specification (BRS), Smart Containers', (2019).

[3] https://tfig.unece.org/contents/buy-ship-pay-model.htm

[4] UN/CEFACT, "Buy-Ship-Pay Reference Data Model, Version 1", (2019). Available at: https://www.unece.org/fileadmin/DAM/cefact/brs/BuyShipPay_BRS_v1.0.pdf

20. Emphasis should be on shared platforms, as these will enable wider sharing of the benefits from innovations through information sharing and access to data on demand. BRS or Requirements Specification Mappings (RSM) should be structured in a way that allows for information sharing through platform-enabled websites that offer private/public access using protocols such as HTTP, and also allows external APIs to add functionality and data access.[5] This will allow the information obtained through IoT devices to be used for efficiency, for reducing the use of intermediaries and for lowering costs.

21. Establishing and adhering to the standards-based semantic models of UN/CEFACT could widen networks among traders and support integration across a diversity of platforms. Developing related BRSs and RSMs will help achieve the deployment of IoT on a wider scale. Similar to the way that UN/CEFACT semantic standards are mapped to UN/EDIFACT[6] and XML, the UN/CEFACT semantic standards should ideally be mapped to syntaxes used with technologies such as IoT, blockchains and web platform APIs. To manage data flows at a more granular level, modelling of the detailed semantics of processes will be increasingly important.

22. The wider integration of IoT with other technologies such as blockchains and AI could create interesting opportunities for facilitating cross-border paperless trade. To support this, the following recommendations for enhancing process standards could be considered:[7]

- Creating a reference architecture to promote a full understanding of specifications and new technologies
- Revising the existing process models for BRSs/RSMs to allow for interoperability of data on the blockchain (once data from IoT has been recorded) in order to support permissioned access to authorities across countries, using smart contracts for events ranging from releasing consignments to invoice approvals
- Developing more granular process models which focus on the state life cycles of key resources along global value chains. These resources range from entities such as contracts and payments to consignments and containers

23. Standards should be designed to create consistency so that, irrespective of the platform hosting information about a resource, as long as the standards are implemented, stakeholders are able to interpret the data in the same way.

24. The capabilities of IoT systems are further enhanced when combined with blockchain technology and standardized data.

25. Standardized data collected using IoT sensors can be stored using third-party digital ledgers (based on blockchain technology) and can also be used for product traceability across supply chains. This can create trustworthy data for use in a variety of applications such as proving country of origin and quantities shipped, insurance claims due to poor transport conditions, etc.

26. Digital ledgers are used in trade processes that involve different parties and, as a result, applications will need to support data exchanges between different digital ledgers—thus calling for standards to facilitate the process. For example, in a single end-to-end import transaction in the future, there may be exchanges across as many different digital ledgers as there are participants in the process: an electronic trade finance ledger may be used by the importer and a different one by the exporter, each with their banks, and then each bank may use different ledgers for verifying licences and product quality assurance certifications. Then, insurance companies could use different digital ledgers for data verification and exchange,

[5] UN/CEFACT, "White Paper: Technical Applications of Blockchain to UN/CEFACT Deliverables, v.2", (2019).
[6] The United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport
[7] UN/CEFACT, "White Paper: Technical Applications of Blockchain to UN/CEFACT Deliverables, v.2", (2019).

while carriers/forwarders may use their ledger to manage shipping documents. Additionally, customs may use yet another ledger to verify documents and to check the past good behaviour of the exporter and importer.

27. If UN/CEFACT standards are established that consider the constraints created by the use of IoT devices and digital ledgers, that will allow for data exchange or interoperability across multiple ledgers. IoT capabilities will also then be further enhanced, providing more security and privacy in managing data. In a nutshell, UN/CEFACT process standards can be useful for supporting the wider adoption of IoT by establishing standards that offer semantic interoperability across multiple ledgers.

IV. Message (information exchange) standards

28. This paper focuses on the need to further develop the BRS document to support international message standards for efficiently exchanging IoT and digital ledger information. Some of the more unique characteristics of this data are the need to exchange relatively small amounts of data (snippets) and/or large quantities of these same data snippets. For example, there is a need to create coherent data and message structures that can be used for exchanging this type of data across different trade models such as those for smart containers, Single Submission Portals (SSP), or the Buy-Ship-Pay model. The BRS document should include standardized data elements that allow for collaboration across platforms and, if the data is recorded using IoT devices, a fully integrated system for data exchanges based on the use of shared APIs—that are, in turn, based on standards. In addition, data obtained through IoT devices should also be compliant with the requirements RSM for mapping data points such as locations, business entities, or different stakeholders.

29. Sharing data efficiently is important for the smooth functioning of logistic supply chains as there are multiple stakeholders involved in transactions and the supply chains are global and diverse. There are many smart containers and devices already in use, but no global standards currently exist for capturing and communicating consistently the array of data captured by IoT devices in smart containers.

30. UN/CEFACT has already created a smart container BRS, which is the first formal standard detailing the data elements of the smart container. It is important to adhere to these standards as the wider adoption of smart containers is greatly needed by different stakeholders. In this context, the use of IoT devices, together with standards, promotes increased adoption and guarantees interoperability.

31. IoT can also be deployed in Single Submission Portals (SSPs) as data-flow standardization is an important element of SSPs and provides the basis for linking governments and businesses in support of cross-border trade.[8] A major goal of any SSP is enabling and facilitating the accurate declaration of data to cross-border regulatory authorities who will use this data for clearances and risk management at the border. Successful implementation of SSPs is reliant upon the use of message/information exchanges in an agreed structure and format so that both transacting parties can read and understand the data through semantic interoperability.[9] Traditionally, this semantic interoperability is based on a common data reference model for the logical flow of information in cross-border trade.

32. Data harmonization is important for achieving the objectives of SSPs, which include eliminating redundancies, data ambiguity and duplications, all of which require, for efficient implementation, the mapping of document data requirements to international standards for

[8] UN/CEFACT, “Recommendation No 37: Single Submission Portal”, (ECE/TRADE/447) (2019). Available at: http://www.unece.org/fileadmin/DAM/trade/Publications/ECE_TRADE_447E_CF-Rec37.pdf.

[9] Ibid.

cross-border trade[10]. Standardized information sharing, supported by the deployment of IoT and blockchain systems which use standardized data, can help achieve the objectives of an SSP if integrated under the processes defined in a BRS and an RSM. Documents such as permits, certifications, and customs declarations can be maintained digitally once key data is obtained using IoT devices and can be stored on a blockchain in order to ensure their continued integrity. But to achieve this objective, appropriate message exchange formats and interfaces need to be established along with the standardization of data elements, taking into account the need for transparency and user privacy in alignment with the General Data Protection Regulation of the European Union (GDPR) and other legislation. Using robust IoT systems along with permissioned blockchains can provide the desired infrastructure for achieving the objectives of an SSP.

33. In the Buy-Ship-Pay model, further development is needed in order to realize the full potential of the model and of IoT deployment. Standards are required to address the following needs where there are gaps in the existing model:[11]

- Support for greater visibility and monitoring within the supply chain via detailed documenting and standardizing of the state changes undergone by Buy-Ship-Pay entities in order to track granular data streams and link them to more insightful higher-level events;
- Support for animal health and wellbeing via process and data standards for the exchange and use of relevant IoT data (for example, on temperatures in cattle cars, state of hydration of animals, etc.);
- Support for tracking and tracing in logistics and the fulfilment of regulatory needs via BRS/RSMs that reflect the use of IoT data (for example from monitoring devices attached to goods or containers); and
- Identification of new opportunities within the Buy-Ship-Pay model for processes using IoT data in data pipelines for regulatory reporting, manufacturing, scheduling, material management, purchase order financing and public procurement.

34. Often a lack of transparency in data exchange among different stakeholders in global cross-border trade is a challenge to realizing the complete benefits of digital supply chains. Blockchain technology provides transparency and a high level of trustworthiness by securely registering and storing the data using cryptography. Once IoT data is obtained from the environment of a container, other information, such as the location/positioning of the container, can be obtained (also using IoT) and added to the shipment record registered on a blockchain.

35. Integration of the data collected using IoT during shipping movements based upon BRS/RSM data standards is vital to enhancing the efficiencies of supply chains and embracing paperless cross-border trade. Further standardizing of these processes in conjunction with the recording of data on blockchains will provide greater visibility and data access (via interoperability) to regulatory bodies at the border, thus allowing them to accelerate trade processes. In a nutshell, embracing IoT along with blockchain technology in BRS and RSM data standards will greatly increase the efficiency of digital supply chains as the standardization will increase data creation and usage. It will also support better data analytics and enhanced decision-making by allowing AI engines to use standardized data from multiple sources.

[10] https://tfig.unece.org/contents/data-harmonization.htm

[11] ECE, "UN/CEFACT Programme of Work 2019 – 2020" (ECE/TRADE/C/CEFACT/2019/21) (2019). Available at https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/PoW_2019-2020_E.pdf.

V. Cybersecurity issues

36. IoT refers to the growing digital network of linkages that connect devices and sensors in order to facilitate data transfer over the Internet without external intervention. In this thriving digital environment, as technology-enabled data transfers grow in their worldwide applicability, international trade continues to expand and cut across jurisdictions. Digitalization through IoT has started to transform the trade landscape, especially in the cross-border context. IoT supports a simplification of electronic trade documents based upon the automatic collection of key data, which, when combined with blockchain technology, has the potential to speed up export and import procedures. The ability to track shipments via IoT has already increased efficiency in shipping[12] while electronic authentication can ease the process of verifying online transactions.[13] As trends indicate, the intertwining of the Internet and computing devices is now integral to future economic activity. In 2020 alone, it is estimated that global e-commerce sales amounted to US$26.7 trillion[14] with cross-border e-commerce expected to reach 22 per cent of all e-commerce sales in 2022 (up from 15 per cent in 2016[15]). Furthermore, it is predicted that 500 billion devices will be connected to the Internet by 2030[16] while the vulnerabilities linked to deploying connected devices remain largely unaddressed.[17] The issues of compatibility and interoperability in hardware and software (lacking security-conscious design) could be exacerbated by the exponential increase in connected IoT devices as we move into the future.[18] With businesses frequently operating across borders to lower trade costs, trade documents and data are exchanged between multiple networks based in different jurisdictions.[19] This has also heightened the cybersecurity threats associated with the influx of cross-border trade data flows.[20]

37. Interconnected IoT devices can enable access to large volumes of data across various sectors where there is a serious potential for misuse. If IoT ecosystems are to enhance trade, then their openness, stability, security and trustworthiness should be made a prerequisite to

[12] World Trade Organization, *World Trade Report 2018: The future of world trade: How digital technologies are transforming global and commerce*, (2018), pages 66-67 and 73. Available at https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf (accessed 24 May 2022).

[13] Maria Ptashkina, "Facilitation 2.0: E-Commerce and Trade in the Digital Age" (RTA Exchange, International Centre for Trade and Sustainable Development (ICTSD) and Inter-American Development Bank (IDB), 2018), p 9. Available at https://e15initiative.org/wp-content/uploads/2015/09/rta_exchange_-_ptashkina_-_facilitation_2.0_-_e-commerce_-_ptashkina_0.pdf (accessed 24 May 2022).

[14] United Nations Conference on Trade and Development (UNCTAD). "Global e-commerce jumps to $26.7 trillion, COVID-19 boosts online sales", (03 May 2021). Available at https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales (accessed 24 May 2022).

[15] Statista.com, "Cross-border e-commerce as share of total e-commerce worldwide in 2016 and 2022", available at https://www.statista.com/statistics/867991/cross-border-e-commerce-share-world/ (accessed 24 May 2022).

[16] CISCO, "At-a-Glance: Internet of Things: Connected Means Informed" (2016). Available at https://emarsonindia.com/wp-content/uploads/2020/02/Internet-of-Things.pdf (accessed 6 March 2020).

[17] EY, 'Cybersecurity and the Internet of Things' (2015), pp. 10-11. Available at https://pdf4pro.com/amp/view/ey-cybersecurity-and-the-internet-of-things-567613.html (accessed 24 May 2022).

[18] World Economic Forum, "Global Risks Report 2020", *Insight Report, 15th Edition* (2020), p. 62. Available at http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (accessed 24 May 2022); Siddiqui, F.M., M. Hagan & S. Sezer,"Embedded Policing and Policy Enforcement Approach for Future Secure IoT Technologies", *Living in the Internet of Things: Cybersecurity of the IoT—2018*, (conference paper). p. 5. Available at https://pureadmin.qub.ac.uk/ws/portalfiles/portal/153474397/Final_Paper_Submitted.pdf (accessed 24 May 2022).

[19] Economic and Social Commission for Asia and the Pacific (UNESCAP), "Mechanism for cross-border mutual recognition of trade-related data and documents in electronic form" (2019) Conference Room Paper for the Fifth Meeting of the Interim Intergovernmental Steering Group on Cross-border Paperless Trade Facilitation by the Legal and Technical Working Groups, p. 6. Available at https://www.unescap.org/sites/default/files/B1900234.pdf (accessed 24 May 2022).

[20] Joshua P. Meltzer, "Cybersecurity and digital trade: What role for international trade rules?", (Brookings Institution, 2019), p.2. Available at https://www.brookings.edu/wp-content/uploads/2019/11/Cybersecurity-and-digital-trade_final-11.20.pdf (accessed 24 May 2022).

their use in international trade.[21] Given that the growth of international trade and the growing reliance on IoT will only increase in terms of scale and scope, the concerns of business should go beyond potential monetary losses to include reputational damage.

38. For the purpose of this report, we assume that developing a comprehensive set of cybersecurity standards through public-private collaboration could facilitate secure cross-border trade.

A. Cybersecurity standards: the wider implications

39. Cybersecurity threats proliferate in an environment of innovative technological growth; however, to date, there is no universally accepted definition as to what cybersecurity standards should entail. Today, such standards can assume the form of legislation, rules, principles, guidelines, best practices, certification schemes, technical specifications and/or other frameworks developed by public, private and not-for-profit entities.[22]

40. The United States' California Consumer Privacy Act and the European Union's General Data Protection Regulation target the use and collection of personal data (which include personal data collected by IoT devices) instead of dealing specifically with IoT security aspects. However, since 2017, the United States Senate has introduced and debated the IoT Cybersecurity Improvement Act, requiring the National Institute of Standards and Technology (NIST) to take specific steps to increase cybersecurity for IoT devices.[23] Likewise, the European Commission set out a voluntary cybersecurity certification framework (based on assurance levels) aiming to increase trust and security in IoT devices in 2018.[24] These regulatory developments reinforce the need to implement cybersecurity as a confidence-building mechanism within IoT ecosystems, in turn enhancing trust in international trade. Managing threats and mitigating risks requires designing a comprehensive framework to shape policies that can broadly secure the interfaces between products, processes and technology with the best conformance practices. Establishing cybersecurity standards is crucial for any enterprise if it wishes to thrive.

41. Determining the form and substance of expected security outcomes is fundamental to cybersecurity assurance. At the outset, it may be difficult to devise a common set of cybersecurity standards across all IoT applications in different jurisdictions.[25] This is unsurprising considering that standard-setters have their own priorities and criteria when assessing the cybersecurity risks within the IoT ecosystem. That said, adopting security-by-design principles as a baseline requirement (i.e. integrating safety features into the IoT devices at the design phase[26]) could be necessary to address pressing interoperability issues.

---

[21] Neha Mishra, "International Trade, Internet Governance and the Shaping of the Digital Economy" (UNESCAP, 2017) ARTNeT Working Paper Series No. 168. Available at https://www.unescap.org/sites/default/files/AWP%20No.%20168.pdf (accessed 24 May 2022).

[22] Brass, I., et al., "Standardising a Moving Target: The Development and Evolution of IoT Security Standards" (June 2018) *Living in the Internet of Things: Cybersecurity of the IoT – 2018,* Conference Paper, p. 2. Available at https://www.researchgate.net/publication/325436966_Standardising_a_Moving_Target_The_Development_and_Evolution_of_IoT_Security_Standards (accessed 24 May 2022).

[23] US Congress, "S.734 – Internet of Things Cybersecurity Improvement Act of 2019" 116th Congress (2019-2020). Available at https://www.congress.gov/bill/116th-congress/senate-bill/734 (accessed 24 May 2022).

[24] European Commission, "The EU cybersecurity certification framework". Available at https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (accessed 24 May 2022).

[25] Brass, I., et al. p.6.

[26] HM Government (UK), 'Internet Safety Strategy—Green Paper 2017' (October 2017) p.11. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet

42. To design a cybersecurity standards framework, it is important to first determine which components needs to be secure.[27] Is it the IoT device, system, process, organization, data and/or the people within the IoT ecosystem? Having identified these components, standard-setters can then define the scope of their own security-by-design principles and decide which IoT security aspects should be included as part of their baseline/minimum security requirements. For instance, Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) considers securing the IoT systems in the designing, development, and operation phases as part of their security-by-design principles.[28] A holistic approach to defining these principles is essential in light of the far-reaching and growing effect that IoT ecosystems have on facilitating international trade throughout supply chains.

43. The global development of baseline security requirements is still in an embryonic state with tremendous scope for identifying protocols for preventive and corrective action. Existing literature has noted an increasingly convergent trend towards developing a set of minimum specifications for IoT security in the U.S. and the EU[29]; however, the most recent and ongoing development of baseline requirements paints a slightly different picture. From the draft version of its core baseline requirements, NIST places greater emphasis on securing IoT at the device level[30] while, conversely, the European Union Cybersecurity Agency (ENISA) endorses the principles of security-by-design and privacy-by-design (data protection) throughout the life cycle of IoT devices and their ecosystems.[31] IoT system developers are also encouraged to prioritize security monitoring and analyse effectiveness.

_Safety_Strategy_green_paper.pdf (accessed 24 May 2022). The UK Government certainly leans towards the concept of security-by-design, as evident in the Department for Digital, Culture Media & Sport's publications of the 'Secure by Design: Improving the cyber security of consumer Internet of Things Report' and the voluntary 'Code of Practice for Consumer IoT Security' in 2018 (although both publications were geared towards the protection of the consumers' interests when using IoT devices).

[27] Carr, M., et al., "Standards, Governance, and Policy Stream – Governance and Policy Cooperation on the Cyber Security of the Internet of Things" (PETRAS Internet of Things Research Hub, (27 March 2018) pp. 22-23. Available at https://discovery.ucl.ac.uk/id/eprint/10063234/1/Carr_Report_Global-governance-of-the-Internet-of-Things-Report-PDF.pdf (accessed 24 May 2022).

[28] Japan NISC, "General Framework for Secure IoT Systems" (26 August 2016), p. 1. Available at https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf (accessed 24 May 2022).

[29] Brass et al. (n. 12) p. 3. The authors observed some recurrence in the minimum IoT security requirements among the IoT-specific and non-IoT-specific NIST papers: At the device level it may include vulnerability disclosure, upgradability, and service life cycle management. At the system level this may entail authentication, authorization, access controls, cryptographic key management, and integrity management.

[30] NIST, "Considerations for a Core IoT Cybersecurity Capabilities Baseline", draft document (2019), pp. 5-9. Available at https://www.nist.gov/system/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf (accessed 24 May 2022). The minimum-security requirements at the device level (which NIST suggests including in its baseline) include the physical and logical identification of the device; update of software and firmware within the device; ability to securely change the device configuration; ability to control local and remote access to the device; use of cryptography; etc. Given the difficulty of verifying the design principles and likely high cost of implementation, NIST suggests excluding the designing and configuration practice of the IoT device from its core IoT cybersecurity capabilities baseline. See also NIST, "NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks" (2019) pp. 11-12. Available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf (accessed 24 May 2022). NIST categorizes the cybersecurity risks for IoT devices in terms of the device security, data security, and privacy. It also considers other aspects crucial for mitigating the risks, including asset management, vulnerability management, access management, incident detection, data protection, information flow management and more. Some of these aspects overlap with the minimum-security measures listed in the ENISA baseline security recommendations (see below).

[31] The European Union Agency for Network and Information Security (ENISA**),** "Baseline Security Recommendations for IoT in the context of critical information infrastructures" (November 2017), pp. 46-52. Available at https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport (accessed 24 May 2022). ENISA classifies the IoT baseline security measures into three areas: policies; organizational, people and process measures; and technical measures. Some of the overlapping security measures with the U.S. NIST include asset

44. IoT standards development and implementation has inherent challenges. IoT technology and the technology of cyber-hackers is constantly developing at a rapid pace. At the same time, developing international standards can take years. For example, developing an ISO standard takes an average of three years from making the first proposal to the final publication.[32] This means that standard setters are constantly struggling to keep up with the fast-moving cybersecurity arena. As another consequence, an increasing number of industry associations have been motivated to develop their own standards in order to fill the void. As a result, implementors are faced with difficulties in evaluating and monitoring standards developments[33] and there is a serious risk of overlapping standards being developed. As a result, while public institutions such as ENISA in Europe or NIST in the United States can issue recommendations that are helpful, these may not be adequate to ensure IoT cybersecurity given the increasingly critical role of IoT ecosystems in facilitating international trade.

45. Public-private collaboration in the development of cybersecurity standards is increasingly perceived as a viable option. The IoT ecosystem has a diverse range of application areas. Therefore, it may be feasible for stakeholders in each sector to work collectively and draw up sector-specific, consensus-based IoT cybersecurity standards.[34] For instance, the Organisation for Economic Co-operation and Development (OECD) digital security recommendation encourages coordination and collaboration between all stakeholders (including governments and the private sector) that rely on "the digital environment for all or part of their economic activities"[35]. Drawing a parallel comparison to the legal sector, the International Bar Association (IBA), for instance, established a dialogue between multiple stakeholders in the legal profession in order to develop a recommended a list of best practices to help law firms safeguard against cybersecurity threats.[36] As part of this process, practitioners, legal experts, IT professionals and cybersecurity consultants were all engaged in crafting the cybersecurity guidelines on strengthening law firms' technology infrastructure, organizational processes and policies on staff training.[37]

46. For the IoT ecosystem to play a pivotal role in trade, it is important to engage with industry experts and bring together different stakeholders (including IoT developers, trade experts and cybersecurity specialists) to work together to determine what needs to be secure, and how, in order to further amplify global trade.

B. Role of trade agreements and e-commerce

47. It is noteworthy that only recently have international trade agreements included specific chapters to deal with e-commerce-related issues as documented in the publication, *Facilitation 2.0: E-Commerce and Trade in the Digital Age*. These issues include the restriction of digital data flows and cybersecurity concerns. In 2007, the International Telecommunication Union (ITU) launched the Global Cybersecurity Agenda as a framework for the international cooperation of member states, with the aim of enhancing confidence and

management, management of security vulnerabilities and/or incidents, access control, secure software/firmware update, cryptography, data protection and compliance, etc.

[32] ISO, "Developing Standards" https://www.iso.org/developing-standards.html (accessed 24 May 2022).

[33] Brass et al. p. 6.

[34] OECD, *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document* (OECD Publishing, Paris, 2015). Available at http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm (accessed 24 May 2022).

[35] Ibid. p. 8

[36] International Bar Association (IBA), "Cybersecurity Guidelines by the IBA's Presidential Task Force on Cybersecurity" (2018), p. 4. Available at https://dokumen.tips/documents/cybersecurity-guidelines-hspi-attacking-unsecured-wi-fi-connections-eg-public.html?page=1 (accessed 24 May 2022).

[37] Ibid, p. 6-21.

security in the context of emerging technologies. The United Nations Commission on International Trade Law (UNCITRAL) has played an important role in facilitating international commerce through the modernization of global trade rules. Its Model Law on Electronic Transferable Records (MLETR) builds on the principles of functional equivalence and technological neutrality underpinning all UNCITRAL texts on e-commerce. There is specific reference to "security of hardware and software" in the list of criteria for the assessment of the general reliability standard for electronic transferable records in Chapter III, Article 12. This is significant since the security of hardware and software has a direct impact on the reliability of the method used by countries for facilitating cross-border digital trade, particularly when data is being taken from IoT ecosystems.

48. Generally, countries can adopt international or consensus-based standards as a basis for trade agreements to support "the development of globally consistent and least trade-restrictive approaches to cybersecurity"[38]. However, the parties negotiating the agreements must first agree on what cybersecurity standards and/or infrastructure each deems mutually acceptable or equivalent within its own regulatory/legislative IoT framework, and this is very often a contentious issue. On top of that, tensions surrounding issues of national security and cybersecurity concerns are not to be underestimated, as the intertwining of numerous interests requires careful consideration and is quite a balancing act. Ongoing disputes involving international trade and IoT data ownership, the application of international law in the digital space, and the desire to preserve state sovereignty will continue to create major bottlenecks to developing a cybersecurity standards framework at the global level.

VI. Conclusion and suggested way forward for UN/CEFACT

49. The Internet of Things as a technology, is going to explode in the near future with the proliferation of communication systems such as those using 5G technology. Given this context, UN/CEFACT is ideally positioned to drive the development of new technical specifications to enhance IoT use in trade and, at the same time, improve the ability of existing standards to meet the needs of an evolving technological environment.

A. Interoperability

50. The evolution of IoT has resulted in different manufacturers and application developers adopting different technologies, standards, and communication protocols for capturing and exchanging information. As IoT usage expands, there will be an increasing need to ensure interoperability so that different IoT devices and systems are able to exchange information with one another.

51. This is an area where UN/CEFACT can play an important role in developing and driving the usage of data standards for IoT interoperability.

B. Resource discovery

52. In the context of cross-border trade, the use of IoT will generate data that could be captured in one system, processed in another system and stored in a third system, all of which may be online and in various jurisdictions. Key elements such as information about the IoT device used to capture data or events or data elements being captured as part of a stream of events need to be discoverable in order to ensure transparency and visibility across the supply chain.

[38] https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/

53. As in the case of blockchain technology, IoT also presents an opportunity for UN/CEFACT to play a vital role in bridging this gap, and to develop specifications that allow various systems and platforms to discover resources such as identity information, event information etc.

C. Legal and regulatory framework

54. The dynamic nature of cybersecurity threats requires a proactive approach to dealing with and mitigating such risks. The recent trend of integrating cybersecurity features into IoT devices and software using security-by-design principles, is a step in the right direction. Adopting a multi-stakeholder engagement approach, with an ongoing dialogue between stakeholders in both the public and private spheres, is essential to determining the best form and substance of IoT security standards. In-depth collaboration among the IoT standards-setting organizations could effectively contribute to developing a comprehensive set of cybersecurity standards for IoT ecosystems. Ultimately, trade and cybersecurity are two cogs in the IoT wheel. Reducing cybersecurity risks within IoT ecosystems through the use of standards would go a long way toward facilitating secure international trade.

D. Internet of Things application data needs

55. In the Smart Containers Project, the UN/CEFACT CCL was enhanced with the addition of 120 new data elements to support the use of IoT devices in containers. This is only one IoT application, so there are opportunities to work with application developers in other areas to identify IoT data that requires definition, but which is not yet included in current UN/CEFACT standards. Given that IoT systems tend to send out frequent bursts of small data, there may also be a requirement to address this need as part of standardization and harmonization efforts and the further development of BRSs/RSMs and the CCL.

56. IoT usage is only going to increase over time and will also interoperate increasingly with other emerging technologies such as blockchain technology, AI, 5G technologies and API platforms. Therefore, UN/CEFACT could play a significant role in engaging with standards bodies to bridge the gap between existing standards and whatever else may be required to increase the adoption of IoT in trade facilitation applications.