THE INTERNET OF THINGS AND OPERATIONAL TECHNOLOGY

Contributors: Chris Hankin, David Luzzi, Kazuo Noguchi, Daniele Sgandurra, Karl Steiner, Satoru Tezuka, Masaki Umejima, Linton Wells

EXECUTIVE SUMMARY

The last few years have seen a significant convergence between Information Technology (IT) and Operational Technology (OT), which controls much of our industrial and critical national infrastructure. This convergence is being accelerated by the rapid growth in the Internet of Things (IoT). Blurring boundaries between IT, OT and IoT are increasing the need for more integrated, collaborative cyber security strategies. The International Cyber Security Center of Excellence (INCS-CoE) plans to pursue collaboration aimed at designing new integrated strategies that combine IT, OT and IoT security efforts and to maximize use of existing and novel cyber security resources.

This paper briefly reviews current activities in the UK, US and Japan in the OT security and IoT spaces. We identify three main areas for potential collaboration:

1. Supply Chain Security
2. Sharing of Testbed Facilities
3. Sharing of datasets

A separate working group within INCS-CoE has concentrated on the challenges of Information Sharing. Whilst the third issue above is more about the creation of benchmark data for research purposes than routine information sharing, we believe that the general policy issues concerning this must be resolved before making concrete recommendations about data sharing. We defer to Working Group 2 on this matter.

Supply chains are global and increasingly recognized as a major source of cyber risk. The governments of all three countries have published guidance on steps that can be taken to improve supply chain security. Much of the current guidance derives from the US National Institute of Standards and Technology (NIST) special publication 800-161. All three countries have updated guidance in this area within the last twelve months. Academic research on the comparison of the different national guidance and development of new techniques to assure supply chain security will benefit greatly from the international perspective that collaboration through INCS-CoE can bring.

Research on security solutions for OT and IoT should be informed by access to experimental facilities that, as far as possible, replicate real systems. Given the extensive choice of devices and protocols in use in the wild, it is important that testbed facilities offer similar diversity and are also scalable to provide faithful representations. All three countries have invested in the creation of testbeds but some of these efforts are fragmented, based on limited supplier heterogeneity and only accessible to a small part of the research base. There would be substantial benefit from international effort to either link existing facilities or replicate them within the INCS-CoE partnership. Again, this would provide a basis for benchmarking research outcomes across the partner countries leading to best-of-breed solutions.

Within INCS-CoE we have substantial expertise in securing industrial and critical infrastructure, but we can achieve much more through collaboration. We recommend the creation of a working group to actively pursue collaboration in the areas identified in this paper.

TABLE OF CONTENTS

1 THREATS

The Mirai botnet[1] from mid-2016 was an early indication of how poor security in consumer IoT devices could lead to large-scale cyber security incidents.

There has been an increasing number of incidents using cyber to target physical infrastructure, the Ukranian attacks in 2015 and 2016 being the most publicised. The major incidents in 2017 (WannaCry[2], NotPetya[3] and Equifax[4]) have involved exploitation of un-patched legacy systems – such systems are pervasive in the OT domain.

Challenges continue to grow for the industrial cyber security community. Broader deployment of operational technology is expanding the use cases requiring protection. Resource shortages are undermining the effectiveness of established defences. Blurring boundaries between IT, OT and IoT are increasing the need for more integrated, collaborative cyber security strategies.

Cyber security challenges are also increasing within traditional plants and infrastructure systems. Many plants still lack the resources to sustain defences or proper strategies to enable external support. Deployment of Industrial IoT (IIOT) strategies is proceeding without real solutions due to critical issues like secure-by-design-devices and secure supply/support chains. Growing use of cloud-based solutions is undermining the ability of in-house teams to govern security practices. Segregating cyber security efforts by technology is no longer a sustainable approach.

Therefore, within the International Cyber Security Center of Excellence (INCS-CoE), we plan to pursue collaboration aimed at designing new integrated strategies that combine IT, OT, and IoT security efforts and maximize use of existing and novel cyber security resources.

2 CURRENT STATUS

The following sections will include a discussion of the status of IoT and OT current activities in in the UK, US and Japan.

2.1 Internet of Things

Several activities related to the Internet of Things are currently being led by UK, US and Japan.

[1] Antonakakis, Manos, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric et al. "Understanding the mirai botnet." In *USENIX Security Symposium*, pp. 1092-1110. 2017

[2] Samuel Osborne, "NHS cyber attack: Ransomware hits 200,000 victims in at least 150 countries, says Europol director", May 2017. Available at: http://www.independent.co.uk/news/uk/crime/nhs-cyber-attack-wannacry-ransomware-victims-countries-europol-rob-wainwright-a7735001.html

[3] Iain Thomson, "Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide", June 2017. Available at: https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/

[4] Krebs, B. The equifax breach: What you should know, 2017. URL Available at: https://krebsonsecurity.com/2017/09/the-equifax-breach-what-you-should-know.

2.1.1 UK

The PETRAS Internet of Things Research Hub is a consortium of nine leading UK universities which work together to explore critical issues in privacy, ethics, trust, reliability, acceptability, and security in the context of IoT. This project runs in collaboration with IoT UK[5].

The PETRAS IoT Hub is led by UCL and includes Imperial College London, Lancaster University, University of Oxford, University of Warwick, Cardiff University, University of Edinburgh, University of Southampton, and University of Surrey. For more details about the work and projects of this group visit: www.petrashub.org.

2.1.2 US

Industrial Internet Consortium is an organization designed to accelerate the IIoT. Based in Needham, MA, the consortium was founded by GE, Intel, IBM, AT&T and Cisco. The Industrial Internet Consortium was formed to help achieve this goal by identifying the requirements for open interoperability standards and defining common architectures to connect smart devices, machines, people, and processes that will help to accelerate more reliable access to big data and unlock business value. It also focuses on innovation through testbeds. The IoT Consortium encourages collaboration concerning IoT in connected homes, automobiles, cities, retail and wearables.

2.1.3 JAPAN

In Japan, National Strategies, e.g. Smart Community in 2011 and Society 5.0, have placed Internet of Things (IoT) as the driver of pursuing data driven economy. To implement it through Public-Private Partnership (PPP), Japanese Government formed up The IoT Acceleration Consortium in grouping up 3,513 companies and research institutions. That main activity is to demonstrate capability of technologies to facilitate new business models by addressing (1) the development and standardization for IoT-related technologies such as AI, Sensing, Data Storage, Data Distribution, Security [Privacy], and interface design, and (2) creation of various IoT related recommendations such as regulatory reform that is necessary for running the open data policy (Figure 1).

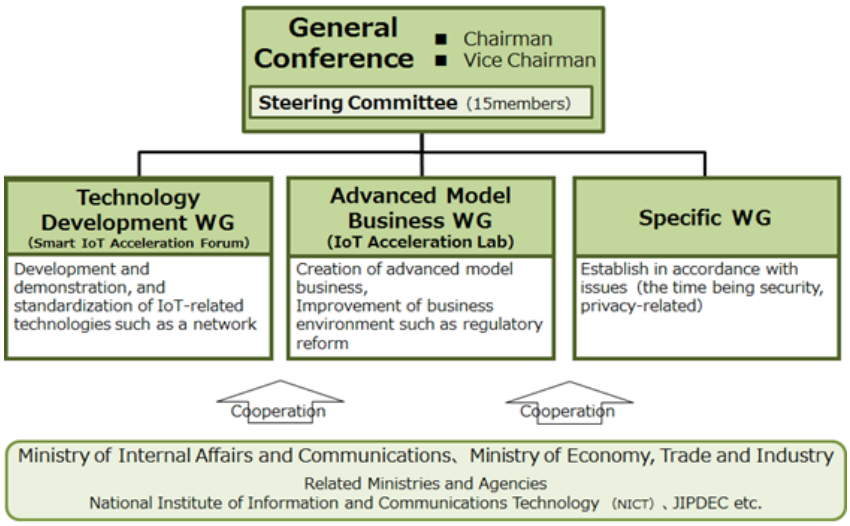

Figure 1: Organization structure of The IoT Acceleration Consortium in Japan

[5] https://iotuk.org.uk/

In continuous effort for 7 years since the earthquake that attacked Japan's east coast "Tohoku" on March 2011 killing 15,895, there are two outstanding activities; standardization to provide network access with all home appliances, e.g. air conditioning, Photovoltaic system(PV), and Battery Storage and the nationwide adoption of a smart metering device in Japan

Firstly, when addressing IoT, two strategies are available: open and closed. Home appliances adopted a closed strategy for many years. However, we can observe the new aspects that 1) home appliances with the open interface named ECHONET Lite make up Energy Management System (EMS) or Virtual Power Plant (VPP) as a new energy system which enables the energy system to be scalable. That ambitious project called ECHONET Lite was started with only 22 industrial participants in 2011. In the last seven years, ECHONET Lite has become an international standard named ISO/IEC14543-4-3 and grown to a large project covering over 250 companies, e.g. Toyota, Panasonic, Toshiba, NTT, Softbank, Tesla motor [U.S.], SMA [Germany], and LG [Korea] (Figure 2).

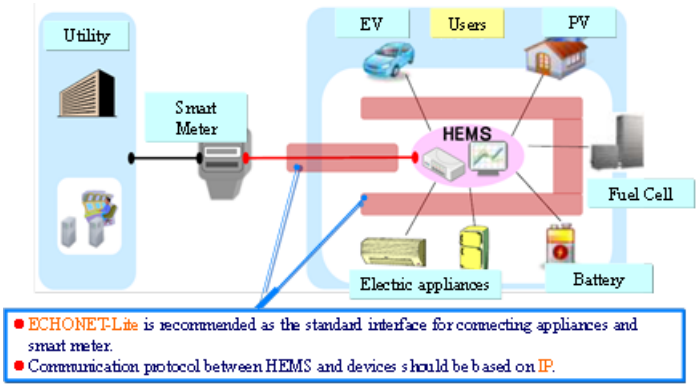

Figure 2: ECHONET Lite

ECHONET Lite has the following characteristics. Firstly, it has been ratified as IEC standard. ECHONET Lite is participating in some working groups in ISO/IEC to adjust with the trends in international standardization and engage in consultations with experts from around the world. It is the main accomplishment that ECHONET Lite specification has become ISO/IEC14543-4-3 as a communication standard.

Secondly, it is being used in a growing number of implementations. The number of devices compatible with ECHONET Lite is continuing to grow steadily. For now, the properties for over 90 different types of home appliances, e.g. air conditioners, lighting, photovoltaic solar cells, fuel cells, and storage batteries, have been defined. In addition, commercial products are on the market in Japan and ASEAN. For example, air conditioners that are newly released in Asian market, exceeded 3.3 million in one year, added on the lineup of the devices that speaks ECHONET Lite over IP (Figure 3). ECHONET Lite is the enabler of bringing network access to home appliances (Figure 4).

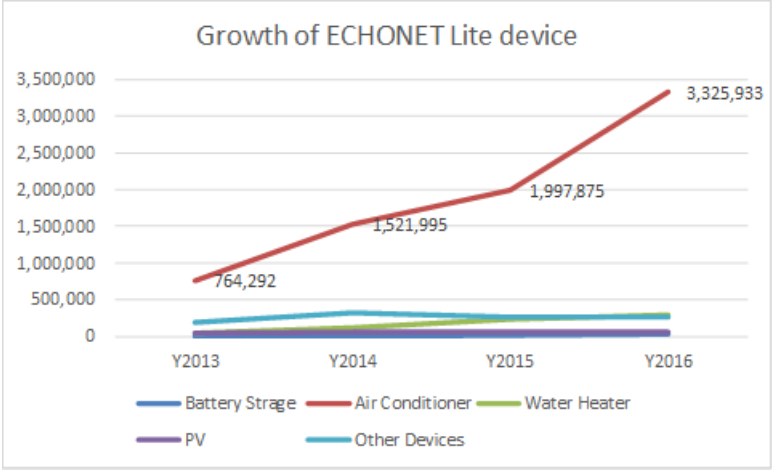

Figure 3: Growth of ECHONET Lite devices

As same as emergence of ECHONET Lite, nationwide adoption of smart metering that provide network access with an electric meter and a gas meter that measures daily energy usage at every household, In March 2012, the Ministry of Economy, Trade and Industry Smart Meter System Investigation Committee announced that electric power usage data is presented through B root which is connected directly to a household. This smart meter specification, which required the implementation of an IPv6 single stack and ECHONET Lite, has achieved global recognition as an advanced architecture.

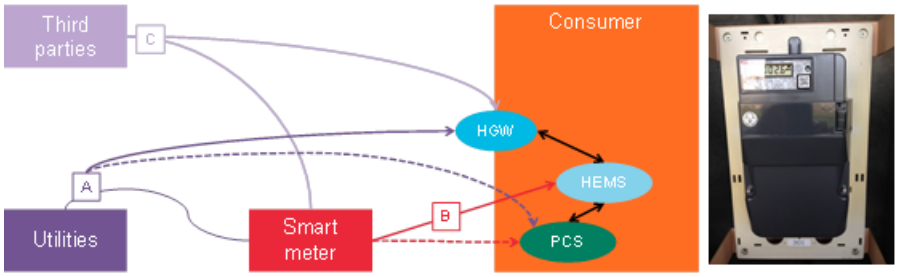

Figure 4: Growth of ECHONET Lite devices

Since announcing it, the smart meters have become a symbol of opening Japan's closed architecture. The implementation of smart meters using B-route is progressing smoothly. This stepped up a gear with the opportunities presented by the July 2014 publication of smart meter specifications for the Tokyo area (TEPCO) and Nagoya area (Chubu Electric Power). The US media company, Bloomberg reported that 85% of Japan's demand for electricity will be obtained through smart meters by 2020. New smart meters are being installed in every home in Japan ahead of the rest of the world, and it is expected that Japan will lead the world in the innovation of smart meters and IOT.

2.2 OPERATIONAL TECHNOLOGY

UK, US and Japan are involved in several activities related to industrial control systems. We will briefly summarize some of the most relevant ones in the following sections.

2.2.1 UK

The Research Institute in Trustworthy Industrial Control Systems (RITICS) consists of a group of academically led and industrially linked projects researching key questions in securing industrial control systems (ICS) against cyber threats. Currently it is focussed on ICS and the projects are trying to answer the following questions:

a. Do we understand the harm that cyber threats pose to ICS and business?

b. Can we confidently articulate these threats as business risk?

c. Are there novel effective and efficient interventions?

For the next Phase of RITICS, from April 2018, its remit will expand to the Critical Systems of the CNI.

The following questions will be used to focus research over the next 5 years:

- *Harm from Cyber:* Do we understand the harm that threats pose to the provision of critical systems?
- *Articulating risk:* Can we confidently articulate these threats as risk to delivery of critical systems at a business and national level?
- *Novel interventions:* Are there novel, effective and efficient interventions for businesses or governments to reduce the risks to critical systems?
- *Economics of interventions:* How can we best understand and compare both the effectiveness and costs of potential interventions? Including technical intervention such as altering system architecture, through to policy interventions by governments and regulators.
- *Intrusion detection and incident response:* How can we best detect intrusion in critical systems, including embedded and bespoke systems, and how should incident response differ to established practices for enterprise IT?
- *Barriers to best practice:* What are the obstacles to (perceived) best practice being applied to critical systems?

Further information about the work and projects can be found at http://ritics.org/

2.2.2 US

NIST research focuses on the connectivity of devices and networks and how to strengthen system and device defences. They developed a guide for how ICS users can apply the approaches to cyber security for users in utilities, chemical companies, food manufacturers, automakers and other ICS users.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), DHS, was created to reduce risks within and across all critical infrastructure sectors. They partner with LE agencies, the IC, and coordinate efforts among Federal, State and local governments and control systems owners, operators and vendors. They also collaborate with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

Idaho National Lab created the INL Cyber Security Research Department in response to the DHS' selection of INL to work on securing critical infrastructures and reduce cyber vulnerabilities associated with control systems. INL offers a sandbox test environment as well as assessments and support to the National SCADA Test Bed, a multi-lab effort to reduce vulnerabilities associated with SCADA systems.

2.2.3 JAPAN

For many years, an infrastructure system, e.g. medical, energy, and transportation, are familiar with a close architecture which data usage is exclusive within an organization. On the other hand, data sharing to support the data driven approach which creates innovation and efficiency of the social system is getting necessary in Japan. The IoT Acceleration Consortium oversees the system and policy design research in collaborating with universities and industries.

3 POTENTIAL AREAS FOR COLLABORATION FOR INCS-COE PARTNERS

Three areas for collaboration have been identified, namely:

1. Supply Chain Security
2. Sharing of Testbed Facilities and creation of the necessary protocols to facilitate this
3. Sharing of datasets – moving towards the creation of open source benchmarks

These areas will be briefly discussed in the following sections

3.1 SUPPLY CHAIN SECURITY

Most organisations in UK, US and Japan rely upon suppliers to deliver to them products, systems, and services. However, supply chains can be large and complex, involving suppliers at different levels, and in different countries with different regulations, and that are working on different things/components. Therefore, making sure that the entire supply chain is "secure" is very hard as bad things can happen at any levels of this chain, e.g. due to inherent vulnerabilities or to bugs/vulnerabilities introduced maliciously.

As exemplified by the recent Bloomberg article[6], which describes how allegedly some Chinese cyber spies had used a U.S.-based firm to secretly embed tiny chips into server motherboards purchased and used by almost 30 different companies (among which Amazon and Apple), threats to the global technology supply chain not only can have devastating consequences but are also hard to detect. In the following, we summarize the main challenges faced in this area by UK, US and Japan by also referencing existing strategies and guidelines to mitigate the risks due to supply chains.

3.1.1 UK

The UK National Cyber Security Centre (NCSC) has recently released a guidance document[7] which proposes a series of 12 principles which designed to help organization to establish effective control and oversight of supply chains. These principles are clustered in four main categories, namely:

- **Understand the risks**: before starting to secure the supply chain, organization need to understand thoroughly the risks and benefits they might face when engaging with a multitude of suppliers.
- **Establish control**: these set of principles are meant to allow organization to analyse strategic risks of supply chain, such as to identify suppliers who continually fail to meet security and performance expectations, as well as to identify critical assets and over-reliance on single suppliers. The goal of this sets of principles is to help organizations to consider building on diversity and redundancy during their planning.
- **Check your arrangements**: to allow organizations to gain confidence in their approach to establishing control over their supply chain.
- **Continuous improvement**: to allow organizations to keep an open eye on how their supply chains evolve, as well as to continue to improve and maintain their security.

[6]The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. 4 October 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[7] Supply chain security collection, 28 Jan 2018, https://www.ncsc.gov.uk/guidance/supply-chain-security

These principles are summarized in Fig. 4[8].

Figure 4: Principles of Supply Chain Security

Finally, the UK Cyber Security Strategy 2016-2021[9] reports as one of the main goals of the strategy to "[...] help industry build greater security into the CNI supply chain [...]" and making organizations more aware and responsible for reducing vulnerabilities in current and future systems, and in their supply chain.

3.1.2 US

In 2012, the White House released the National Strategy for Global Supply Chain Security[10]. This document focuses in particular on the worldwide network of transportation, postal, and shipping pathways, assets, and infrastructures including communications and information infrastructures.

The US Strategy establishes two primary goals:

[8] https://www.ncsc.gov.uk/guidance/supply-chain-security-12-principles-infographic

[9] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[10] Available at: https://obamawhitehouse.archives.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf

Goal 1: Promote the Secure and Efficient Movement of Goods. Promote the timely, efficient flow of legitimate commerce while protecting and securing the supply chain from exploitation and reducing its vulnerability to disruption. To achieve this goal the U.S. will enhance the integrity of goods as they move through the global supply chain. In addition, they will also understand and resolve threats early in the process, and strengthen the security of physical infrastructures, conveyances and information assets, while seeking to maximize trade through modernizing supply chain infrastructures and processes.

To accomplish this goal, the US Government will seek to:

- Resolve threats early to expedite the flow of legitimate commerce
- Improve verification and detection capabilities to identify goods
- Enhance security of infrastructure and conveyances to protect the supply chain and critical nodes
- Maximize the flow of legitimate trade

Goal 2: Foster a Resilient Supply Chain. Foster a resilient supply chain that is prepared for, and can withstand, evolving threats and hazards and can recover rapidly from disruptions. To achieve this, the U.S. will prioritize efforts to mitigate systemic vulnerabilities and refine plans to reconstitute the flow of commerce after disruptions.

To accomplish this goal, the US Government will seek to:

- Mitigate systemic vulnerability to a supply chain disruption
- Promote trade resumption policies and practices

Finally, the approach is driven by the following guiding principles:

- Galvanize Action: integrate and spur efforts across the United States Government, as well as with state, local, tribal and territorial governments, the private sector and the international community.
- Manage Supply Chain Risk: identify, assess, and prioritize efforts to manage risk by utilizing layered defenses, and adapting.

On April 9, 2015, the National Institute of Standards and Technology (NIST) announced the publication of "Supply Chain Risk Management Practices for Federal Information Systems and Organizations (SP) 800-161"[11]. This special NIST publication:

- Provides guidance for federal agencies to identify, assess and mitigate information and communications technology (ICT) supply chain risks.
- Integrates ICT supply chain risk management (SCRM) into federal agency risk management activities. This is accomplished by:
- applying a multi-tiered, SCRM-specific approach; and
- assessing supply chain risk and applying mitigation activities.
- Builds on existing practices from multiple disciplines.

[11] Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf

- Is intended to increase the organizations' ability to strategically manage ICT supply chain risks over the entire life cycle of systems, products and services.

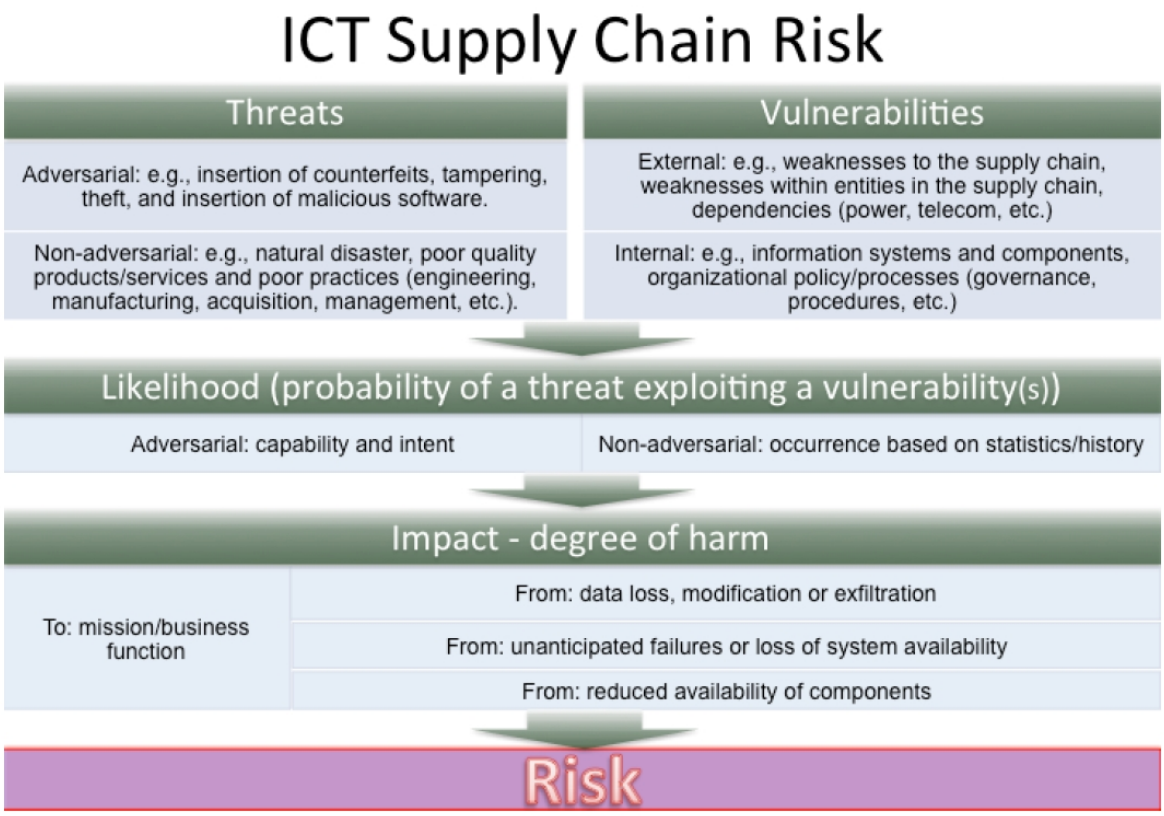

Figure 5: ICT Supply Chain Risk (NIST SP 800-161)

Although this publication is directed at federal government agencies, the guidance it provides may be useful for government contractors and other private industry organizations.

Finally, the US 2018 National Cyber Strategy[12] reports that risk management frameworks will be integrated in supply chain according to existing industry best practices aimed at ensuring that the deployed technology is secure and reliable. In particular, one of the goals is to improve awareness of supply chain threats as well as to provide more streamlined authorities to exclude risky vendors, products, and services when justified. This effort will synchronize with existing ones to manage supply chain risk in the Nation's infrastructure.

3.1.3 JAPAN

In Japan, the Cyber/Physical Security Framework[13] shows how in Society5.0 (human-centered society) cyber attacks will have more impact on physical space than before. In addition, the rise of "Connected Industries" will increase the opportunity to create new added value, in particular by creating more flexible and dynamic configurations of supply chains. The report, however, points out that from the

[12] Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[13] Available at: http://www.meti.go.jp/press/2018/05/20180502003/20180502003-1.pdf

perspective of cyber security this will create a larger attack surface. The report finally describes how in Society5.0, composed of the Internet of Things devices, artificial intelligence and so on, the starting points for cyber attacks increase and the range of the cyber risk expands due to supply chains connected in more complicated ways. Finally, the document reports that the envisioned cyber-security framework should ensure that the companies (e.g., SMEs) which form the whole supply chain are able to find a right balance between the expected risks and the costs for necessary measures, and that can actually implement these measures.

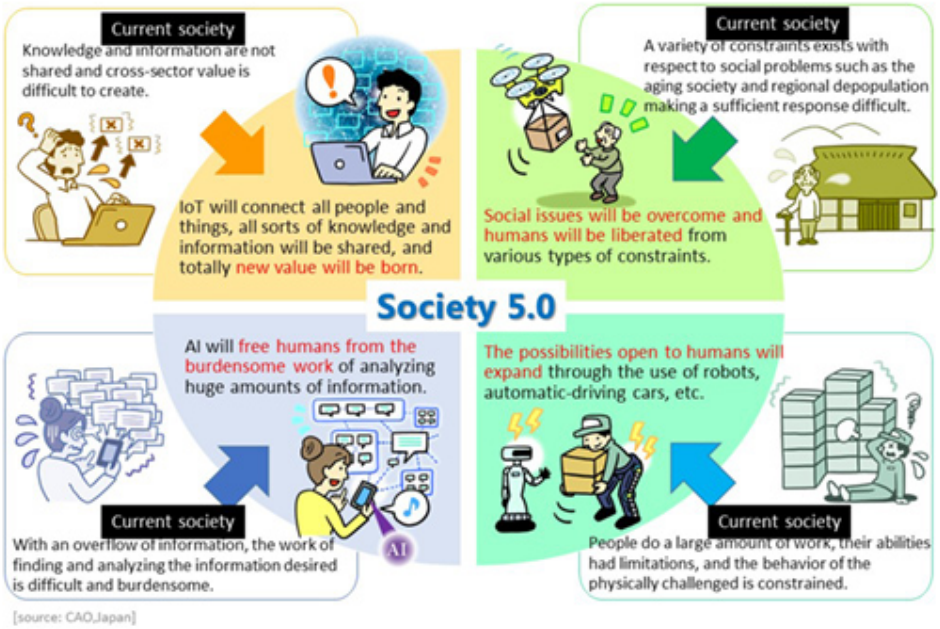

Figure 6: Society 5.0

Finally, in 2018 Cybersecurity Strategy[14], one of the envisioned approaches to achieving the objective of the strategy is to develop a supply chain that creates Values through Diverse Connections, for example by formulating a specific cybersecurity framework for supply chain risk of business operators including small and medium-sized enterprises.

3.2 SHARING OF TESTBED FACILITIES

ICS are complex systems composed of combinations of hardware, software and ICT networks, and are being increasingly used in smart-cities and in IoT-based environments. As ICS systems are becoming ubiquitous, accessible and transformative to the society (and its economy) as a whole, the need to understand their security characteristics also increases. Therefore, it is vital to understand how these complex systems may react in different scenarios, also to understand their impact on other sectors and the interdependencies between them.

The first potential area collaboration for INCS-CoE partners is the development and sharing of IT and ICS testbed facilities, in which components and system instances are configured to resemble, as closely as possible, the real-world counterparts. These shared testbed facilities would enable INCS-CoE partners to jointly perform a set of activities, such as simulating cyber-attacks against CI, e.g. to understand the possible impact of target and untargeted attacks or real systems and develop countermeasures before

[14] Available at: https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-zentaigaiyou-en.pdf

they happen or, providing a training area to develop new cyber-skills and to helps trainee improve their capability to respond to cyber incidents.

In the following, we will summarize the current range of some testbed facilities in the UK, Japan and US, by also including a set of recommendation for building future testbed systems.

3.2.1 UK

Research Institute in Trustworthy Industrial Control Systems (RITICS)

The Research Institute in Trustworthy Industrial Control Systems (RITICS)[15] activity has focused on identifying existing technical and practical problems that surround the development of secure and trustworthy ICS. In order to develop realisable solutions to these problems RITICS has conducted a research programme that includes work in:

- Theory and analysis
- Simulation and experimentation
- Testing and implementation

RITICS ambition is to interconnect the existing systems together in order to achieve the scale of real-world systems and to use the capabilities to accelerate and increase efficiency/effectiveness of the UK investment.

The Lancaster ICS Testbed

The University of Lancaster is responsible for the MUMBA project[16] ("MUMBA: Multi-faceted Metrics for ICS Business Risk Analysis"), which includes a lab-based environment that can be configured in several ways. Lancaster has also developed a table-top water treatment demonstrator. With the Mumba project team's move to the University of Bristol, a new ICS testbed is being set up that will include multiple field sites and industrial processes to support research on security of industrial control systems, including both legacy and non-legacy devices and Industrial Internet of Things (IIoT).

ITRC's DAFNI project

The Infrastructure Transitions Research Consortium (ITRC) is a consortium of 7 universities (Cambridge, Cardiff, Leeds, Newcastle, Oxford, Southampton and Sussex), investigating ways to improve the performance of infrastructure systems in the UK and around the world. In particular, the Data and Analytics for National Infrastructure (DAFNI) project[17] will create a national infrastructure database for visualisation and analysis. This will be a shared, secure system for academic research and a resource for businesses, innovators and policy-makers. A key feature will be DAFNI's simulation and visualisation facilities to allow use of models in a more flexible way, enabling the systems of systems analysis and incorporating observed and simulated datasets. DAFNI will benefit from the experience of the ITRC, which has been developing a one-stop database for UK infrastructure (National Infrastructure Systems MODel – NISMOD).

[15] https://ritics.org/

[16] http://www.research.lancs.ac.uk/portal/en/upmprojects/mumba-multifaceted-metrics-for-ics-business-risk-analysis(6f3f4009-8b3d-4c54-82ed-511f27903927).html

[17] https://www.itrc.org.uk/dafni-data-and-analytics-facility-for-national-infrastructure/

5G Testbeds

5G research institutions at King's College London and the Universities of Surrey and Bristol have been awarded £16m to develop the cutting-edge 5G test network that will bring academia and commercial companies together to trial the technology and make sure people and businesses can realise the benefits sooner. This test network will trial and demonstrate the next generation of mobile technology and is the first part of a four-year programme of investment and collaboration in the Government's new 5G Testbeds and Trials programme. The universities will work together to create three small-scale mobile networks which together will form the test network. Each network will have a number of the elements expected in a commercial 5G network - including mobile signal receivers and transmitters and the technology to handle 5G signals - to support trials of its many potential uses.

UKCRIC

The UK Collaboratorium for Research in Infrastructure & Cities (UKCRIC)[18] will provide leadership and support for the development and growth of a coordinated and coherent, world class, UK-based national infrastructure research community, spanning at least 14 universities. UKCRIC will understand how to make the system of systems that constitutes the nation's infrastructure more resilient to extreme events and more adaptable to changing circumstances and contexts, and how it can provide services that are more affordable, accessible and usable to the whole population.

PETRAS Hub

The PETRAS Hub[19] has funding for the creation of several demonstrators, which are currently under investigation.

RHUL

The Information Security Group at Royal Holloway University of London[20] has recently developed an internal system to mimic a variety of ICS systems as well as to perform, among others, simulations of cyber-attacks. The system will be used in collaboration with Hitachi, and their simulator SeTA, and with University of Keio for joint arena exercises and for training of penetration and incident response using a set of different scenarios thanks to the system virtualization capabilities. The RHUL simulation system also includes a large wall screen that helps trainee monitor the status of the exercises and select countermeasures.

3.2.2 US

We report in the following a list of some notable existing testbed facilities in the US.

Power-Cyber

Power-Cyber[21] is a smart grid testbed at the Department of Electrical and Computer Engineering Iowa State University with the purpose to perform vulnerability assessment (i.e., inspect weaknesses within the infrastructure), design mitigation methods, and develop cyber-physical metrics (i.e., metrics combining cyber-physical properties), cyber forensics tools (explore ways to detect cyber-attacks specific

[18] http://www.ukcric.com/

[19] https://www.petrashub.org/

[20] https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/

[21] http://powercybersec.ece.iastate.edu/powercyber/welcome.php

to industry protocols and field devices), and secure models (exploration of innovative security approaches).

Cyber-Physical Experimentation Environment for RADICS (CEER)

The University of Illinois at Urbana Champaign has developed the Cyber-Physical Experimentation Environment for Remote Access Distributed ICS (CEER)[22]. An approach taken by the colleagues behind this testbed is to use high-fidelity simulators of the "physical world", which enables close-to-true impact of cyber-attacks to be accounted for.

NIST Testbed

The US National Institute of Standards and Technology (NIST) is developing a cybersecurity testbed whose aim is to measure the effect of prevailing standards and guidance on the performance of control systems. The testbed is designed as a series of enclaves that address different industrial sectors. The testbed uses simulation where appropriate and HIL components simulating the interfaces between sensors/actuators and the controller. The different enclaves allow the study of continuous processes (such as chemical manufacture), discrete processes (such as automotive assembly) and hybrid processes (such as pharmaceutical manufacture). Performance is measured using appropriate technical performance indicators for the processes.

3.2.3 JAPAN

IPA (Information-technology Promotion Agency, Japan, under METI: Ministry of Economy, Trade and Industry) started Industrial Cybersecurity Center of Excellence (ICSCoE). This year long educational and training program focusing on the industrial control systems was headed by Hiroaki Nakanishi, Chairman, Hitachi Ltd. ICSCoE started on April 2017 for wide range of ICS to train variety of industry experts for under 100 students.

NICT (National Institute of Information and Communications Technology, Japan, under MIC: Ministry of Internal Affairs and Communications) started in 2016 also started for more IT and telecommunications for 1,500 students for rather short term. The number of students. CYDER (Cyber Defense Exercise with Recurrence) for more than 3,000 students is launched in 2017, while Cyber COLLOSEO for and year-long SecHack365 have been started.

Hitachi's Security Training Area (SeTA)

Hitachi is developing a Security Training Arena (SeTA) at their Omika Works in Japan, focusing on deeper and very specific OT needs. The emphasis of this center at this point is to train operators how to deal with cyber incidents in a nuclear power plant. The training facilities and systems including SCADA systems were simulated for controlling systems of a nuclear power plant based on the manufacturing infrastructure experiences for many years in OT and IT. The training includes hands-on training and Red-Blue-executive role play.

They plan to run joint exercises with the UK (and possibly US) in 2018. They have had preliminary discussions with Imperial College London and Royal Holloway University of London as potential academic partners in this programme.

3.2.4 RECOMMENDATIONS FOR FUTURE TESTBEDS

[22] https://iti.illinois.edu/research/energy-systems/cyber-physical-experimentation-environment-radics-ceer

RITICS's whitepaper "Open Testbeds for CNI" recalls three recommendations for future testbeds, namely:

- **Diversity**: an effective testbed should be able to mimic a variety of ICS setups, in particular offering a large choice of devices and protocols, providing different configurations of devices/manufacturers that are typical in ICS settings, and balancing device and protocol diversity against other requirements, such as the implementation of the physical process itself;
- **Scalability**: testbeds need to be designed for scalability to provide faithful representations of real systems. Software should provide simulations of many essential types of devices and from different vendors (or the same vendor but distinctive versions). In addition, the accuracy and reliability of such simulations in mimicking real-life operations is important. Therefore, while the cost of physical equipment can be a limiting factor, virtualisation and VLANs can provide ease of integration and scaling of the testbed infrastructure.
- **Complexity**: although the underlying architecture may be very complex and involve a number of layering and abstractions, this should be as transparent as possible to users of the systems. For instance, transparency can be achieved by providing a single point through which access to and extraction of data from these layers can be managed. Similarly, it is necessary to create and maintain a good documentation of the testbed throughout the evolution of the testbed.

3.3 SHARING OF DATASETS

We refer the reader to the results of the whitepaper published in WG2 "Policy with Info Sharing".

4 CONCLUSIONS AND RECOMMENDATIONS

By 2020 most devices connected to the Internet will be controlling physical systems – be they the industrial/national control systems that we are familiar with today or the heating and lighting systems of our domestic households and drive systems in our cars. Within INCS-CoE we have substantial expertise in securing this infrastructure, but we can achieve much more through collaboration. We recommend the creation of a working group to actively pursue collaboration in the areas identified in the previous section.