

1



STANDARDS, GOVERNANCE, AND POLICY STREAM

Governance and Policy Cooperation on the Cyber Security of the Internet of Things

27 March 2018

Institution of Engineering and Technology,
London, UK

Madeline Carr, Feja Lesniewska, Irina Brass and Leonie Tanczer



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 of the IoT. 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. Funding for the Hub includes a £9.8 million grant from the Engineering and Physical Sciences Research Council (EPSRC) in addition to partner contributions of approximately £23 million in total. This project also runs in collaboration with IoTUK.

Workshop delegate list (in alphabetical order):

Greg Akers (CISCO)	Feja Lesniewska (STeAPP UCL)
Sam B (NCSC)	Apostolos Malatras (ENISA)
Irina Brass (STeAPP UCL)	Carsten Maple (Warwick University)
Madeline Carr (STeAPP UCL)	Rafael Montalvo (CISCO)
Graca Carvahlo (PETRAS, UCL)	Simon Parkin (UCL Computer Science)
Tristan Caulfield (UCL Computer Science)	David Pym (UCL Computer Science)
Liz Coll (Consumers International)	David Rogers (Copper Horse Solutions)
Nicholas Davis (World Economic Forum)	Martin Sadler (University of Bristol)
Peter Domican (Institute for Strategy, Resilience & Security, UCL)	Mike Short (Department for International Trade)
Ana Saldarriaga Gomez (UCL)	Jesse Sowell (Stanford University)
Louise Marie Hurel (LSE)	Leonie Tanczer (STeAPP UCL)
Tony Jeffs (CSICO)	Jeremy Watson (STeAPP UCL)
Olaf Kolkman (Internet Society)	Robin Wilton (Internet Society)



Executive Summary

On March 28 and 29, 2018, the inaugural PETRAS/IET Living in the IoT Conference took place at the Institution of Engineering and Technology, London. As part of this event, the PETRAS Standards, Governance and Policy (SGP) team hosted a workshop on March 27 to explore how global policy approaches to the cyber security of the IoT could be improved to achieve more effective cybersecurity governance across the IoT ecosystem.

Key workshop messages:

1. The IoT is not yet discussed in any depth at forums where global cyber security is taken up.
2. Policymaking at the pace of change of emerging technologies like the IoT is difficult in a domestic context and coordination at the international level will be much more so.
3. Innovation in the governance of technology emerging from the technical community has not been replicated in the policy community.
4. Policymakers and those in the technical community face persistent communication challenges that go beyond terminology. Understanding one another's perspectives better will be fundamental to moving forward with a global approach to shared cyber security problems in the IoT.
5. While policymakers would benefit from more technical literacy, the reverse is equally important. The technical community would greatly benefit from a better understanding of policy processes.
6. A much more effective dialogue between the policymaking and technical communities needs to be established to move forward. One way to do this will be to create a global community of researchers and practitioners who work specifically to communicate better and develop a shared knowledge space.



The impetus for this workshop was the recognition that international policy cooperation on the cybersecurity aspects of the IoT has made little progress. This is due in part to a failure to establish a functioning community of technicians and policymakers who are jointly focusing on these issues. From a technical perspective, the IoT will significantly increase opportunities to breach security via new attack surfaces. For policymakers, the heightened insecurity created by the rapid expansion of the IoT marks a significant governance challenge. Addressing these security deficiencies will require an increase in the capacity to share threat information as well as a range of innovative technical and policy solutions. The workshop marked a starting point in building a global community of security practitioners and policymakers who are interested in these issues and who are working on similar topics.

Given the scope and nature of the problem outlined above, the ambition of this workshop was not to explore possible remedies to the cyber security of the IoT. Rather, our intention was to facilitate a conversation about a changed way of working through these problems. We all understand that close engagement between the policy community and the technical community is essential to address cyber security challenges at a domestic or global level. And we also recognise that communication between these groups is frequently lacking – even when they are around the same table. We wanted to better understand why this is and what steps we might take to improve it.

To achieve this, we wanted to work with three groups of people in a pilot facilitated environment. We invited people who work in domestic or global cyber security policy communities. We also invited a group of people from the technical community who we knew already have an interest in and appetite for policy issues. Finally, we included some academics, especially early career academics who we expect will go on to play a role in these debates over coming decades. The workshop was organised around keynotes with associated break-out sessions. The first half of the day threw us into the communication challenge by asking participants to work on a specific problem that is currently being widely debated in both communities – the potential for introducing a certification or labelling scheme for IoT devices. The second half of the day was spent discussing innovation in governance arrangements with an eye to blue sky thinking that was not constrained by existing mechanisms. We wanted to know from these people, *if the technical and policy communities could work together more effectively, what would be needed?*



Apostolos Malatras from ENISA and Nick Davis from the World Economic Forum gave the two thought provoking keynote presentations. Irina Brass and Leonie Tanczer (both from PETRAS) designed and facilitated the two break-out sessions. Predefined questions and scenarios guided the conversation and were used to incentivise a debate amongst workshop participants. We are extremely grateful to them and to all the participants who played a role in this day. We anticipate that it is the first of many such engagements that will be necessary to move forward global policy approaches to the cyber security of the IoT

This report summarises the keynote presentations and the discussions that took place during the break-out sessions. We are grateful to Feja Lesniewska, a PETRAS research associate at STEaPP, for collating the workshop materials to write this report.





Table of Contents

<i>Executive Summary</i>	3
<i>Table of Contents</i>	7
<i>Workshop Background and Rationale</i>	9
<i>Bridging the Communication Divide: One Issue - Two Approaches</i>	14
Fostering IoT Cybersecurity in Europe and the Communication Challenges	14
Break-Out Session: Certification and Labelling	19
<i>Session Two: New Approaches to Governance in the 21st Century</i>	30
Can Global Governance Be Agile?	31
Break-Out Session: Making Governance Agile	36
<i>Conclusions</i>	43
<i>Further Resources</i>	45





Workshop Background and Rationale

After a brief welcome address to the workshop by Professor Jeremy Watson CBE, Director of the PETRAS IoT Research Hub, (STeAPP, UCL) the background and rationale to the workshop was provided by Dr Madeline Carr (STeAPP, UCL)



Jeremy Watson CBE FREng FIET FICE DPhil is Professor of Engineering Systems at UCL STeAPP. He also has responsibility, as Vice-Dean of Engineering Sciences, for the engineering mission at UCL. Jeremy is a Chartered Engineer, a Fellow of the Royal Academy of Engineering, a Fellow of the Institution of Civil Engineers and the Institution of Engineering and Technology.



Dr Madeline Carr is an Associate Professor of International Relations and Cyber Security at UCL STeAPP. She is also the Co-Investigator of the Standards, Policy and Governance Stream of PETRAS. She is the Director of the UCL Digital Policy Lab and Director of the Research Institute for Science of Cyber Security (RISCS) which focuses on human and organisational factors in cyber security.

Alongside widespread optimism about the huge potential for the Internet of Things (IoT) to deliver a wide range of social and economic benefits, the significant security vulnerabilities are widely recognised. IoT security issues have far-reaching implications for deeply held values of privacy, autonomy, democracy, equity and order. There is a clear understanding that if IoT technology threatens core values, people will be less inclined to adopt it. Given that the implementation of IoT systems relies upon widespread participation and take up, getting security right is fundamental to fully realizing the potential benefits.

Significantly for those of us attending this workshop, the **IoT is not simply a domestic issue**. It is a global coordination challenge and while all states will develop their approach to this technology in ways that best address their own national interest, they will do so within a global, interoperable and interdependent ecosystem of complex supply chains, data flows,



services and infrastructure. Many of the governance challenges that we have been facing for the past two decades of digital technology (like jurisdiction, for example) will be exacerbated as we rethink the ownership of personal data collected via the IoT.

The IoT will stretch (perhaps to breaking point in some cases) the structures and mechanisms for governing technology that have endured until now. The IoT will also require changes to the allocation of liability and responsibility. Understanding what these changes should be in the context of the IoT is important to developing effective governance. Once a million internet enabled lightbulbs, installed in buildings all over the world, are found to be vulnerable, thereby potentially opening up millions of gateways to sometimes critical networks, questions arise about who will be responsible for removing or replacing them – especially once the manufacturer has gone bankrupt. How will product liability (which is how we currently think about vehicles) have any meaning when a family car relies on Internet delivered services, data flows and networked infrastructure to operate safely? The standards, governance and policy implications of this complexity for international trade, for global security and for global governance are significant. Given the rapid rate at which the IoT is being implemented around the world, the technical community and policymakers need to prioritise thinking them through.

Yet, despite the clear need for action, international policy coordination on emerging technologies has not progressed. At key fora where these negotiations take place, the focus continues to remain firmly fixed on the cyber security problems of the last few decades. The challenges faced in the UN Group of Governmental Experts (GGE) in 2017, competition and conflict within the International Telecommunications Union (ITU), and the uncertain role and future of the UN Internet Governance Forum (IGF) all exemplify the way that politics can get in the way of innovation and technological progress. Yet, at the heart of these forums and negotiations are people who understand the issues and care about them. Despite recognition from some of them that the cyber security of the IoT is an immediate problem which demands rapid, global coordination, there seems limited capacity to incorporate or introduce emerging challenges. This applies to the IoT, which is already rolling out. It does not bode well for our capacity to incorporate those challenges that we know will develop further down the track – like Artificial Intelligence (AI).

In examining this issue, it would seem that there are *two truths* which are not entirely compatible. The first truth is that the *technical community has been remarkably successful*



at coordinating the build out and interoperability of a global network over the past 25 years. It is too easy to take this for granted and to simply accept that Internet technologies work. Through innovative governance mechanisms, people all over the world have developed, maintained and secured the domain name system. They have resolved differences when they arise and they have addressed challenges to the legitimacy of those governance mechanisms – adapting and responding to change in an effective and efficient way. So this is the first truth – we’ve seen agility, innovation and successful coordination in the governance of technology from the technical community that has not yet been replicated in the global policy community.

The second truth is that ***technology is political***. Technology is the domain of politics because technology inevitably develops in ways that privilege some and disadvantage others. Technological innovation has economic implications. It has implications for important democratic institutions like elections and a rigorous free press which underpin our social structures. Technology impacts on deeply personal factors like privacy, the management of our own identities, access to knowledge and others’ access to information about us. Technology shapes the economy and it impacts how the law is applied and upheld. It shapes international law – humanitarian law and the laws of armed conflict. These are deeply political considerations and they cannot be left to the technical community, to the private sector or to the amorphous and indistinct communities that we refer to as ‘NGOs’ and ‘civil society’.

One of the key challenges of our time then, is to narrow the gap between these two truths – to bring the discourse and practices of the technical communities and the global policymaking communities into much closer contact to create a shared knowledge space.

To conclude I want to share an experience I had at the 2017 UN IGF, that highlighted the gap that exists between the technical and the policymaking communities. The SGP team were presenting on the role of Computer Security Incident Response Teams (CSIRTs) in international cyber norms negotiations and were confronted with the reality that most of the CSIRT community is completely unaware of the fact that they feature in international agreements about responsible state behaviour in cyberspace. Also, in a major push by Microsoft, there were what seemed like a dozen panels on their Digital Geneva Convention proposal. I went to many of these panels but one of them clashed with a session on emerging identifiers and Digital Object Architecture that I wanted to see. As I was sitting in this large auditorium listening to internet engineers talking about the development and



implementation of changes that would profoundly affect the way the Internet works, with all kinds of interesting implications, it occurred to me that the people who were upstairs talking about the ‘politics of the Internet’ really needed to be in this room. And vice versa. Even though we had all travelled to Geneva to attend the same meeting in the same venue, the political and technical communities were, for all intents and purposes, at two different events.

Many people in the technical community have an appetite for and appreciation of policy problems. Similarly, plenty of policymakers think creatively and innovatively about alternative approaches to governing technology. Some of you are here today and others will join us at future meetings of this working group. I want to suggest today that developing a community of people like us – who have expertise in one area but a real interest and willingness to engage in others – developing that community holds as much potential for positive change as any governance mechanism or institution. Without doubt policymakers would benefit from more technical literacy. But the technical community would also benefit from having a better understanding of policy processes, as well as the pressures, constraints and influences that policymakers face so that it may become less mystifying why they sometimes reject or ignore sound technical advice.

At this workshop, we are initiating a project that specifically seeks to understand why communication between the technical and policy community on international issues frequently fails. In doing so we will gain insights into how the policy community needs information packaged and presented and why the technical community may not always provide information in this way. Understanding this information and communication gap is an essential step in helping us move beyond it. By the policy community making it clear what they need to help them make more informed decisions, the technical community may become more effective at providing advice that could be implemented more readily.

To this end, the workshop focuses on a particular issue – certification and labelling schemes – not to debate whether these are a good or bad idea – but simply as a mechanism to help us think through communication between the communities in a concrete context. We will creatively reflect on the future (or possible futures) of the global governance of technology – specifically prompted by the emerging challenges of the cybersecurity of the IoT.

The agenda for this initial meeting is structured around two focal points; first, the work on IoT cyber security produced by ENISA and second, the thought leadership of the World



Economic Forum on the Fourth Industrial Revolution. At the end of the workshop, ideas about the next steps necessary for continuing this dialogue and creating a community of researchers and practitioners are to be collected. Ideally, I would like to reconvene next year to reach a broader group of technical/policy/academic and industry colleagues also willing to engage in integrating emerging cyber security challenges into international policy discourse.

Dr Madeline Carr

Associate Professor of International Relations and Cyber Security

PETRAS and STEaPP, UCL



Bridging the Communication Divide: One Issue - Two Approaches

In this first session, Dr Apostolos Malatras set the scene with his keynote presentation on ENISA's initiative to achieve improved IoT cybersecurity in Europe. He highlighted both the technical and policy challenges that are commonly identified in discussions on IoT and cybersecurity but he also underscored the extensive need for open, effective dialogue between the two communities. An ongoing failure to prioritise building this cross-community understanding and dialogue undermines interventions designed to address problems. It is integral to the successful upscaling of IoT systems that knowledge and information are effectively articulated across the communities.

The follow up break-out session designed and facilitated by Dr Irina Brass aimed to help participants understand how differently the technical and policy communities can perceive and articulate IoT issues. Dr Brass presented a real-world policy challenge so that participants could discuss in groups and identify the communication obstacles that occur between the communities in a simulated environment. Participants were asked to discuss certification and labelling schemes for the IoT. The break-out session helped bring into focus and make more explicit the communication challenges between the technical and policymaking communities that Dr Malatras had discussed in his opening keynote as had Dr Carr in her introductory presentation.

These communication challenges are immense given the parallel universes each community has operated in for many years. Yet the IoT and other emerging technologies are forcing the technical and policymaking communities together to address new problems. Investment is urgently needed to build the collective capacity to communicate and create solutions for the future IoT landscape to be sustainable at a global scale.

Fostering IoT Cybersecurity in Europe and the Communication Challenges



Keynote Speaker: Dr Apostolos Malatras, Network and Information Security Expert at European Union Agency for Network and Information Security (ENISA). Apostolos has worked for many years in the industry (Thales Research & Technology, Ltd. UK) and academia (University of Fribourg, Switzerland). For the last three years, he has been working for the European Commission. He



received a BSc in Computer Science from the University of Piraeus, Greece, a M.Sc. degree in Information Systems from the Athens University of Economics and Business, Greece, and a Ph.D. degree in Networking from the University of Surrey. He is the author and co-author of more than 60 research papers and scientific reports.

Background

ENISA is a centre of expertise for cyber security in Europe. It was established in 2004 and is located in Greece. Its mission is to build capacity through hands-on activities including training, developing expertise, issuing recommendations and independent advice, and finally, contributing to policy development by supporting Member States and the European Commission with a view to fostering harmonisation across the EU. It is actively contributing to the network and information security (NIS) within the Union, to the development of a culture of NIS in society and to raising awareness of NIS issues.

ENISA works closely together with Member States and the private sector to deliver advice and solutions. This includes, the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, Computer Security Incident Response Team (CSIRTs), and cooperation and capacity building measures. It also includes addressing data protection issues, trust services, privacy enhancing technologies and privacy on emerging technologies, as well as identifying the cyber threat landscape.¹

The IoT – New Opportunities and Threats

Europe faces new challenges with the IoT. ENISA defines the IoT as “a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making”.² Stemming from the definition is the fact that information lies at the heart of the IoT, feeding into a continuous cycle of sensing, decision-making, and actions. The IoT becomes an enabler of Smart Infrastructures, such as Industry 4.0, smart grids, and smart transport by enabling services of higher quality and facilitating the provision of advanced functionalities.

The original business case driving the IoT was to transform critical infrastructure into smart infrastructures. The resulting paradigm shift could lead to increased productivity, reduced

¹ Further information on ENISA available - <https://www.enisa.europa.eu/about-enisa>

² ENISA, IoT and Smart Infrastructures - <https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot>



costs through integration and novel value-added services increasing economic growth. Yet the widespread adoption of the IoT brings with it multiple cybersecurity risks due to the following challenges:

- An increased attack surface
- New problems with interoperability
- Lack of expertise and a lack of incentives for security
- Security by design is not supported by market drivers
- Problems with applying updates to some very simple but critical devices
- Insecure development continuing to build in insecurity
- Unclear lines of liability
- Ongoing fragmentation of good practices and standards (experiments)

Securing the IoT

Ensuring the security of the IoT is both application and context-specific. A nuclear power plant is going to need a different approach to achieve security than the IoT system that controls autonomous vehicles or children's toys for instance. By taking a sectoral approach, it is possible to begin to understand the threats for each sector and the use of the IoT in that sector. Good practices identified in one sector may be advantageously replicated in another sector. Building sector specific expert groups can help to embed good practice and enhance cyber security in each sector. But of course, IoT devices are often mobile and it is therefore important to ensure that devices are still secure when they move from one sector to another. There are also issues within some sectors of legacy systems using older software that will vary depending on individual cases. Given this, communication across sectors is a key component in developing a resilient IoT based smart economy and society. Although the IoT is not covered by the EU Network and Information Security Directive (NIS), it can be found *within* all sectors covered by the NIS so policymakers should not be ignoring it.³

To move ahead and promote the ENISA Baseline IoT Security Recommendations it will be necessary to:

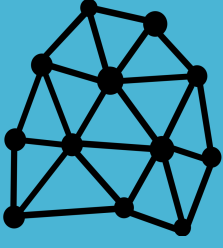

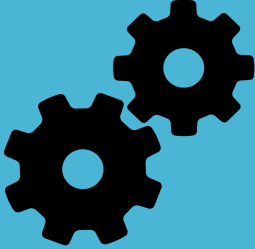
³ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union, L 194/1, 19.7.2016 available <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN>



- Harmonise IoT security initiatives and regulations;
- Reach consensus on interoperability across the IoT ecosystem;
- Promote economic and administrative incentives for IoT security;
- Secure both software and hardware development lifecycles;
- Adopt circular IoT product/service lifecycle management; and,
- Clarify liability for IoT systems.

All of these will require extensive engagement between the technical and policymaking communities. At this current time, there is a scarcity of people in each community who can effectively understand and articulate the necessary knowledge and information to a broad range of stakeholders involved in regulation and governance. Building a community of experts is integral to achieving effective solutions presented by the IoT for all stakeholders.

Table 1: ENISA Baseline Security Recommendations for IoT (2017)

<p>Policy and Organizational Approaches</p> <ul style="list-style-type: none"> ▪ Security by design ▪ Privacy by design ▪ Asset management ▪ Risk and threat identification 	
<p>People and Processes</p> <ul style="list-style-type: none"> ▪ End-of-life support ▪ Proven solutions ▪ Management of security vulnerabilities and/or incidents ▪ Human resources security training and awareness ▪ Third-party relationships 	
<p>Technical Issues</p> <ul style="list-style-type: none"> ▪ Hardware security ▪ Trust and integrity management ▪ Strong default security and privacy ▪ Data protection and compliance ▪ System safety and reliability ▪ Secure software/firmware updates ▪ Authentications ▪ Authorization ▪ Cryptography ▪ Secure and trusted communications ▪ Secure interfaces and network services ▪ Secure input and output handling ▪ Monitoring and auditing ▪ Access control-physical and environmental security 	



There remain many open questions regarding IoT security. It is clear there are divergent views on what IoT security entails; this can depend on the level of abstraction adopted. Although a sector and context specific approach is often envisaged, there remains discussion of whether there should be an entire IoT ecosystem solution to address security issues – and whether this is realistic or necessary. Regardless of the approach, there needs to be agreement on what **benchmarks** to apply for IoT security efforts. Discussions on all of these issues continue to take place in different fora amongst different communities of actors. It is important that shared knowledge spaces are created to improve communication and improve understanding of these problems from all sides.

The next session creates a simulated space in which technical experts and policymakers focus on the open questions and knowledge exchange surrounding certification and labelling of IoT. While this is actually a question that ENISA and others are deeply engaged in, the purpose here is *not* to try to resolve whether **performance-based or process-based criteria** should be used in **certification or labelling schemes**. Rather, the focus here will be *how well can we articulate respective positions on this issue across the techno-policy divide in such a way that counter-parts can understand?*

Break-Out Session: Certification and Labelling



Facilitator Dr Irina Brass is Lecturer in Regulation, Innovation and Public Policy at UCL STEaPP. She is the Co-Investigator of the PETRAS Standards, Governance and Policy Stream. She is also the Chair of the IoT-1 Technical Committee of the British Standards Institution (BSI) – the national standards body of the UK. Dr Brass holds a PhD in Government from the London School of Economics and Political Science (LSE).

Problem Identification

As the keynote presentation illustrated, knowledge and expertise in the technical and operational community frequently fails to be conveyed effectively to support policy-makers in developing goals and objectives to overcome economic, social and environmental challenges associated with technology. This can have costly consequences for citizens, governments and businesses alike. To alter this situation, it is vital that the policymaking and technical communities can more effectively and productively communicate.



A salient example where communication is fundamental between the technical community and policymakers in order to generate effective outcomes is certification and labelling schemes for the IoT. Certification and labelling for IoT is often perceived as potentially advantageous for both users and manufacturers as a means to enhance users' trust in IoT. The recently proposed EU cybersecurity certification framework is a first attempt to explore compliance of specified requirements.⁴ This may form the basis for future discussions on a range of issues including the measurability of cybersecurity, the consistency and equivalence of evaluation methods, benchmarking as well as the enforceability of certificates across the entire lifecycle of IoT products and services. However, certification and labelling of IoT devices is contentious for a number of reasons including: a) that cybersecurity is more dynamic than product safety; b) the boundaries between physical security, cyber security, data integrity, data protection and product safety become increasingly blurred with emerging technologies such as the IoT; c) there is currently no consensus on whether the best way to standardise IoT is through a horizontal baseline of minimum requirements upon which to devise an overarching certification scheme, or whether this should happen in verticals. This contention makes it a perfect issue around which to structure our facilitated conversation in which different perspectives must be communicated with clarity and with an understanding of both technical and policy implications.

Method:

This break out session was designed to foster discussions between the technical and policymaking communities to understand how each perceived of, and communicated about, “what is known” and “what is not known” about the IoT vulnerabilities and risks that an IoT security certification schemes would address. The participants were divided into small groups

⁴ Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act"), Brussels, 13.9.2017 COM (2017) 477 final 2017/0225 (COD)



to collectively answer two questions. Following on, there was a feedback session for all participants to share their responses.

Thus, the aim of the session was not to discuss whether IoT certification is “good” or “bad” – a common direction that a lot of debates around cybersecurity certification and labelling schemes tend to take. Instead, the aim of the session was to facilitate discussion on:

How do we communicate technical and operational expertise for policy-makers to make informed decisions about certification and labelling?

The participants were invited to work in small groups to address two questions that would help identify any gaps in the knowledge exchange between the technical and the policy community on this issue.

Question 1: What critical evidence is needed in order to establish, measure, and assess the kind of IoT cyber security risks that could be addressed by certification and labelling initiatives?

1. Measuring IoT threats / vulnerabilities and categorising risks

One of the main challenges that the participants identified is the issue of measuring threats and vulnerabilities in IoT, and the wider economic, social and environmental risks that these might trigger. Although there are several information security processes, practices and standards already in place, the question is whether they are fully adequate for the IoT, which embeds day-to-day physical products with connectivity to the Internet and its global infrastructure, while delivering new digital services. Several groups acknowledged that the technical community has information about bad traffic and potentially compromised points on their network, the problem is what actually should we measure: e.g. do we measure the number of external points in a network and use existing indicators? Or do we measure their impact on the integrity of the network. Ultimately, the participants concluded that in order to fully understand IoT threats and vulnerabilities, one needs to move away from the issue of “measurement” to understanding the “characterising structure”. This stems from the reality that IoT vulnerabilities, threats, and subsequent risks, are context dependent.



Another approach to uncovering low hanging IoT security vulnerabilities is to use the “story telling” methodology. Some participants indicated that this methodology was used to inform the DCMS “Principles for IoT Security by Design”, where technical, industry and policy experts came together to identify the main IoT security vulnerabilities reported in the media about recent IoT security breaches and their risks for consumers (e.g. Kayla doll; default passwords and the Mirai DDoS attack).

2. What is being certified? The device, the system, or the process?

The participants were quick to acknowledge common challenges on the IoT and certification that span the technical and policy communities: What do we measure? Is it the device, the system or the organisational process? In addition, the participants noted that understanding the boundaries of the system in which several connected devices operate is crucial for deciding upon the evidence needed to inform a certification scheme. In this case, we need to know the boundaries of the system and the governing rules: what is the relationship between these devices within the system and what are the risks of inserting a new element, especially as one of the key characteristics of the IoT is its mobility, which may confound the character of those boundaries?

Some participants used the example of the Connected and Autonomous Vehicles (CAVs) to exemplify the potential gaps between system design, system boundaries (i.e. technical aspects) and the rules that govern those systems (i.e. rules, regulations, policy). In the case of CAVs, the system boundaries for the vehicle itself may be bound, but that system interacts with several others (e.g. smart grid), so technically we need to understand the structure of the system-of-systems at large. But we also need to be aware of the rules, regulations and policies that govern those different systems and the different jurisdictional boundaries. Are there common principles that the technical and policy communities are working towards? This is the current technical – policy gap that IoT exposes and exacerbates.

3. IoT in context

A final issue that the participants emphasised is that knowledge about the context in which IoT operates represents a clear gap if a certification scheme is to be promoted. It was highlighted that the technical and policy community need to work together more closely to understand how different classes of devices play in a particular context (i.e. a technical matter) and the existing rules that govern those contexts (i.e. a policy issue). For instance,



one participant proposed that mapping these contexts to conventional safety regulations, data protection rules or building standards could be a starting point to understand what rules apply in given contexts that might enable or disable cyber security vulnerabilities.

Representatives of the technical community also highlighted the importance of understanding IoT use cases, i.e. how IoT is actually used in a particular context. Once again, this is a gap in knowledge that needs evidence and co-design between the technical and policy community. A technical expert asked: “One can only design a comprehensive certification scheme when understanding all the potential uses and misuses of IoT, and how it behaves in diverse environments. How can we then design certification schemes that reflect IoT uses across multiple contexts, from consumer to industrial IoT?” Once again, CAVs were used as an example. Vehicles have multiple uses: busses, taxis, private use, etc. Understanding, identifying and clarifying these different interactions with IoT are essential for designing comprehensive standards and certifications schemes.

Lastly, the participants noted that there has been an assumption in both the technical and the policy communities that there is an alignment between “user” and “intended use”, and that the IoT challenges this premise in a way that makes it imperative for these two communities to come together, understand their knowledge base and align technical design with policy interventions.

Concluding Remarks for Question 1:

For an IoT security certification scheme to be successful, we need to be clear from the outset what exactly is being certified. Is it a device, a part of a device, or a system? To design certification systems, it is necessary to determine which risks are critical, what evidence to use, which criteria are to be used to measure and assess the risks, and how best to derive and categorise evidence and knowledge from different contexts in which IoT operates.

Key questions that need to be asked include:

- What is the nature of the object?
- What does the object want to do?
- What is the context in which it operates and the system boundaries?
- Can these interactions be categorised?
- What are the risks that emerge when objects and contexts are mixed up?



- What are the acceptable mixes?
- What should not be happening either to the function of the object or the requirements of the object?

In terms of future steps, technical and policy experts in the room agreed that more common ground needs to be achieved on the following issues:

i) Critical evidence

- **People/types/categories** - critical evidence is diverse and context dependent for example it can come from children, vulnerable people, critical infrastructure.
- **Users** - pay no attention to 'evidence', especially consumers of domestic IoT.
- **'Stories' and 'narratives'** are better mediums to communicate the threats from IoT cyber vulnerabilities, for example the 'spying on children' teddy bear case.

ii) Measures and assessment

- **Dialogue is crucial** across sectors to help understand different priorities amongst vested interests – industry (small medium sized enterprises), consumer groups, and government departments.
- **Quick fixes do not work** because they cause conflicts within a complex governance landscape often resulting in problems further down the line.
- **Working outside sector silos is important** – it helps to prevent a stovepipe mentality when designing measures and assessments.

iii) Security risks

- Security **definitions depend on the advisory body** – individual, group, state (public/private) and scale (for example home vs critical infrastructure) that is being targeted.
- The **type and target** of security threats varies significantly.
- A **story board approach** - 'how did we get here?' - can help to develop greater understanding across different communities.
- **Scale**, and how this is linked to the degree of security threat, needs to be considered when developing design measures.



iv) Certification and labelling initiatives design

- **Always find the middle way** – with interoperability for instance.
- **Informed consensus** should be used to agree procedures.
- **Power dynamics between different representatives** – and how this affects the process in developing and agreeing policy – needs to be understood.
- **Capacity building within all sectors** is necessary to understand the threats, risks and security dimensions so policy approaches can be fully informed.

Question 2: What kind of research is needed to support informed policy decision-making about domestic and/or regional initiatives such as the EC Cybersecurity Certification Framework?

This question was designed to take the findings and learning from Question 1 in order to identify directions that would inform future socio-technical research on IoT security and trust. In particular, participants were asked to focus their answers on:

- Communicating technical “known-knowns” (i.e. technical issues policy makers are aware of and understand).
- Understand policy “known-unknowns” (i.e. technical issues policy makers are aware of but might not fully understand).

The participants identified the following research areas that require a closer alignment between technical and social scientific experimentation and understanding.

1. The security checklist approach

One of the key areas that requires further socio-technical research is whether the checklist approach that is recommended by voluntary standardisation bodies such as the IoT Security Foundation, is useful, efficient and sufficient to mitigate IoT cyber security threats and risks.

Some policy and technical experts in the room highlighted that a checklist is useful to expose known, low hanging security vulnerabilities such as default passwords or the need to ensure that software is updated throughout the lifecycle of an Internet connected consumer product.



As long as this is explained in clear ways, it could drive the market to eliminate known cybersecurity security risks.

However, technical experts in the room highlighted that this is problematic for cyber security in general, and IoT cyber security in particular, because in the IT industry security is a process, not a state. How would we then know if the checklist is up to date? How often should these standardisation organisations update it and how quickly should they disseminate it to the wider audience?

In addition, technical experts noted that if both technical and policy communities start thinking of security as a cycle, then they can jointly map out the evidence needed as part of a techno-social feedback loop. They emphasised that this approach, which departs from a rigid design of a checklist, has been successfully used in the airline industry, spotting near misses and incorporating that evidence into business and organisational learning processes. The airline industry has collectively recognised that this information is actually valuable business intelligence. The sector as a whole can benefit from that information being shared.

- What is known now (e.g. default passwords, policy coverage?)
- What is not known now (e.g. is the checklist up to date?)
- Does the checklist have an ongoing feedback loop making it more dynamic?

2. Consumer behaviour

Consumer behaviour is another area that the participants identified as crucial for more socio-technical research. Given IoT security is ultimately contextual (see Question 1), technical participants highlighted that we don't have enough knowledge of what happens when we interconnect devices in environments that have particular specifications or when the anticipated use case may change. This is why a systematic scenario methodology into understanding consumer behaviour and use cases is required. Technical experts showcased this with an example from sharing datasets: we know the risks or privacy challenges of a particular data set, but when we start correlating, we see new risks that emerge. The same issue applies to IoT security: it is not enough to know what happens in a particular system that has predefined boundaries; more work needs to be done in order to understand what



happens when we start interconnecting systems and the datasets they rely upon to automate certain processes.

Social scientists in the room pointed out that behavioural literature is producing very interesting findings on how consumers become informed about uses and share information - findings that the technical community could make more use of (e.g. cyber hygiene).

In terms of consumer behaviour, the experts noted that we are already seeing trends whereby consumers want their devices to be intelligent, smart, capable of, but not necessarily, being connected to third parties. More research needs to be done in understanding these trends, and the balance between functionality – connectivity – data protection – security.

- What will happen when we **interconnect things** - anticipated use cases may change.
- **Scenarios methodology** – understanding the cascade effects of these systems.
- Know what the **risk or privacy challenges of a particular data set** when start correlating, understand new risks.
- **Understanding users' needs and expectations** when designing interventions like labelling/certification.
- Not only what are the systems, but **what happens when start interconnecting these systems/data sets**.

3. Internet protocol developers

Another area that requires further research is whether Internet protocol developers and users are considering how IoT devices are communicating. Technical experts in the room noted that there is a clear link between the protocol and the performance of a device. Developers are mostly concerned with how to make the best protocol for their devices. A key driver for developing proprietary protocols is so a manufacturer can benefit commercially not just from sales of the device, but from the brand lock-in associated with having their own protocol, and perhaps from the intellectual property rights if their protocol goes mainstream. Whatever the driver, they should equally consider the interoperability level, especially how devices understand each other.

- Protocol developers and Internet Service Providers (ISPs) need to think more about **how IoT devices are communicating**.



4. Economics and externalities

A final area that both policy and technical experts identified as crucial for further research is the economic – business question. The experts agreed that more research needs to be done in understanding the implications of IoT (in)security on business models, organisation processes and products/ services.

Technical experts in the room noted that if we just look at the issue of securing the Internet, or the IoT device, we haven't secured the core of the system. Ultimately, IoT is increasingly becoming a service, and, this leads not only to new business models, but also raises new concerns for how businesses understand and implement 'good' cyber security practices throughout the system.

Policy experts in the room also highlighted that the lack of IoT cyber security has externalities that go beyond organisational boundaries, that are systemic at national and international level, and that need to be addressed and understood at this systemic level.

In addition, it was highlighted that the economic nature of our interactions is changing because of the IoT, information flows differently, it is not just devices that are low cost, it is also the transport of information that comes with new risks.

- **Big known unknown** is the economic question – the **complexity** is little understood.
- **The economic nature of our interactions is changing** because of IoT, not just the devices that are low cost, but it is the **transport of information** that also **comes with risks**.
- Need to **understand the externalities** to the IoT: **economic, social and environmental**.

Informed policy decision-making requires quality research. Researchers need to understand what research will deliver effective outcomes for targeted policymakers. The situation for researchers will be challenged by new risks that emerge as things become increasingly interconnected. This will change the research and policy landscape, potentially causing cascade effects within and between systems/data sets that were previously unconsidered or even unknown.



Researchers need to identify what are the questions that need to be answered. There is also a need for researchers to understand which research methodologies should be applied to deliver the relevant outcomes. Outcomes similarly need to be delivered in output formats that communicate effectively with targeted policymakers. Researchers need to develop innovative communication strategies to increase their impact.

Part two of the session highlighted the breadth of the research agenda that needs to be addressed to deliver a safe, secure and reliable IoT. Key to meeting the research needs effectively will be developing a community of both technological experts and policymakers who achieve a common understanding and approach to communicating problems and solutions.



Session Two: New Approaches to Governance in the 21st Century

In the second session, Nicholas Davis from the World Economic Forum (WEF) set the scene by outlining the ways in which conventional governance instruments and mechanisms are running up against their limits in the face of the demands introduced by rapidly emerging technologies. Nick introduced some of the World Economic Forum's work on the concept of the 4th Industrial Revolution (4IR) and how 'agile governance' may offer a more adaptive and flexible approach than traditional processes and practices, many which were designed to address problems in a pre-digital era. Nick highlighted the lessons that WEF drew on from software developers when designing the concept 'agile governance'. Agile governance, although considered a 'work in progress' by the WEF, it is a living example of the cross-community knowledge sharing outlined by Madeline Carr in her opening address to the workshop. Borrowing governance approaches from the technical community may open up pathways for innovative governance design that meets the needs of a new era.

Dr Leonie Tanczer, followed up Nick's presentation with a break-out session designed to proactively explore areas for collaboration and synergy between the technical and the policy community. The exercise aimed to foster a creative environment in which representatives from the technical and policymaking communities could generate novel ideas for governance in the 4IR.

The session highlighted the potential that exists when the space is created to engage in cross-community dialogue. This valuable snap shot illustrated the opportunities that can be capitalised on if more investment is made to build and foster the relationships between the technical and policymaking communities to address the myriad of pressing challenges of IoT governance.



Can Global Governance Be Agile?



Keynote Speaker: Nicholas Davis, Head of Society and Innovation, Member of the Executive Committee, World Economic Forum, Geneva. Nicholas has Bachelor of Laws (Hons), University of Sydney; and MBA (Hons), University of Oxford. Between 2001-03, he was a Commercial Lawyer at Windeyer Dibbs Lawyers. He was admitted to the Supreme Court of New South Wales as Solicitor and Barrister.

The World Economic Forum (WEF) was established in 1971 as a not-for-profit foundation in Geneva, Switzerland.⁵ The forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas. In 2016, the WEF's "Shaping the Future of Digital Economy and Society System Initiative" was established to ensure the digital future is inclusive, trustworthy and sustainable too. The Internet of Things (IoT) is a key focus. Looking beyond the IoT's economic impact, the WEF is researching its effect on society and on the UN's sustainable development goals (SDGs). Most current IoT projects can contribute to achieving both the SDGs and the UN's 2030 mission. Indeed, 84% of existing IoT deployments can address the SDGs.⁶ To benefit from the IoT, governance will need to adapt. The WEF is proposing that a more agile governance approach is needed to address the complex new challenges presented in the 21st century to co-create solutions.

Innovative technological capabilities are being enabled by digital infrastructure, not just digital applications, that offer new economic, social and environmental opportunities. These include:

- Extending digital technologies (IoT, new computing, blockchain).

⁵ White Paper on Agile Governance: Reimagining Policymaking for the Fourth Industrial Revolution (January 2018); K. Schwab and N. Davis, *Shaping the Fourth Industrial Revolution*, World Economic Forum (2018)

⁶ See World Economic Forum, *Internet of Things Guidelines for Sustainability*, (2018) available <http://www3.weforum.org/docs/IoTGuidelinesforSustainability.pdf>



- Reforming the physical world (Artificial Intelligence (AI) and robotics, 3D printing, advanced materials, drones).
- Altering the human being (biotech, neurotech, Virtual Reality (VR) /Augmented Reality (AR)).
- Integrating the environment (geoengineering, energy capture and storage, space resource extraction).

These emerging industrial technologies are challenging existing governance tools that were designed in a different era. As Madeleine K. Albright insightfully observed "People are talking to governments on 21st century technology, the government hears them on 20th century technology, and responds with 19th century ideas." The implications for global governance will be potentially catastrophic if new innovative and more effective tools are not developed and deployed soon.

Governance processes need to be designed with the following three assumptions in mind:

- **Technology is political:** The political nature of advanced technologies requires close attention and governance because we are building economies, societies and world views through them. In turn, they shape how we interpret the world and the possibilities we envision. Agile governance can proactively help shape and direct how technologies impact people and communities in a malleable way through an iterative process.
- **Decisions taken today matter:** As 4IR technologies mature, it is important that we make considered decisions now and take action if we are to shape the configuration and impact of technologically driven systems for a shared, common objective.
- **Empowering people at all levels:** Positioning values that promote societal benefit and well-being as priorities for governance can direct the development and use of emerging technologies and who they benefit. Existing governance tools are unable to address the challenges that the 4IR presents as technologies from different disciplines have their interoperability and combinatory capacities supported by increasing computing power, bandwidth, and machine learning algorithms.



Shifting Governance: From Traditional to Agile

Traditional governance is distinct in that it is periodic, moving from the general to the specific, using incentives to create effects, employing targets, monitoring activities and outcomes (usually top-down), applying sanctions or fines where compliance is breached.

The governance tools used for traditional governance include international conventions and agreements (the Montreal Protocol, Cartagena Protocol and the Paris Agreement) usually led by governments but also sometimes by non-state actors like international organisations (WTO, WIPO), non-state led influencers (ISO, certification), powerful sub-national leadership (California emissions trading standards), hybrid groups (ICANN), and investor influences (Bill and Melinda Gates Foundation). Common problems associated with these traditional tools are:

- These instruments can take a long time to sign and ratify,
- They face enforcement problems,
- They can be difficult to update,
- Agreements can be highly challenging when interests diverge,
- They can also be highly challenging when the subject is technical and uncertain.

An alternative model to the traditional approach is **agile governance** which blends intrinsic and extrinsic approaches. By doing so, more often than not, this governance approach will create a better dynamic between the general and specific. It does set limits, but these are more on outcomes than a specific activity. Also, agile governance will create effective, relevant incentives that are linked to the bigger picture e.g. sustainability. Monitoring of activities and outcomes will come from the bottom-up rather than the top-down. This will use automatic / pre-triggered mechanisms. This dynamic approach is apparent in the principles that have informed agile governance conceptual development.

Agile governance draws on principles developed in the technical community found in Agile Software Development:

- Outcomes over rules
- Responding over following a plan
- Participation over control
- Self-organization over centralization



Yet these principles need to be aligned with clear ethical foundations. As such, agile governance should also be guided by the following normative principles:

Human-centered: Agility can also enable policymaking that is more inclusive and “human-centred” by involving more stakeholders in the process and allowing for rapid iteration to meet the needs of the governed.

Inclusive: Inclusion may seem at odds with the interpretations of agile, which anticipate increases in speed. While more timely experimentation and decision-making may be warranted in many cases, agile governance does not privilege speed over the duty of public and private governance processes to empower and protect those they serve.

Sustainable: Agile governance can also ensure long-term sustainability by creating mechanisms to constantly monitor and “upgrade” the policies governing emerging technologies, as well as by sharing the workload with private sector and civil society to maintain the relevant checks and balances.

Flexible and adaptable: Agility is by its very nature flexible and adaptable. Incorporating these qualities into innovative governance should be at the forefront of regulatory design principles.

Innovative and creative approaches to designing and implementing tools are required for agile governance to be achieved in practice. To date **governance tools** used in **agile governance** include:

- Policy Labs
- Regulatory sandboxes
- Crowd-sourced policymaking
- Collaboration between regulators and innovators
- Direct representation in governance
- Cross-industry self-regulation
- Ethical standards and local responsibility
- Collaborative governance eco-systems
- Transparency and trust building mechanisms



The combination of **systems and design thinking** provides an iterative and cumulative learning process by exploring a **complex and fast-moving ecosystem**, sense-making of observed variables, and shaping of possible outcomes, while analysing the influence of those outcomes on the status quo. Using collective and collaborative models will create a governance environment that has reflexivity and feedback loops. However, for **agile governance** to be successful **new mind-sets** are necessary. Governance must become a **multi-stakeholder** endeavour that is inclusive, transparent and participatory. Greater informed citizen participation, partnerships and responsible and responsive leadership is needed for this to be achieved. **Leadership in four areas is necessary** for agile governance to take hold: **technology; governance; values; and systems.**

The 4IR is setting the world community new challenges that require a new governance approach. Agile governance combines elements of traditional governance with innovative, flexible and adaptive tools that are founded on guiding principles from both the technical and the policymaking communities. Technology is disrupting the existing governance order and unless leaders adapt quickly, the opportunity to shape the future for the benefit of all may be lost.



Break-Out Session: Making Governance Agile



Facilitator: Dr Leonie Tanczer is a Lecturer in International Security and Emerging Technologies at STEaPP. Leonie is former Fellow at the Alexander von Humboldt Institute for Internet and Society in Berlin. She studied Political Science (BA) at the University of Vienna and University of Limerick (Republic of Ireland) and Political Psychology (MSc) at Queen's University Belfast where she also completed a PhD student at the School of History, Anthropology, Philosophy and Politics on the (in)securitisation of hacking and hacktivism.

Problem Identification

As Nicholas Davis' keynote emphasised, agile governance will only be successful if new mind sets are fostered and developed. This is key for individuals who are engaged across the four leadership areas: technology; governance; values; and systems. There needs to be capacity building and skills development amongst leaders in these areas if agile governance systems are to be put into play. One way to develop innovative thinking skills is to enable creative problem identification and problem-solving environments bringing together different communities of practitioners around the same table. This break-out session uses a simulation exercise to provide such an environment for the workshop participants. a simulation exercise to provide such an environment for the workshop participants.

Method

This two-hour long break-out session was structured around the questions of "what needs to be done" and "how" to make governance agile. It was designed to proactively explore areas for collaboration and synergy between the technical and the policy community and was centred on a structured exercise designed especially for the session.

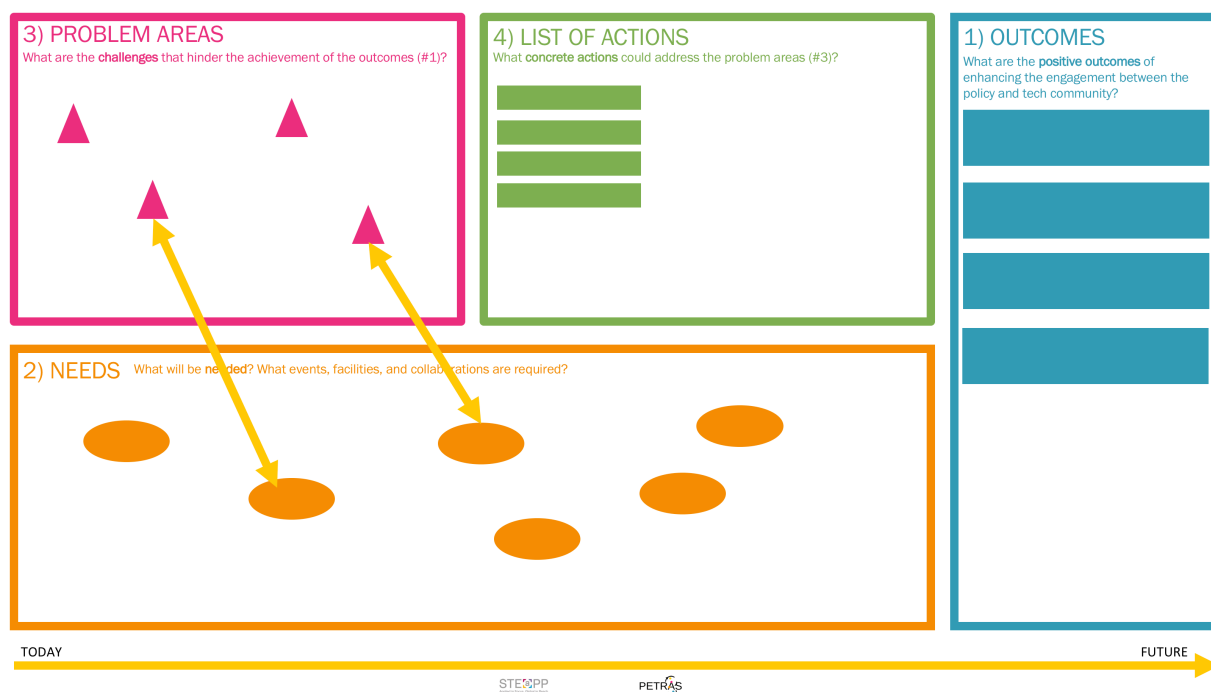
The exercise made use of a worksheet (see: Figure 1) through which focus group discussions across five different groups (each with approximately 3-5 participants) were coordinated. These focus groups were asked to address the following four issues:

1. **Outcomes:** What are the positive outcomes of enhancing the engagement between the policy and technical community?



2. **Needs:** What will be needed to enable the successful delivery and achievement of these outcomes?
3. **Problem Areas:** What are the challenges that hinder the achievement of the proposed outcomes?
4. **List of Actions:** What concrete action points need to be implemented to address the stated problem areas and ensure the achievement of the outcomes?

Figure 1: Exercise Hand-Out Break-Out Session 2
(Developed in collaboration with Dr Ine Steenmans (STeAPP, UCL))



The groups had 20 minutes to provide responses to each of the four issues and were instructed to report back and address two aspects:

1. **Diagnosis:** What do you think are the three key problem areas?
2. **Intervention:** What are the three key actions that need to be taken?

The following section summarises the highlighted problem areas and the list of actions that were discussed by workshop attendees in each of the groups.



Group One

Problem Areas:

1. To have a **non-ideological debate** which helps to build a willingness to talk about IoT security.
2. To build **skills and the desire** for policymakers to understand IoT security.
3. To promote the engagement with **small and medium size enterprises (SMEs)**.

Recommended Actions:

Group One focused on three different ways to enable a structured and "soft" way of engaging with policymakers and technologists:

1. To build an **IoT governance boot camp**, similar to cybersecurity boot camps taking place globally. This boot camp would be a multi-stakeholder space (e.g., mayors, individuals from different sectors working on the local level) and a place where one can engage with different representatives who work on various issues, including capacity building. The model could be replicated in different spheres such as, for example, on the city level. This model would also build some form of legitimacy to the engagement between various communities.
2. Engage with **operation centres** on the city level to exchange lessons learnt. One way to engage with these centres in a more structured way would be through the C40 Cities Climate Leadership Group.
3. To set up **workshop and conference structures** such as the National and Regional Internet Governance Forum (IGF) initiatives that could support this process from the national, regional, and international level.



Group Two

Problem areas:

1. Lack of **long-term commitment** to initiatives and bodies as well as efforts and processes in terms of IoT security.
2. Lack of **Sherpas/facilitators** that can liaise between governance, policy, and technology communities.
3. Commitment to **diversity and plurality** that frequently stand in the way of **efficiency and the ability to reach conclusions**.

Recommended Actions:

1. Pursue **long-term funding** initiatives that could be focused on *how* to solve IoT security, rather than *what* particular issues need to be solved and addressed.
2. To ensure a **buy-in from existing initiatives** to integrate those existing initiatives that have certain constituent followers to be included in any future proposed scheme.
3. To offer **training for facilitators** to talk and interpret the language of technology and policy communities. Training should also focus on how to involve citizens in IoT security processes. Training should be inclusive and the impact of initiatives and technologies assessed so lessons can be learnt and incorporated into subsequent training.

Group Three

Problem Areas:

1. A prevailing "**fear of being shut down**" for speaking out. This leads to an unwillingness to engage because one is worried about the consequences of speaking up. This is a process that is evident both in both the policy and technical communities.
2. Another problem is the **scope of the working group** and is centred on the issue that one can "go too far with diversity". This problem is evident in existing operational working groups (e.g., the IGF). The issue with diversity is that one has too many voices that can lead to the discussion becoming too messy and disciplinary opaque.



3. There are **too few incentives** to bridge the gap between policymakers and technologists. It is often difficult to get people out of their professional 'comfort zones'. There needs to be professional development incentives to change the mind set in both the technical and policymaking communities.

Recommended Actions:

1. To produce a "**Code of Conduct**" using a bottom-up approach and be supported by facilitators. Abiding by the Code of Conduct will require a cultural shift in many technical and policymaking communities.
2. To tackle the disciplinary messiness, one has to ensure that **the right people are in the room**.
3. To offer **more incentives** to bridge the gap between policymakers and technologists.

Group Four

Problem Areas:

1. Frequently **not the right people** are in the same room.
2. Too many **negative externalities**, for instance companies are pushing insecure products on the market and are not able to bear the liability nor the cost and inconvenience resulting from them.
3. **Perverse incentives** in the process. Often the regulatory environment gives some stakeholders an incentive to get involved in discussion processes and to lobby for their perspective which will ultimately benefit only them.

Recommended Actions:

1. **Reduce barriers to stakeholder participation** to help get the right people in the same room at the same time. How should this be done?
 - a. Appoint a "**proxy**" to deal with stakeholders who cannot attend meetings;
 - b. Establish a **sponsorship or fellowship** scheme for less well-resourced stakeholders. They should feed any of the learned insights back into their countries or communities.



- c. Distribute **simplified materials to** users physically and directly e.g. via schools and/or roadshows.
2. To tackle the negative externalities and perverse incentives one should **underline the incentives**. If there are negative externalities one should try to close the loop. Hence, the negative effects should be fed back to the entities that caused them. An analogy for this action point could be the process of recycling plastic bottles or recyclable cans where the drinks provider assumes responsibility for the management throughout its lifecycle.
3. To **go to the user** instead of expecting them to come to the process. To do this, one should recruit the "**David Attenborough of IoT**". The latter can be the face of IoT security. S/he can convene the message, can be put on Youtube, is on documentaries and has a virtual presence.

Group Five

Problem Areas:

The group's suggestions were all about power, knowledge, and interest.

1. Lack of cross-fertilisation between disciplines, as well as policymakers / government and technology, at the senior level.
2. **Language and assumption problem**: Both communities do not share the same language and have different assumptions about each other's motivations.
3. Lack of **trust** between both communities and a persistent belief that "the other side" is lacking necessary expertise.

Recommended Actions:

1. The engagement on the junior level should be complemented with **high-level secondments** of people who have both the mobility and influence to evangelise their organisation. A concrete action to achieve this would be to draft a two-dimensional **stakeholder mapping** that draws on a power vs. interest matrix. This way, capable individuals who are also willing to strike a balance between both communities can be identified.



2. To address the language and assumption problem, Group 5 proposed the "**Helter Skelter**" exercise. The idea of Helter Skelter came from the Beatles song where band members swapped instruments. Policy Makers would design a user interface in the role of Technologists. They would then invite Technologists to play in the role of Policy Makers and attempt to write a policy describing the system's correct usage. There would then be some ensuing discussions about how it went. Basically, it is intended to provide an opportunity for the two disciplines to wear each other's shoes for a day. There will be friction but ultimately the exercise is designed to help foster amongst both groups a shared vocabulary.

3. To tackle the trust and expertise issue, Group 5 has developed a "**Fried Egg**" exercise. The activity involves going into separate rooms (policymakers in one, technologists in another) and both groups reflecting on their expertise as well as stating "what do we know" (i.e., their core expertise). Additionally, both groups state what one knows about the other group's expertise. Then each group develops their own 'fried egg' (a bubble that is one colour and characterises the groups' core expertise; and a bubble that is another colour that describes the others group's expertise). The exercise ensures that technologists and policymakers can compare their 'fried eggs' which should support trust building and allows both groups to fill each other's knowledge gaps.

The session resulted in some creative proposals. The problem areas and the list of actions identified here provide useful pointers on how to best influence and frame the agenda for follow up workshops and meetings. They provide a "cookbook" for policymakers and technologists who are both equally encouraged to make use of the insights derived from this break-out session. They are aimed at helping to reduce the barrier of engagement and incentivise the bridging of a long-standing gap between both communities. Measures such as the implementation of Codes of Conduct, the simplification of language, as well as exercises such as the Helter Skelter might not be the only solutions to address the problem areas during the workshop. Nonetheless, based on the activities conducted during the workshop, participants feel confident that they provide a stepping stone towards a more open encounter between these technologists and policymakers, both of which in the current climate should be speaking and engaging with each other.



Conclusions

If the increased economic and non-economic values of incorporating the Internet of Things (IoT) into the world are to be realised then knowledge and information needs to be communicated more effectively between communities – both the technical and the policy-making – to address cybersecurity risks. Society will not trust IoT systems that put at risk their security. Neither will they tolerate institutions whose governance models fail to protect them from cyber-harms. A great deal is at stake both in the public sector and the private sector as emerging technologies rapidly alter the governance landscape. A business as usual approach to cooperation between the technical community and policy makers is no longer fit for purpose.

The workshop on ‘Governance and Policy Cooperation on the Cyber Security of the Internet of Things’ revealed a number of fundamental flaws that currently threaten the successful adoption of emerging technologies. It also laid out useful stepping stones to use to actively foster capacity building and skills development, between and across all communities to deliver a future that works for all.

Introducing the workshop Dr Madeline Carr (STeAPP, UCL) highlighted two truths to guide participants through the activities and discussions. The first truth being the success that the technical community had experienced over 25 years, and continue to experience, to build a multilevel agile, innovative and effectively coordinated governance framework for digital technology. Yet this occurred with limited involvement from the policy-making community leaving a legacy of misunderstandings, tensions and at times hostile relations. The second truth is that technology is political - innovation always has economic, social and environmental implications that privilege some whilst putting others at a disadvantage. Nick Davis (World Economic Forum) observed that existing governance models developed prior to the digital age are unable to resolve the multilevel complexities that emerging technologies like the IoT bring. Governance systems need to be reformed for the digital age, yet this cannot solely be left to policy-makers because future governance systems will depend on emerging technologies to govern. This dilemma was acknowledged by Dr Apostolos Malatras (ENISA) who highlighted the ongoing failure to build cross-community understanding and dialogue to more effectively communicate the vital information and knowledge needed to secure the future of emerging technologies in society.



The session coordinated by Dr Irina Brass (STeAPP, UCL) brought to the fore the divergent views that exist in determining problems, identifying questions and agreeing on criteria and processes to address security issues for certificate and labelling schemes amongst the technical and policy-making communities. Participants emphasised the need to adopt new dialogues, new stories to communicate with users, question the limitations of established systems such as checklists and promote informed consensus to arrive at a middle-way. The outcomes from Dr Leonie Tanzcer's (STeAPP, UCL) session, which focused on promoting more agile governance, underscored the importance of long-term commitment (including funding), representative diversity, training and dedicated centres of excellence to foster innovative approaches and to build skills and capacity across all sectors and at all levels. Agile governance, a concept promoted by the World Economic Forum, needs ethically informed innovative regulatory processes and mechanisms to deliver outcomes that are human centred, inclusive and sustainable.

The workshop demonstrated a consensus between the technical community and policy-making community that cooperation is currently sub-optimal. The major obstacles to improving cooperation primarily lie in a long-standing failure to communicate effectively. Building knowledge spaces to bring the technical and policy-making communities together is vital to achieving transformations in governance to achieve outcomes that are politically acceptable for all. Engagement will only come about if there is active commitment to deliver using existing forums in innovative ways, creating new forums and spaces and using language that is inclusive to communicate ideas, concepts and processes.



Further Resources

Brass, I., Tanczer, L., Carr, M., & Blackstock, J, Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things? (2017), 33 *Risk & Regulation* 12-15 available http://discovery.ucl.ac.uk/1544261/1/Brass_IoT%20Regulation_Risk%20and%20Regulation%20Magazine_Accepted%20Version.pdf

ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, (November 2017) available <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>

Institute for Strategy, Resilience & Security at UCL, *Towards Trustable Software, A Systematic Approach to Establishing Trust in Software*, (October 2017) available https://docs.wixstatic.com/ugd/154eeb_ed44980b9ce64105adfa2314b2f6dc31.pdf

Institute for Strategy, Resilience & Security at UCL, *Digital Resilience - Understanding the Challenges of Resilience in Digital Environments*, (August 2018) available <https://www.isrs.org.uk/publications>

Internet Society, *Global Internet Report 2017: Paths to Our Digital Future* (2018) available <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

Tanczer, L. M., Steenmans, I., Elsdon, M., Blackstock, J., & Carr, M, *Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge?* (2018) available <http://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0033>

World Economic Forum, *Agile Governance: Reimagining Policy-making in the Fourth Industrial Revolution*, (January 2018) available http://www3.weforum.org/docs/WEF_Agile_Governance_Reimagining_Policy-making_4IR_report.pdf