Putting the IC into ‘Policy’: strategic analysis for optimising the role of ICT in EU policy delivery
Cave, J.; Joyce, C.; Shahin, J.B.M.M.Y.; Cave, B.; Schindler, R.

DOI: 10.2759/48259

Citation for published version (APA):
Putting the IC into ‘Policy’

Strategic analysis for optimising the role of ICT in EU policy delivery

FINAL REPORT

A study prepared for the European Commission DG Communications Networks, Content & Technology by:

C360
Abstract

This document presents the conclusions of the Optimising ICT study into the effects of ICT on the policy process. The remit of the study has evolved to examine the disjunction between physical markets and their online counterparts caused by the presence of ICT factors that either elude policymakers altogether or cannot be avoided. The report traces the study from its inception and intellectual origins in the Eco Search initiative to optimise online energy labelling through to conclusions and recommendations in the form of a tool box.

The starting point is the recognition that ICTs profoundly influence policy formulation and effectiveness across a range of domains. This linkage is (potentially) two-way: ICTs may contribute to or help address problems in ‘non-ICT’ areas; conversely, ‘non-ICT’ considerations may need to be taken into specific account when formulating ostensibly ICT-centric policy. One source of this linkage is the emergence of on-line substitutes or complements for off-line activities; another is the potential of data generated and mediated by this on-line migration to expose incorrect or obsolete assumptions and to indicate where interventions could be improved, reduced, cross-linked or reoriented. The potential of these links is limited by the fact that institutions with specific policy responsibilities tend to collect information of most relevance to their own obligations and perspectives and are sometimes reluctant to share information, collect data on behalf of others or collaborate in developing solutions.

We use the term ‘Internet-ready’ to denote areas with the potential for more effective and appropriate interventions based on the on-line migration of off-line activities – and especially where existing instruments and legal frameworks allow as-yet-unrealised adaptation in interventions and policy processes. This report considers their identification, prioritisation and management.

The document should and must be read as a first foray into the domain; therefore we have used three indicative examples (Deep Dives) in order to develop a general approach and a series of conclusions. The first part of the document discusses the intellectual and operational context of the study.
The Deep Dives themselves represent three distinct ‘levels’ of Internet readiness:

1. understanding the role of ICT in exacerbating, assessing and/or resolving current problems;
2. using ICT-based data and models to develop a deeper shared understanding of the behavioural and systemic origins of policy issues and the likely response to interventions; and
3. analysing the extent to which the collection, sharing and analysis of data may redefined or moot problems and change the case for intervention and the ownership of policy issues.

Chapter 1 discusses the policy context and the antecedent (EcoSearch) initiative. This is followed, in chapters 2-5, by a more detailed presentation of the results of Deep Dives into the domains of Food Labelling (Level 1), Transport (Level 2) and Cybersecurity (Level 3).

Chapter 6 presents conclusions in the form of a practical toolbox designed to guide policy interventions from their earliest point to be Internet-aware. Chapter 7 concludes with some general observations to highlight key lessons and demonstrate the potential and need for further progress in this field.
Executive Summary - Optimising the role of ICT in EU policy delivery (OptICTs)

Optimising ICT (OptICTs) sought to answer a specific yet complex question: How can policymakers better understand and improve the effects of the Internet on the domains or markets for which they are responsible? To address this pressing challenge, OptICTs took a 3-phase approach: 1) Identify 2) Understand 3) Mitigate. The study is a first advance into the largely uncharted territory surrounding the long-term effect of online factors on existing regulatory environments. As with any vanguard action, it does not provide a magic cure, panacea or blueprint for exact solution. Rather, the study provides an approach, recommendations and the basic tools necessary to begin integrating a response to the challenge into any policy domain. Extensive and diligent work will be required from all those involved in the policy process but our hope is that this study can provide an orientation to begin this journey.

Internet-Aware Policy – The Scope of the Challenge

Today the Internet pervades every area of society. In most policy areas, virtual expressions of the physical world arise and change with a speed and agility that renders much existing policy obsolete. These changes are not all negative - online environments often provide more visible, secure, easy-to-regulate or self-regulating environments. Nevertheless, there is a major risk of policy obsolescence or drift; in the majority of today's policy areas, laws exist that were created without the Internet in mind or with only a superficial understanding of its capabilities and impacts.

The Internet is already altering the fundamental relationships and assumptions on which policy interventions are based by changing the ability of individuals to understand, choose or give consent or by replacing traditional objectives and mechanisms (profit maximisation, competitive markets) with others (the search for cybersecurity and transparency or networks of innovation) that may be harder to assess. The speed of Internet development requires forward-looking, adaptive and collaborative methods of assessing policy issues and interventions and a more open and agnostic approach to evidence collection, situational awareness and option formulation.

OptICTs sets out specifically to identify the challenge of Internet awareness, understand how the challenge manifests in different policy areas and finally to make a set of
recommendations to help policymakers adopt proactive, forward-looking engagements that can create Internet-aware policy for the future.

**Framework for Action**

The OptICTs study began by creating a framework for selecting and prioritising policy areas that merit intervention. This framework uses a number of qualitative measurement criteria to assess the suitability of an area for Internet-aware policy. The following long-list of criteria was arrived at following extensive consultation with stakeholders across different DGs:

- Existing pollution/infiltration of traditional area by Internet or ICT
- High potential for the contribution of ICT to policy problem
- High potential for the contribution of ICT to resolution of policy problem
- High potential for short and long term gains
- Ease of collecting concrete and robust measurements
- Comparability, reusability, transferability of lessons
- Ability to mandate or implement common definitions, principles, requirements and procedures
- Scope to adopt a broad definition of relevant information, sources and ‘target audiences’
- Flexibility to keep up to date with new information requirements of consumers and other key stakeholders
- Potential to level the playing field across different channels (online, offline)

These were then condensed to give five simplified and practical indicators of promising topic areas (described in detail in Section 2.2.1):

1. A high potential for the contribution of ICT to resolution of policy problem
2. A high contribution of ICT to the policy problem
3. Short and long term gains
4. Ease of collecting concrete and robust measurements
5. Comparability, reusability and transferability.

Combining these qualitative criteria with the expert judgement of key stakeholders, the study identified ‘candidate areas’ where Internet-aware policy intervention had both a high probability of success and high potential benefit. A practical application of the criteria was then used to identify three policy areas for subsequent ‘Deep Dive’ assessment using a wide range of techniques including horizon-scanning, trend analysis and issue identification and prioritisation. In addition to the need to generate a set of initial exercises that illustrate the toolkit, we also wanted to ‘span’ a range of ‘depth’ and timescales. This is represented by three levels (discussed in detail in Section 2.2.3): 1) solving problems, 2) understanding problems and 3) rethinking the case for action.
The most suitable Deep Dive areas were food labelling, transport and cybersecurity. In addition to representing very diverse challenges, these policy areas exemplify three distinct ‘levels’ of Internet-readiness. Food Labelling provides a clear example of a Level 1 (Solving Problems) domain - one that is already experiencing Internet-readiness challenges to its governing policies and regulations. The purpose of a Level 1 Deep Dive is therefore to identify potential responses to these challenges.

Transport is a Level 2 (Understanding Issues) domain - one where Internet-awareness challenges are not currently causing problems but have the potential to do so in near-future if current trends continue. The Deep Dive therefore focusses on identifying the prospects for developing a better understanding of the behavioural roots of the issue, potential pressure points for the future a framework for monitoring and mitigating.

Finally, Cybersecurity is a Level 3 (Rethinking the Case for Action) domain - an area where the landscape remains unclear. A level three Deep Dive is therefore dedicated to considering the potential evolution of the area – and the way it is understood in policy, suggesting new future-scoped framings of the issue, signposts and triggers and the long-term effect of policy interventions.

But note that each Deep Dive has implications across all levels, which can enrich the understanding of Internet readiness.

<table>
<thead>
<tr>
<th></th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Food (DGC acting in other areas)</td>
<td>Detecting and controlling e.g. contamination, origin</td>
<td>Perceptions of quality and safety and responses to information</td>
<td>Food as engine of civilisation, collective vs. private environment, food vs. other security, etc.</td>
</tr>
<tr>
<td>Transport (DGC acting in other areas)</td>
<td>Congestion, emissions, safety problems</td>
<td>“Intelligent” mobility, urbanisation: Intelligent design and intelligence in systems</td>
<td>Fast and slow networks and the right to move; public vs. private space</td>
</tr>
<tr>
<td>Cybersecurity (DGC opening to other areas)</td>
<td>NIS incidents, surveillance, TOR</td>
<td>Security and privacy Role of 3rd parties</td>
<td>SplInternets, patchworks or a global commons</td>
</tr>
</tbody>
</table>
Deep Dives – Internet-Awareness in Action

The following present the principal conclusions of each Deep Dive:

Food Labelling

The Deep Dive into food labelling concluded that a key factor frustrating the development of Internet-ready policy was the lack of requirement to keep the valuable data generated at every step of the food supply chain. The ‘data deficit’ in food chains has exacerbated current challenges including underreporting of food safety failures, incomplete information about food provenance and supply chain inefficiencies. The Deep Dive concluded that a concerted drive to mandate the production and publication of high-quality data has the opportunity to bring significant benefits to the food chain including new business models, greater public trust and better management of food safety.

Transport

The Deep Dive into transport found a policy area on the threshold of transformational change. The shift away from industry-specific and behaviourally unsophisticated thinking about trains, airlines or roads toward an appreciation of integrated transport systems is driving profound alterations in the way we approach the gathering and publication of transport data. The Deep Dive concluded that to minimise the adverse impacts of industry silos, sharing of data, common practices and increased data-sharing and cooperation must be introduced not only into the transport and communications industries but also the diverse regulatory and policy bodies who govern them.

Cybersecurity

The Deep Dive into cybersecurity revealed complex dependencies between policymakers and those who seek to circumvent policy for criminal means. Contrary to the received logic that policy can prevent threats or malpractices, in some cases not responding to a new threat through policy is an effective way to detect and combat breaches because it does not drive criminal activity back ‘underground’. The Deep Dive concluded that in the future a system of light-touch regulatory interventions, combined with the self-organised activity of Internet providers and users, may be more effective than heavy, prescriptive interventions more often associated with security policy. In addition, cybersecurity is an emerging and complex issue that changes daily so the Deep Dive recommends actions to broaden the reach, strengthen the links and intensify the information sharing network across different policy bodies to continuously monitor and assess the case for interventions.
**Toolkit – Recommendations on Making Internet-Aware Policy**

OptICTs’ work on the framework for identification and the Deep Dives provided a vivid illustration of the diverse challenges Internet-awareness can create in any policy domain. The study further highlighted that no two policy areas are the same and that prescriptive recommendations at the global, EU level would not effectively balance their common and distinctive aspects. Instead the most useful approach is to create a loose ‘toolkit’ containing approaches, techniques and actions that have been proven effective in creating more Internet-aware policies. The horizon-scanning, mapping and related tools allow the creation of ‘stratified’ and flexible policy processes and interventions and a structure for drawing broader lessons\(^1\).

Alongside these techniques, the report makes clear recommendations on engaging the correct teams early, sharing personnel and data, and creating a ‘sandbox’ where staff can explore potential solutions for Internet-aware policy. Finally, OptICTs recommended an end to the ‘dossier silos’ that bind specific personnel to given domains and embrace a more collaborative trend analysis so that information can be taken out of the hands of the few and shared with the many who can act upon it.

In addition to the tools developed to support all policymakers, the Deep Dives provided OptICTs with the basis for a concrete framework to assist DG CONNECT in providing deeper insights into Internet-readiness issues and leveraging a potential new transversal remit to best assist in developing Internet-aware policies. Specifically, the study has recommended four clear steps for CONNECT:

- Identify emerging Internet-readiness policy challenges using adaptive horizon-scanning
- Prioritise areas for action on the basis of Internet-readiness, ‘level’ and urgency
- Quantify the effort required to intervene in terms of the personnel cost, likelihood of success, legislative difficulty and man hours involved\(^2\)
- Act or Withdraw - DG CONNECT acts to mitigate a policy challenge or withdraws from co-development of policy in the relevant areas.

---

1 For example, the food labelling application yields new insights into ‘informational remedies’ that can be used in the transport and cybersecurity areas; in turn, the behavioural modelling needed to tackle e.g. intermodality can be used to deepen the analysis of how individual and social food choices interact with changes in food industry behaviour, and how users and providers are likely to respond to cybersecurity information transparency.

2 This is particularly important because the time and effort needed to change policy is generally much greater and the visibility of the benefits within the ‘home’ organisations is reduced in inter-organisational settings.
At a more granular level the Act or Withdraw stage can also involve recommendations that the EC intervene, change or withdraw current policy, embrace self-regulation or pursue other courses of action. Section 6 of the report also contains a series of more specific recommendations directly developed from the Deep Dives that can provide policymakers with a more concrete set of action lines.

In summary, OptICTs has determined that Internet-awareness in policymaking is a pervasive challenge that has the potential to profoundly alter the intervention process in every domain. OptICTs provides policymakers with the means to identify the problems arising from this challenge, understand their root causes and begin to mitigate them through a flexible collection of tools and approaches. Our study has not provided a roadmap for Internet-ready policy but we hope it has given policymakers a guide to the path.
# Table of Contents

Preface .......................................................................................................................................... iii  
Abstract ......................................................................................................................................... v  
Table of Contents ........................................................................................................................ vii  
Figures .......................................................................................................................................... ix  
Tables ........................................................................................................................................... xi  
Executive Summary - Optimising the role of ICT in EU policy delivery (OptICTs) .................. xiii  
Acknowledgements .................................................................................................................. xviii  

1. **Context, putting the IC into policy** ........................................................................ 19  
   1.1. Introduction .....................................................................................................................19  
   1.2. From ‘Better’ to ‘Smart’ to ‘Fit’ Regulation ....................................................................20  
   1.3. Context for the current study: an example of past optimisation through the EcoSearch initiative ........................................................................................................ 24  

2. **Deep Dives** ................................................................................................................. 31  
   2.1. Introduction .....................................................................................................................31  
   2.2. Rationale ..................................................................................................................31  
   2.3. Methodology ...........................................................................................................34  

3. **Deep Dive 1 (Food labelling)** ............................................................................... 37  
   3.1. Introduction ....................................................................................................................37  
   3.2. Context: Evolving Global Governance ..................................................................38  
   3.3. Statement of the Issues .......................................................................................... 44  
   3.4. Food Chain Relationships ...................................................................................... 44  
   3.5. Sustainable Food and Internet Ready Policy processes ............................................ 53  
   3.6. Potential Top Level Policy Decision Model ........................................................... 59  
   3.7. Deep Dive Conclusions ................................................................................................... 59  

4. **Deep Dive 2 (Transport)** .................................................................................. 61  
   4.1. Overview .................................................................................................................. 61  
   4.2. Context ....................................................................................................................... 62  
   4.3. Statement of the issues ............................................................................................ 67  
   4.4. Drivers and constraints ............................................................................................ 71
4.5. Baseline – Institutional Context of Transport Policy Processes ......................... 81
4.6. Nature of the challenge .......................................................................................... 82
4.7. Deep Dive Conclusions .......................................................................................... 85

5. Deep Dive 3 (Cybersecurity) .................................................................................. 89
   5.1. Overview ........................................................................................................ 89
   5.2. Context ............................................................................................................ 90
   5.3. Statement of the Issues: Evolving Cybersecurity Governance ...................... 92
   5.4. Drivers and constraints: Internet Readiness .................................................. 100
   5.5. Deep Dive Conclusions .................................................................................. 101

6. Bringing Together the Tool Box: Prepositioning Commission Policy Processes for Internet Readiness ................................................................. 105
   6.1. Introduction ..................................................................................................... 105
   6.2. Pre Policy Positioning of the Toolkit .............................................................. 107
   6.3. Toolkit Components ...................................................................................... 109
   6.4. Toolkit Methodology ..................................................................................... 110
   6.5. Toolkit Processes ........................................................................................... 114

7. Conclusions and desiderata .................................................................................. 121
   7.1. Lessons emerging from the Deep Dives ......................................................... 121

References ........................................................................................................ 129
Figures

Figure 3-1: Global food chain legislation chain ................................................................. 38
Figure 3-2: Food chain actor process and data relationships ........................................... 45
Figure 3-3: Food chain data flow steps .............................................................................. 45
Figure 3-4: Structure of the food value chain in the EU (EU-27, 2008) ............................ 46
Figure 3-5: Food issue by type .......................................................................................... 49
Figure 3-6: Food issue by location .................................................................................... 50
Figure 3-7: Cost per genome 2001 - 2013 .......................................................................... 51
Figure 3-8: DNA megabase 2001 - 2013 .......................................................................... 51
Figure 3-9: Health map of reported food issues................................................................. 52
Figure 3-10: Regulatory support for EcoSearch-type process ......................................... 55
Figure 3-11: Toolkit fit and (Regulation Statement) support for EcoSearch-type process... 56
Figure 3-12: Food chain information flows and uses ........................................................... 57
Figure 4-1: Data flows among ICT elements ..................................................................... 68
Figure 4-2: Policy stakeholders ......................................................................................... 77
Figure 4-3: Policy-relevant transport player relationships ................................................. 77
Figure 5-1: The cybersecurity institutional landscapes ...................................................... 93
Figure 6-1: Issue lifecycles and policy Internet readiness .................................................. 114
Figure 6-2: Issue lifecycle stages and involvement curve .................................................. 116
Figure 6-3: Potential issue metrics and KPIs .................................................................... 117
Figure 6-4: Key issue identification sources and methodologies ....................................... 118
Tables

Table 2-1: Mapping the levels of the Deep Dives............................................................... 34
Table 3-1: Economic significance of the food sector ......................................................... 46
Table 3-2: Impact of horse meat scandal on businesses ..................................................... 47
Table 3-3: Size and income of EU farm holdings ............................................................... 47
Table 4-1: Low-end smart transport revenue forecasts...................................................... 66
Table 4-2: Potential ICT-intensive applications relevant to issues .................................... 69
Table 5-1: Main actors in Internet standards setting and Internet security....................... 92
Table 6-1: Toolkit techniques ........................................................................................... 109
Table 6-2: Tools and methodology ................................................................................... 110
Table 6-4: Key issue sources, drivers and roles ................................................................. 119
Acknowledgements

The study itself drew heavily on contributions from a range of individuals across a number of Directorates-General. In addition to CONNECT, these include: ENER, MOVE, SANCO, SECGEN, HOME and RTD. We also benefited from the generous contributions of staff at the ITRE and IMCO Committees of the European Parliament.
1. Context, putting the IC into policy

1.1. Introduction

As EU competencies expand and the complexity of the issues to which they have to respond grows the need for better management processes at the EU level increases commensurably. This is not limited to the EU institutions: as the world becomes flatter and interdependencies become more visible and less predictable, effective policymaking has become a key objective of most public administrations, including those of the Member States. Engagement with a wide range of stakeholders has become crucial in order to: identify and anticipate policy problems; formulate suitable objectives; devise policy options and assess their likely impacts; ensure effective implementation, compliance and coordination; and measure, understand and respond to planned and unplanned outcomes.

The governance of complex and interwoven policy issues has not been facilitated by legacy separations between organisations and policies that focus on specific aspects; this has encouraged administrative ‘silos’ (relatively insular units) to develop and entrench themselves in policy processes. Such separated organisations tend not to coordinate, adapt to changing circumstances, anticipate emerging challenges or facilitate effective cooperation. This has not gone unnoticed; referred to by some theorists as ‘Whole of Government’/‘Governance without government’ studies, an emerging set of discussions around the concept of governance has taken traditional methods of policy analysis to task (Drucker 1995; Dubnick 2005; Behn 1998; Bourgon 2007; Peters and Pierre 1998).

The potential for such fragmentation is particularly strong in the face of so-called ‘wicked problems’ - problems that are difficult or impossible to solve as a result of a variety of reasons e.g.: incomplete or contradictory knowledge; the number of people and opinions involved; large economic burdens; and interconnectedness with other problems.

---

3 Better regulation has a range of meanings, depending on institutional context and stakeholder perspective. Formally, it may be linked to the Better Regulation principles: proportionality; accountability; consistency; transparency; and targeting. These principles can be translated beyond the purely government context (e.g. design and assessment of self- and co-regulatory arrangements (Cave et. al. 2010)) or operationalised (e.g. S.M.A.R.T. objectives, flexibility, (cost-) effectiveness, and equity/fairness). From the perspective of the regulated, better regulations involve reduced compliance or competitive burdens, shortened time to market, and responsiveness or neutrality with regard to business and technological dynamics.

4 Originally defined in Rittel and Webber (1973).
1.2. From ‘Better’ to ‘Smart’ to ‘Fit’ Regulation

In the face of a succession of challenges and transformation, policymaking at the European level has evolved in a variety of ways, many of which sought to make policy processes more joined-up, adaptive, participatory, efficient, effective and anticipatory.

For one thing, the stated priorities have changed. As the global policy landscape has evolved a succession of position papers and initiatives have emphasised (at different times): the competitiveness of Europe; its internal, societal and economic integration; the need to support and exploit Europe’s innovative potential; the potential for collective activity to promote employment and growth; the need to streamline, simplify and reduce the burdens (in time and cost) of government *per se* and (latterly) the imperatives of recovery from the economic crisis; addressing grand challenges (e.g. the environment or the ageing population); and balancing the benefits of economic recovery (regionally and intergenerationally).

As regards the scope and methods of policy, the discussion has embraced new and deeper understandings of policy processes, a wide range of new instruments and working methods. The European discussion has now focused on the role of the Commission in enabling the full benefits of the Digital Single Market (DSM) to be realised. Despite the hyperbole of such language, it contains a clear challenge to the European institutions: to create a more dynamic and responsive regulatory environment.

Starting with the baseline of the Internal Market, discussions were launched in the late 1990s concerning the so-called ‘New Approach,’ which focused on the implementation of Directive 98/34/EC (and the revision for Information Society Services, Directive 98/48/EC). This legislative framework set out to enhance EU technical standardisation by trying to ensure transparency in adoption, amendment and (policy) acceptance. The New Approach introduced a mechanism for streamlining processes to assure the quality of certain products throughout the EU — notably, it required standards bodies to exchange appropriate information. Within the European Commission, this approach was codified in a DG Enterprise White Paper explaining the implications for EU governance.

As a result, various ICT-based tools were developed to ensure smooth, effective, efficient and proportional information sharing among national administrations, such as CIRCA, an intranet for use by civil servants for sharing information related to EU policy discussions.

Around the turn of the century, the Commission launched several processes to reinforce Single Market harmonisation including the ‘Interactive Policy Making’ initiative. This was part of a wave of institutional innovations (also including databases and online tools for participation, CONECCS and Your Voice in Europe) intended to use the Internet to

---

5 These developments cover a vast scope — for a discussion of one narrow aspect (self- and co-regulation in Impact Assessment, see Cave et. al. (2010).

6 See in particular: European Commission (2011a)


strengthen stakeholder involvement in the policymaking process and which culminated in the Commission’s Guidelines for Consultation (European Commission 2002).\(^9\)

The above discussion illustrates the European Commission’s rich history of developing ICT tools for stakeholder engagement and processes to develop harmonisation and information sharing within European policymaking processes, particularly between Community and national administrations. Moreover, these developments started an overarching trend toward harmonisation and standardisation that is now further enabled and facilitated by appropriately used technologies in policy and business.\(^{10}\)

To address the current crisis and engage the best contributions of existing and new stakeholders, EU legislative processes need more effective and efficient strategies for identifying, measuring and achieving public policy objectives. In order to fit with new governance requirements (e.g. REFIT), EU legislation must demonstrate clear added value, deliver full benefits at minimum cost, respect the principles of subsidiarity and proportionality and be open and responsive to changing information flow and stakeholder developments. Only in this way can legislative and associated non-legislative actions provide a simple, clear, stable and predictable governance framework for administrations, trading partners, businesses, workers and citizens.

REFIT (discussed in the following section) follows and builds upon the successful Action Programme for Reducing Administrative Burdens that exceeded its 25% burden reduction target.\(^{11}\) This has improved the partnership between the European Commission, Parliament and Council in simplifying and codifying legislation. It encourages use of the ‘Think Small First’ principle, as evidenced by the inclusion of an increasing range of light-touch and collaborative regulatory instruments (from enhanced consultations and impact assessment to specific implementation monitoring) in adapting EU regulation to the needs of microenterprises.\(^{12}\)

Pilot policy evaluations (‘fitness checks’), initiated in 2010,\(^{13}\) identify excessive administrative burdens, overlaps, gaps, inconsistencies and/or obsolete measures, and help to assess the cumulative impact of legislation. Their findings will serve as a basis for rethinking the future of the regulatory framework.


\(^{10}\) More specifically, the imperative has three aspects: i) the increasing importance of data, computation and communications (including big data, clouds and IoT) in the policy world, the global business environment and civil society – understanding the problems means understanding these trends; ii) the modernisation of working methods and organisational networks around the collective use of ICT-enabled tools – to engage effectively with these players means speaking their language and using their technologies, services and applications; and iii) the prior investment and experience associated with tools in business and societal use – and with the process changes associated with the adoption of these tools – makes their use by government cheaper, more effective more transparent and engaging and more adaptable than it would otherwise be.

\(^{11}\) European Commission (2010a).


\(^{13}\) European Commission (undated b). Between 2010 and 2012, pilot exercises were held in four policy areas; environment, transport, employment and social policy and industrial policy.
These efforts to improve governance are closely linked to ICTs; because the entire EU socio-economic and political system is spanned and underpinned by ICT tools and applications. ICTs are critical to the daily lives of citizens and business operations and to the analysis, formulation, implementation and monitoring of legislative and non-legislative instruments.

The enhanced connection between ICTs and policy for which this document argues thus reflects the increasing importance of ICTs in relation to policy issues, the availability of new forms of information and analytic and communication tools for identifying problems and devising, implementing and monitoring solutions and the increasingly-virtualised way in which key stakeholders (in and out of government) conduct their affairs and interact with each other. The resulting ‘Internet-ready’ policy actions should therefore be: more effective; more efficient; more appropriate; lighter-touch; self-monitoring and self-improving; adaptive; participatory; and future-scoped. This last term is particularly important – it means that the policies themselves, and the processes by which they are formed and implemented, anticipate both emerging changes and those likely to result from policy implementation. Where –as is inevitable – challenges arise from the complexity and unpredictability of the policy landscape, the policy processes should be able to detect and analyse changes and mobilise the partnerships necessary to address them.

1.2.1. REFIT

The Regulatory Fitness and Performance Programme (REFIT) constitutes a programme to review all EU legislation to identify and address burdens, inconsistencies, gaps or ineffective measures. REFIT reviews have identified a range of measures aligned with the objectives of this project (and the Deep Dives presented in below). These measures (taken from the REFIT documentation) include the following.

The use of Smart Regulation tools - impact assessment, stakeholder consultation and evaluation – each of which has been or can be made ‘Internet ready’ in specific ways.

Regulatory simplification and reduction of compliance burdens (esp. for SMEs), frequently involve enhanced and consolidated reporting of relevant information and access to information (e.g. the YourEurope portal to inform SMEs and citizens about Single Market rights and opportunities). This is facilitated by suitable data sharing and curation platforms and possibly by automated ‘scraping’ of data from publicly available sources (to permit regulators to collect up-to-date data when needed rather than requesting specific submissions).

Enhancing the rigour of regulatory assessments and evaluations is facilitated, especially for Smart Regulation and other light-touch or shared-responsibility measures, by ICT-based collection, analysis and modelling of a wide range of relevant information. These automated and ICT-enhanced measures can build engagement and quality by providing and efficacious platform for monitoring and action.

The interim assessment of REFIT also identifies a range of initiatives in each of the DGs. A sample aligned to the Deep Dives in this document is provided here.
It has been noted that the rapid pace of change in the ICT arena forces frequent and wide-ranging reviews, and that these could be more pro-active and open. Specific examples (described in their own terms) include the following.

Going Local – “DG CONNECT’s visit programme to Member States and neighbouring countries to discuss progress on key DAE issues, identify future challenges, and generate commitments amongst key national stakeholders”\textsuperscript{14}.

Futurium – “an online platform launched by DG CONNECT to facilitate a broad reflection on future European policies”\textsuperscript{15}.

Digital Agenda Assembly (DAA) – “an annual event for assessing progress and identifying challenges for the Digital Agenda for Europe”\textsuperscript{16}.

Collective Awareness Platforms for Sustainability and Social Innovation (CAPS) – “ICT systems leveraging the emerging "network effect" by combining open online social media, distributed knowledge creation and data from real environments ("Internet of Things") in order to create awareness of problems and possible solutions requesting collective efforts, enabling new forms of social innovation”\textsuperscript{17}.

Other elements of a more general nature include Open Data (mentioned in the Web Accessibility Directive\textsuperscript{18}); cloud computing; reuse of Public Sector Information, use of demand-side instruments (procurement).

Food labelling (see Chapter 3) - DG SANCO – activities in respect of Food Safety and e.g.

The Food Information for Consumers (FIC) Regulation\textsuperscript{19} - requirements for labelling and for on-line provision of label information.

Studies of the behavioural underpinnings of ‘impact of food information on consumer’s decision-making’\textsuperscript{20}, (it is unclear how directly this addresses the specificities of the Internet).

Application FIC Regulation rules (e.g. “additional forms of expression and presentation”).

\begin{footnotesize}
\begin{enumerate}
\item[20] i.e. whether and how consumers absorb label information that appears on the label and whether the presentation could be more effective.
\end{enumerate}
\end{footnotesize}
Intelligent Transport (see Chapter 4) - DG MOVE:

The Intelligent Transport System (ITS) Directive\(^{21}\).

Sustainable transport policies (including integrated traffic management).

Cost reduction, speed, reliability and safety objectives.

Cybersecurity (see Chapter 5) - various DGs

DG CONNECT:

The Network and Information Security Directive\(^{22}\) – including Computer Emergency Response Team (CERT) notification of incidents.

Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) for easier access and more secure cross-border online services\(^{23}\).

The E-Privacy Directive\(^{24}\) and the proposed General Data Protection Regulation\(^{25}\).

DG HOME: especially with regard to EuroDAC\(^{26}\) but also ENISA\(^{27}\) and related agencies.

The list could be extended – the main point is that the framework and approach outlined here, while intended to build specifically on the underexploited potential of ICTs in policy making, is entirely consistent in concept and substance with the REFIT initiative.

1.3. Context for the current study: an example of past optimisation through the EcoSearch initiative

In mid-2010, the preparation of the Consumer 2020 report for DG INFSO identified a number of areas where ICTs facilitated rapid information collection, analysis and exchange and associated management innovations. The area with the highest unrealised potential impact was the provision of online information on energy consuming appliances. This was named EcoSearch. We describe it at some length because the present report represents an attempt to t

1.3.1. The EcoSearch Premise

EcoSearch was based on a simple premise. Online consumers were increasingly disadvantaged by the dearth of timely, useful and comprehensible information on the energy usage and other characteristics of appliances. Legislation stipulating the off-line labelling of  

\(^{21}\) European Parliament and Council (2010).
\(^{23}\) European Commission (2013c).
\(^{24}\) European Commission (2002).
\(^{25}\) European Commission (2012)
\(^{26}\) European Dactylography, the EU asylum fingerprint database.
\(^{27}\) European Network and Information Security Agency, see Section 5.3.3.
energy using products had not been transposed by business or enforced by the EU or Member States for the online retail environment. Due to the double-digit growth in online shopping, this was seen as a threat to the sustainability of the environmental gains made by physical labelling in the previous decade and as a missed opportunity in exploiting the enhanced capacity of on-line information sources and search functionality to inform consumer choice. Addressing this issue was therefore chosen as the focus of the EcoSearch initiative.

The ‘deliverables’ of the process evolved through the interaction. The issue was framed by two existing Directives; the EcoDesign Directive that established minimum standards for a range of products and the (recrafted) Energy Labelling Directive that established a framework for the issuance of product-specific Delegated Acts that identified the form and contents of labels and the responsibilities of suppliers, dealers and Member States. The Energy Labelling Directive required the specified information to be available on-line but did not go into detail as to what that meant in practical terms; the Delegated Acts (some of which antedated the recrafted Directive) took a range of partial approaches. There was thus considerable discussion as to whether the intention was – or should be – to change the conditions of the existing Directive, reword the Delegated Acts, create a new ‘horizontal’ Delegated Act (or product-specific Delegated Acts) or feed into the revision of the ‘master’ Directive.

Of course, the intended outcomes of these deliverables also evolved. They ranged from the minimal objective of ensuring that the same information was available on-line as off-line, in a form that offered equivalent contents, comparability, recognisability and understandability (thus in effect seeking to sustain the gains associated with the original Directive) to a maximal objective of harnessing the power of on-line information and the efforts of third parties (including search engine authors and providers of comparison services and platforms) to produce even more effective communication, more powerful feedback from consumer behaviour to product design and marketing and greater consistency between environmental preferences as expressed in equipment purchase decisions and product use patterns.

As a result of the interactions indicated below, these changes did not go in lock-step; it was eventually recognised that ambitious outcomes could be attained via relatively light-touch means, and that the ‘deliverables’ (meaning the product-specific, Internet-ready Delegated Acts that were eventually produced) could contribute to subsequent policy actions and to the accumulation of a better shared evidence base and suite of impact assessment and analysis tools. This was implemented by the joint activity of multiple DGs and by the integration of expert analysis and policy development with other functions (e.g., Impact assessment, consultation and legal drafting).

The essence of the broader context can be briefly summarised.

There were two existing Directives which originated with and were managed by DG ENER. They were periodically adjusted via product-specific Delegated Acts – in particular, the Energy Labelling Directive was recrafted in a way that mentioned the Internet. However, while the recrafted Energy Labelling Directive mandated online provision of specific information, it lacked necessary details about how this should be done and how the requirement could be monitored and enforced.
The initial idea to tackle this situation was jointly conceived and shared between DG ENER and DG INFSO/CONNECT. The initiative was further developed using prior work from both DGs; the technical preparatory studies commissioned by DG ENER and the network built up around this work; and prior studies and associated networks commissioned by DG INFSO to shed light on the importance of (especially electronic) information in governance, market and civil society processes.

The substantive process elements of issue analysis and development and agreement of policy options (as described below) paralleled and fed into the usual formal Impact Assessment and drafting processes.

As the initiative progressed, a broader range of individuals and functions within the participating DGs and other EC entities were involved at different points in the process. This widening participation and consultations with Member State and industry representatives exposed many ‘tacit agendas’ and issue linkages. These created some difficulties, but also exposed some subtle implications of the initiative. In addition, the dynamics of regulatory reform (especially the pending revision of the Energy Labelling Directive) also played a role. It reduced the urgency of addressing some contested aspects, allowing participants to concentrate on finding areas of agreement and ‘quick wins.’ In addition, it provided an attractive future opportunity; some of the disagreements over current options stemmed from the lack of direct and comprehensive evidence; monitoring of the instruments produced by EcoSearch will provide much of this information, which can then feed into the pending revision of the Energy Labelling Directive, allowing more fundamental reform based on a more mature and shared understanding. Working through these issues in a spirit of cooperation and collaboration led, in the end to a stronger set of legal measures and to a better understanding of inter-DG policy making.

1.3.2. The EcoSearch Process

The EcoSearch Initiative underwent many process changes during the period 2010 – 2013. These changes mainly related to the stakeholder and competency requirements - the intention was to simplify the deliverables of the initiative (the legislative instrument, supporting analysis and requirements on suppliers, dealers and Member States) in order to reduce business overhead, achieve technology neutrality, future-scope the deliverables and ensure a consumer friendly outcome. This evolution in turn led to a constantly changing set of stakeholders who engaged with the work of a core team of experts and EU Commission managers.

The process started by defining the end goals. These fell into four broad categories: legislative; business; consumer; and technology.

The next stage was discussion and documentation of the key assumptions underlying the participants’ understanding of the issue, the barriers to appreciating and exploiting the role of ICTs and the possibilities for resolving the difficulty. For completeness, and to ensure that relevant insights from other contexts could be translated, these were grouped into the following (overlapping) clusters.

- Legislative
- Business
- Consumer
- Technology
- Behavioural
- Positive Potential Impact
- Potential Negative Impact  •  Cost/Benefit  •  Stakeholder participation
- Competency requirements  •  Hard legislation  •  Potential groups  Pro EcoSearch
- Candidate Approached  •  Soft Legislation  •  Potential groups  Anti EcoSearch
- Business voluntary  •  Capability led

A core team of experts met regularly to provide a sounding board and input to the evolving process. It comprised:

<table>
<thead>
<tr>
<th>EU staff:</th>
<th>Commission</th>
<th>legal</th>
<th>procedural</th>
<th>management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ecommerce experts:</td>
<td>Researchers</td>
<td>online traders</td>
<td>National associations</td>
<td></td>
</tr>
<tr>
<td>Specific experts:</td>
<td>Search engine</td>
<td>Logistics</td>
<td>Technology</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Web design</td>
<td>Data Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A stakeholder and competency map was started and kept during the initiative process. This helped manage the inclusion and phase out of experts and expertise as the process proceeded. These stakeholders provided the majority of the labour and time to the initiative process.

1.3.3. Initial Approach

In the early stages of the initiative, the use of search engines and their information management capabilities were considered to be the ideal candidate for the realisation of EcoSearch. After a major search engine supplier withdrew from the Initiative a competitor put considerable effort into defining and creating a working example of a search engine “EcoSearch” deliverable. It became evident very quickly (within 2 – 3 months) that this approach was impractical in terms of participation and the difficulty of implementation.

As regards participants, some search engine businesses wanted to own the deliverable; in consequence, they refused to engage in cooperative efforts on a single delivery and failed to deliver/maintain their commitments.

At the implementation level additional problems arose from:
- The complexity of data management in the search domain;
- The sourcing and methods of search information acquisition;
- Legal issues on the reuse, retention, basing and use of data;
- Business and ecommerce issue with “external “ deliverables;
- Lack of flexibility for change management processes; and
- Different approaches to display and data presentation.
This, after detailed discussion, caused the search engine approach to be dropped. An analysis of the problems yielded a far simpler, more business friendly and less complicated approach that sought to reuse existing processes, procedures and responsibilities carried out for compliance with physical labelling rules.

1.3.4. The Revised Approach

The revised approach was based on a single key insight from the analysis of the search engine experiment; compliance with physical labelling requirements was already highly computerised and a simple parallel digital information flow could provide all necessary data and information to ecommerce sellers. One additional resource was needed; detailed definition of the business rules related to the use of these data and their graphic representation to consumers.

The design work and construction of a prototype were carried out in a single afternoon. This provided a number of core elements to progress the initiative:

- A map of the information flows and content availability;
- A set of consistent graphics (size, shape, colour, orientation);
- Clear business rules for usage, placement and display;
- A clear set of use cases (must use, need not use);
- A definitive set of rules related to non-compliance (no display, no sale); and
- Concrete roles and responsibilities.

The importance of this prototype cannot be overestimated. It provided a single, live, usable web based example of what the consumer would encounter after transposition of physical labelling data to the online environment. This facilitated and accelerated the discussions and agreements from core stakeholder groups such as: manufacturers; eCommerce retailers; technology groups; online capability designers; and EU and Member State government officials.

EcoSearch progressed in a non-confrontational manner through the legislative process due to its clarity of purpose, inclusiveness of process and high, fast to market, low cost positive impact.

1.3.5. Lessons Learnt

Important lessons have been learnt that can easily be reused in future initiatives:

- High impact initiatives need not be expensive;
- A visible and involved senior EU champion is critical;
- Cooperation across DG boundaries is absolutely essential and easy to achieve;
- Internal lower-level EU resistance is greater than business resistance;
- EU staff education and skill improvement and creation of mutual understanding are major overheads;
- The most obvious (direct, ambitious) approach may not be optimal;
- Stakeholder mapping and management are very useful for problem diagnosis and creating solutions;
• Clear and open processes create mutual confidence in the aims and outcomes of the initiative;
• Issue ownership, discretion to participate and efficacious voice (the ability to make a difference) for external stakeholders facilitate effective partnerships;
• Repurposing of existing processes reduces resistance and may even generate enthusiasm; and
• A working prototype facilitates and accelerates the entire process.

1.3.6. Results

The EcoSearch prototype was incorporated, unchanged, into the final deliverable of the project after extensive stakeholder consultation, which included business, consumer, Member State, Commission and EU Parliament groups and responsible parties.

The legislative instruments resulting from the EcoSearch project were published in the Official Journal on (05/03/2014) - 44 months after it was first proposed (May 23 2010).

The EcoSearch approach has been referenced by stakeholders in other Internet labelling and information provision initiatives as an example of methodological best practice.

1.3.7. Generalising From EcoSearch

The EcoSearch initiative represented a ‘Deep Dive’ – the simultaneous development of a deeper understanding of a policy area where ICT formed a crucial – but under-exploited – part of both a problem and a solution; a framework for identifying and prioritising similar issues and a method for working across institutional boundaries on cross-cutting problems. The next Chapter elaborates a more general framework for formulating and conducting similar Deep Dives to apply and extend the lessons.
2. Deep Dives

2.1. Introduction

To raise the Internet-readiness of policy across the broad range of Commission concerns it is necessary to build knowledge, methods and networks incrementally. This means using the urgency and discretion to act provided by evolving challenges (targets of opportunity). To create sustainable and effective change in the way policy is made it is therefore necessary to think of each challenge as an opportunity to improve policy and policy-making. Each such initiative contributes to a portfolio. This starts with the low-hanging fruit (problems whose urgency and Internet-relevance are obvious to all) but must eventually evolve to deal with more subtle issues, develop methods capable of broader application and anticipate new issues arising from the wider world or as by-products of today’s ‘solutions.’ Therefore this Chapter sets the stage for the three Deep Dives to come by providing a general framework for the selection, prioritisation and structuring of Deep Dive areas.

2.2. Rationale

2.2.1. Criteria

The development of a case-based approach to improving policy-making via explicit and collaborative exploration of the ‘ICT-specificities’ of ostensibly non-ICT policy areas should seed the evolution of a more mature integration of ICTs with policy processes. This integration will yield sustainable and cumulative development of Internet-ready policies, improved procedures, an expanding and useful body of experience and a proactive network of practice across the DGS. To initiate this process, the issues selected for proof of concept had to combine ‘face validity’ with the potential for gains that could justify tackling harder problems in a collaborative way. The relevant characteristics were derived from suggestions by workshop participants and key informants interviewed for the project. The original, longer and more detailed list (see p. xiv of the Executive Summary) was condensed to five characteristics:\n
1. A high potential for the contribution of ICT to resolution of policy problem

Whether or not ICTs create, exacerbate or complicate a policy problem, they may be substantively useful in developing, implementing and monitoring common, consistent and coherent solutions. The problem must have an important European dimension and related to one of the key (potential) activity areas of DG CONNECT.

\footnote{These are closely aligned with the definition in the original study objectives.}
2. A high contribution of ICT to the policy problem

Policy issues that are not shaped by ICTs are rare, but attention should be limited to issues where the role of ICT makes sense in the institutional context of DG CONNECT – for instance, policy issues concerning (sharing of) data and standardisation.

3. Short and long term gains

As pilots, these cases will need to demonstrate the utility of the exercise, in order to facilitate adoption by (or interaction with) other Commission services.

4. Ease of collecting concrete and robust measurements

Given the nature of this pilot study, there is a need to ensure that data concerning the cases will be easily available.

5. Comparability, reusability and transferability

As a series of pilot cases, the capacity to provide durable and useful lessons and to adapt developed solutions to other policy instances is useful for this study. Hence, the cases selected must allow participants and researchers to transfer lessons learned to other situations. The transferability of solutions to other domains will facilitate the production of a toolkit and strategy for future use.

2.2.2. Relevance of the Criteria

The issue of Internet readiness is directly relevant to the forthcoming Work Programme of the European Commission. A cursory reading of the current Work Programme reveals that the vast majority of areas either have or will have an Internet/technology requirement in the coming years. The three examples below illustrate the obvious or potential use of the Internet or technology in one or more aspects of its operation. Major consideration was given to efficiency, transparency and fraud.

Item 2: Review of regime for agriculture in the outermost regions (POSEI):
Among the issues raised are whether the Common Agricultural Policy should include technology/Internet considerations in relation to monitoring and providing traceability of crops, pesticides and live stock.

Item 4: Framework for safe and secure unconventional hydrocarbon extraction: What impact will consumer accessible air and water sampling technologies have?

Item 6: State aid modernisation: Is there a need for a central register of state aid at a business levels to reduce fraud, identify true levels of state aid, assist in TTIP negotiations and monitoring and help ensure eligibility criteria are respected for grants and vouchers?

Any review of work packages under this programme will therefore need to look beyond the conventional attitudes and existing mechanisms to identify areas in which a potential need for Internet technology can address existing shortfalls, increase efficiency or avoid future issues.

2.2.3. Deep Dive Levels

As mentioned in Section 2.1, the Deep Dives operate in distinct ways depending on the urgency of the issue, the obviousness or common understanding of the ICT connection and the extent to which the ICT aspect contributes to the origin of the issue, inhibits or facilitates ‘conventional’ policy intervention or challenges fundamental policy assumptions. To capture this richness, we have identified three distinct ‘levels’ of areas for Internet readiness activity. The selected Deep Dives span these to some extent.

**Level 1: Solving problems** – Level 1 Deep Dives concentrate on solving immediate problems caused by uncontrolled, misunderstood or emergent ICTs and/or addressed by clever use of ICTs (e.g. labelling, infrastructures and legal basis for citizen monitoring). This is the starting domain of the Food Deep Dive. Because this is also the most detailed Deep Dive and because the specifics of this level are most strongly influenced by particular problems, we defer discussion to Chapter 3.

**Level 2: Understanding issues** A Level 2 Deep Dive concentrates on using ICTs to collect, share, model and explore information-spaces (including data mashing and big data and small data analytics) in order to understand behaviours and how those understandings affect outcomes. Level 1 instances – e.g. ITS, automatic calling of emergency services, self-organising traffic lights – of transport policy start from transport modelling and the parallel assessments of time use, emissions, safety and so on. These tend to be separated and based on isolated data sources. The reason is that they are used for Level 1 purposes; solving existing problems, in the ways that make sense to those who currently ‘own’ the problems or the ‘direct’ tools used to fix them. By taking a more capability-orientated (the data and sharing/modelling/exploration tools represent a capability rather than a functionality in Sen’s definition) we can figure out why the problems are there and produce general-purpose, reusable ICT tools – the more the tools are used (in different contexts) the better they become and the better they are understood. This also means collecting and wiring in data and analytic capabilities for which we (or the entity collecting the data) have no (current) use. There is a danger of ‘fishing’ and of ‘creep’ – this leads us to the next level.

**Level 3: Rethinking Case for Action** a Level 3 Deep Dive entails reconsideration of whether “we” need to act – either now or at all. It is a collaborative endeavour from the outset, building on collective reimagining. For instance, in some cases stakeholder, institutional or expertise-based culture splits lead to policy incoherence or inconsistency. In such cases, rather than rushing to intervene it may be best to wait, combining light-touch intervention with an active ‘watching brief.’ Because progress in such areas may entail substantial transfers or abdication of power and responsibility, it is useful to create a ‘serious sandbox.’ This is a shared domain for exploring new possibilities in which mistakes matter, but do not create permanent damage. Playing together in the sandbox lets participants observe and understand the issues in common or in connectedly ambiguous ways. Based on this shared experience, the parties can think seriously and collectively about whether they need to solve the problems at all. This builds on a collective reimagining of what the participants think the essence of problem is. This is the starting point of the cybersecurity Deep Dive. We (as stakeholders) have the technical tools; we have even got some understanding of how security and privacy are connected (at present), but we struggle to keep pace with citizens’, businesses’ and governments’ evolving understandings of these things and the actions they take in response. If we are able to step back and see these actions as the behaviour of a
system, rather than as the intentional behaviour of individuals, we can come to a deeper sense of where intervention, withdrawal or shared responsibility (new roles) are important.

### 2.2.4. Selection – Applying the Criteria

This section uses the framework/template to justify the three chosen areas. It is useful to map the ‘levels’ occupied by these Deep Dives. Table 2-1 shows the primary level for each (shaded cell) and the implications for other levels.

#### Table 2-1: Mapping the levels of the Deep Dives

<table>
<thead>
<tr>
<th></th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Food (DG CONNECT playing in other areas) – See Chapter 3</td>
<td>Detecting and controlling contamination, food origin, etc.(^{30})</td>
<td>Perceptions of food quality and safety, responses to information.</td>
<td>Food as engine of civilisation, rural areas as collective vs. private environment, food vs. other types of security.</td>
</tr>
<tr>
<td>Transport (DG CONNECT playing in other areas) – See Chapter 4</td>
<td>Congestion, emissions, safety problems</td>
<td>“Intelligent” mobility and urbanisation(^{31}), Intelligent design and intelligence in systems</td>
<td>Fast and slow networks and the right to move, public vs. private space</td>
</tr>
<tr>
<td>(Cyber)security (DG CONNECT opening to other areas) – See Chapter 5</td>
<td>NIS incidents, surveillance, Darknets (TOR)</td>
<td>Security and privacy, Role of 3rd parties</td>
<td>Splinternets, patchworks, global commons(^{32})</td>
</tr>
</tbody>
</table>

More details of these implications are provided in the indicated chapters.

### 2.3. Methodology

Each Deep Dive will have a roughly similar structure, varying by maturity and “level” (see Section 2.2.3); a canonical version is outlined here. However, note that Deep Dives at different levels will of necessity use different structures – the imposition of a generic template is itself a barrier to effective cooperation, as interviews have shown; practitioners from different organisations, especially experienced practitioners, will have their own well-developed framing and understanding of a given area. To provide a fruitful basis for collaboration, the application of the method and the resulting organisation of the Deep Dive analysis must be a joint product. This means that the structure should be flexible by mutual agreement. At the same time, the requirements of the broader policy process (e.g. the formulation of legislative proposals and the conduct of Impact Assessments) do impose a consistent framework on the outputs from the exercise – but the inputs, the activities and the outputs are not identical.

**Introduction/overview:** The introduction will sketch the issues, the level and the prime facie case for/against Internet readiness. Although the present Deep Dives are more exemplary in

\(^{30}\) Section 3.3

\(^{31}\) Section 4.3

\(^{32}\) Section 5.3
character, when developing them for ‘live use’ as a shared activity between different institutions and audiences, it may be useful to facilitate internal execution, fix ideas and facilitate communication by means of an ‘exemplar’ - a specific instance of something that is technically feasible right now but not done. This can be done as a set of parallel narratives for each Deep Dive: e.g. "a day in the life of"

- [for food labelling] Bob, the supermarket shopper; Farah the supermarket manager; Vanessa the farmer; Dawn the food safety regulator;
- [for transport] Elise, the commuter; Jim the tourist office employee; Sarah the city transport planner;
- [for cybersecurity] Janine, the organiser of a big event at Wembley Stadium; Samir the electrical supply manager; Jody the network operator.

The team conducting the Deep Dive can also (optionally) add a narrative description of annoying, burdensome or intrusive current activities that no longer need to be done.

At a finer level of detail, this section may map the candidate against the selection criteria, identifying: existing data, obvious benefit in terms of acknowledged issues and problems, obvious risks or costs and global ramifications (perhaps by highlighting the interactions and overlaps with other policy fields).

**Context:** Main initiatives and legal instruments especially in areas where ICTs are not fully recognised.

**Issue Statement:** A concise discussion of the nature of the underlying problem(s), data flows in the system (e.g. food distribution, transport, security) and a summary of the policy objectives and tools available.

**Drivers and Constraints:** legal, political and institutional restraints: reasons why progress has or has not been made. This should include maps of (policy or intervention) stakeholders and key information flows among them. It should take into account information gleaned from key informant interviews.

**Baseline:** Existing efforts to interact across units, directorates, DGs, EU institutions and agencies, Member States and – if relevant – global institutions and actors.

In developing the baseline, it is useful to:

- focus on human-level interactions (e.g. participatory leadership seminars);
- search for institutional interaction opportunities (e.g. interservice consultations);
- carefully consider the role that change can/should play to the overall function of the institutions as well as the specific policy area;
- take into account individual and institutional allegiances, attitudes and incentives; and
- place findings into the policy process (e.g. in developing existing policy: at what point attempts to collaborate were made; how and by whom cooperation was linked to formal processes; which of the existing possibilities was used and with what result).

---

33 Such narratives are often developed to illustrate policy scenarios for use with non-technical and lay stakeholders.

34 E.g. Green/white papers, Interservice Groups, legislative proposals, impact assessments
If the evidence permits, the baseline can provide an account of how the framing of the issue, the options proposed and the evidence regarding impacts evolved through the lifetime (to date). This account can be used to articulate the nature of the challenge in a substantive way.

**Nature of the challenge:** The analysis should stress that the challenge is not technological, but political and institutional.

**Conclusions:** The conclusions should indicate findings and next steps both for the specific issue area and for the approach as a whole.

Note that the Food Labelling Deep Dive, being closest to both the antecedent EcoSearch work and to an immediate problem/potential for action, is considerably more detailed than the Transport and Cybersecurity Deep Dives.
3. Deep Dive 1 (Food labelling)

3.1. Introduction

Ensuring adequate food security, supply, quality, safety and affordable pricing are critical to the social and political stability in any society.

The management of pathogens and contaminants in the food chain from field to fork is extremely complex especially when responsibilities for process and quality cross national boundaries and administrative responsibilities. Global, supra national and national legislation provides the framework within which global food chains operate.

The preventative and protective effectiveness of formal processes and informal (industry/enterprise standards) is only measurable in the failures that emerge in the form of foodborne infections and product contamination incidents. However estimates of reported incidents vs. actual consumer infections range from 10% to 25% depending on the source 35.

As each incident of foodborne illness in the UK was calculated 36 to cost €1,700 the total cost of allergies in the US calculated 37 at €34 billion a year illustrate that foodborne or caused illnesses have a significant ongoing economic impact.

Changes in technology, especially at the consumer level, provide potent new ways to identify, quantify, manage and prevent food related illness. However these emerging capabilities are also likely to provide far greater visibility on the presence of pathogens, contaminates, allergens and product contents that impact human health and wellbeing.

Planning and prepositioning future food and safety interventions to take account of the changing technologies for identification, data flows, visibility, roles and responsibilities will be the key to being able to manage the dynamics and stresses that these will place on the food chain stakeholders and administrators.

In view of the maturity of this Deep Dive and its close relationship to the antecedent EcoSearch initiative, it is more fully developed than the others, and contains an explicit identification of the legal basis for specific interventions (Section 3.5) and a concrete decision model (Section 3.6).

---

36 FSA (2013).
3.2. Context: Evolving Global Governance

Because the food chains servicing the EU are global the governance of these chains is a complex mix of global, EU and national rules, regulations, principles, norms, guidelines and exceptions. Three major regulatory players of note are examined below: GATT, The UN and the EU. Each plays a different role and has different net levels of “authority” in relation to the governance of the globalised food chain. They therefore frame the context within which Internet ready legislation must operate, and implicitly identify levels where progress could be made.

**Figure 3-1: Global food chain legislation chain**

### GATT/World Trade organisation

The General Agreement on Trades and Tariffs (GATT) has been negotiated since 1947. It recognises exceptions for actions required to protect health, under which parties to the agreement may adopt laws “necessary to protect human, animal or plant health” as long as...
they are “not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade”.38

During the Uruguay Round of negotiations (1986–1994) GATT was placed under the WTO (World Trade Organisation). One important outcome of this round of negotiations was the creation of the Sanitary and Phytosanitary (SPS) Agreement. This defined the difference between legitimate and protectionist use of safety and phytosanitary (relates to the health of plants, especially for the requirements of international trade) laws and to encourage their legitimate use39.

Under SPS, WTO members agree to accept the food safety rules of other nations as equivalent to their own if the exporting country can show that its rules provide the same level of protection as the importing country’s rules. As such, SPS helps nations and their suppliers who comply with GATT food safety rules to enter and participate in the globalised food chain.

### 3.2.2. United Nations

In 1963 the Codex Alimentarius Commission was established in 1963 by the United Nations’ Food and Agriculture Organisation (FAO) and World Health Organisation (WHO)40.

Members or associate members of the FAO or WTO (175 countries, representing 98 per cent of the world’s population) are Codex Alimentarius members. Membership in the Codex Alimentarius is open to nations that are members or associate members of the WHO and FAO. 72 other countries, International nongovernmental organisations, organisations and individuals may be observers in the Codex.

It provides a forum for international technical collaboration on the development of food safety and quality standards. It was created with two primary goals: protecting human health and promoting fair trade practices and it provides an international forum for discussing and agreeing model standards, principles and guidelines as input to national government policy processes.

Codex Alimentarius agreements are not binding on nations but rather form a baseline against which national laws can and are measured.

Much of the effort of the Codex Alimentarius focuses on producing model standards. These include commodity standards aimed at preventing consumer fraud, quantitative standards for food additives, and quantitative tolerances for contaminants such as pesticides and veterinary drugs. The commission has also developed a set of recommended practices

---

38 General Agreement on Trade and Tariffs (GATT 1947), art. XX
referred to as codes of practice or guidelines. These include guidelines for HACCP\textsuperscript{41} systems and an international food hygiene code\textsuperscript{42}.

To date, the Codex has adopted over 200 standards, 50 hygiene and technological codes, 60 guidelines, 1000 food additives and contaminants evaluations and 3200 maximum residue limits for pesticides and veterinary drugs.

3.2.3. The European Union

Up to the mid-1990s European food law could be characterised as focusing on reducing the barriers that prevent the emergence of an integrated internal food market. This focus changed radically to food safety with the emergence of BSE (bovine spongiform encephalopathy or ‘mad cow disease’) in the UK and the consequent public pressure for wholesale reform of European food safety law. In view of the critical role of information collection and dissemination and the extensive policy consequences of this crisis, we describe it in some detail.

The BSE Crisis

In November 1986 BSE was first officially reported in the UK\textsuperscript{43}. In 1988 cattle feedstuffs containing ruminant-derived protein (meat-bone meal, MBM) was identified as the cause. This feed stock led to an estimated 2 million infected bovines entering the human food chain in the UK leading 1884 human deaths (1990 – Dec 2013) (annual mortality 1.2%, median age at death 28) due to human disease variant Creutzfeldt-Jakob disease (vCJD) in the UK alone.

In 2000 the UK Phillips BSE Inquiry concluded that the BSE crisis was the result of:

- Intensive farming practices\textsuperscript{44};
- significant shortcomings in the way things were done;
- Poor response to evidence of an issue;
- Poor and late implemented actions;
- Inadequate enforcement of actions;
- The belief that BSE was not a real threat to human health;
- Lack of transparency; and
- Unjustified reassurance by governmental bodies in order to protect the agricultural industry\textsuperscript{45}.

\textsuperscript{41} HACCP is a management system in which food safety is addressed through the analysis and control of biological, chemical, and physical hazards from raw material production, procurement and handling, to manufacturing, distribution and consumption of the finished product


\textsuperscript{43} The first case was reported in 1985, by 1988 there were over 2000 cases; the epidemic peaked in 1993. The widespread and simultaneous appearance indicated a foodborne cause (need for surveillance).

\textsuperscript{44} This also highlights the policy spillovers between e.g. animal health and welfare, agricultural market policy and competition policy, which influence the pressure and scope for intensification.

\textsuperscript{45} UK Government (2000).
In 1989, the EU prohibited export of cattle born before 1988 from Britain and subsequently banned British export of offal from cattle older than six months on the basis of animal health concerns\textsuperscript{46}.

In July 1996, the EU Parliament formed a Committee of Enquiry into BSE/TSEs, \textit{(transmissible spongiform encephalopathies)}. This reported in early 1997, and found that the structure of EU food safety governance allowed domination of decisions by a single member state, politicisation of science, and lack of transparency. It concluded that these all contributed to the inability of the EU to respond quickly to this or any other food crisis. It also clearly illustrated the need for reform Europe’s food safety policy structure\textsuperscript{47}.

In 2000 the European level BSE crisis emerged when active surveillance proved that BSE was present in European bovine herds. This resulted in the rapid issue of the EU TSE Regulation of 2001\textsuperscript{48}.

This provided a comprehensive set of harmonised rules for the prevention, control and eradication of TSEs, \textit{(transmissible spongiform encephalopathies)} including an EU-wide total ban on the feeding of animal proteins to farmed animals.

The impact of this and other measures has been the virtual elimination of TSEs in the EU.

The response to the European BSE crisis was not confined to the EU. Recognising the possibility of BSE infected food stuff entering the globalising food chain, in 1996 the WTO made a number of recommendations to protect global human health\textsuperscript{49}.

- No tissue that is likely to contain the BSE agent, nor part or product of any animal which has shown signs of a TSE should enter the (human or animal) food chain. All countries should ban the use of ruminant tissues in ruminant feed;
- The pharmaceutical industry should avoid the use of bovine materials and materials from other animal species in which TSEs naturally occur. If their use is absolutely necessary, these materials should be obtained from countries which have a surveillance system for BSE in place and which reports zero cases of BSE;
- The \textit{Guidelines on tissue infectivity distribution in transmissible spongiform encephalopathies} in 2006 provide information and assist national regulatory authorities in conducting risk assessments of vCJD transmission; and
- In 2010, WHO updated the \textit{Tables on tissue infectivity distribution in transmissible spongiform encephalopathies}. The Tables reflect the current status of knowledge about infectivity in body tissues, secretions, and excretions of humans and animals, and thus provide information about potential transmission of vCJD through human blood and

\textsuperscript{46} These actions should be seen in their member State context: in addition to the 1988 UK ban on ruminant-derived protein feeds and slaughter policy, by 1989 brain and spinal cord (beef on the bone) was banned from human food chain in the UK, where the government also established a vCJD monitoring programme. In 1990, a number of nations – including France, Germany, Italy and Russia banned UK beef; most of these bans were dropped after the EU tightened its rules later that year.


\textsuperscript{49} This came 7 years after the UK ban – see WHO (1996).
Further EU food safety crises followed\(^{50}\). These clearly showed the need for better, faster communication about food crises among European national food authorities and consumers. Moreover, they demonstrate the advantages of EU leadership, as member State responses tend to be spread over time and reflect different national interests as well as common interests.

Recommendations for structural change led to the issuing of a Green Paper\(^{51}\) in 1997 and a White Paper\(^{52}\) on food safety in 2000. The expressed purpose of the EU was stated to “re-establish public confidence in its food supply.” The White Paper lays out the EU’s vision for reform of European food safety law and is a guide to subsequent legislative action.

The experience with BSE and subsequent animal feed crises changed the focus of food safety policy to assuring that every link in the food supply chain protects consumer health. Five central principles emerged:

1. Clearly defined food safety responsibilities for all actors in the food supply chain;
2. Traceability of food, feeds, and food ingredients to their sources;
3. Transparency and separation of scientific analysis from risk management to reduce the role of influence or corruption in food safety policy decisions;
4. Risk analysis as the framework for science-based policy; and
5. The precautionary principle to guide risk management.

The White Paper of 2000 scheduled 84 legislative and policy initiatives with clear goals to upgrade European food law to be more coherent and comprehensive whilst strengthening consistency and enforcement across Member States.

In January 2002 the European Parliament and Council adopted Regulation 178/2002\(^{53}\), the General Food Law (GFL) which was immediately binding on all EU Member States. The GFL placed greater emphasis on horizontal regulations, makes greater use of regulations that set objectives to be achieved rather than govern the means of achieving them. Between 2002 and 2007, regulations on GMOs, food hygiene, and food contact materials and rules for coordination of food safety law enforcement were issued. Work is on-going in further food safety areas such as updated food labelling, novel foods, pesticides, and food additives\(^{54}\).

The GFL led to the creation of European Food Safety Authority (EFSA) (Article 22 of the GFL). Two key EFSA roles of direct Deep Dive relevance are i) developing systems to monitor emerging risks and collect relevant data on the prevalence of foodborne hazards and ii) contributing to risk communication for consumers. The GFL also drove the creation of the Rapid Alert System (Regulation 178/2002). This is used to rapidly communicate food and

\(^{50}\) E.g. increased incidence of verotoxin-producing E. coli (VTEC) in meat and dairy products, continuing public concern about genetically modified food, and black markets for diethylstilbestrol (DES) as a feed additive and dioxin contamination of feed in Belgium in 2000.


\(^{52}\) European Commission (1999).


\(^{54}\) See [http://ec.europa.eu/food/food/index_en.htm](http://ec.europa.eu/food/food/index_en.htm).
consumer safety risks identified and to coordinate the response to such risks across the Member States.

The EFSA and the Rapid Alert System are designed to provide the European Union with an integrated food safety responsibilities and enforcement that are supported by a fit for purpose monitoring and communications systems to identify and communicate emerging food safety issues. In 2004 the system proved highly effective in assisting in the rapid control of chloramphenicol contamination in honey. Further alerts have been issued such as alerts on lead paint on imported Chinese toys.

However two of the key goals of the GFL [Clearly defined food safety responsibilities for all actors in the food supply chain and traceability of food, feeds, and food ingredients to their sources] were found to be fundamentally lacking in capability, capacity, coordination and enforcement in the Horsemeat scandal of 2011.

The market consequences of that failure are still emerging. However, certain conclusions have emerged, which can be used to identify Internet-readiness issues:

- The food industry has identified the commercial benefits of traceability;
- De-globalisation of meat product sourcing is a serious competitive advantage;
- Innovation in food quality/safety related consumer technologies is accelerating;
- Internet and social media are powerful “Risk avoidance” tools for consumers;
- The market consequences of the crisis has a continuing product level impact;
- There is little of any explicit reference to technology or the Internet in legislation; and
- Member States are taking (fragmented) action across the domains of food safety and animal welfare, especially with regards to e.g. disease (where ICTs can play a vital role in providing epidemiological information and operationalising both veterinary and market solutions\(^5\)).

This emphasises the importance of mechanisms that can be strengthened by ICTs (e.g. traceability in global food chains) and at least a prime facie case that the area – if not current legislation is Internet ready.

### 3.3. Statement of the Issues

Efficient modern global food chains have emerged due to trade liberalisation and rapid innovation and improvement in ICTs, life sciences, productivity, materials and supply chains. These enablers have led to globalisation of food production, increased the complexity of food chains and driven increased concentrations in food production and marketing.

Rapid innovation in material (e.g. packaging and preservatives) and life sciences (genetic modification, DNA testing, cloning, test tube meat) and transport (freezer containers, computer controlled environmental systems....) contribute opportunities for increased production, alternative flexible sourcing and longer shelf life for products. The net effect has been lower unit cost per calorie for consumers.

\(^5\) Carslake, et. al. (2010). See also extended discussion in McEldowney, et. al. (2013).
These trends and innovations have also delocalised food production, commoditised products and created a market of “process passive” consumers who are only active in the food chain at the points of purchase, preparation, consumption and waste disposal. Delocalisation of food production and the globalisation of food chains have also created new challenges for the administration of food supply, product content, product information and consumer safety. Globalisation of sourcing and production has driven the creation, implementation and consistent enforcement of multi-national governance mechanisms that can deliver food supplies and consumer safety to levels required by national governance requirements.

Food related scandals such as BSE (bovine spongiform encephalopathy) beef (UK), dioxin in animal feed (Belgium), adulterated meat (Ireland/EU/South Africa), contaminated spices (USA), melamine in Chinese food exports and food poisoning (Germany/EU/US) are only the more public of the food chain issues that have emerged during this period of globalised food chains. These scandals and other issues with globalised food trade flows, provenance, content, governance, safety and trust have driven global, multi-national and national attempts to arrive at a fit for purpose food governance structure and capabilities.

The successes and failures of these efforts illustrate the increasing necessity for present and future food chain governance structures, mechanisms and capabilities to be examined for and inclusive of the principle of Internet readiness in order to have more rapid identification, more detailed visibility and faster control responses to food related incidents.

3.4. Food Chain Relationships

The stakeholders, information flows and policy options central to an OptICTs Deep Dive into food are played out throughout the global food chain. In its broadest sense, this chain can be summarised as a network of one-on-one physical and data relationships designed to transfer produce via intermediaries to consumers.

It can be characterised as having weak vertical integration (field to retail control by a single brand) and inadequate inter network actor visibility (visibility on process and data requirements beyond an immediate relationship).

![Figure 3-2: Food chain actor process and data relationships](image-url)
This leads to a situation where optional data of downstream value for traceability, auditing and consumer support are gradually eliminated from the food data chain as they are not legally required and their downstream value or use is not understood or planned.

![Material Flow Diagram](source: Joyce 2014)

**Figure 3-3: Food chain data flow steps**

Each actor’s perceived responsibility for data and information is driven primarily by the legal and process requirements of the relationship with the actor one step upstream (supplier) and one step downstream (the customer). In effect there is little emphasis on a full network (360°, end-to-end process or field to fork) access to data, which is not legally required. In consequence, data sets actually available for enhanced food tractability, content types, process visibility, product labelling and consumer support (decisions on purchasing and use) are far less rich and useful than they might otherwise be.\(^56\)

Understanding the size of the Industry and its network is essential to understanding how to approach Internet readiness in relation to the food chain even inside the EU alone – where the writ of EU policy runs. The food and drink industry is one of the largest elements of national and EU economies as is illustrated in Table 3-1 below.

**Table 3-1: Economic significance of the food sector**

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Value</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn over</td>
<td>€1,017 Billion</td>
<td>Eurostat 2011</td>
</tr>
<tr>
<td>Value add</td>
<td>€203 billion</td>
<td>Eurostat 2011</td>
</tr>
<tr>
<td>Employment</td>
<td>4.25 million</td>
<td>Eurostat 2011</td>
</tr>
<tr>
<td>SMEs</td>
<td>285,000</td>
<td>Eurostat 2011</td>
</tr>
<tr>
<td>SME % involved in sector</td>
<td>49.3</td>
<td>Eurostat 2010</td>
</tr>
<tr>
<td>SME % employment in sector</td>
<td>63.4</td>
<td>Eurostat 2010</td>
</tr>
<tr>
<td>SME as % of companies in sector</td>
<td>99.1</td>
<td>Eurostat 2010</td>
</tr>
<tr>
<td>Sector Supply chain value</td>
<td>€ 4000 billion</td>
<td>Eurostat 2011</td>
</tr>
<tr>
<td>Sector Supply chain value add</td>
<td>€ 800 billion</td>
<td>Eurostat 2011</td>
</tr>
<tr>
<td>Sector Supply chain employment</td>
<td>32 Million</td>
<td>Eurostat 2011</td>
</tr>
<tr>
<td>Sector Exports</td>
<td>€ 86.2 billion</td>
<td>Eurostat 2012</td>
</tr>
<tr>
<td>Sector Imports</td>
<td>€ 63.2 billion</td>
<td>Eurostat 2012</td>
</tr>
<tr>
<td>% of EU produce processed</td>
<td>70%</td>
<td>Food and drink Europe 2013</td>
</tr>
</tbody>
</table>

\(^{56}\) These conclusions are based on key informant interviews.
This industry is the link between primary producers (agriculture) and consumers. In view of the way information tends to be eliminated along the value chain, it is important to get a sense of the number of associated actors at different stages along the food chain in the EU as shown in Figure 3-4.

![Figure 3-4 Structure of the food value chain in the EU (EU-27, 2008)](image)

However there are significant issues in the understanding of the supply chain by the food manufacturers who are vital intermediaries in physical and information flows and are thus essential to the success of Internet ready legislation. Internet ready legislation relies for its intended effects on the availability and appropriate use of suitable data; insight into the potential impact of Internet ready legislation is therefore provided by issues identified by recent research into supply chain mapping by food manufacturers, summarised in Table 3-2 below.

### Table 3-2: Impact of horse meat scandal on businesses

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>82%</td>
<td>The percentage of food and drink manufacturers who said the horsemeat scandal had not affected the way they manage information about suppliers</td>
</tr>
<tr>
<td>50%</td>
<td>The percentage of manufacturers reliant on paper records to manage information about suppliers across the world.</td>
</tr>
<tr>
<td>40%</td>
<td>The percentage of manufacturers who have never mapped their entire supply chain to identify all their suppliers.</td>
</tr>
</tbody>
</table>

Source: Food Quality News (2014)

As the agricultural sector is the primary producer for the food chain it is important to understand its capacity to implement technologies or processes that can support an Internet ready legislative environment.

One proxy for this capacity is the size distribution of farms in terms of area and standard output in euros (Table 3-3) which calibrates both short (local produce to local consumers)

---

57 Food Quality News (2014).
and long (produce to intermediaries) food chain supply. Larger holdings are better able to undertake technological investments.

Table 3-3: Size and income of EU farm holdings

<table>
<thead>
<tr>
<th>EU Total Holdings (millions)</th>
<th>’000</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; €2000</td>
<td>240</td>
<td>44.6</td>
</tr>
<tr>
<td>€2k - €3,99k</td>
<td>1,939</td>
<td>15.8</td>
</tr>
<tr>
<td>€4k - €7,99k</td>
<td>1,529</td>
<td>12.5</td>
</tr>
<tr>
<td>€8k - €14,99k</td>
<td>982</td>
<td>8</td>
</tr>
<tr>
<td>€15k - €24,99k</td>
<td>602</td>
<td>4.9</td>
</tr>
<tr>
<td>€25k - €49.99k</td>
<td>627</td>
<td>5.1</td>
</tr>
<tr>
<td>€50k - €99.99k</td>
<td>467</td>
<td>3.8</td>
</tr>
<tr>
<td>€100k - €249.99k</td>
<td>149</td>
<td>3.4</td>
</tr>
<tr>
<td>€250k - €499.9k</td>
<td>149</td>
<td>1.2</td>
</tr>
<tr>
<td>€500k &gt;</td>
<td>81</td>
<td>0.7</td>
</tr>
</tbody>
</table>

Using €25,000 as an indicative threshold for the viability of “reasonable” investments in traceability technologies, only 14.2% of agricultural enterprises could reasonably be expected to adopt them.

However the situation changes radically when we take account of mature mobile technologies such as smart phones enabled through apps and interfaces to provide the necessary data sets for traceability, compliance monitoring or other legal or process needs.

Indeed, this capability can be put in place today to “Internet enable” existing legislation whilst positioning ever larger numbers of agricultural enterprises for future “Internet ready” soft or hard legislation.

One example is bovine tags. Were these to be bar coded and machine read via smart phone apps on the farm for transport load and for unload at point of sale and point of slaughter, a continuous data stream from farm to slaughter could be established, monitored and enforced for the EU’s 64.05 million cattle, using cloud based methods to make data accessible to farmers, intermediaries and administrations.

After the horse meat scandal, the tagging of additional species is being considered (e.g. Ireland for horses). Potentially, 135.212 million animals (cattle, sheep, goats, pigs, poultry) could be cheaply and efficiently monitored throughout their lifecycle.

With 51% of the EU livestock located in 4 of the richer countries (France, Germany, Spain and the United Kingdom) the cost of achieving significant Internet readiness would be quite low per unit covered.

3.4.1. Consumers

Historically, political legitimacy and societal stability have rested heavily on the ability of governments to maintain adequate food supplies, reasonable quality and acceptable pricing.

See e.g. European Commission (2009) for a discussion.
But ensuring the actual and perceived safety of food is challenging. The vast majority (estimates range from 75% to 90%) of foodborne illnesses do not get reported due to a variety of reasons such as mild infection, short duration, self-medication or -treatment, embarrassment or death due to other causes. Therefore, the collection and dissemination of more accurate data on the incidence of foodborne illness (e.g. as facilitated by ICTs) is of significant importance.

In 2011, 5,648 foodborne outbreaks were reported in the European Union resulting in 69,553 reported human cases, 7,125 hospitalisations and 93 deaths. In the same year the United States CDC (Centre for Disease Control) estimated that foodborne diseases annually cause roughly 1 in 6 Americans (48 million people) to get sick, 128,000 hospitalisations and 3,000 deaths. In the UK, it is estimated that each year as a result of foodborne illness: around a million people suffer foodborne illness; around 20,000 receive hospital treatment; and 500 die. The cost to the economy was estimated £1.5 billion (€1.7 billion) or £1,500 per infection.

These statistics do not take into account other food-related health impacts such as those caused by short and long term chemical contents or contaminants or allergies. A study of food allergies in the United States put the cost to the US economy at $25 billion (€34 billion) annually.

3.4.2. Sources and Location of Infections

The potential of consumer-collected information to improve our understanding of disease and the scope of improved provision of information to help end-users to mitigate risks depend on the sources and locations of infections. Eggs and egg products were the highest source of human infections from food but infections were reported as coming from all major food types except alcohol (see Figure 3-5 below).

---

60 See e.g. Roberts (2001) or http://www.cdc.gov/foodsafety/facts.html.
61 European Food Safety Authority (2013).
62 CDC (undated).
63 FSA (2013)
64 Medical News Today (2013).
The largest source of food infections were from eating out in a professional food preparation establishment such as restaurants or cafes. Infections from food prepared or consumed at home came second. Takeaways or fast food was the lowest reported source of food infections.

The sources and potential location of food infection or contact with foodborne allergens cover all major food sources and centres of activity that a consumer is likely to encounter. Until recently, consumers’ ability to identify actual or potential sources of infection was limited to smell, taste, vision and touch.

---

65 European Food Safety Authority (2013).
66 European Food Safety Authority (2013).
This is beginning to change as life sciences develop and miniaturise capability to identify pathogen species through DNA tests, antigens and other biological markers. Key to these capabilities is the ability to cost effectively sequence genomes and then manufacture consumer level tests.

The tipping point for costs of such sequencing to move into the mainstream is likely to be reached soon.

This cost reduction will accelerate the availability of consumer level self-testing kits and sensors based on mobile technology. Early examples of self-tests can be seen in monitors for heart rate, blood pressure, blood sugar and exercise and a rapidly growing stable of other devices and applications linked to health and wellbeing. The implications and challenges are enormous for local and global food chains and their administrators as the ability to monitor quality and safety moves into the consumer domain.

The ability personally to report and share more detailed data on personal disease incidents and on foodborne risk factors has major implications for health service demands, data administration, health and safety warning processes, risk and issue management, response management, consumer behaviour, monitoring, metrics, designation of technologies and confidence in health and safety administration.

Appropriate consumer response depends on more than simple data availability – the data must also be provided in understandable and meaningful form. In the domain of contagious disease, various categories of medical/disease visualisation app are available for mobile devices to provide information on epidemiology or current outbreak situations.

*Outbreaks Near Me*[^68] (free download) uses news media reports, medical e-mail list services, and alerts from official national and international organisations and a range of Internet sources to monitor the occurrence and impact of global infectious diseases via the HealthMap database[^69].

---

[^67]: Ramadhar (2014).
Figure 3-9: Health map of reported food issues

The project is funded by Google and receives support from the CDC, the National Library of Medicine and the Canadian Institutes of Health Research; it compiles information about international human and animal infection-related outbreaks. Infections are indexed (and can be searched) by disease state and displayed as push pins within the embedded Google Map to indicate disease locations and associated information. The app also includes outbreak information listed regionally or by city.

Indications of the commercial opportunities related to disease and health information can be seen in the market responses to H1N1 (swine Flu) apps such as Swine Flu Up-to-the-minute, Swine Flu (H1N1 Virus) and Swine Flu Guide, all of which were available during the outbreak. Many are now closed as the H1N1 issue is past.

71 Cost $0.99 - http://web.me.com/jbmjbm22/JBMJBM/JBMJBM.html.
These apps all rely on data from media and disease reporting centres. The emerging capabilities to personally detect pathogens, allergens and chemicals in food or substances for personal use due to miniaturisation of personal test devices and transmission of the resulting data to GPs, national authorities or open/shared databases will provide far more detailed data for a range of uses by consumers, health care and public health authorities, pharmaceutical companies, food suppliers and the like.

However, information on outbreaks is of limited use if the food supply chain cannot trace outbreaks in detail back to their origin (including all intermediate handlers and processes) in order to understand the cause, potential size, and geography of an outbreak and to play their part in preventing its spread. Such interventions may themselves by ICT-based, such as point of sale warnings triggered by scanning of a products that may be from (or have come into contact with) an infected batch. This is and will remain in the near future the Achilles heel of food and product safety.

The capability of consumer level devices to provide personal testing for substances and conditions has already driven consideration of re-classification of such technologies. In 2008 Apple was successfully lobbied to create a separate medical classification for iPhone applications, its first spin-off category. In its first year the medical category grew from 82 to more than 1200 applications. In early 2009, the medical category became the third fastest growing App Store category. The status of such applications is also changing – the US FDA (Food and Drug Administration) is monitoring developments in consumer level detection capabilities with a view to reclassifying such devices/capabilities as medical devices.

On 23 September 2013, FDA released a final guidance on mobile apps indicating its intention to "focus oversight on mobile medical apps" that:

- are intended to be used as an accessory to a regulated medical device – for example, an application that allows a health care professional to make a specific diagnosis by viewing a medical image from a picture archiving and communication system (PACS) on a smartphone or a mobile tablet; and/or
- transform a mobile platform into a regulated medical device – for example, an application that turns a smartphone into an electrocardiography (ECG) machine to detect abnormal heart rhythms or determine if a patient is experiencing a heart attack.

Interestingly it does not specifically reference pathogen, chemical or other consumer based tests.

3.5. Sustainable Food and Internet Ready Policy processes

Sustainability of food is another area of particular note in the Deep Dive – the data provided by the food supply chain are of only limited use in promoting socio-political, cultural or environmental sustainability. Ideally, consumers would use information about the sustainability footprint of food to inform their choices, but the rich information available in the food sector is not made available in usable form.

---

73 Dolan (2009).
74 FDA (2013).
Food sustainability is also the subject of a consultation\textsuperscript{75} process whose preliminary results were made available in January 2014, which have been examined for the purposes of this report.

Unusually, food sustainability is also Internet ready in a legal sense. This is because the Food Information to Consumers (FIC) Regulation\textsuperscript{76} contains 4 key preamble statements that provide for or do not preclude key mechanisms for ensuring that all future food information laws are Internet ready.

Note in the following paragraphs drawn from the Regulation key words and phrases are highlighted in \textbf{bold}. Their implications are summarised under each article in \textit{italics}).

- **Statement (13)** “It is necessary to set \textbf{common definitions, principles, requirements and procedures} so as to form a clear framework and a common basis for Union and national measures governing food information.”

  Article 13 enables the flexibility noted in article 16.

- **Statement (14)** “In order to follow a comprehensive and evolutionary approach to the information provided to consumers relating to food they consume, there should be a broad definition of food information law covering rules of a general and specific nature as well as a \textbf{broad definition of food information covering information provided also by other means than the label}.”

  This statement ensures that the push or pull display of information is future-scoped without prejudice to existing, emerging or latent technologies or mechanisms.

- **Statement (16)** “Food information law should \textbf{provide sufficient flexibility to be able to keep up to date with new information requirements of consumers} and ensure a balance between the protection of the internal market and the differences in the perception of consumers in the Member States.”

  This statement makes provision for future improvements in the display of information without prejudice either to existing consumer needs for data or information or to those that may emerge due to consumer level concerns or capabilities related to food safety or sustainability.

- **Statement (27)** “In order to ensure the provision of food information, it is necessary to consider all ways of supplying food to consumers, including selling food by means of distance communication. Although \textit{it is clear that any food supplied through distance selling should meet the same information requirements as food sold in shops, it is necessary to clarify that in such cases the relevant mandatory food information should also be available before the purchase is concluded}.”

  This statement allows all the existing, emerging or future channels of food provision to consumers to be required to comply with pre purchase information standards in force for pre-existing channels. Articles 13, 14, 16 all form the foundations of this articles implementation).

\textsuperscript{75} http://ec.europa.eu/environment/consultations/food_en.htm.

\textsuperscript{76} Regulation 1169/2011 – see European Parliament and Council (2011)
In essence these 4 statements contained in the preamble of the FIC Regulation form an Internet readiness legislative template. They are the source of the Internet readiness aspects detailed in Sections 4.4.3 and 6.1.1. They are easy to tailor as questions and be used in any form of policy/legislative intervention. They contain the core ICT related considerations that should be at the centre of any policy process if it is to position for or seek to ensure eventual interventions are Internet aware and consequent legislation is Internet ready. In addition they can be used to set parameters, metrics and standards against which the quality/effectiveness of past, present and emerging voluntary market self-regulation/intervention logics can be created, monitored and audited. This in turn allows a sequence of policy area specific transparent trigger points that can be used to alert DGs to the potential need to initiate a policy process.

To illustrate the implications of these 4 articles, we examined the EcoSearch process\textsuperscript{77} to show how these statements (had they been available) would have facilitated and potentially speeded up the process. The findings are summarised in Figure 3-10; Figure 3-11 shows how the toolkit supports this process.

\textbf{Figure 3-10: Regulatory support for EcoSearch-type process}

Figure 3-11: Toolkit fit and (Regulation Statement) support for EcoSearch-type process

The EcoSearch process had none of the explicit legal underpinnings that the 4 statements provide to future initiatives. It relied instead on Article 7 of the Ecolabelling Directive:

- **Article (7)** Distance selling and other forms of selling: “Where products are offered for sale, hire or hire-purchase by mail order, by catalogue, through the Internet, telemarketing or by any other means which imply that the potential end-user cannot be expected to see the product displayed, delegated acts shall make provision to ensure that potential end-users are provided with the information specified on the label for the product and in the fiche before buying the product. Delegated acts shall, where appropriate, specify the way in which the label or the fiche or the information specified on the label or in the fiche shall be displayed or provided to the potential end-user.”

This meant that most aspect of EcoSearch had to be justified through its impact merits, design simplicity and low process disruption/high end user value.

The key statement that would have radically changed this situation is statement 13 of the FIC Regulation described above. It allows authorities to establish “common definitions” (what: data types/characteristics and content), “principles” (why), requirements (who, what, when and where) and “procedures” (how) “so as to form a clear framework and a common basis for Union and national measures.” This statement allows the creation of an idealised data/information flow environment that can be voluntarily adopted or legally required by initiation of a policy process.

Statements 14, 16 and 27 would have significantly influenced, facilitated and speeded up the process of defining form, format, content, presentation, display logics, display guidance, wording, roles, responsibilities, alternative use cases, channel focus, metrics, monitoring
capabilities and implementation/review cycles. Applying these mandates and enablers to food sustainability throughout the food chain yields Figure 3-12.

**Figure 3-12: Food chain information flows and uses**

As can be seen, this model addresses the information needs, transparency, accessibility and flexibility needed to gain an understanding and enhance the management of many of the food chain elements that contribute to greater food sustainability.

It shows that a comprehensive open data and information flow strategy and design opens new opportunities for providing significant new data and information sets to business and consumers. This resource could enable a range of opportunities including:

- Enhanced consumer purchase support information;
- Reduced consumer exposure to allergens and undesirable substances;
- New and more detailed automatic monitoring and reporting;
- More granular reporting of food incidences to authorities;
- Reduced food fraud through enhanced traceability;
- Faster more responsive responses to food chain issues;
- Reduced risk to business through enhanced tractability and quality control;
- Reduced waste and enhanced waste monitoring;
- New third party value added service to consumers;
- Increased tax revenues through better automatic monitoring; and
- Reduced food chain transport costs through better supply and demand management.

The above model is fully achievable within the present legal framework, technologies, processes and information in a non-disruptive fashion.

The toolbox (see Chapter 6) is therefore designed to provide senior management the capabilities to identify, prioritise and resource policy areas in need of “Internet-readiness” input.

It cannot take into account the Political priority that may or may not be attached to crafting specific policy initiatives or legislation in this way.

3.6. Potential Top Level Policy Decision Model

A top level model for assessing whether past present or future legislation is Internet aware, ready or fit for purpose was created. This is illustrated in Figure 3-12.

![Figure 3-12: Top level policy decision model](image-url)
The 4 statements provide 4 questions (see Section 3.7) that allow any piece of legislation or any intervention to be classified as being positioned for an Internet enabled or rich environments. The answers to these questions provide a clear indication as to whether a policy, process or intervention is likely to be fit for purpose in an Internet mediated environment.

3.7. Deep Dive Conclusions

The food area has one of the most Internet ready legislative baselines available. This, if correctly understood and actioned, can have significant impact on Internet use in consumer information provision, traceability, public health and environmental impact of the food chain.

The starting point is the recognition that significant losses of valuable data and information occur due to the lack of end-to-end requirements to ensure their retention and availability throughout the food chain.

Implementing and enforcing open data requirements opens significant new opportunities for new value added services, food chain efficiencies, supply and demand mapping, issue identification and management, food fraud reduction, traceability and visibility of food provenance, handling and quality, increased consumer confidence in food chain management and governance, reduced costs to business and increased tax revenues to Member States.

Improved performance and reduced costs of complementary technologies such as smart phones, genome mapping, and analytical enabler miniaturisation are likely to provide users with enhanced capabilities to monitor and test domestic and non-domestic (e.g. restaurants, fast food outlets) food for pathogens, allergens and contents (cultural or health related restrictions). The cumulative impact of large amounts of consumer generated food quality information is likely to disrupt public trust in existing food safety and health statistics. Therefore the use of such technologies is likely to require significant reappraisal of their current categorisation and governance (e.g. smart phones or test/analytical dongles) due to their potential significantly to affect food and health decisions and outcomes.

It is relatively simple to segment past present and future interventions or mechanisms in relation to their Internet fit for purpose by asking 4 simple questions:

1. Does it provide for legally compliant similar, equivalent or better information than existing processes?
2. Does it prevent data and information presentation through existing mechanisms or preclude presentation through future mechanisms?
3. Does it provide adequate definition to ensure data and information types, formats, flexibility and sourcing for collection, flow, presentation and measurement that are fit for present and future purposes?
4. Does it preclude the addition or repositioning of data and information (sets and flows) that may emerge from future stakeholder needs?

78 In particular, food safety failures and associated public health and economic impacts are massively underreported in the EU.
Building out and mobilising the policy processes necessary to adapt to these possibilities and to exploit the Internet readiness of existing rules (e.g. the FIC Regulation) can be done rapidly using tools and techniques that are common, off the shelf and cost effective in the market today.
4. Deep Dive 2 (Transport)

4.1. Overview

Transport is the lifeblood of any modern economy. The ability to move freely, cost-effectively and simply is one of the most important drivers of economic and of societal development. It is also both a cause and a cure for environmental damage associated to that development. In these functions, ICT modifies the nature of transport; it transports and connects information rather than people and goods, and changes the nature, costs, benefits and impacts of transport. Indeed, in the early stage of Europe’s economic development, transport was the most important ICT.

Transport is also a policy domain that has matured at local, national and transnational level. Transport policymaking, in the broadest possible sense, has focussed on expanding service, driving competition and latterly on mitigating the sector’s environmental impacts.

Transport was until recent years, a comparatively staid field in terms of Internet-readiness. The offline nature of activities has led policy in the transport domain to focus on management and regulation of the physical activities of transport providers. Especially in those regulatory areas where ICTs have the greatest potential (e.g. road use, licensing, enforcing insurance, and safety) the legislative frameworks have concentrated on the physical aspects and online development was primarily a means of simplifying compliance rather than a force for changing the nature of regulation.

The impact of technology on transport domain, however, exploded in the previous 20 years in a manner that presents a suite of new challenges for effective creation of policy. Many of the Internet-readiness issues that will dominate the domain in the future are currently in their infancy and have yet to make a significant impact on policy. The challenge of the transport Deep Dive has been to cast forward into the future, in the knowledge of the emerging data and technology conditions currently taking route, to determine the pressure points where future policy interventions seem probable.

In particular, many of the applications and technologies that can most profoundly tip the regulatory playing field are already under active development around the world and across the various transport sectors. Others, not yet at the deployment stage, are described in well-articulated visions. But the separation between the transport and the ICT worlds remains and the potential of these two network-based sectors to interact at the governance level remains underdeveloped.

79 The framing in this section represents the judgement of the study team, based on experience, general reading and the opinions expressed in workshops and interviews.
Put simply, we have developed ICT ‘solutions’ for many of the problems created by increasingly dense, complex and critical transport systems but, like much of transport policy per se they have focused more on past or existing problems or on the continuation of past trends, than on changing the problems themselves (e.g. by active demand and supply shaping). As a further result of this asymmetric (principal-agent) relation between transport and ICT our understanding of how human behaviour got to be the way it is and how it is likely to change as ICTs develop remains limited.

It should be underscored that this differentiates this Deep Dive from the Food example above. In food supply chains, Internet-readiness issues are a current reality for the policymaking community. In transport, our conclusion has been that technology implementation to date has been largely instrumental, serving specific offline priorities of the sector (e.g. the release of ‘big’ flight data by the airline industry to generate more effective sales). Only once such issues take on a complexity and emergent character such that they begin to further separate agendas or begin to circumvent the current regulatory environment will they become policy challenges. Therefore this Deep Dive seeks to focus on the identification of potential stress points and suggested actions to forewarn and forearm policymakers against unexpected developments in the technological reality.

4.2. Context

4.2.1. Transport Policy Context

The transport domain can be considered mature in its proliferation, policy environment and function. The focus of this overview will therefore not be transport per se but rather the interaction between transport systems. Such interaction is termed, by Directive 2010/40/EU, ‘multi-modal transport systems’ and for the purpose of clarity this Deep Dive will persist with this definition.

The focus of the Deep Dive is to forecast the main ‘pressure points’ on which the transport domain’s Internet-readiness may rest in future years. The transport domain in its entirety would be too large to provide meaningful recommendations within the scope of such a study. For this reason, OptICTs took the decision, on the advice of stakeholders familiar with the issue, to focus on those areas where the intersection of transport and ICT are most apparent and offer the most fecund subject for examination in the Internet-awareness context.

One of the main challenges faced by transport is the integration of ‘big’ and ubiquitous data capture. The explosive increase in transport data has three key drivers: 1) The increasing release of proprietary data by industry sectors 2) The rise in IoT and other monitoring technologies that increase the potential for data harvest 3) Growth in the range of online channels through which data can be accessed and used. Together the three factors above have driven significant expansion in the data-driven business models in the transport domain.

In the European context, the drivers noted above have come under the aegis of the Commission’s work through a white paper entitled "Roadmap to a Single European

---

Transport Area - towards a competitive and resource efficient transport system. The paper proposes a roadmap of 40 concrete initiatives aiming to build a competitive transport system that will increase mobility, remove major barriers in key areas and foster growth and employment; while at the same time reducing Europe's dependency on imported oil and cut carbon emissions in transport by 60% by 2050. Despite its broad ambition and long term perspective, the white paper lacks a closer link to the Intelligent Transport Systems (ITS) Directive adopted on 7 July 2010, and leaves open how ITS can improve the transport modes.

4.2.2. Focus Area – Intelligent Transport Systems (ITS)

The ITS programme recognises the role of ICTs to contribute to cleaner, safer and more efficient transport system. It is an area that requires and has a long tradition of close collaboration with other DGs. It is supported by several Directorates-General: DG Move, DG CONNECT, DG Research, DG Enterprise, DG Environment and DG Regio.

The current legal framework, EU Directive 2010/40/EU of 7 July 2010 on the framework for the deployment of intelligent transport systems in the field of road transport and for interfaces with other modes of transport defines ITS as

“advanced applications which without embodying intelligence as such aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated and ‘smarter’ use of transport networks.”

It promotes

“advances in the field of the application of ICT to other modes of transport to be reflected in the developing in the road transport sector, in particular with a view to ensuring higher levels of integration between road transport and other modes of transport”.

The Directive requires the European Commission to adopt specifications to address compatibility, interoperability and continuity of ITS solutions across the EU by 2017. Priorities in the first years are the development of: traffic and travel information, the eCall emergency system and intelligent truck parking.

There have been at least 20 years of cooperation between DG MOVE and DG CONNECT (and their antecedents) on issues relating to transport. Among the earliest examples was ERTICO, a joint effort between DGs 7, 12 and 13. This promising beginning was followed by

---

82 This section is based in large part on key informant interviews with DG MOVE and DG CONNECT staff conducted under Chatham House rule (non-attributable).
83 European Parliament and Council (2010).
84 ERTICO – ITS Europe was founded at the initiative of leading members of the European Commission, Ministries of Transport and the European Industry in 1991. Today, it represents the interests and expertise of around 100 Partners involved in providing Intelligent Transport Systems and Services (ITS). It facilitates the safe, secure, clean, efficient and comfortable mobility of people and goods in Europe through the widespread deployment of ITS. ERTICO’s activities are carried out by its Brussels-based team after approval by its Supervisory Board. ERTICO’s vision is to bring intelligence into mobility, working together in public private partnership towards: zero accidents, zero
a period of relative separation, during which relatively few joint activities were pursued. An exception was the e-Call initiative. This began within DG INFSO but migrated to DG TRANSPORT as the focus shifted and transport specificity deepened. Interestingly, this illustrates a strong difference of perspective. The E-Call initiative was viewed by DG CONNECT as a locally-originated initiative that migrated to focus on transport and safety and thus transferred to DG MOVE. Conversely, DG MOVE tended to regard it as a technology-driven idea that (initially) lacked business case orientation. The e-call reached fruition with the 11 February 2011 vote ensuring that all new cars will have to be equipped with e-call starting in October 2015.

There was also a form of parallel evolution in the TENs programme, but this fell into abeyance when the focus of TEN-Telecom turned from infrastructures to applications, and only resumed in the context of the successor programme (CIP).

More recently, the joint space has been linked to the evolution of the Intelligent Transport Systems (ITS) cluster of initiatives, and by Smart City initiatives, actions and programmes. These are not limited to direct policy actions, but also include strong research components, active links to other DGs and policy objectives, and extensive and complex external stakeholder engagement.

Beyond direct government activities, the European Commission has established Technology Platforms, Joint Technology Initiatives, Public Private Partnerships and expert groups to collect and share information. Collaborations range from international personnel exchanges (e.g. EU-Japan Cooperation in Intelligent Transport Systems to city-based, independently or in conjunction with the Smart Cities Programme (Manville et. al. 2014). Other noteworthy examples include:

- London congestion charging – which uses ICT-based sensing and charging systems to tackle traffic problems;
- FREVUE (Validating Freight Electric Vehicles in Urban Europe); and
- Efficient Consumer Response – an industry-led group that provides a wide range of scorecards, tools and information for identifying opportunities for collaborative management along supply chains, including the organisation of transport.

delays, reduced impact on the environment, fully informed people, where services are affordable and seamless, privacy is respected and security is ensured. To achieve this vision, all modes of transport should cooperate to achieve an optimal and sustainable use of all transport modes. Source: http://www.ertico.com/about-ertico.

There is no clear ‘one or the other’ rule, instead a case-by-case approach requiring close collaboration and coordination between DGs. ITS started at DG CONNECT, DG MOVE was involved early on, now a shared topic. Joint activities under Horizon 2020, with some parts managed by DG MOVE & RTD (Directorate H – Transport).


85 There is no clear ‘one or the other’ rule, instead a case-by-case approach requiring close collaboration and coordination between DGs. ITS started at DG CONNECT, DG MOVE was involved early on, now a shared topic. Joint activities under Horizon 2020, with some parts managed by DG MOVE & RTD (Directorate H – Transport).


88 http://frevue.eu/.

As noted above, transport, unlike food, has the luxury of relative segregation along the local, national, European and global boundaries. Therefore it has been possible to observe the effect of ‘scope’ on the maturity of transport data interoperability on different industry sectors, leading first to variation between sectors in the policies laid out and secondly to the evident drive toward convergence ongoing in European policy. Three common priorities emerge in the current legislation surrounding transport policy that can be said to summarise the intended objectives: 1) Economic benefits (including competitiveness); 2) environmental benefits; and 3) social/societal benefits. Because these are shared across DGs, they provide a basis for the sort of joint action studied in this report.

4.2.3. Focus Area – Geographic Reference and Smart Cities

The development of truly multimodal transport systems requires a ‘common denominator’ across which developments can be forged. One of the key components of growth in transport data has been the rise of Geographic Information (GI) as a common reference framework for positional information across different transpiration sectors. The following case study will detail some of the key developments in GI and spatial data with reference to transport.

One key piece of work currently ongoing at the European level that has a potential impact on the data of the transport domain is the INSPIRE Directive. Introduced by the EC in 2007, INSPIRE established the principles of a European spatial information infrastructure. INSPIRE applies to all spatial data sets and services that are held by or on behalf of public authorities and used in the performance of their public tasks. INSPIRE has given rise to a number of projects in the transport domain and most recently OpenTransportNet, a CIP-funded effort to harmonise and expose transport data with a common spatial reference format. The team feels it important to draw the attention of the reader to the work being undertaken in reference to INSPIRE because the development in spatial data and its application in transport drivers including satellite navigation systems and journey planners have the potential to make GI a significant area of policy consideration in future.

The presence of common reference frameworks such as geospatial data also has significance in relation to the smart city environment. Smart cities were found, among interviewees, to be a primary envisaged application of ITS and the EC Horizon 2020 pillar on transport also makes significant reference to the application of transport within cities. As the language of Smart Cities moves increasingly from the integrated back-end operating environment of the city manager to the more open consideration of how citizens repurpose services and data to create new things, the presence of common reference schemas, location-based or otherwise, will become a key approach for driving standardisation and release of transport data. One of the projects interviewed by the Deep Dive, European Cloud Marketplace for Intelligent Mobility, was keen to stress that when considering any ‘end-to-end’ (integrated) transport system, the ability not only to obtain but to render interoperable the rich data of the different services is critical to the successful integration of transport into the Smart City ecosystem.

4.2.4. **Smart Transport Market Context**

A Smart Transport Market\(^{91}\) is a hybrid comprised of transport and ICT value chains. It emphasises multi-modality and safe, interoperable connectivity between vehicles of all types, infrastructure and devices (V2X). It can be partitioned into 2 components/areas:

- V2X cooperative systems; and
- Infrastructure (traffic signals controllers; parking or ramp meters; dynamic message signs; and (Centre to Centre, Centre to Field) traffic information centres.

Research organisation valuations of the size of the smart transport market vary with assumptions about its likely disruptive influences. Based on conservative estimates of these disruptions, Pike research forecasts suggest rapid growth (from a low base) around the world, with Europe leading the way:

Table 4-1: Low-end smart transport revenue forecasts\(^{92}\)

<table>
<thead>
<tr>
<th></th>
<th>2012</th>
<th>2015</th>
<th>2020</th>
<th>CAGR(^{93}) (2012-2020)</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>€ 464.60 M</td>
<td>€ 1,005.98 M</td>
<td>€ 1,836.28 M</td>
<td>18.70%</td>
</tr>
<tr>
<td>Europe</td>
<td>€ 416.45 M</td>
<td>€ 985.16 M</td>
<td>€ 1,997.65 M</td>
<td>21.60%</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>€ 724.88 M</td>
<td>€ 1,503.12 M</td>
<td>€ 3,054.39 M</td>
<td>19.70%</td>
</tr>
<tr>
<td>Latin America</td>
<td>€ 93.70 M</td>
<td>€ 144.46 M</td>
<td>€ 218.64 M</td>
<td>11.10%</td>
</tr>
<tr>
<td>Middle East and Asia</td>
<td>€ 40.34 M</td>
<td>€ 71.58 M</td>
<td>€ 117.13 M</td>
<td>14.40%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>€ 1,739.97 M</td>
<td>€ 3,710.29 M</td>
<td>€ 7,224.07 M</td>
<td>19.50%</td>
</tr>
</tbody>
</table>

More generous estimates are obtained by taking into account the ‘knock-on’ effects of initial investments in and deployments of these technologies on new businesses and services, reductions in the socio-economic costs of congestion\(^{94}\).

Moving beyond the purely urban environment, additional benefits are expected by industry analysts. Markets & Markets\(^{95}\) place the current size of the Smart Transport market at €34.75 B in 2012 with a CAGR of 23.6%, reaching €133.15 B by 2018.

The technologies included in these estimates fall into two broad categories. The first comprises *transport information* application development:

- GIS/traffic management service application model integration and convergence;
- GIS based mass traffic information management;

---


\(^{92}\) Pike Research (2011). This is limited to urban applications such as (in decreasing order of investment): integrated traffic monitoring and management services and congestion management; road user charging; public transport systems; enhanced emergency response; real-time public information systems; smart parking solutions; and vehicle-to-vehicle (V2V) technologies.

\(^{93}\) CAGR = Cumulative Annual Growth Rate

\(^{94}\) EU estimates place this at around €100 B or 1% of GDP on an annual basis.

\(^{95}\) See e.g. Markets and markets (undated).
• Traffic information resource integration;
• Traffic data centre and traffic flow data survey and analysis; and
• Traffic data collection, statistical analysis and presentation.

The second group comprises intelligent traffic features:

• Dynamic traffic information acquisition, integration, processing, forecast and distribution;
• Electronic toll collection;
• Intelligent parking guidance system;
• Vehicle license plate automatic identification;
• Traffic event automatic detection; and
• GPS monitoring/dispatching and information service.

4.3. Statement of the issues

The record of policy engagement within transport per se and its linkages with other policy areas and actors shows a wide range of fragmented initiatives. Many of these are linked (or could be) and draw (or could draw) on common and consistent data. Overall, the policy players within and beyond the EC can make much better use of information. Beyond this, many of the existing policy initiatives rest on simplistic models of how information affects transport behaviour. Therefore, if policies are contemplated that seek to influence individual behaviour or to draw inferences from observations about the need for intervention, it is essential to lower barriers to inter-institutional information collection, communication, analysis and modelling in order better to understand how people’s behaviour will change if they are: i) measured and monitored or asked to volunteer information; ii) provided with a range of relevant information to inform their short- and long-term decisions; and iii) provided with platforms on which to make new business models and connections.

Several specific developments are required in order to build this understanding.

Process changes are needed to facilitate the collection, mashing, analysis (big and small data) of a wide range of existing information.

There is also a need to conduct behavioural studies (and social experiments or gamified initiatives) to build a common understanding of how different stakeholders actually behave and how their individual and collective behaviour might evolve.

At a deeper level, this requires – or may give rise to a change in the policy mind-set to move beyond a reactive ‘predict and provide’ stance to a more anticipatory approach. We note that the need for anticipation and active demand management is recognised in policy analysis and some visionary transport policy documents, but the passive approach still pervades even state of the art transport demand modelling, and that policy modelling makes only scant use of supply-side, behavioural and strategic models.

The policy options can also usefully be expanded to include coordinated policy changes such as: urban renewal; reconfiguration of transport, communication and power infrastructures; and targeted support and team-building initiatives to ensure that the results are usable and used across an urbanising Europe and not just in a few pilots that are already progressing well (in ways that other areas find hard to follow).
Finally, it will be necessary to develop and apply new modelling and simulation techniques to allow players to explore medium-to-long term policy changes in ways that reflect - but do not trivialise - short-term responses (e.g. modal choice, transport prevention).

The Deep Dive is based around two connected issue sets; both are affected by the same set of ‘Level 2’ considerations and relate to a common set of potential technologies and policy changes.

“From smart transport to intelligent motion” – the policy issues are flexibility and adaptation - the need to move beyond predict and provide to active ‘traffic shaping’ (including active demand and supply management via informational linkages) to enable transport flows to self-organise in response to relevant data (including e.g. weather data) to facilitate ‘downstream’ uses (e.g. logistics, retail, scheduling).

“From Smart Transport and Smart Cities to Smart urbanisation” – the policy issue here is sustainability – transport contributes an enormous proportion of urban-associated pollution (and other problems) and facilitates the unsustainable configuration of urban spaces. There is therefore a lock-in to urban sprawl (which militates against transport efficiency and maximises pollution per capita) and to turbulent and inefficient transport arrangements (too much autonomy, justified by a dense but spatially and temporally-dispersed network of ‘necessary’ and ‘feasible’ connections. It can also be seen as a set of interconnected components including: the built environment; the supporting information, transport, power and other utility infrastructures; and public and private transport systems. It is difficult or impossible to ‘fix’ any one of these components in isolation. Only simultaneous reconfiguration will produce a scalable and extensible model for break-out; otherwise Smart Cities will remain isolated pilots, and the current inverse correlation between progress towards urban sustainability and the need to make progress will continue.

4.3.1. Associated Data Flows and Applications

The data flows in modern traffic systems that lie at the heart of these issues, are indicated in Figure 4-1:

![Data flows among ICT elements](image)

**Figure 4-1: Data flows among ICT elements**
The data flows in the transport domain translate into a wide variety of potential Internet-awareness issues. To ensure that the data flows are adequately expressed in their scope and complexity, the team complied Table 4-2 in consultation with our interviewees to provide the reader with an indicative overview of the typology of Internet-awareness issues that could potentially present themselves in the domain.

**Table 4-2: Potential ICT-intensive applications relevant to issues**

<table>
<thead>
<tr>
<th>Transport network management</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Air</strong></td>
<td>Air traffic control systems (proximity avoidance, satellite-based ATC), whole-network interactive management</td>
</tr>
<tr>
<td></td>
<td>Weather information and forecasting</td>
</tr>
<tr>
<td><strong>Road</strong></td>
<td>Traffic signals, speed limits, ramp access metering, Lane control, predictive congestion modelling, track and trace systems.</td>
</tr>
<tr>
<td></td>
<td>Networks of sensors (vehicle-based, road-based, mobile devices, NFCs</td>
</tr>
<tr>
<td></td>
<td>Centralised, decentralised (vehicle operator, passenger) or P2P self-organising control</td>
</tr>
<tr>
<td><strong>Maritime</strong></td>
<td>Anti-collision systems, load management, scheduling, routing applications</td>
</tr>
<tr>
<td></td>
<td>New forms of shipping contract and insurance</td>
</tr>
<tr>
<td></td>
<td>Weather information and forecasting</td>
</tr>
<tr>
<td><strong>Intermodal</strong></td>
<td>Multi-mode scheduling and real-time information</td>
</tr>
<tr>
<td></td>
<td>Combined freight/passenger management</td>
</tr>
<tr>
<td></td>
<td>Load management with mix of book-ahead and ad hoc booking.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traveller and shipper information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(Historical, real-time and predictive) traffic condition, public transport departure/transit/arrival, weather.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Mutual location and transit information (for real-time travel coordination)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Displays (e.g. radio, road signs, web, text, NFC)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Mobile devices (as sensors, actuators and communications devices; includes vehicles as mobile devices and mobile device plug-ins to vehicles)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Travel decision support and automation systems for e.g. routing, charging, emergency service access.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Important (and appropriate shaped) real-time information, mashed up with personal information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Support range of vehicle configurations: platforms (on which apps run), identity (SIM), wireless/IoT</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Variable spectrum/system capacity allocation geometry (e.g. in case of accident or emergency)</strong></td>
<td></td>
</tr>
</tbody>
</table>
52

### In-vehicle

<table>
<thead>
<tr>
<th>Applications</th>
<th>Speed (adaptive cruise control), electronic stability control, lane departure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation</td>
<td>Individual; cooperative; centralised; self-organising (vehicles, traffic lights)</td>
</tr>
<tr>
<td>Nodes</td>
<td>Apps, plug-ins, (semi) autonomous vehicles (already in air, maritime and port use)</td>
</tr>
</tbody>
</table>

### Charging and payment

- Public transport, e-tolling (with ANPRS), parking and taxi payment
- Road use charges (location, traffic sensitive)

### Future infrastructure and network

- Use data from above applications (and other sensor and NFC devices) to model and simulate individual and systemic behaviour; signal need for road and bridge maintenance; integrate with planning

These are not wholly new issues. To determine the scope for Internet-readiness, it is necessary to identify the existing policy settings; the associated policy objectives and goals of intervention; and the relevant policy instruments.

#### 4.3.2. Policy Setting and Priorities

The issues themselves represent well-recognised and interconnected challenges for the transport domain. As such these issues have been tackled in a variety of settings. While most of these – as noted above – are not explicitly legislative or regulatory, they do have (distinct) legislative footprints or will have as they mature. To fix ideas and provide examples used in the following discussion, we mention only three:

- ITS;
- Smart Cities; and
- Industry groups (e.g. ECR).

Each of these contributes to a range of external priorities to a greater or lesser extent: economic growth; value for money; safety; environment; security and amenity. These shared priorities can serve as a basis for initial coordination among transport initiatives, between transport and other policy domains and between government, private and civil society bodies.

Using ITS, Smart Cities and Industry Groups as a touchstone for Internet-awareness priorities in the transport domain, our interviewees identified a number of specific priorities that help to link transport policy issues to the wider goals of economic, environmental and social benefits:

- Effectiveness (timely, affordable passenger/freight mobility) can be improved by traffic management systems (centralised or decentralised) to improve reliability and throughput times, reduce transit time variance and cost, keep passengers and shippers informed and facilitate new forms of transport payment;
- Infrastructure cost/performance can be enhanced by *ICT-based (pro)active demand and supply management* when it is used to improve utilisation of existing infrastructure, reduce peak-load and accident 'slack', thus reducing or delaying infrastructure upgrade investments;

- Future-scoping can be ensured by use of *real-time information* on events likely to affect networks (e.g. to prevent bunching), support for *self-organising or vehicle-to-vehicle (V2V)* solutions, lower costs and fairer allocation from ‘smart’ insurance and road charges and *data collection on individual and systemic behavioural responses* to incidents, policies, technologies and ‘knock-on’ locational effects; and

- Mitigation of adverse effects by e.g. reduced crashes through use of *on-board and V2V systems*, improved emergency response times from *enhanced automated communications (eCall); traffic management* to minimise speed variance and emissions and ‘*smart feedback*’ to tune driver behaviour and improve supply chain costs and other aspects of transport system performance.

*4.3.3. Instruments*

Finally, we note specific scope for action in terms of legal initiatives that can in principle be made ‘digital by design’ and which go beyond generic support via e.g. declarations of intent, procurement, R&D funding, adoption subsidies). The Digital by Design approach may entail modifying existing instruments (e.g. the ITS Directive) or creating new rules consistent with its principles (see Section 4.4.3) - it includes:

1. Removing existing barriers to transport-related ICT deployment
2. Opening markets e.g. by adapting antitrust and consumer protection rules (related to net neutrality) and/or mandating standards (e.g. a (road) vehicle standards map\(^\text{96}\));
3. Requiring adoption of specific features where there is clear public benefit e.g. extending the range of mandated automatic safety measures to include e.g. electronic stability control.
4. Modifications to make existing rules for e.g. charging (road use, congestion, emissions) ICT-friendly (by mandating information provision, or providing alternatives for self-documented use)
5. Legal frameworks for data collection, analysis and sharing from multiple sources; and
6. Impact assessment in relation to broad range of possible impacts

We are not calling directly for such actions – this is primarily a second-level Deep Dive: using ICTs to understand the origins and nature of a wicked problem (see discussion on page 19), rather than addressing an immediate problem or evaluating the case for laissez-faire or blue-sky possibilities.

However, the issue area has elements of both. This is important, because the Level 1 urgency of issues relating to transport (including the ‘sector-specific’ issues of managing congestion

---

\(^{96}\) A standards map is a device for providing ‘forward guidance’ to industry players. For example, The New Zealand Ministry of Transport and the NZ Transport Agency are developing a vehicle standards map as part of the Safer Journeys Action Plan for 2013-15. The map will “identify existing safety technologies, such as electronic stability control and eCall, and when they might be mandated in New Zealand”.

53
and supporting other economic societal and environmental goals (from current outcomes to sustainability) provides the political and commercial impetus for a range of actions and the allocation of considerable resources.

4.4. Drivers and constraints

4.4.1. Operational and Institutional Factors

From the interviews and desk research, it is possible to identify a range of factors that encouraged joint working and the introduction of ICTs into transport-related policy. These are briefly described below.

As noted, there were considerable early successes based in part on the fortuitous availability of motivated and capable individuals, the political salience of suitable issues and a simpler and more flexible working environment (with fewer individuals, more broadly defined responsibilities and lower levels of internal bureaucracy. Paradoxically, this early success made further progress more difficult, in at least three ways. First, it created expectations that attempts to tackle subsequent, more complex problems struggled to fulfil. Second, the policy actions taken to address specific problems (e.g. road safety) ran into diminishing returns. Finally, as noted in our interviews, the rotation system tended to prevent the formation of deep knowledge and rich organisational capital.

These changes were also affected by flows of responsibility and information within the hierarchies; in order to proceed, both the ‘bottom’ and the ‘top’ share a sense of the essence and the importance of the issue and of the relation between ICT and the associated transport issue on one side and among the various policy objectives (e.g. safety, environmental impact) on the other. Moreover, the process is strongly path-dependent; within the ITS ‘movement’ are a considerable number of past initiatives and legacy vehicles used to attain progress each of which contributes legacy momentum and inertia and brings with it a network of concerned personnel.

Another constraint noted by those interviewed arose from differences in maturity of understanding between ICT and transport sectors. These sectors had a different sense of ‘pace’ (e.g. the slow pace of change in automobile manufacturing and the durability of its products compared with the rapid pace of change and associated obsolescence in the ICT domain). Therefore, they tended to disagree about the relative importance of the benefits of technological possibility as compared to the costs of disruption of existing arrangements and about the likelihood that current developments would be rapidly adopted and adapted97.

Sometimes the mixture of different policy agendas (e.g. environment, economy, fuel prices) and sources of inertia (e.g. ‘sunk cost’ infrastructures and transport behaviour patterns (e.g. if you have a car, you will use it)) and the complexity of the processes and divergence of stakeholder interests lead to incoherence, fragmentation or frustrating delays. In some cases,

97 This does not imply that ‘faster change is better’ - investments in equipment and business process change required to exploit new technologies inevitably take time. Where consistent adoption of compatible approaches is critical (e.g. ICT systems embedded in automobiles that must communicate with third-party systems and applications), there may be excess volatility on the ICT side (to pursue first-mover advantage and lock in new standards) and excess inertia on the automobile side (to avoid stranded investments in a technical approach that may not survive).
progress could be compromised if personnel or policy priorities changed before policy could converge.

Some of the constraints were specific to the industry, e.g. the global nature of key parts of the industry (e.g. automobile design and manufacture, ICT suppliers) combined with the geographic localisation of physical transport. This in turn led to other complexities in terms of the need to manage local planning processes, to balance the needs of different parts of holistic initiatives (esp. for Smart Cities) and a lack of joined-up approaches to the ownership, completeness and modelling of relevant data.

Institutional attitudes and memory also played a specific role. In particular, over the long history of interactions, some long-time observers within DG MOVE saw a tendency to isolationism and a technology-driven perspective on the DG INFSO side.

Beyond the characteristics of individual Directorates-General, the proliferation of DGs and Commissioners was seen by those interviewed as contributing to the instability of partnering relations and to what those interviewed saw as a gradual loss of effectiveness in handling novel cross-cutting issues. Compared to their predecessors, the new entities had smaller remits and more cumbersome and slow policy processes. A consequence has been a greater need to ‘show impact’ and a shift from issue-motivated and visionary perspectives towards ministerial and politicised views extending down to desk officer level.

Perhaps for this reason, those interviewed agreed that collaboration was strongest on issues related to standardisation where ‘ownership’ was clearest (e.g. DG CONNECT handling spectrum).

Joint working on the basis of complementary competencies involves both shared resources and shared perspectives. Interviewees noted that, despite the growing importance and use of data resources, databases are not shared between the DGs.

Concerning perspectives, those interviewed from DG MOVE regarded their counterparts as overly technology-centred, to the deficit of business case identification. According to them, the business case perspective is not merely a way of thinking about industry players but also highlights the need for explicitly developing the EC’s business case for intervention– at least to the level of cost-benefit analysis.

In pursuing joint initiatives, especially in areas such as safety that have traditionally been of higher priority to DG MOVE – the value of simplicity was emphasised. Specific parameters (e.g. the value of a (statistical) life, the value of time) have been extensively studied, but revisiting these studies and the complex array of values they produce can easily lead to delays and complications. Therefore, common ‘reference’ values (e.g. the fixed figure of 1M€/life, or the threshold value of \(10^{-6}\) risk) may be useful if developed and maintained across DGs or at least within a DG as it pursues joint endeavours.

However, quantification should be appropriate and adjusted to the needs of the audience – this is particularly true where progress towards policy objectives (e.g. safety, environment) is costly to consumers. But apparent conflicts may be a matter of timing. For example, the costs of ecological improvements in transport equipment are coming down as fixed costs are amortised and marginal costs fall due to such factors as economies of scale or technological maturity. As noted in relation to the costs of consumer food-safety monitoring (see Section
3.4.2, esp. discussion on p. 50), the case for public intervention may shift as the cost barriers to effective action fall.

Interviewees also reinforced the findings from the workshops about the importance of sequencing policy interventions in the right way; tackling low-hanging fruit (obvious areas for intervention) may provide proof of concept and build confidence and trust, but can also lead to diminishing returns. Safety was cited as an example. Automotive death rates have been coming down for a range of reasons. This reduces the apparent importance of any improvements and leads to a bifurcation in policy objectives. On one side are cost-effectiveness improvements (reducing the costs of current levels of performance). On the other are visionary goals (e.g. zero risk, zero delays) that may not be attainable. This split may lead to misallocation of effort that weakens the internal case for joint activity.

This is not merely a matter of internal coordination. The public (and their representatives and Member State governments) also have preferences over policy areas (safety, environment) and types of goal (pragmatic or visionary). External pressure can help to raise awareness and maintain momentum, but will not make up for lack of individual ‘champions’ and the right mix of expertise. One cited instance of external pressure involved mandatory vehicle recalls – this policy instrument was urged on the EC from the outside and contributed to embedding safety as an important area of DG MOVE competence. It thus indirectly led to an enhanced potential for collaboration with DG CONNECT in the ITS context.

4.4.2. Key Relationships and Data Flows

Transport is itself a network industry. The connections between transport providers therefore manifest themselves as a deep set of connections between individuals and companies that constitute crucial communication networks. This network is critical in the provision of information (routing, pricing, time, scheduling, quality) that can strongly influence transport decisions ranging from the very short-term (journey timing and duration, individual modal choice) to the very long-term (infrastructure planning, land use policy).

In most situations, this impact of such networked communications is complementary – information can enhance the value of transport by magnifying the network externalities of transport – the more one party uses it, the more other parties will tend to use it.

However, the interrelation between partners in such a network also has the potential to lead to adverse effects on the market. Primarily, this Deep Dive foresees a danger of collusion (tacit or active) between the providers of given transport services. The recent trend toward price comparison, itself driven by the increasing release of open data intra-industry, has the potential to lead to ‘price normalisation’ as companies are able to quickly see their competitors’ price points and adjust fares accordingly. The problem with data-rich, Internet-aware industries such as transport is that such collusion is almost impossible to counteract, as it is asymptomatic at the policy level. The importance for ITS is that multi-modal transport systems do not converge to uniform pricing across the options available to users in the long-term.

A further consideration is the long-term effect of communications on the value proposition of the transport industry itself. It was broadly thought that communication could substitute
for transport. This principle was the thinking behind many e-work and telecommuting initiatives, and contributed greatly to at least the initial emergence and success of globalised production and distribution chains.

Both transport and communication networks share a set of common characteristics. These are consequences of their networked character and are well-known in the theoretical literature \(^{98}\); each of them was reinforced through our interviews:

- Structure (e.g. clustering, isolation, centrality) matters\(^ {99}\) as much as connectivity;
- The static or expected performance of a network is not the same as its resilience or robustness in the face of unexpected shocks;
- Networks tend to be regarded as shared ‘commons’ in that people come to rely on their existence and smooth functioning\(^ {100}\);
- The potential network (reachability) works in a different way than the actual network (flows through the network);
- Network externalities (the benefits or harms to others arising from joining or leaving a network) mean that self-organised network structures are rarely optimal;
- The dynamics of innovation on networks are likewise likely to be too fast or slow relative to the optimum;
- The behaviour of individuals and groups are affected by their network connections; conversely, the structure of networks (who is connected to whom) tends to be rewired in response to the behaviour of participants; and
- Networks contribute to tipping - the dominance of markets\(^ {101}\), information systems\(^ {102}\) or policy decisions\(^ {103}\) by one or a few firms, ideas and institutions.

On the other hand, the interconnection of different forms of transport network (e.g. passenger and freight, sharing infrastructures or merely hubs) and of communication and transport network leads to new complexities and to emergent behaviours.

This last is critical; emergent behaviour cannot be anticipated but can (to a degree) be predicted\(^ {104}\). Therefore,

- Any attempt to predict the behaviour of (part of) a complex system requires information about its performance in the past and in other parts;
- This prediction may be essentially imprecise – in other words, it may only be possible to say that some aspect will cycle, or that a period of increase will be followed by a

\(^{98}\) See e.g. Shy (2001), Goyal (2012), Katz and Shapiro (1994)

\(^{99}\) To the benefits of the network to society, to its ability to transmit or isolate unexpected events, to its vulnerability in the face of accident or attack.

\(^{100}\) In other words, even if people have not travelled to a particular destination before, they tend to rely on being able to reach it – this is important when trying to understand the prospects for cooperation or the extent of competition.

\(^{101}\) Katz and Shapiro (1994).

\(^{102}\) Galeotti and Goyal (2010).

\(^{103}\) Vedres and Scotti (2012).

\(^{104}\) Ball, Diakonova and Mackay (2010).
downturn, but not to say with certainty how the cycle will unfold, or when the turning point will come;

- Therefore, policy must be approximate (not sensitive to unpredictably precise information), adaptive and self-monitoring.

On the other hand, transport and communications are not the same kind of network; cost structure, accessibility, the level at which different decisions are made, and the permanence of investments and business models are very different. Therefore, their interactions are crucial, whether they arise within organisations (e.g. the ‘smart transport’ solutions developed by Efficient Consumer Response\(^\text{105}\)) or from the interaction of different parties operating over a common infrastructure.

Finally, each type of network contributes directly to the other. For instance, road and traffic sensors form increasingly important parts of the data traffic generated by the Internet of Things while transport infrastructures (e.g. rail lines) lower the costs of long-distance communications networks\(^\text{106}\)

As a result of these complexities, by and large policy has not managed to understand or predict the need for and interactions of transport networks, so a better understanding of the influence of different forms of) information on the full range of transport choices and their systemic implications is required.

Conversely, transport – or at least the availability of transport networks and systems – can influence the availability, exchange and analysis of information. For example, the availability of affordable transport links to urban clusters changes both the extent of interpersonal communication and the commercial viability of investments in enhanced ICT facilities (e.g. fibre rings and data centres)\(^\text{107}\). This is particularly important in respect of ICT-based industries, which paradoxically depend on the close physical proximity of a critical mass and a critical range of individuals\(^\text{108}\). This does not, of course, mean that these individuals will follow the classical patterns of living in the suburbs and commuting to the cities to work; recent examples involve reverse commuting and sustainability enhancements.

These complex interactions raise a wide range of issues. Some idea of the unanswered questions can be gained by considering the issue of congestion (noting that similar arguments could be made regarding pollution, safety, and other concerns).

Because transport flows (both passenger and freight) share many of the same networks, congestion is a permanent problem. Where routes and timing are dictated by outside factors

---

\(^{105}\) See footnote Error! Bookmark not defined.

\(^{106}\) A more transitory example is provided by the recent growth in physical transport of large data uploads to cloud computing data centres (examples include major players such as Amazon, Google and Microsoft and new players such as Dollydrive). See e.g. NetWorkWorld (2010).

\(^{107}\) Although ICTs were originally seen as contributing to the “Death of Distance” (Cairncross 2001) economic agglomeration and clustering have not disappeared; rather, they have been reinforced by economies of scale and co-location into strong (e.g. rural-urban) divides. Even the shape of cities (e.g. extent of urban sprawl) is responding because the ‘gravitational pulls’ of transport and of communications are different. See e.g. i) Shieh and Searle (2013); ii) Marsal-Llacuna, Colomer-Llinàs and Meléndez-Frigola (2014); and iii) Gupta, Roy and Sarkar (2013).

\(^{108}\) This is exemplified by the classical “Silicon Valley model” and by the initiation and (uncertain) dynamics of ICT-based clusters in Europe.
or driven by non-interactive and non-real-time information) these problems may be more or less predictable (e.g. rush hours). Nonetheless the decentralised and uncoordinated nature of individual decisions means that accurate information alone will not resolve the problem.

In other cases, congestion arises from the complexity of the network and the lack of suitable information (e.g. knock-on effects of weather incidents, traffic accidents) and is not predictable.

Even where information does not allow individuals to adjust their journeys, it can help them to cope with unavoidable delays and contribute to a sense of being kept informed that can make them feel better off.

Some decisions are not so centralised – e.g. public transport and aggregative freight logistics. Nonetheless, there is often an element of individual choice and potential coordination failure at some part of the value chain (e.g. individual drivers or passengers) and a high degree of feedback from both experience and policy (price and schedule decisions, traffic management practices) which complicates planning even at the systemic level. In other words, flows though the network self-organise in response to information from a range of sources. These changes quickly become locked in by e.g. residential and business locational decisions, scheduling of meetings, deliveries and other flows involving multiple users and ‘predict and provide’ policies designed to mitigate specific problems associated with current traffic patterns.

To identify the current and potential points of traction for Internet-ready policy processes, it is useful to consider both the policy stakeholders and the transport network participant value chains.

Figure 4-2: Policy stakeholders
Figure 4-3: Policy-relevant transport player relationships

At a finer level of disaggregation, there are a range of interactions – both current and potential – that operate along the transport value chain. They are also different depending on the policy context e.g. Smart Cities, ITS, ECR. For this reason, we do not describe a generic map. But certain characteristics can be identified and used in building up such a map.

For example, a multi-modal ICT-enhanced Freight value chain is:

- Not always distinct from value chains of sector whose goods are shipped;
- Likely to extend up- and down-stream (e.g. vehicle manufacturers, fuel suppliers, warehouse/distribution) and to connect to existing ICT value chains;
- Strongly connected to existing logistic chains – and to their industry and policy stakeholders;
- Primarily relevant to the near term (“From smart transport to intelligent motion”) issue; and
- Not as integrated and organic as e.g. food value chains (due to need to share infrastructures and variety of ownership/management models (from in-house fleet through to FOB shipping with all decisions delegated to shipper).

The decisions made by key participants and the need to collect and exchange information will not be constant along the chain, but instead will vary with organisation, the extent to which transport networks are shared with other (types of) users and the nature of the contracts between participants.

Therefore, both policy modelling and policy itself must look beyond traffic levels
4.4.3. Principles Referred to in the Legal Instruments

The starting points are four aspects used to assess Internet-readiness. Because these are meant to form a common part of the toolkit, in this section we link them to references in the principle existing legislation – the ITS Directive. The four aspects are:

1. The ability to mandate or implement common definitions, principles, requirements and procedures;
2. Scope to adopt a broad definition of relevant information, sources and ‘target audiences’;
3. Sufficient flexibility to be able to keep up to date with new information requirements of consumers and other key stakeholders (e.g. smart infrastructures, smart vehicles, information to/from shippers, utility operators, environmental/weather monitors); and
4. Neutrality across different channels (e.g. freight vs. passenger, public vs. private transport, on-board vs. centralised systems (note that – for environmental and societal objectives, consistent with the “Smart Urbanisation” issue - it may be desirable in formulating policy options to tip the playing field by giving public transport users enhanced information and planning functionality).

The following extracts drawn from the ITS directive link these aspects of Internet-readiness to successful operation of ITSs. These excerpts (emphasis added) further indicate the advances that have already been made in current guidance toward a more robust and Internet-aware policy process:

- “(3) Intelligent Transport Systems (ITS) are advanced applications which without embodying intelligence as such aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated and ‘smarter’ use of transport networks.”
  
  Note: This covers the main objectives listed above, but explicitly stops short of embracing the full potential of a network of semi-autonomous interacting systems. It thus creates a platform on which the potential for “intelligent motion” could be realised but places pilot implementations outside the Directive. It is thus consistent with aspects I and IV, but may raise problems in relation to II and III.

- “(4) ITS integrate telecommunications, electronics and information technologies with transport engineering in order to plan, design, operate, maintain and manage transport systems. The application of information and communication technologies to the road transport sector and its interfaces with other modes of transport will make a significant contribution to improving environmental performance, efficiency, including energy efficiency, safety and security of road transport, including the transport of dangerous goods, public security and passenger and freight mobility, whilst at the same time ensuring the functioning of the internal market as well as increased levels of competitiveness and employment. However, ITS applications should be without prejudice to matters concerning national security or which are necessary in the interest of defence.”

“(5) Advances in the field of the application of information and communication technologies to other modes of transport should now be reflected in developments in the road transport sector, in particular with a view to ensuring higher levels of integration between road transport and other modes of transport.”

“(11) ITS should build on interoperable systems which are based on open and public standards and available on a non-discriminatory basis to all application and service suppliers and users.”

“(18) Major stakeholders such as ITS service providers, associations of ITS users, transport and facilities operators, representatives of the manufacturing industry, social partners, professional associations and local authorities should have the possibility to advise the Commission on the commercial and technical aspects of the deployment of ITS within the Union.”

These principles cover the full scope of aspects 1-4 (page 78), especially as regards flexibility, future-proofness, balancing objectives and stakeholder interests and intermodality. Other sections (12-14) cover specific issues – already well-developed in the ICT domain – that may assume special significance in transport applications – anonymisation and privacy (the distinction between public and private values of transport-related information) and reuse of information held by the public sector. As befits the fundamental uncertainties regarding behaviour reflected in the issue statement, section 17 makes explicit provision for RTD and the exploratory use of information generated by ITS.

Furthermore, the Directive specifically emphasises the importance of making data available to the public in open formats. Many of the Priority actions (Article 3) in effect make it compulsory for public bodies to share transport, road and traffic data, both static and real-time, that they already hold – though it does not mandate the collection of additional data by public bodies.

The legal basis for addressing the issues identified is further strengthened in Annex II, which says:

“The adoption of specifications, the issuing of mandates for standards and the selection and deployment of ITS applications and services shall be based upon an evaluation of needs involving all relevant stakeholders, and shall comply with the following principles. These measures shall:

(a) Be effective – make a tangible contribution towards solving the key challenges affecting road transport in Europe (e.g. reducing congestion, lowering of emissions, improving energy efficiency, attaining higher levels of safety and security including vulnerable road users);

(b) Be cost-efficient – optimise the ratio of costs in relation to output with regard to meeting objectives;

(c) Be proportionate – provide, where appropriate, for different levels of achievable service quality and deployment, taking into account the local, regional, national and European specificities;

(d) Support continuity of services – ensure seamless services across the Union, in particular on the trans-European network, and where possible at its external borders, when ITS services are deployed. Continuity of services should be
ensured at a level adapted to the characteristics of the transport networks linking countries with countries, and where appropriate, regions with regions and cities with rural areas;

(e) Deliver interoperability – ensure that systems and the underlying business processes have the capacity to exchange data and to share information and knowledge to enable effective ITS service delivery;

(f) Support backward compatibility – ensure, where appropriate, the capability for ITS systems to work with existing systems that share a common purpose, without hindering the development of new technologies;

(g) Respect existing national infrastructure and network characteristics – take into account the inherent differences in the transport network characteristics, in particular in the sizes of the traffic volumes and in road weather conditions;

(h) Promote equality of access – do not impede or discriminate against access to ITS applications and services by vulnerable road users;

(i) Support maturity – demonstrate, after appropriate risk assessment, the robustness of innovative ITS systems, through a sufficient level of technical development and operational exploitation;

(j) Deliver quality of timing and positioning – use of satellite-based infrastructures, or any technology providing equivalent levels of precision for the purposes of ITS applications and services that require global, continuous, accurate and guaranteed timing and positioning services;

(k) Facilitate inter-modality – take into account the coordination of various modes of transport, where appropriate, when deploying ITS;

(l) Respect coherence – take into account existing Union rules, policies and activities which are relevant in the field of ITS, in particular in the field of standardisation.”

These principles establish an Internet ready basis for the transport area, by permissively including the most relevant of current ICT approaches without ruling out new ones, establishing a functional rather than a technology-specific foundation for initiatives and explicitly allowing the cooperation of a broad range of relevant stakeholders.

4.5. Baseline – Institutional Context of Transport Policy Processes

This section discusses the historical and institutional features affecting the Internet readiness of the transport area – specifically the legacy context within which cooperation between DG MOVE and DG CONNECT must develop. For transport, the current state of play is strongly affected by the personal legacy of specific issues, especially the relation between the objectives, tools and networks that focus on the environment, transport system capacity and safety. The present relations are also coloured by the heritage role and vision of specific individuals in DG 7/MOVE and DG 13/INFSO/CONNECT. As mentioned, much early progress was attributed at least in part to the fortuitous co-location of logistics, policy and research functions in a single unit, the presence in those units of a range of disciplines and
skills and the associated variety of external connections, bringing the influence of/ opportunity to engage with rest of the world.

The rotation system is seen to work against the development of trust between individuals and the acquisition of knowledge and understanding by individuals. A potential solution is a 'smart rotation system' organised along thematic and topical lines. This requires a conscious choice between sharing knowledge and deepening the expertise and experience of specific individuals.

This has HR/career implications as well – for example, the possibility of a cadre of experts alongside the fonctionnaires. The former might better be able to engage with external (e.g. industry) stakeholders, especially in the context of shared governance (e.g. standards body participation, self-regulation).

Moreover, rotational changes at the top can weaken the level of support from management and the discretion or 'space' given individuals to follow good ideas and/or work with external stakeholders.

Some issues and initiatives are more suited to joint work than others – especially: a) standardisation initiatives where the roles of the DGs are clearly separated and b) holistic ones where the contributions of different perspectives are clearly complementary. An example of the latter is provided by Smart Cities, though it is interesting to note that DG MOVE expressed less confidence in the strength and momentum of that initiative, at least in its interim phases.

In this respect, the interviewees recognised the value of DG CONNECT's perspective – that ICTs are general purpose technologies (which can be modularised and re-used for different purposes) and that they can be provided over common service platforms. On the other hand, the reuse of ICT tools and instruments has not always generated 'feedback learning' into DG CONNECT or (in the case of holistic initiatives) between the other external DGs (e.g. between ENER and MOVE). It was hoped that DG CONNECT could serve as a platform or connector for this kind of knowledge sharing. Examples included security (of networked systems).

To further reinforce this 'balanced' approach, it is necessary to involve a range of disciplines (economists and lawyers were particularly mentioned).

The ITS 'community' has other striking features, notably the prominence of women in their 40s and of individuals with PhDs in a range of disciplines. This may reflect the holistic and visionary nature of the stakeholders attracted to the issue area; conversely, it is regarded as influential in the growth of ITS. The baseline activity (research, exploration of deeper implications) has begun to take off, but concrete progress is still held back by governance and liability issues.

The role of research and innovation is increasingly seen as important; whether this comes from having units with a mixed portfolio or by the inclusion of suitable external partners (e.g. DG RTD or JRC). Therefore, in areas that have broader implications or where fundamental scientific (social-scientific) uncertainty remains, three-way partnerships or diversified DG teams are useful.
Initiating contact can be easy, where the organisation chart or responsibility for relevant portfolios enables identification of counterparties.

4.6. Nature of the challenge

One challenge that was noted on both ‘sides’ was the best way to recapture the entrepreneurial and mission-driven spirit behind past successes, which involves bringing together a diverse range of individuals in a collegial context, and providing them with a degree of discretion provided the initiatives on which they proposed to work could pass a business case test.

Another challenge concerned the collection and use of information. This involves shared databases and modelling resources, but also means careful attention to information framing and exchange. This framing may entail e.g. strategic choice of a fixed values for key parameters (e.g. 1M€ for a human life r fixed value per minute for time savings) or agreement to include or exclude specific impacts (e.g. insurance, location of economic activity, impact on property prices and housing) from explicit consideration.

This knowledge sharing may be particularly important and viable in the face of ‘wicked problems’\(^{110}\) that have resisted prior (often parochial) efforts at solution.

To sustain effective cooperation, there seems to be a case for a “durable intersection” within which individuals can specialise and cross-fertilise, and where appropriate joint specialisations can develop. This can also counteract the impression of an overemphasis on technological possibilities from the DG CONNECT side and consequent neglect of other considerations (including business cases).

The nature and importance of attaching a clear business case to a policy initiative varies by the sector affected – some are far less willing to innovate than others.

The multi stakeholder perspectives on external engagement are necessary to balance or prioritise objectives. For instance, according to the DG MOVE interviewees, automobile manufacturers cited consumer protection as a reason to raise the threshold for crashworthiness from 4* to 5*, even though there was little evidence that consumers valued this highly. In the EcoSearch case, something similar was observed – price premia for higher-rated appliances typically exceeded energy cost savings by a wide margin (merit goods). In this sense, the different DGs can usefully work together to a) ensure a balance of external stakeholder views, b) collect and share the necessary data (e.g. on willingness-to-pay for specific improvements) and c) insist on the testing of policy options against such evidence.

Beyond these operational challenges, there are a range of specific policy issues arising from the convergence of transport and ICT which are likely to be picked up by the actions recommended in this document. While our task was not to catalogue or even to précis the range of such issues, it may be useful - briefly and by way of example – an area in which the need better to model and understand individual and system behaviour is particularly acute.

\(^{110}\) See discussion on page 1.
Data collection, sharing, data privacy and data security

There is already considerable data collection and (limited) sharing among a range of government agencies, extending under some circumstances to private sector data controllers and processors. At the same time, there is growing recognition that neither individual nor institutional behaviour in response to evolving privacy landscapes fits the rational behaviour and informed consent assumptions underlying much existing policy. Therefore, inferences drawn from revealed preference (actual behaviour), stated preference (privacy and security experiments) and participation in consultative processes may lead to very different conclusions, and may not reflect actual outcomes. This is particularly relevant to transport, in view of the very different privacy expectations associated with different modes and the wide range of privacy concerns raised by existing and emergent new ITS technologies. It leads to three broad areas of potential concern.

Privacy: Many of these data are already covered by privacy rules but others are not, often because under existing technologies they do not constitute protected personal data. However, new technologies can – and increasingly will – change both the status of these data and the extent to which individual interests are affected, individual control is feasible and the balance between individual and collective interests is struck. For instance, Article 20 of the "General Data Protection Regulation" concerns immunity from automated profiling except under specified circumstances. It is conceivable that this may affect future applications of e.g. ANPRS systems (which already permit the automated and undetected identification of vehicles) combined with CCTV and face recognition software, especially if cross-linked to other individual data. However, such cross-linking could conceivably be necessary in order to model and understand the behaviour of drivers and the extent to which it can be explained by other attributes, even if ‘measures’ such as personalised traffic management are not implemented. The ITS Directive currently indicates that such issues should be referred to the Article 29 Working Party (par. (13)).

Data sharing: A related issue concerns the sharing of data across agencies and other bodies. This area involves the Data Protection rules (the proposed Regulation and other existing or proposed measures) but also provisions for the re-use of public information. This may become more important as new ICT-enabled services are deployed, particularly when provided by third parties and/or based on sensor-derived information. Such ‘wider

---

111 A possible action point emerging in this area would be to establish a working group sponsored jointly by DG MOVE and CONNECT, but also including European Parliament representation (esp. IMCO, ITRE, JURI and EMPL), the Article 29 Working Party and the Interoperability Solutions for European Public Administrations programme (ISA) to examine both the General Data Protection Regulation and the European Interoperability Framework for Internet-ready opportunities and challenges.

112 E.g. in the increasing interest in behavioural economics as an adjunct to policymaking. See e.g. [http://ec.europa.eu/consumers/behavioural_economics/index_en.htm](http://ec.europa.eu/consumers/behavioural_economics/index_en.htm).

113 See e.g. Cave et al. (2011) and Cave et al. (2012).

114 This proposed Regulation (European Commission 2012) is intended to replace the existing Directive (European Commission 2002).

115 Presumably, no issues arise when the transport data are anonymised instead of cross-linked and cross-linked on a locational rather than an individual basis.

deployment’ may be controlled by explicit contracts and delegated compliance with applicable rules, but this may be harder to enforce (and more costly in terms of innovation) when such information is made available to the public at large for use in app development, data-mashing and other information intermediary functions. Within the government itself, concerns may be raised regarding the exchange of identified traffic data with other agencies\textsuperscript{117}. On the external level (between similar agencies in other jurisdictions) such exchanges are well-established across a range of transport modes (esp. air and maritime) and policy areas (esp. migration, law enforcement and taxation); most of the relevant instruments make at least some provision for automated collection and sharing of specific types of data. Data exchanges within administrations have also been studied extensively; the European Interoperability Framework\textsuperscript{118} lays down extensive and explicitly Internet-ready provisions for exchanges of such data; it was later adopted in conjunction with the ISA Programme as Annex II - EIF (European Interoperability Framework) of the Communication “Towards interoperability for European public services” on the 16th of December 2010\textsuperscript{119}.

The Underlying Principles forming Chapter 2 of the EIF are fully consistent with the four criteria for Internet-readiness. However, the modest level of recent activity under the Interoperability Solutions for European Public Administrations Programme (ISA), the growth of new tools for data sharing and collective modelling and the overall recommendation in this Report for much richer information collection and joint exploitation in order to put all legislation an Internet-Ready footing suggest that more needs to be done.

Security: The third issue concerns the security of transport-related data and the impact of data collection and use on the security of the transport network itself. From the policy perspective, the latter is covered by Priority III of the ITS Directive. However, a common policy approach to the security of transport-related data is less developed.

The advent of new technologies such as big data analytics, combined with the data mobility, processing and long data storage, curation capabilities of cloud-based data repositories, may lead to conflicts among network safety and management, security and privacy. Each of these domains has its own well-established legal and governance frameworks, and each has some provision for balancing the needs of other domains. However, this situation is far from Internet-ready:

- Existing arrangements were predicated on the capabilities, costs and benefits associated with existing technologies – as new technologies appear, the appropriate trade-offs may shift; and
- Data collection, analysis and sharing reflect existing arrangements (e.g. different organisations tend to collect, analyse and share data in ways that relate to their current

\textsuperscript{117} Scott, Thuemmler and Uthmani (2010) describes a communication infrastructure that allows Data Protection-compliant information sharing by design.

\textsuperscript{118} See http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529. This was developed by the “Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens” (IDABC) programme, which ended in 2009.

\textsuperscript{119} European Commission (2010c) - this established the successor programme to the IDABC, known as Interoperability Solutions for European Public Administrations (ISA) – see http://ec.europa.eu/isa/. [However, the programme does not appear to be very active]
responsibilities – changes that imply a shift in these responsibilities may not be picked up\textsuperscript{120}.

4.7. Deep Dive Conclusions

The Transport Deep Dive has provided a highly illustrative example for the team of a field where the potential Internet-awareness issues undoubtedly latent within the domain are not yet at the level of ‘challenges’. The approach the team has taken, in line with Level 2, is to forecast the typology and general nature of potential issues for the future and make a series of concrete recommendations based on the framework and capabilities of the toolkit found in section 6 of this document:

4.7.1. Current Situation

The following presents in summary form our conclusions about the current state of the transport field with reference to the regulatory environment and particularly Internet-readiness issues:

- Transport is a mature regulatory domain with a strong set of policies governing the physical operation of all sectors;
- Policy objectives have successfully been transitioned away from purely ‘pragmatic’ legislation to improve operations toward a broadly sustainable goal of economically, environmentally and socially productive systems;
- The tension between pragmatic and visionary goals has led to some fragmentation of perspectives;
- Progress towards some goals (e.g. safety) across a broad range of areas has reduced the perceived importance of further incremental progress;
- Some policy instruments (e.g. mandatory recalls) have originated outside government;
- Data capture has increased exponentially across the transport sector;
- Certain industry sectors such as airlines have led the way in the release of their data, primarily driven by positive commercial factors;
- Other industry sectors such as railways and roads have been slower to release data because of geographic limitations and a lack of proper commercial/policy incentive; and
- A common reference framework is available through Geographic Information (GI) and Resource Description Framework (RDF) to render data interoperable.

These conclusions indicate that progress is being made on a number of fronts from the technical to the operational, but also that they are not being uniformly translated into practice or keeping pace with the increasing potential for truly Internet ready policy.

\textsuperscript{120} For example, traffic flow information relating to central management of signals may not pick up patterns of systemic response that could support a more decentralised organisation of flow control. See e.g. Helbing, Siegmeier and Lämmer (2013).
4.7.2. Opportunities for Internet–Aware Transport Legislation

The team through our interviews has identified opportunities exist for improving the operation of the transport field, in particular ITS, through advance considerations of Internet-aware policy:

- Integrated Transport Systems offer the potential to achieve major operational, environmental and economic benefits – existing transport rules could be examined for compatibility with the ITS Directive;
- Cross-sectoral regulations and policies can stimulate and lead the integration process through a data-driven approach – this requires greater use of shared data and integrated (especially intermodal and behavioural) modelling in formulating and implementing integrated transport policy; and
- Transport policy can be made Internet-aware at the trans-national level in advance to prevent possible challenges.

As befits a Level 2 Deep Dive, these opportunities are not concrete recommendations; the ITS programme is well under way and the basic enabling legislation is in place. However, some advance cooperation and shared modelling could help ensure that the potential offered by this promising beginning is effectively translated into practice, since truly integrated and 'smart' transport policy has yet to be achieved.

4.7.3. Possible Internet–Readiness Issues

The team drew a number of specific conclusions from consultation with transport experts. Chief among these conclusions was that, in the context of a Level 2 Deep Dive, the Internet readiness issues affecting transport have yet to become full-scale challenges. As a result and taking into account the emergent nature of Internet readiness challenges as experienced through the Level 1 (food) Deep Dive, it would be premature and potentially misleading to draw firm conclusions on the challenges that will arise in the future. Nevertheless, the team have identified from the experts and our research a number of possible issues with the potential to develop into policy challenges:

- The prevalence of proprietary formats may create problems for consumer protection and access particularly in areas like rail, which increasingly cross national boundaries;
- Growing information sharing across industries has the potential to reinforce tacit collusion or ‘price convergence’ among different multi-modal options in ITS. The competitiveness of such systems must be closely monitored to ensure that pricing for ITS modes remains relationship-independent as has been seen for example with high-speed rail alternatives to air travel;
- Greater opportunities to integrate safety data across networks could be missed without advance policy intervention at the European level;
- Integration of transport data with geographic information (GI) formats such as INSPIRE is critical to developing a common data framework;
- The growing importance of environmental performance must be built into the data gathering and publication practices of the different industry sectors to safeguard accountability and transparency and ensure alignment of internal and external priorities;
• ‘Smart’ policy requires Internet-aware transport policy to effectively integrate in wider management systems; and
• Policy for network industries may need to be approximate (e.g. principles-based or guidelines rather than precise rules) and bounded by the availability of information necessary to predict emergent behaviours (e.g. the partial unpredictability of network users’ behaviour and response to information).

These issues are already to some extent recognised within the policy research community, but policy in many parts of the transport value network is still largely reactive and selective as regards safety, environmental and economic objectives. Therefore, there is scope for ‘collective re-imagination’ of transport policy by multiple DGs and between the policy, industry, civil society and research communities.

4.7.4. Concrete Recommendations for Policymakers

Throughout the process of the Deep Dive into transport, the team has been conscious of the way in which our toolkit can be best applied to the policy domain. Having closely mapped the potential ‘pressure points’ for Internet-readiness issues noted in 4.7.3 to the OptICTs toolkit outlined in section 6, the team has produced for the reader a number of beneficial actions that we feel would advance the Internet-awareness of policy actions with respect to transport. Again the following should not be treated as an exhaustive or even necessary list but rather as a set of recommendations that will provide a useful jumping off point for inter-agency working in the field:

• Use stakeholder mapping tool (see toolkit section) to map policy stakeholders at the European level first at the sector level (rail policy, road safety policy, airline policy, GI policy, Freight Policy, Maritime Policy) and second at the inter-sectoral level;
• Establish a common baseline for policy analysis that a) ensures a balance of external stakeholder views, b) collects and shares necessary data (e.g. on willingness-to-pay for specific improvements) and c) insists on testing policy options against such evidence;
• Create a horizon-scanning network (see toolkit section) of senior figures from the relevant sectoral bodies at the European level (such as EAFDM121 & EASA122 for airlines, ERA123 for rail, ERSO124 for Road Safety, TEN-T125, DG MOVE, ERTICO126 overall) to forecast pressure points for interoperability and alert policy teams in advance of issues;
• Establish common facilities, allocate resources and provide legal and administrative frameworks to support the on-going collection and curation of a range of unstructured data, the collective development and use of analytic procedures (including big data analytics and visualisation) modelling and simulation/scenario exploration to serve as platforms for coordination and shared policy processes;

122 http://www.easa.eu.int/.
126 http://www.ertico.com/about-ertico/.
• Create an issue alert flow that periodically harvests outstanding issues from all mapped stakeholders through enquiries and collates results for analysis by relevant senior figures in DG Move/Energy/Connect
• Implement procedures for classifying alerts for immediate, delayed, monitoring, referral or no further action and for identifying the stakeholders, systems and policy objectives involved (in order to identify potential synergies or conflicts when setting priorities; and
• Jointly conduct ongoing Regulatory reviews to identify aspects that might encourage, inhibit, or 'shape' the introduction and impacts of ICT-related development (in transport)\textsuperscript{127}.

\textsuperscript{127} Such reviews would have two complementary and simultaneous aspects. The first is to examine the degree to which existing regulations embed potentially obsolete behavioural assumptions that might need to be updated in view of new technological, communication and information capabilities. The second is to consider – across a range of regulations – synergies, conflicts and gaps relating to a range of specific issues. Horizon scanning itself will progressively refine both of these aspects.
5.1. Overview

Cybersecurity has been selected as the third Deep Dive in order to show a slightly different perspective on Internet-readiness in EU policymaking. This case shows that a tendency for intervention that we see emerging in ICT policies may need to be reassessed.

The ability to trust the networks that enable today's information economy is a paramount consideration for policymakers. Information flows generated by and driven through ICT are necessary for the functioning of today's interconnected society; stability of these flows needs to be protected in order to ensure that the digital component of economic and societal growth is not hindered in any way. Securing the movement of information across the network is not an easy task, as it forces us to reassess our very understanding of how we treat the data that flow along these critical infrastructures.

In the light of the transnational nature of cyberspace, the Internet has often defied many of the classic conceptions of 'public space' applied to other areas of communication and exchange. This is as much because the polis to which the Internet belongs remains global, placing security online outside the effective reach and remit of national actors. Despite such difficulties in regulation, Cybersecurity remains a top priority for Europe and the EC. Unlike the other Deep Dives conducted by this study, Cybersecurity cannot truly be spoken of as an 'Internet awareness' issue because unlike food or transport, policymakers are without a 'roadmap' of physical market conditions on which to replicate their preferred online environment. Instead Cybersecurity is a uniquely online issue that presents a unique challenge to the policy community.

A further source of difficulty in Cybersecurity policy is the behaviour of those who attempt to circumvent regulations be they national governments or criminal gangs. Cybersecurity has an observable and close correlation between the behaviour of policymakers and the behaviour of criminals. For this reason, policy must be considered carefully before it is enacted because, like pressing down on a half-inflated balloon, the only effect of prohibitive policies will be to 'push' the criminals into new fields that the policymakers are unaware of.

Cybersecurity – even more than food or transport - has been a topic for a diverse range of policy actors, all appearing to treat the issue in the context of their own specific policy domain with little operational interaction. In this context, the cybersecurity Deep Dive assesses the capacity of DG CONNECT to interact with other DGs in a field that is primarily concerned with communications and networked technology (i.e. where DG CONNECT has a natural predisposition to lead policy development). It provides an apposite opposite to the
other two Deep Dives, which concentrate on the role that DG CONNECT can play in supporting policy development led by other DGs.

Cybersecurity contains a few key areas of policy sector interaction that may not – at first glance – be self-evident. As more services and appliances are connected to the open Internet, the need for security and stability of the network arises; concomitantly, the need for user awareness and self-maintenance of security is necessary. Connection to the Internet also implies that national or even supranational control over these issues of security and stability are no longer assured. Similarly, policies that can seem to be logical responses to technological development, such as encouraging the release of public data (such as transport information) are potentially counterproductive if not dealt with in accordance with respect for legacy challenges and market dominance. Finally, the Internet’s domain naming system is regulated and governed outside of the EU’s jurisdiction. Thus, adequate global governance mechanisms need to be in place in order to ensure stability of this system.

Cybersecurity is an exceptionally broad area that covers every aspect of online behaviour. For the purpose of this Deep Dive, the team have constrained our examination of cybersecurity to three concrete challenges: 1) privacy and cybersecurity, 2) critical information infrastructure protection, and 3) global Internet governance (in the narrow sense relating to domain name and technical standards governance). Each focus area provides an opportunity to examine a different potential for optimising the role of policymaking in the domain and provide illustrative examples for the reader surrounding the application of our toolkit. Additionally, each focus area lends itself to a discussion on the role of different stakeholders.

The challenge areas selected by the team are also in closed conformity both with the views of our interviewees and the typology of issues outlined in current literature. The Internet is currently governed through many different policies and practices trying to adapt to the Internet environment (Dutton, Dopatka, Law, & Nash, 2011; Mueller, 2010). William Dutton and Malcolm Peltu (2007) offer a useful categorization of Internet governance issues, which are useful in helping determine the activities and structure of the discussion on global Internet policy issues. They divide these issues into Internet centric; Internet-user centric; and non-Internet centric. Internet centric covers the core technical areas of Internet governance, such as Internet protocols, standards, and addresses. Internet-user centric deals with uses and abuses of the online space. Problems concerning privacy, (child) pornography, spam, cyber-crime and security are considered Internet-user centric. Non-Internet centric issues are broader and have extensive legacies in policy and practice. Dutton and Peltu (2007) include intellectual property rights, as well as human rights and telecommunications transmissions in this last category. The significant difference with the Internet and Internet-user centric categories is the approach taken to the issues at hand. In non-Internet centric areas existing non-digital regulatory processes are dominant.

5.2. Context

5.2.1. Recent Policy Context

In the early months of 2013, two years after DG INFSO initially launched the idea of developing an ‘Internet security strategy’, the European Union issued a Joint Communication (Commission and EEAS) detailing the Union’s Cybersecurity strategy. The communication was stimulated by the need to deal with growing threats to stability and
security in a Europe increasing ruled by communications networks. In one sense, the communication is the natural continuation of the policies developed at the turn of the Century (eEurope 2002, 2005).

The current policy environment is also characterised by the recognition that existing efforts fall well short of the levels needed to provide meaningful protections universally. Particularly, the team noted the EC’s acknowledgement that CERTs, ENISA, and EC3 require further development. CERTs act as the primary centres for response to cybersecurity threats. EC3 is an entity embedded within Europol that was established to deal with cybercrime, and ENISA works as an information sharing agency to collect and distribute information on Network and Information Security in Europe. The policies were designed to develop trust in the Internet, as a global space for economic, social and political development. Trustworthiness is also a key pillar of the Digital Agenda, further reflecting the centrality of the issue to the policy community. As a result of the Commission/EEAS Communication, the Council adopted conclusions in June of 2013 that supported the implementation of the strategic objectives described therein.

The recent attention paid to cybersecurity has been driven by political concerns, which have emerged from a realisation that such a framework is necessary for the continued growth of the European Digital Single Market. It was given a boost by several high-level political events taking place around the world, notably in Estonia in 2007. The perception of the threat has also been very high in this area, in the wake of incidents such as Stuxnet, which have shown the potential frailty of our information and communications networks.

The process of developing the EU’s cybersecurity strategy, which has now been adopted, cannot be said to have been a swift one, as it has taken (circa) two years from inception to Council conclusions. Directives and Regulations that need to emerge from this process have still not emerged. This Deep Dive will focus on the evolution of pre-policy issues; in line with the study objectives, the idea is to look at pre-policy areas of activity, and the role of the Commission in highlighting certain areas for consideration within an EU policymaking framework.

Cybersecurity policy in the EU consists of a focus on several key areas: resilience, crime, defence and international cooperation. It touches on fundamental rights issues, such as data protection, privacy, and freedoms of expression. It is essentially a very broad-ranging policy area in itself. All these areas are dealt with by different entities within the European Commission, other EU bodies (EEAS, ENISA, EC3, EDA, bodies responsible for technological standards (e.g. CEN-CENELEC), as well as external parties such as the Internet Governance Forum, NATO, the OECD, various strategic partners, and beyond.

5.3. Statement of the Issues: Evolving Cybersecurity Governance

5.3.1. Stakeholders

The European Commission has played various roles in cybersecurity practices from both technical and political stances, and has contributed to the broader stakeholder engagement

---

by trying to engage with the different stakeholder communities. As public bodies traditionally endowed with responsibility for communications networks have largely relinquished their roles in the new global information and communications sector, the stakeholder map, and consequently, the way in which management of information flows between stakeholders needs to be carefully addressed. For the building up of a stakeholder map, focus will be placed upon the so-called technical institutions that define and maintain Internet security and standards, and the interaction between them and other actors who are engaged with debates concerning a broader interpretation of Internet governance.

Several categories of actors can be discerned through an analysis of the debates surrounding the main developments in the cybersecurity domain. These actor types have motivations and desires that are shown to be distinct. Whilst this categorisation is helpful, it is arbitrary and does not provide an absolute picture; it merely enables analytic clarity. These actors and their preferred models of governance are outlined below. A categorical breakdown enables analysis of the differing models of governance, which reveals how different actors contribute to the Internet’s maturation into a General Purpose Technology. Actors sometimes act together to achieve agreement, but even if this is the case, agreement on outcomes has been difficult to achieve in practical terms. Regarding the Domain Name System (DNS) debate, Paré has claimed that the actors involved have often been able to agree on mutually undesirable outcomes, but that “they have tended to disagree on their preferred outcomes” (Paré 2003: 58). The majority of literature on cybersecurity has failed to develop an understanding of the decision-making process and has mainly focused upon these outcomes.

### Table 5-1: Main actors in Internet standards setting and Internet security

<table>
<thead>
<tr>
<th>Actor category</th>
<th>Models of governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Academic/Epistemic</td>
<td>Bottom-up (decentralised), lightly coordinated where necessary</td>
</tr>
<tr>
<td></td>
<td>Pre-existing model – informal epistemic community, self-regulation</td>
</tr>
<tr>
<td>Commercial</td>
<td>Non-governmental, market-based, self-regulation</td>
</tr>
<tr>
<td></td>
<td>Shares libertarian approach with academic model</td>
</tr>
<tr>
<td>Civil Society and citizens</td>
<td>Non-governmental, (largely) rights-based, self-legitimating</td>
</tr>
<tr>
<td>Governmental and International Organisation</td>
<td>Hierarchical, top-down, co-regulation with different actors</td>
</tr>
<tr>
<td></td>
<td>Regulation, based upon formal epistemic communities</td>
</tr>
<tr>
<td>Users</td>
<td>Bottom-up, dispersed</td>
</tr>
</tbody>
</table>

As noted above, a high degree of fragmentation exists in those stakeholder communities tasked with regulation and enforcement of Cybersecurity. To provide the reader with an overview of the area and prepare the ground for use of the toolkit in identifying and reacting to emerging trends, the following graphic highlights the complexity of the institutional environment in which cybersecurity issues are discussed in a European context. Hence, it is
useful to break the topic down into different focus areas (see below), where interactions can be more explicitly found.

Source: Robinson et. al. (2013)

Figure 5-1: The cybersecurity institutional landscapes

5.3.2. Statement of the Issues

As shown above, the range of stakeholders in the cybersecurity domain is huge. This is to be expected, given the broad nature of the topic. This has led to fragmentation, claims over ownership, difficulties in harmonising and coordinating responses to common threats and generally a broad set of challenges needed to be overcome in order to bring coherence and common understandings to the field. In the current approach, it could be postulated that the framework developed is actually attempting to address the wrong question. If we focus purely on the topic of cybercrime, we can see that attackers and defenders are locked in a dynamic equilibrium – each attack (defence) shapes the next, and it is not reasonable to concentrate on plugging today’s leaks – especially if it leads to tomorrow’s more dangerous attack. Some of the defensive moves are specific and proportionate; others are apocalyptic. For example, some administrations have implemented so-called ‘Internet kill switches’. As Thompson (2011) states, such kill switches can also be used for defensive purposes. These concerns and justifications are also raised through the ‘precautionary principle’ behind

129 Thompson (2011). See also Chen (2011).

130 The precautionary principle creates a presumption in favour of inaction in cases of uncertainty and places a premium on the collection of all available information. It is detailed in Article 191 of the
Total Information Awareness\(^{131}\) (TIA) and surveillance initiatives like PRISM or ECHELON – this also shows that one person’s defence may be another’s attack. This elaboration on the attack/defence mentality (positivist and rational, assuming that there is always a winner and a loser) that is present in most forms of policymaking seen that certain key policymakers still have a 19\(^{th}\) century approach to dealing with new forms of communication and the central role they play in maintaining the smooth functioning of society.

On the other hand, outside of the institutional sphere, interesting initiatives are springing up. For example, from the netizen community, the ‘Chokepoint’ project\(^ {132}\) which is “a non-profit organisation that collects, analyses and reports on data relating to network neutrality and civil rights in the digital domain.” This information may pre-empt the need for regulatory intervention and may also provide useful crowd-sourced evidence as to the scope of potential problems.

The dichotomy between closed and open models of security leads to deeply ambiguous outcomes – for example, The Onion Ring (TOR) is a highly-anonymised web-based network using software and protocols first developed to provide secure communications in insecure environments; it was then dispersed (via e.g. ‘no disconnect’) to provide ‘security from security’ in order to promote freedom on the Internet around the world. Interestingly, this has recently come under fire as a platform for criminal activity and has assumed a distinctly asymmetric character – the EC’s homepage\(^ {133}\) blocks TOR traffic\(^ {134}\) on the grounds that “the Commission is obliged to keep the Commission websites available for all citizens. You can only realise this objective by implementing security measures, in this case preventing cyber-attacks that typically use the TOR network or similar VPN mechanisms. So to satisfy the higher rights of the general public, you are forced to block the TOR network and some other similar services, which implicitly blocks the possibility of some individuals to use anonymous access. It should however be noted that The Commission strictly respects the Personal Data Protection legislation, which assures citizens that their IP-addresses won't be used for illicit purposes. This principle protects therefore the anonymity of the europa websites users.”

This raises a ‘Level 3’ question: whether privacy, anonymity, data protection and (individual or political) security mean the same things on- and off-line and whether they are in a fixed or stable relationship to each other. It has direct implications for the Internet-readiness of many public services, but also for security promoting, enabling and defeating policies aimed at the Internet and its users and abusers.

To understand it, it is useful to describe several ways in which our inherited assumptions and models may be materially obsolete.

---

\(^{131}\) Stevens (2003).

\(^{132}\) Hosted on Facebook at: [https://www.facebook.com/ChokePointProject](https://www.facebook.com/ChokePointProject).

\(^{133}\) www.ec.europa.eu

\(^{134}\) SpyBlog (2013).
'Cyberspace' battles are not fought to control data any more than privacy battles are limited to access to about personal information. That was a transitional interpretation; the security battle rages in our expectations. Can we trust the network, apps, providers, people and firms with whom we do on-line business and the government and self-regulatory bodies that try to ‘protect’ us? Large-scale or publicised data breaches undermine this trust, regardless of whether the data are useful or used to our detriment (or the attackers benefit, which may be different)\textsuperscript{135}.

There is a cyclicality or positive feedback to the security cycle; the more we trust (and rely on) on-line systems (and others) the more attractive they may be as targets.

Businesses have a range of strategic choices: they may find it profitable to try to secure the system as a whole, to protect their own data against intrusion and compromise (even if this increases risk for others) or simply to appear more secure than their rivals. These behavioural strategies affect their willingness to develop and share automated, behavioural, organisational and other defences.

Cybersecurity risks and breakdowns come from many sources, whose behaviour and motives are similarly diverse: thieves, organised criminals, white- and black-hat hackers and the interaction of complex and fast-moving systems.

The following focus areas highlight the need for common sources of information, the types of stakeholders that are engaged in the areas, and some of the paradoxes apparent in current policy activity. Combined, this reveals the need to rethink the EU’s approach to cybersecurity to make it more ‘Internet ready.’

5.3.3. Focus Area – Privacy, Cybercrime and Cybersecurity

In the light of the ‘Snowden revelations,’ cybersecurity has taken on a new tone. The response that governments have had until now for need for security has now been firmly placed in contradiction with the need to respond to threats through adequate legal, technical and political frameworks that operate according to basic principles of liberal democracy as it is supposedly practiced in the European Union.

One of the key areas in which this tension was first seen was in the area of child protection on the Internet. The growing concern with keeping children safe from online threats emerged around 2001. As a consequence the European Commission was striving for a more unified approach to surveillance, monitoring and security online. As the basis, reference to an international convention was made: the **UN Convention on the Rights of the Child** (1989), which was signed and ratified by Member States of the European Community. This provides a strong background for European programmes dealing with child protection online: ‘State Parties shall ensure that the institutions, services and facilities responsible for the care or protection of children shall conform with the standards established by competent authorities, particularly in the areas of safety, health, in the number and suitability of their staff, as well as competent supervision’ (Article 3.3).\textsuperscript{136} It is worth noting that the European

\textsuperscript{135} This is analogous to the war on terror – the terrorists may attack physical locations, but their target is the minds of much larger populations.

\textsuperscript{136} United Nations (1989).
Union was not the first to consider safety of children on the Internet, the United States enacted the Children’s Online Privacy Protection Act in 1998.

In 2004, the Council made its first recommendations and provided guidelines on how to protect minors in audio-visual and information services. This marked the acknowledgement that audio-visual material could be harmful to minors, and that in the context of a growing digital society, measures had to be taken in order to protect minors.

Moreover, the Communication of the Commission concerning network security in 2001 initiated a proposition of exchange and cooperation between Member States regarding information security: “The Lisbon and Feira European Councils recognized the Internet as a key driver in the productivity of EU economies when launching the eEurope 2002 Action Plan.” This was followed by the 2002 Council resolution, which noted the need for a common cross-border approach in information security.

Also in 2002, the Council of Ministers put forward a resolution advocating a common approach to cybersecurity, with a focus on child protection. A major problem was that not all Member States had an equal level of competency, an equal focus, and/or had the same amount of resources to deal with the challenges provided by cyber threats. Therefore, the Council welcomed the Commission’s initiative to establish a European centre of Cybersecurity expertise, which would come to be known as the European Network and Information Security Agency (ENISA) in 2004. ENISA focuses on research and providing expert opinion (e.g. on best practice) to Member States and stakeholders, focusing mainly on network security.

In 2007 cybercrime was defined as traditional crime (committed using computers or computer systems); the transmission and distribution of illegal content of electronic media; and crimes unique to computer systems (e.g. denial of service attacks or hacking). In 2013, the European Cybercrime Centre (EC3) was established and located within EUROPOL’s offices in the Hague. They have the mandate to fight crime on the Internet, and to help allow the Internet to maintain its open, secure and free.

In 2010, the Commission published the Action Plan for the implementation of the Stockholm Programme, which covered a wide range of issues, including ‘protecting citizen’s rights in the information society.’ Links to policies concerning organized crime, border management, child protection, privacy and trust and a whole range of other issues were brought into the fray through this programme, effectively opening up cybersecurity as a policy issue from technical discussions to much broader discussions on civil liberties.

A wide range of institutions (ENISA, EC3, DG HOME, DG CONNECT to name just a few) are engaged in protecting the open and free nature of the Internet, while simultaneously attempting to assure the stability and security of this network of networks.

---

139 European Council of Ministers (2002).
142 European Commission (2010b).
In conclusion: this focus area shows that there has been a huge amount of institutional interest in the role that data networks play in transborder crime. Many different institutional actors have emerged as desiring to play a key part in fighting the effects of networks on traditional criminal activities. We also see a challenge at the European level to the consistency of national responses and capacities, and thus to the role that European Union institutions can play.

5.3.4. Focus Area – International Cooperation in Internet Governance

Players in the Internet governance game

An alternative to reducing the prevalence of privacy and security threats is to mitigate their consequences. This is a matter of Internet governance, both within and between nations.

Both the US\textsuperscript{143} and the EU\textsuperscript{144} have recently established Internet Freedom Funds to train and empower bloggers, online journalists and human rights defenders to circumvent censorship and evade cyber-attacks. These engage with the debates over the complex relationship between the principles of openness, control and surveillance that permeate almost all contemporary discussions about the politics of the Internet in Europe.

At an international level, the EU’s “No Disconnect” strategy\textsuperscript{145} seeks to promote (esp. for citizens in non-democratic countries) tools to fight “arbitrary censorship restrictions and protect against illegitimate surveillance.” This strategy includes technological development, training/awareness-raising, situational awareness (Internet monitoring and Open data) and cooperation (with industry, within the EU and with other countries (especially the US).

Global Internet governance provides analysis of a new opportunity to address our understanding of the ‘readiness’ of DG CONNECT to deal with an international policy area, and specifically one that is situated in a context of emergent global governance networks. By shifting the focus of research from the role of governments to the process of governance (e.g. Rosenau and Czempiel 1992; Rosenau and Singh 2002; Finger and Rossel 2007; Shahin and Finger 2008), we are able to understand the shift from state-based organisations to more flexible arrangements for managing global resources; the European Commission is well-placed to benefit from such a shift, given its non-state actorness at the international level. ICANN, with its roots in a private corporation established on U.S. territory, is a prime example of such a new institution. However, at the same time, governments wish to participate in the processes of Internet governance, and like to keep a role in governing this global phenomenon: the creation of ICANN’s Governmental Advisory Committee (GAC), and the Internet Governance Forum (IGF) is testament to this dual process of re-assertion of state power and broadening of the stakeholder debate in the global arena. The tensions apparent between state and non-state controlled global governance mechanisms are epitomised in the Internet governance debate. These tensions lie at the heart of the theoretical and very practical debate around governing technology and a policy process comprising of a multitude of different stakeholders.

\textsuperscript{143} Sheridan, M. (2011).
\textsuperscript{144} European Parliament (2012).
\textsuperscript{145} European Commission (undated a).
The difficulty in determining the appropriate policy environment for governance of the Internet is reflected in its institutional ownership. After the division of responsibilities for ARPANET between ARPA and MILNET, the growth of private and public communications networks that could connect to the ARPA Internet (and then the Internet), and the subsequent transfer of responsibility for the ARPA Internet to the NSF, as well as the increased connectivity to other countries, made it difficult to understand which organisation had general control of the Internet itself.

The Internet’s early days were characterised by an organic growth pattern. This took place through funding from DARPA’s IPTO and subsequently the NSF, with private networks also playing a crucial role. The openness of the TCP/IP standard and the willingness of ARPA and NSF project managers to allow external networks to connect to the backbone helped create an environment where it became highly beneficial for any type of institution to be connected to the Internet. Due to this untraditional development of the communication network, traditional understandings of governance have great difficulty in dealing with its emergence.

Given the number of actors that were involved in just the first steps of the Internet’s development, and particularly the mixture of private and public networks that were involved, it was difficult to establish a direct source of accountability. The Internet was largely confined to academic researchers and private corporate networks in its early stages. Advisory groups effectively carried out the management of the Internet and there was no apparent need for a traditional governance structure to be developed. The structure of any such organisation, in any case, would have been highly challenging to develop.

As these different stakeholders have developed their own strategies, communities and working patterns over time, it becomes increasingly important to try to find a way to enhance the connectivity between these different groups, to ensure that power does not accumulate in one particular interest group, and that the global Internet is in fact governed in a way that can be seen as in line with fundamental principles of global governance.

The most recent actor in Internet governance is the Internet Governance Forum (IGF). Desiring a global discussion on the societal, political and economic changes caused by the Internet and ICT, the intergovernmental United Nations International Telecommunications Union (ITU) organized a World Summit on the Information Society (WSIS) in 2003 and 2005. The Internet Governance Forum was recommended during the second phase of the World Summit (ITU, 2006). This forum is a prime example of the contentious fragmentation that we need to deal with when governing the Internet. First, the IGF covers a broad set of issues, such as cloud computing and Internet infrastructure, but also access and diversity, openness, security and privacy. Secondly, the IGF illustrates contentious fragmentation in its governance structure. It favours bottom-up regulation, bringing together a wide range of stakeholders on an annual basis to discuss Internet issues. However, it does not have a mandate to produce binding agreements and it is not necessarily accepted as a global forum for Internet governance affairs. Certain national governments, such as China, have been open advocates to dissolving IGF and giving ITU a more significant mandate.

One Internet or many?

In keeping with the Level 3 nature of this Deep Dive, after considering what different actors have done, it is appropriate to ask what they should have done – in particular, whether the challenges posed by cybersecurity constitute global public bads (in other words, purely
collective problems to be dealt with by a unified and fully-connected Internet) or whether they are instead a patchwork of more-or-less local challenges, to be dealt with: a) by separate authorities and actors; and b) to be managed at least in part by separation between different parts of the Internet. These ‘parts’ may be geographical, technical or organisational.

Back in 2001, libertarians argued\(^{146}\) that (the right kind of) fragmentation, rather than unified and intrusive regulation, was the solution to problems caused by an Internet that was too big, too complex and too full of incompatible groups, technologies and business models. By 2010, mainstream journals like *The Economist*\(^{147}\) were discussing this fragmentation, and pointing out that we did not understand it well enough to tell good from bad, let alone to stimulate good structural changes. Some of the fragmentation, and some attempts to undermine it, come directly from governments and are strongly driven by security agendas. Examples of the former include the “Golden Shield Project.”\(^{148}\)

Other sources of fragmentation are technical e.g. the advent of different devices that perform Internet-like functions without using the Internet (LTE, *ad hoc* networks) or Web-based applications and interfaces. This lack of technological neutrality means that policies designed for one technology may not work for another. In this way, the fundamental ‘Level 1’ issue of off-line assumptions and arrangements not surviving the shift on-line is replicated when Web-based assumptions and arrangements do not survive shifts to other parts of the Internet, or when even Internet-ready arrangements do not work as expected in a digital world that has outgrown the Internet.

Technical fragmentation can also give rise to further fragmentation at a cultural level. Just as the memes by which security is understood, valued and promoted are different in the off- and on-line worlds, so too do the cultures of (in) security differ across operating system communities; because different operating systems attract different levels and types of threat – e.g. LINUX, Android, Windows, iOS.

Finally, organisational fragmentation has long been problematic for the security world, whether as a by-product of the different views of security, law enforcement and economic government agencies (pace the traditional I/II/III pillar distinction) of between government and industry. Internet-based enterprises (e.g. Google, Facebook) are increasingly asked to play front-line roles in cybersecurity policy, from providing information to authorities to providing users with technical and policy-based protections. Increasingly, however, they see themselves\(^{149}\) as scapegoats for unaccountable government policies – either through legal or reputational third-party liability. The consequences to which they draw attention (e.g. SplInternets) are certainly a valid reason for suggesting that cybersecurity policy, for all its Internet focus, is not Internet-ready.

\(^{146}\) Crews (2001).
\(^{147}\) *The Economist* (2010).
\(^{148}\) Also known as the Great Firewall of China, this programme provides authorities with technical tools to censor China’s Internet and block access to various foreign websites. It has been cited as a model in e.g. the preparation of the US SOPA law. See e.g. Hughes and Wacker (2013).
\(^{149}\) Levy (2014).
5.4. Drivers and constraints: Internet Readiness

This section will address the question: Is Cybersecurity positioned to be a CONNECTED policy area? In examining the case data we have seen that security threats are increasingly ICT-driven.

A number of drivers and constraints have limited (and also provoked) action within the Commission and the EEAS in the area of Cybersecurity. First and foremost, the political impetus must be mentioned as the principal driver in this case: it was clear that after the cyber-attack on Estonia in 2007, other countries felt a need to protect their critical information infrastructures. It was also clear that within the EU there was a large disparity in the level of awareness, capacity, approaches and resources to deal with the challenges posed by cyber risks.

5.4.1. Operational and Institutional Factors

Legal and institutional restraints that were noted during the identification of the policy area stemmed mainly from issues of ownership of the policy process. The initial plans for a Cybersecurity strategy were initially seen\textsuperscript{150} within DG INFSO as a policy statement on Internet security. DG HOME raised the issue after seeing this activity in the Commission’s own annual working programme, and expressed interest to develop something in tender with DG INFSO. Likewise, the External Action Service was already developing a more detailed strategy focused on security and defence as part of the follow up from the 2003 European Security Strategy (revised in 2008).

Cybersecurity and cybertrust form the basis for 14 specific Digital Agenda actions\textsuperscript{151} - they cover a wide range of topics. All are web-orientated, but not all are equally Internet-focussed or Internet-ready. In particular, information collection, sharing and analysis are still somewhat fragmented — see Robinson et. al. (2013)\textsuperscript{152}, which notes:

“Understanding how co-ordination and co-operation is achieved in the European cybersecurity policy puzzle is very complex. No-one currently has a clear understanding of how all the different pieces fit together. There are many institutions, each working on a specific part of the problem. The European Network and Information Security Agency (ENISA) has been strengthening its efforts with CERTs and formulation of practical guidance on implementing Article 13a but lacks links with the end-user community. The future of the European Public–Private Partnership for Resilience (EP3R) is uncertain, especially its potential interaction with the recently announced NIS platform. The European Forum for Member States (EFMS) has been instrumental in formulating guidance for Member States to operate the incident notification regime under Article 13a of the Framework Directive. The European Cybercrime Centre has been established since 2013 and will become fully operational in 2014. It is planning discussions with market players active in reporting cyber-crime on

\textsuperscript{150} Except where otherwise referenced, information in this section is based on key informant interviews.
\textsuperscript{151} European Commission (undated c).
\textsuperscript{152} Robinson, et. al. (2013).
the Internet. A number of other organisations in the public and private sector (such as the CERT-EU, the European Cybercrime Training and Education Group (ECTEG), Trust in Digital Life public–private partnership, the Advanced Cyber Defence Centre (ACDC) initiatives and global CERT peer networks) have varying levels of capability and capacity with regard to responding and dealing with the consequences of incidents.

In addition to those organisations covered above, there are a number of other entities that somehow play a role in responding to and managing facets of the Cybersecurity incident problem. These include public–private partnerships (PPPs) such as the European Security of Control Systems Information Exchange (EuroSCSIE), the 2CENTRE network (which aims to facilitate research, training and education concerning tackling cyber-crime) and numerous non-government initiatives such as training for computer incident emergency response teams (TRANSITs).

5.5. Deep Dive Conclusions

5.5.1. Findings

Cybersecurity is a highly network-enabled policy area, where, until now the policies put in place have emphasized the means and not the ends: for some actors, the technological considerations have been more important than the goals. Our assertion is that this is due to the institutional setup of the cybersecurity policy framework, where ownership of specific parts of the policy framework seems to be important. As a natural realisation and logical consequence of this, the norm for security policy has been development-led, reactive legislation. The key to understanding cybersecurity threats and their effects lies in access to information – the very thing the threats are about. The motives for collecting, analysing and sharing this information are complex and conflicting. One way out of this situation may be, for example, to ensure that for common rules regarding reporting to CERTS implemented, in order to ensure that threats are dealt with in a common framework across the EU and that ownership of the ‘threat assessment’ does not lie with one specific party.

Threats to security are real, and do involve ICT to some degree. The solution is not to analyse all data everywhere. However, an assessment of when, where and who should act needs to be part of the fundamental process of reaction. In the pre-policy phase, new roles must be created for fast-acting, democratically legitimate action to take place. Some internal contradictions do exist (for example, blocking TOR net access to the European Commission’s servers).

Dealing with today’s threats (Level 1) requires enhanced information collection, sharing and exploitation; but this increases the stakes and raises the possibility of clash with e.g. privacy, competition policy or net neutrality. It also means ‘joined-up’ information and action coordination across a range of interests that are: affected by on-line security; able to collect and share information on-line to detect, assess and counter (not necessarily on-line) threats; and concerned with different objectives and systems that are affected by ‘horizontal’ (esp. ICT-founded) developments. For example, the areas of transport, health, commerce/competition, energy, movement of persons, and crime prevention are primary
areas for consideration where security and integrity of networks and information flows are requirements for the successful functioning of the systems.

Understanding individual and systemic behaviour (Level 2) requires a more sophisticated use of empirical and experimental data, and a sharing of responsibility with business, civil society and other stakeholders. A wide variety of EU institutional actors are working within the European policy field on policies that are explicitly linked to cybersecurity, but the exchange of information, interaction between policymakers and space in which decisions can be made is heavily determined within what appears to be a very hierarchical environment, dependent upon approval and authorisation for each joint activity. It also needs a possible reinterpretation of the costs and benefits of treating the Internet as a public rather than a private space (as with the Transport Deep Dive).

It is possible that the entire issue has been framed in the wrong way (Level 3); self-organisation may allow a dynamic balance between how people use and rely on on-line systems and the security characteristics of those systems (and thus the organisation and behaviour of Internet Service Provider/Carrier Access Provider value networks). In the same way, imposing privacy regardless of whether it is beneficial or too-rigorous ‘protection’ of a limited framing of privacy rights will produce resistance and threaten innovations (like anonymous profiling) that might provide better understanding and more effective protection in the medium term.

Internet-awareness can also mean less intervention when technological development can overtake current threats. Light-touch intervention at specific points in the chain may be preferable to heavy intervention at the ‘easiest’ point of regulatory traction (this echoes REFIT), but they must be assessed as ‘real options in a complex context’ – they are valuable only if they induce the right kind of responses. To support this kind of policy decision requires – in addition to conventional policy analysis and formulation tools and processes - the application of behavioural analysis and complexity science to data gathered by active and agnostic monitoring and weak signal detection.

A further conclusion that has emerged from our examination is that Internet-aware policy in the Cybersecurity field can often mean no policy at all. Due to the high degree of correlation between new policies and new developments by cybercriminals, it is reasonable to conclude that the horizon scanning undertaken in the Cybersecurity arena must be aware of the dangers of interventions. In many cases, this Deep Dive recommends treatment of existing problems as ‘chronic’ rather than forcing illegal activities to find new avenues which are then more difficult for policymakers to identify and combat.

5.5.2. Conclusions on Internet-readiness

Governments have the power, through existing instruments and frameworks for both off-line and on-line security, to develop and act upon common definitions. Critical in this regard is a definition of cybersecurity that takes account of its special features but also recognizes the connections e.g. between off- and on-line security and between information security, privacy and information assurance.

The need to coordinate security, law enforcement and socioeconomic policy and the development of a patchwork of interacting governance institutions provides the scope necessary to adapt to different definitions of information and to address and engage the
widest possible range of target audiences – indeed, many of the failings affecting existing regulatory and technical solutions come from a failure to do what existing arrangements permit.

More challenging is the maintenance and use of sufficient flexibility to be able to keep up to date with new information requirements of consumers and other key stakeholders. In general, these include data subjects/processors/controllers/collectors, authorities, and third party exploiters. However, they also include many ‘third parties’ (e.g. cloud providers, app developers) whose connections to security breaches and ability to improve security are neither obvious nor codified in law. Finally, there are a range of entities who are implicated by means of their duties to others and ability to demand changes e.g.: health authorities; financial institutions; utility companies; cryptocurrency providers/miners; tax authorities.

Finally, as noted the issue of neutrality must take into account the level and nature of Internet fragmentation. Different channels and parts of the Internet are not equivalent, and even security itself is different in different contexts. Therefore, cybersecurity neutrality must be based on transparency, accountability and the availability of reliable, understandable and comprehensible information to key stakeholders, rather than on a blanket ‘equal treatment’ principle, even if such a thing could be agreed. (The long travails of the proposed General Privacy Regulation provide ample evidence of these difficulties).
6. Bringing Together the Tool Box: Prepositioning Commission Policy Processes for Internet Readiness

6.1. Introduction

A number of policy areas have been worked through the Deep Dive process, cross-DG and policy needs to drive the development of toolkit capabilities. This process has led to a fundamental repositioning of the purpose and positioning of the toolkit from ICT support of the existing policy process to a new function focused on pre policy identification of Internet readiness and Internet impact issues, an introduction to policy processes and their lifecycle management throughout the policy process.

This toolkit will contribute to policy processes by early identification of issues of potential importance emerging in the market environment, Cross DG knowledge sharing, filtering proposed policy action options; identifying policy initiatives of best fit/degree of engagement, resource impact for DG CONNECT. It will also contribute to measuring the degree and depth of consultation and support for Internet readiness in policy processes; provide input information for impact assessment, policy reviews or REFIT; and identifying and help manage stakeholder engagement efficiency, roles and responsibilities.

The Toolkit may also be used to backcast existing and completed policy processes to analyse supported initiatives for Internet readiness issue relevance to areas of policy depending on their varying levels of issue awareness/knowledge/expertise and consequential need for present or future DG CONNECT support.

In essence the core purposes of the toolkit are to facilitate the transition to Internet ready policy by:

- Assisting in ensuring that intervention processes are more fully and comprehensively informed of market driven Internet readiness issues;
- Identifying and making visible across DGs Internet readiness issues that are not yet central to current and future intervention debates but likely to acquire legislative relevance over the lifetime of an intervention;
- Enabling Internet readiness inputs to intervention/non-intervention decision processes; and
- Helping ensure that issues are identified and engaged far earlier in their lifecycle (Pre policy cycle soft engagement) in order to reduce the necessity for later legislative intervention.
6.1.1. The Toolkit Principles

The 4 preamble articles in the FIC regulation\(^\text{153}\) identify key areas of EU activity. Restated in more general terms, they define four screening aspects identified on page 78):

1. The ability to mandate or implement common definitions, principles, requirements and procedures;
2. Scope to adopt a broad definition of relevant information, sources and ‘target audiences’;
3. Sufficient flexibility to be able to keep up to date with new information requirements of consumers and other key stakeholders (e.g. smart infrastructures, smart vehicles, information to/from shippers, utility operators, environmental/weather monitors); and
4. Neutrality across different channels (e.g. freight vs. passenger, public vs. private transport, on-board vs. centralised systems (note that – for environmental and societal objectives, consistent with the “Smart Urbanisation” issue - it may be desirable in formulating policy options to tip the playing field by giving public transport users enhanced information and planning functionality).

There are logical tools, available in the market or internally, to support the effective management of such activities. They are listed here and discussed in more detail below. The most critical are:

- Legislation review (what is fit for Internet purpose today);
- Stakeholder mapping/horizon scanning; and
- Behavioural analysis (consumers and firms).

Complimentary tools and techniques include: competency analysis; SWOT and other analysis techniques; trend analysis; scenario development and gaming; and impact assessment.

6.1.2. Toolkit Approach

The toolkit is positioned to operate prior to policy cycle initiation. Its key purpose is to inform and educate policy actors (and stakeholders) as to Internet readiness issues likely to affect areas of potential policy intervention. It is designed to:

- Be resource efficient – for this reason, it builds on existing data resources, clearly indicates where new data would be useful and how they can be reused and minimises participation and compliance burdens both inside and outside the Commission;
- Be rapidly implementable within DG CONNECT – for this reason, it is positioned early in the policy life cycle and clearly linked to existing processes, to take advantage of the impetus and discretion provided by potential interventions;
- Use only market standard/available tools, techniques and approaches - the use of existing tools extensively used and well understood in the business world minimises risk, maximises opportunities for mutual understanding and exemplifies the perspectives of important policy counterparties;
- Provide information and continuing support to all DGs –creation of a common toolkit, methods and data resources, incremental application through an evolving set of cases

\(^{153}\) European Parliament and Council (2011) – see discussion in Section 3.5 above.
and simultaneous support for issue scanning are intended to create a platform for increasingly efficient and effective collaboration;

- Inform intervention consideration processes – the explicit criteria for selection and prioritisation are tied to progress in applying the toolkit, which creates the potential for deferred action or (as in the case of EcoSearch – for a modest initial intervention intended to build understanding and result in the capture of better information;

- Assist in lifecycle management of issues and intervention mechanisms – the process is structured around cycles of engagement from initial issue detection to intervention and subsequent monitoring and re-evaluation. Because many Internet-readiness issues arise from the need for transitory intervention to help non-government players to develop, test and adapt to their own solutions, many interventions themselves must be revisited – this ‘sunsetting’ is explicitly embedded in the toolkit;

- Ensure policy interventions are future scoped – the toolkit engagement processes are intended to mix foresight and situational awareness, to bring into contact stakeholders with very different time perspectives and to emphasise co-regulation and light-touch intervention. In this way (at least potentially) the advantages of relatively slow policy processes (commitment power) can be maximised and the disadvantages (obsolete or captured policies) minimised; further gains in this direction come from the way the toolkit processes can;

- Help avoid legislative intervention through early issue lifecycle engagement – which reduces the risks of regulatory institutionalisation, creep and capture.

6.2. Pre Policy Positioning of the Toolkit

The Deep Dives reveal a consistent theme. The policy process is increasingly affected by accelerating changes in technical, operational or consumer baselines. Consideration of baselines is increasingly significant role in the logic of policy intervention and provides useful calibration and ‘sanity checking.’ However, it has also left policy processes highly susceptible to the ‘fallacy of history’ (namely that future performance can be adequately extrapolated from past behaviours). Intervention mechanisms studied have tended to cater to past realities and often lack the flexibility and ‘hedged’ approach to reflect emerging realities driven by innovation in technology, business methods/models and consumer behaviour.

This tendency to see the future as a continuation of the past makes it difficult to detect, let alone anticipate exactly the kinds of disruptive change to which the growing penetration of ICTs has given rise. It is reinforced by the apparent ‘solidity’ of empirical data as compared to scenarios about the future, a rooted aversion to – and profound disagreements about - the fundamental uncertainties associated with disruption and a tendency to ‘lock in’ our understanding of recent history.\(^\text{154}\).

Rigid and backward-looking intervention in a highly dynamic market and societal environment rapid erodes relevance and magnifies inefficiencies. Over and above the missed

---

\(^{154}\) This is a triple lock: we build our models and communications around such understandings, we have a vested (and often useful) interest in the relevance and appropriateness of existing policy interventions and we tend to concentrate on the data and evidence that we already know to be relevant.
opportunities for advancement, it can diminish or even reverse the benefits of previously successful interventions\textsuperscript{155}. To help overcome the ‘fallacy of history’\textsuperscript{156}, our Toolkit is firmly positioned in the pre policy phase.

\textsuperscript{155} Such as product labelling, where the rise in online trading has effectively reduced both consumer information on product efficiency and the influence of such information on consumer choice.

\textsuperscript{156} Santayana warns us that “Those who cannot remember the past are condemned to repeat it” Even more strongly, Hegel notes that “We learn from history that we do not learn from history.”
6.3. Toolkit Components

All of the tools and techniques contained in our toolkit are in widespread use – at least in the private sector - today. Our investigations have shown that for any toolkit to be credible, it must not require the user to make demanding and unrealistic adaptations. Further, our market-standard tools have already been refined and improved by thousands of trials in public and private sector scenarios to provide full confidence in the toolkit’s validity and efficacy. As a result, there is absolutely no need to develop bespoke solutions for make the toolkit become operational and effective. The techniques are shown in Table 6-1.

Table 6-1: Toolkit techniques

<table>
<thead>
<tr>
<th>Technique</th>
<th>Purpose</th>
<th>Deliverable</th>
<th>Use</th>
<th>Time scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon scanning</td>
<td>Early identification of issues of note that have an immediate, intermediate or likely long term impact on intervention considerations or decisions</td>
<td>Time/impact sorted Issues list</td>
<td>Provides a list of issues that are prioritised for analysis and documentation for distribution</td>
<td>Continuous process</td>
</tr>
<tr>
<td>Stakeholder analysis</td>
<td>The documentation of all internal (EU) and external (market) issue relevant stakeholders.</td>
<td>Issue Stakeholder map. Updated overall stakeholder map</td>
<td>Assure the policy process is appropriately inclusive and balanced during all phases</td>
<td>Dynamic. Updated continuously during issue lifecycle</td>
</tr>
<tr>
<td>Issue analysis</td>
<td>To identify the drivers, dynamics and implications of an issue</td>
<td>Issue Analysis and supporting data for capture in an issues database/document</td>
<td>To form the baseline information for Issue alerts to DGs. Create an issues data base for use in issue lifecycle analysis and knowledge updates.</td>
<td>Dynamic. Updated continuously during issue lifecycle</td>
</tr>
<tr>
<td>Issue Alerts</td>
<td>To provide a consistently formatted, agnostic, documented analysis of the issue of note for other DGs and internal DG CONNECT staff.</td>
<td>Written document in a standard format. Database of evidence and reasoning which is maintained during the issues lifecycle.</td>
<td>Advise other DGs and DG CONNECT staff of emerging issues and their implications/evidence base for consideration in policy considerations.</td>
<td>Single release after issue analysis is done. Watching briefs can also be issued as situations change and additional evidence is gathered.</td>
</tr>
</tbody>
</table>
6.4. Toolkit Methodology

The techniques above are fully supported by tools and methods that are immediately fit for purpose and accessible. Specific tool sets have not been recommended to promote flexibility and adaptation during internal organisational decisions.

**Table 6-2: Tools and methodology**

<table>
<thead>
<tr>
<th>Technique</th>
<th>Major Tools/methods</th>
<th>Availability and skill levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Horizon scanning</strong></td>
<td>The main horizon scanning tools available are:</td>
<td>Horizon scanning is a free form activity that relies on multiple techniques to identify issues and dynamics in the market that have current or likely future implications for the logics or mechanisms of intervention.</td>
</tr>
<tr>
<td>Media Monitoring</td>
<td>Story analysis</td>
<td>Market standard tools for monitoring the various sources of information are available with those related to social media being especially important.</td>
</tr>
<tr>
<td>Word analysis</td>
<td>Start-up monitoring</td>
<td></td>
</tr>
<tr>
<td>Social Media trend analysis</td>
<td>VC and grant investigation</td>
<td></td>
</tr>
<tr>
<td>IPO data</td>
<td>Company reports</td>
<td></td>
</tr>
<tr>
<td>Tech trend analysis</td>
<td>Retail analysis tools</td>
<td></td>
</tr>
<tr>
<td>Standards bodies analysis</td>
<td>Consumer complaints/reactions</td>
<td></td>
</tr>
<tr>
<td>Consumer trends</td>
<td>Retail trends</td>
<td></td>
</tr>
<tr>
<td>Logistic Trends</td>
<td>Spending pattern dynamics</td>
<td></td>
</tr>
<tr>
<td>Litigation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technique</td>
<td>Major Tools/methods</td>
<td>Availability and skill levels</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Stakeholder analysis</strong></td>
<td>The tools available for stakeholder analysis and management are limited but off the shelf, low priced, scalable, fit for purpose candidates have been identified. The chosen tools are updated continuously as new stakeholders are identified and categorised throughout the analysis and engagement process.</td>
<td>Stakeholder analysis and management tools are available and easily managed by computer literate staff.</td>
</tr>
<tr>
<td><strong>Issue analysis</strong></td>
<td>Issue analysis tools of all levels of sophistication are available on the market. In addition the IPTS is a resource available to manage the analysis of large data sets that will be created during the lifecycle of an issue. Suggested analysis criteria include: Issue Category, Type, Source, Stakeholders; Sector(s) – Size, Expertise, Engagement, Economic relevance; Players – Incumbent/New/Emerging/potential - identity, policy relevance; Issue maturity level, Positives, Negatives, Implications; Issue impact - Present/Emerging/Future; Issue specific impacts – Privacy/Behavioural/Technical/Economic (Internal and External Market)/Social/Environmental/Political/Policy area; DGs affected – Now/in future; Business sector impacts; Existing Policies – EU/Member State/Standards bodies/Global; Intervention Logic (including no intervention and self/co-regulation); Necessity of intervention (existing policies, Soft/Hard Intervention); Intervention signpost and triggers; Impact, Key Issue metrics for each option; EU Issue Expertise required; and Monitoring Capabilities Conclusions, Recommendations, Next Steps.</td>
<td>Issue analysis can take two forms: • Impression/opinion (soft analysis); and • Evidence based (Hard analysis) Immature or emerging issues may lack the hard evidence of impact till late in their lifecycle. Prior to this softer analysis is likely to be more important and require less formal skill sets. Hard analysis of extended data sets will require skills in data management and sophisticated tools such as those in IPTS. These analyses are carried out in an agnostic manner in order to provide a landscape analysis of the issue that provides an objective input against which DGs can be made aware of the issue and take consideration of its implications in pre policy considerations.</td>
</tr>
</tbody>
</table>

\(^{157}\) Signposts are tracking indicators of need for new or changed intervention; triggers are critical events or values.
<table>
<thead>
<tr>
<th>Technique</th>
<th>Major Tools/methods</th>
<th>Availability and skill levels</th>
</tr>
</thead>
</table>
| **Issue Alerts**| Any word processing package will suffice for this. Email or download capabilities for distribution.  
These are used to issue managed scheduled, consistently formatted, agnostic issue briefings to the DGs and stakeholders | Market available and basic computer literacy.  
The analysis and issue processes should ideally be managed by a single responsible group tasked with ensuring that issues of present or future importance are identified, analysed and issued in a consistent format.  
The management, scheduling and consistency are critical to avoiding information overload and the consequent loss of impact of the deliverables. |
6.5. Toolkit Processes

The following section provides a practical illustration of tool-kit operations. The section provides simple details of the impact the toolkit can have on Internet ready policy processes from issue identification to the re-establishment of a new market norm.

6.5.1. Identifying Internet readiness

One important point that should be noted at the outset is that Internet readiness is multi-dimensional. No single tangible set of tools can completely envision and ensure the awareness, let alone understanding of Internet readiness challenges that should be embedded in the culture, processes and outputs of any intervention.

At the basic level, lack of Internet readiness is easily identified e.g. from the existence of gaps between existing physical markets and their online counterparts. Physical markets, usually mature and relatively stable, operate in a context of firm expectations and stable regulatory frameworks. In contrast, many online markets display completely new models of operation that challenge or defeat the assumptions behind classic physical markets and legislation.

The ability to identify and then manage or mitigate the emergence of such ‘gaps’ between physical and parallel online environments creates the opportunity for policy processes to deliver more flexible and appropriate intervention decisions.

Figure 6-1 provides a visual overview of the issue lifecycle mapped against Internet readiness issues:

![Figure 6-1: Issue lifecycles and policy Internet readiness](image)

Internet readiness issues already arise in a wide variety of forms. As the Internet becomes increasingly pervasive in traditionally regulated domains, such issues are increasingly critical not just to DG CONNECT but to every DG since the Internet and the structures and
behaviour it supports are truly borderless (sectorally and geographically). There is therefore a growing need to identify, prioritise and manage the introduction and incorporation of the key Internet readiness issues to the policy process.

A sense of the diverse range of areas affected by the discrepancy between physical and online markets is provided by the following examples of policy domains directly affected by Internet readiness issues.

- Crypto Currencies;
- Wearable technologies;
- Embedded technologies;
- Technology and taxes;
- Secure browsing;
- Facial or personal identification technologies;
- Internet of things/nanotechnology;
- Situational aware technologies (TVs that watch you);
- Consumer based bio reactive/health self-testing;
- Big and Small data;
- Driverless cars and transport modes;
- Hacking and Data Leaks;
- Terms and Conditions;
- In shop/In life monitoring;
- Surveillance and privacy;
- Digital life and death; and
- Intellectual property.

The ability to spot issues and trends early in their lifecycle may improve the outcome of conventional interventions; more importantly, it may also allow forms of “soft” engagement (such as discussion, input, education, briefings, knowledge, analysis, expertise, information, data, self-regulation...) that influences development trajectories in a way that avoids the necessity for legislative intervention and/or improves the match between intervention and the specifics of the issue.

6.5.2. Soft engagement

Soft engagement has the further benefit of being continuous, current and comprehensive; the input is made to a stakeholder-mediated environment free from many of the formal constraints of the policy process. Soft intervention can be seen as a potential ‘pre-emptive strike’ against Internet readiness challenges that can obviate the need for policy intervention altogether.

Issues with policy implications can emerge at different times for different reasons and are initiated by different drivers and circumstances. In general three major causes for issues to emerge in the market are:

- Break out technologies/innovation (physical, virtual and hybrid);
- Business model innovations; and
- Behavioural adaptation (driven by circumstance, environment or policy).
Usually these are linked in the order shown; technological change that creates new enabling environments (and potential Internet readiness issues) for business models triggers the emergence of new models, which in turn induce, encourage or initiate behavioural change in consumers and other stakeholders. Soft engagement early in this process is highly likely to be more meaningful and effective than post-fact intervention based on enforcement or strong regulation. Note that, while it can be triggered by evidence of breakout innovation, it must also be capable of anticipating and appreciating business model and behavioural consequences.

The soft engagement process\textsuperscript{158} lends itself to a linear progression from innovation to a market paradigm as illustrated in Figure 6-2.

![Figure 6-2: Issue lifecycle stages and involvement curve](image)

### Figure 6-2: Issue lifecycle stages and involvement curve

Figure 6-2 illustrates the major stages in the management of an Internet readiness issue requiring policy intervention, from innovation to the new business as usual. Each stage has its own sub stages, dynamics, management requirements, stakeholders, resource needs, methods, feedback loops, outcomes, KPIs (Key Performance Indicators), metrics and monitoring needs and capabilities.

An important takeaway is way the process is designed to manage Internet readiness issues in a way that identifies, supports and then transfers responsibility to a prepared logical owner in an appropriate DG. Such ownership may be singular or multi DG. That is unimportant. What is critical is that such DGs are proactively informed and prepared to take up issue ownership and manage its solution process to include Internet readiness as a core consideration.

The capture and analysis of the metrics or KPIs for each stage provides a detailed overview of progress in managing the issue. These metrics are outward-facing and designed to support

---

\textsuperscript{158} It is highly likely that many Internet readiness issues will be engaged with at any given moment with each being at a different stage of maturity (defined as “being integrated as part of a new societally acceptable market norm”).
decisions about the appropriate form of intervention (if any). These decisions are made on the basis of agreed (cross DG) issue specific trigger points.

Figure 6-3 illustrates some of the metrics and KPIs that could be considered in relation to gaining and maintaining evidence-based, transparent views of the progression of an issue.

---

Figure 6-3: Potential issue metrics and KPIs

These metrics (or others considered relevant) serve a number of purposes. They can:

- Measure market penetration and impact on the market;
- Provide visibility on stakeholder engagement and dynamics;
- Enhance understanding on the internal and external factors influencing development of the domain;
- Illustrate likely paths for issue evolution;
- Identify positive and negative trends in issue evolution;
- Outline a series of triggers for considering different types of policy intervention;
- Indicate the impact of soft engagement and the likelihood of harder intervention;
- Maintain a continuous flow of information and data into the policy making process;
- Establish an issue specific evidence based, “real time” justification for the type of intervention (or not);
- Enable the development of evidence based scenario opportunities for policy responsible;
- Contribute to policy analysis, relevance, development, review, recasting and timing; and

---

159 Defined as “a set of criteria, results or activities that define the necessity to take formal intervention position.”
• Generate a data set for analysis of effectiveness, approach success and process impact assessment.

They also contribute to more effective, focused and timely allocation and management of DG resources.

6.5.3. Intelligence Gathering: the Toolkit Core

The key to effective toolkit implementation and use is a mature understanding of the emerging market and social environment that generates a challenge of social, market or policy relevance. Figure 6-4 illustrates the major sources of data, information and input to the intelligence gathering process.

Figure 6-4: Key issue identification sources and methodologies

The five core areas of input to the intelligence gathering process (Stakeholders, Media, Start-ups, EU, and Behaviour) have the greatest consistent relevance to issue generation, understanding and socio economic integration and impact. Table 6-3 helps illustrate why.
Table 6-3: Key issue sources, drivers and roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Drivers</th>
<th>Influence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholders</td>
<td>Established and emerging social, economic and political players who provide the structure and resources for issues to evolve. They may be positively or negatively inclined. Some issues may have stakeholders who are not aware that they are affected or have a role</td>
<td>The establishment, maintenance, repositioning or destruction of power or influence on existing or emerging social, economic or behavioural spaces likely to positively or negatively impacted by an Internet readiness issue or trend.</td>
</tr>
<tr>
<td>Media</td>
<td>Players who actively engage in searching out and revealing (via various channels and mechanisms) stakeholders, activities, innovations, data and information related to socio economic and behavioural evolution.</td>
<td>Reputation, mission, commercial, Interest</td>
</tr>
<tr>
<td>Start Ups</td>
<td>Innovative ideas in a form that can engage in structured funding, RTD, and market exploitation of new technologies, mechanisms, business models and exploitation strategies.</td>
<td>Innovation, personal interest, wealth aspiration, social conscience,</td>
</tr>
<tr>
<td>EU</td>
<td>These represent mechanisms by which innovations and issues are formally or informally mediated to a societally acceptable structure and expression.</td>
<td>Political and societal mandate.</td>
</tr>
<tr>
<td>Behaviour</td>
<td>The instinctive, induced, influenced or imposed actions by individuals of organisations in the face of a situation.</td>
<td>Survival, sex, culture, circumstance, capability, conscience, commerce.</td>
</tr>
<tr>
<td>Role</td>
<td>Drivers</td>
<td>Influence</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>impacts and inform corrective or supportive responses.</td>
</tr>
</tbody>
</table>
The intelligence gathering activities of the toolkit systematically scan the social, economic, technical and political “ecosystem” in order to identify present or emerging issues that facilitate or undermine the establishment of a policy environment that is: Internet ready; legislatively light; and which compliments/accelerates social and economic progress that is both compatible with and supportive of cultural and ethical norms.

6.5.4. The Fruits of Intelligence Gathering

A consistent and structured approach to intelligence gathering, capture and analysis will provide a set of specific outputs. These include:

1. Earlier identification of issues and trends of positive and negative importance;
2. Identification and inclusion of issue relevant stakeholders outside the “usual suspects”;
3. Early engagement with the process of issue evolution;
4. Identification of concerns or support needs in relation to policy;
5. Early Identification of metrics to monitor understand issue impact;
6. Data and information sets to arrive at an agnostic analysis of emerging trends and issues;
7. Creation of information and knowledge sharing resources with DGs and stakeholders;
8. Identification of trigger points in relation to soft or hard (formal intervention) engagement;
9. Identification and monitoring of likely impact of evidence based scenarios; and
10. Qualification of roles, responsibilities and resources for issue lifecycle management.

The creation and use of these elements provides the opportunity to make progress towards the overarching goal of better policy making. The joint working and dissemination of the intelligence will assist in embedding Internet readiness in EU thought, analysis, operation and policy processes without the need for cumbersome and potentially inappropriate mandates. Moreover, by providing early indications based squarely in the actions of important participants, such intelligence can minimise the risk of unnecessary policy initiation. Instead of setting in motion formal policy processes that may provoke resistance or respond to slowly to a fluid situation, early soft engagement can identify areas where apparent problems will be resolved by the stakeholders themselves (e.g. by self-regulation), will pass away or may be better handled in conjunction with other issues. The net result over time will be the creation of a more lightly loaded and appropriate policy intervention agenda.

A further advantage is a more bottom-up architecture, with policy initiated and managed at unit level in DG CONNECT and its partner DGs. Peer-to peer linkages will strengthen mutual understanding and policy coherence. A related benefit is an increase in the inclusiveness and degree of future scoping of both light and heavy policy intervention.

Finally, through continuing engagement with the evolution of the areas from which policy issues arise (rather than in response to crises), both the relevance and impact of policy interventions should be improved, contributing to the overarching goal of regulatory fitness.
7. Conclusions and desiderata

7.1. Lessons emerging from the Deep Dives

The Deep Dives exposed both successes and failures in the identification and mitigation of policy challenges within the European Commission. Some of the challenges that had been encountered have lessened – or are expected to be surmounted by on-going initiatives and developments. Others have become more serious, making it difficult to reproduce earlier successful examples of joint activity or to sustain early progress.

The Deep Dives exemplify three different levels:

Level 1: Solving problems caused by uncontrolled, misunderstood or emergent ICTs and/or addressed by clever use of ICTs;

Level 2: Understanding problems - using ICTs to collect, share, model and explore information-spaces to understand behaviours and how those understandings affect outcomes; and

Level 3: Rethinking Case for Action – collaborative consideration of whether “we” must act now or at all.

The time-frame for these challenges varied by area; so, too, does appropriate use of the toolkit.

7.1.1. Food labelling

Food Labelling provides an example of an area in which Internet Ready policy development can yield immediate benefits in relation to pressing problems, by redirecting and reinvigorating existing interventions. In the transport area, existing interventions are actively being pursued in an increasingly cross-linked and complex domain; this evolution has clearly exposed the need for a deeper understanding of the nature and evolution of individual behaviour, made necessary by the widening range of ICT-enabled alternatives and made possible by the flood of new data ranging from the individual to the network level. In both of these cases, the initial ownership of the issue (or at least of the central legislative instruments) lies outside DG CONNECT. In contrast, the responsibility for cybersecurity lies with DG CONNECT; the issue is almost by definition Internet Ready, but the toolkit and associated processes are needed to ensure interventions are appropriate across the wide range of other policy and market sectors where cybersecurity concerns arise and simultaneously to determine whether cybersecurity constitutes a policy challenge or issue set in its own right and thus requires ongoing specialist intervention.
Food was examined as a Level 1 issue; the basic – and pressing - problems arose from the movement of off-line behaviour on-line. As a result, the focus is on restoring the effectiveness of off-line-derived rules and on reaping additional advantages by unlocking the innovative potential of the on-line world, without the need to fundamentally change our understanding of human behaviour or the information linkages in the food system responsible for the problem and useful in its solution.

7.1.2. Transport

By contrast, the issues highlighted in the transport Deep Dive can be traced at least in part to changes in the evidence and analysis used to formulate policy. Policy documents for over a decade have widely discussed multi-modal transport policy. However, much remains to be done and the data used to analyse the functioning of the sector and the models used to predict and analyse policy interventions remain fragmented and (at least outside the academic literature) do not make use of the latest advances in e.g. complex systems analysis and behavioural science. The drive to develop integrated and ICT-ready transport policies and accompanying data and tools has been driven by the increasing strength and complexity of linkages across modes and between transport and communication and by the availability of a wealth of new data. These highlight the limitations of simplistic models of transport users’ behaviour (and the ‘predict and provide’ policies to which they give rise). From the emergence of inter-sectoral (including ICT) complexity and increased data and modelling capabilities come new Internet readiness issues and new forms of converged or integrated governance.

This creates a Level 2 challenge on top of the Level 1 issues. At Level 1, transport policies were increasingly struggling to keep pace with new technologies, some of which failed to reach critical mass, and with the growing recognition of the need – in principle at least – for more effective integrated transport policies. This is not the most serious challenge, however, as initiatives such as ITS have at begun to make substantial progress. However, the full power of the data collected or collectable as a by-product of modern transport (and the new initiatives) has yet to be fully realised and is expected (at least in the academic literature) to lead to profound improvements in transport policy based in e.g. behavioural science and complex network theory.

A further aspect of the challenge comes from the increasing policy involvement of areas other than transport and ICT per se. As noted in relation to “Smart Urbanisation” many of the problems affecting transport policy stem not just from short-term journey choice and long-term transport infrastructure, but also from the forces shaping the topology of necessary

---

160 The 2001 Transport White Paper referred to “multimodal corridors giving priority to freight.” Despite this promising beginning, the memo introducing the new transport policy in 2013 notes “Transport infrastructure between the transport modes is fragmented. As regards making multi-modal connections, many of Europe’s freight terminals, passenger stations, inland ports, maritime ports, airports and urban nodes are not up to the task. Since these nodes lack multi-modal capacity, the potential of multi-modal transport and its ability to remove infrastructure bottlenecks and to bridge missing links is insufficiently exploited.” See European Commission (2013a).

161 These complexities are magnified by recent events relating to e.g. floods and other phenomena arising from the combined effects of land use and climate change, which increase network maintenance costs.

162 See page 50.
journeys (e.g. where people live, work and where production and sales occur) and from the spillover effects of urbanisation on e.g. climate and weather vulnerabilities. For this reason, a wider range of data and behaviour may need to be included and stakeholders from DGs concerned with economic geography and environmental change included.

7.1.3. **Cybersecurity**

Cybersecurity differs from food and from transport in that there does not exist a satisfactory and agreed set of ‘off-line outcomes’ that can be translated into the online environment. Security and privacy are fundamentally different on-line; the policies and assumptions that ‘work’ in the off-line world have not worked on-line and show no signs of being ‘fixable.’ It is not even clear to what extent the policy response should emphasise prevention, mitigation or adaptation.

The cybersecurity case highlights the intricate balance between technological solution and non-technological ‘problem.’ In the first focus area (cybercrime and privacy), policy responses are indeed considered necessary to meet already-visible societal and legislative challenges such as the shift of organised crime to what has been regarded as an open and free Internet. The clash between this assumption of a largely self-regulating Internet and the ineffectiveness of controls devised for an off-line world in the on-line environment has polarised attitudes to attempts to extend off-line controls to the on-line world. This polarisation has grown because successive policy responses have been triggered by each new threat – this reactive stance has increasingly weakened the common view and consent on which such policies rely.

There is a dynamic aspect as well: the failures of reactive policy have increasingly led to calls for faster reaction rather than for anticipation (e.g. security or privacy by design). This has bred complacency and cynicism in equal measure. Citizens are both the “eyes and ears” and the “hands and feet” of cybersecurity; if they do not look for, are unwilling to report or unable to recognise new threats, the system is - if not blind - myopic\(^{163}\). Even where fast reaction succeeds, the result may be a rapid transition from a problem that can be addressed to a harder problem. Slower responses, by providing incentives for citizens and businesses to take a more active role and to control risks, may improve the cybersecurity ‘immune system.’ More generally, fast responses may limit current damage, but also speed development of new exploits and/or encourage complacency. It is felt by some that growing threat levels are inevitable consequences of complexity and the emergence of professional attackers driven by commercial, criminal, political or national interest objectives. Against these, some argue for the creation and exercise of enhanced powers to monitor and manage such threats. These powers are naturally sought by and for large system operators and appropriate government agencies. This creates a strong feedback loop; one party’s ‘security protection’ becomes

---
\(^{163}\) Of course industry-side organisations (e.g. CERTs) detect intrusion attempts and other exploits and exchange and coordinate information. But their detection, sharing and action thresholds are often high and orientated to organisational objectives that may not fully reflect end-user or broader societal interests. In this respect, the exchange of information among users and user feedback are vital cybersecurity tools. See e.g. Palmer, A. (2013) "The evolving online consumer threat landscape: creating an effective response" pp: 139-146 in Hsu and Marinucci; Kandias, Virvilis and Gritzalis (2013); or Kandias, Stavrou, Bozovic and Gritzalis (2013).
another’s ‘cybersecurity threat’ and so on. This coordination failure – at least between sectors of government or between sovereign jurisdictions or large economic actors – can be damped or eased by a greater degree of agnostic data collection, sharing and analysis; if the focus is on understanding the threat landscape, this need not further infringe privacy or security. But these perspectives and the feedbacks to which they give rise define the dynamics of cybersecurity; it may be, for instance, that even if the reaction to the original threats does not resolve the issues, the reactions to attempts to manage or limit damage or to take advantage of those responses, may trigger an effective solution from within the system. In this sense, cybersecurity is essentially a Level 3 issue.

Clearly, an effective response cannot be rooted in institutional stovepipes and 19th century legislation. Institutional ‘path dependency’ (i.e. doing it as we’ve always done it) cannot continue as this creates a paradoxical situation where society is protected (cf. NSA and GCHQ treatment of online communications) by mechanisms that infringe on our rights as citizens in a liberal democratic society.

The ‘problems’ of cybersecurity depend on off-line assumptions about the extent to which people can be expected to look out for their own interests and the resulting division between individual and collective interests and between self-regulatory and command-and-control mitigation. There is no doubt that cybersecurity does create problems; but whose problems they are and what can be done about them is much harder. In an on-line world, these assumptions do not always work. As a Level 1 issue, protections cannot be assessed because the information needed to gauge the extent of infringement, the impacts it has and the ability of different parties to do something about the likelihood and extent of damage are systematically censored or suppressed; also, solutions implemented thus far have neither alleviated existing threats nor kept pace with emergent ones.

From a Level 2 perspective (understanding behaviour), the choices made by individuals and groups are only selectively observed and cannot be reliably modelled or taken into account. Even basic assumptions that might stand in for such models, such as notion that more trust is always better, that cybercrime is always motivated by greed or by ideology, or that cybersecurity failures always result from criminal or malicious intent or from dereliction of duty on the part of cybersecurity officers are routinely violated.

**Note:** it is not just the use of surveillance data for purposes other than cybersecurity protection or the motives of the original collectors of such data to which people and organisations object and around which new network clusters form. Much of the discussion around surveillance is concerned with other uses that may be discovered (even by third parties) or the mere idea that these data can be seen. Privacy and security, in this sense, are not simply instrumental virtues or matters of data access and integrity, but states of mind. Again, the formulation of policy ‘in a vacuum’ tends to perpetuate framings of the problem based on the remit of the organisation concerned or observations from the past that may no longer be valid.

165 This does not mean that key institutions cannot develop precautions. Many things are possible – but they are not all equally desirable and many of them will happen without conscious policy decisions if enough people take them up. It is expectations that determine reliance on and use of different channels. One manifestation may be the waning use of email among significant parts of the population and the very different approaches taken by e.g. ephemeral data apps like Snapchat, Gryphn, Wickr and Silent Circle. As Viktor Mayer-Schönberger of Oxford says: “As users of digital tools discover that the ephemerality they are so used to...is largely gone, they will become wary of the comprehensive digital memory that has replaced it—and look for market-based solutions to reintroduce it. That’s just what this breed of new apps provides.” See Mayer-Schönberger (2011).
This leads on to Level 3 questions: is cybersecurity a problem distinct from security overall (and thus from e.g. privacy); and whose problem or responsibility is it? Because the landscape is both subjective and dynamic, this Deep Dive recommends measures to recognise, embrace and work with its inevitable evolution, rather than to try to outguess and pre-empt it. Moreover, it concludes that both cybersecurity and security are needed and that neither is a special case of the other.

### 7.1.4. Recommended elements

Some recommendations apply across all three levels. Among the elements that should be put in place or reinforced are the following (which have been extensively discussed in the earlier sections).

**Issue identification** – this involves establishing shared processes for co-identifying issues – including intelligence gathering and data-sharing.

**Early engagement** – this means opening communications before turf lines are established, in order to identify the most appropriate roles and integrate different objectives, perspectives, policies and stakeholders. It also entails identifying and correcting ‘balance of power’ issues early on and developing partnerships and joint issue ownership.

**Business case development** – this involves explicit requirements for developing the internal business case for joint working on specific issues using methods that transverse hierarchical and institutional arrangements (whilst recognising that specific institutions have evolved to meet specific purposes).

**Balancing support** (vertical and horizontal) – this means channels of communication and procedures for obtaining and linking to top-level support (endorsement by hierarchy) while preserving discretion for bottom-up and peer-to-peer interaction (this balance will change along the policy life cycle).

**Fitting the approach to the origin of the pressure** – differential methods for policy issues that are: i) forced on the Community institutions from outside - industry, civil society, Member States, other European institutions or non-European actors; or ii) originated within the European Commission - within DG CONNECT, from other Directorates-General or at Collegiate level.

**Room to grow** – working together across institutional lines is always difficult, and complicated by the demands of accountability and by the need to include distinct stakeholder constituencies. It is therefore necessary to give individuals – especially those at desk officer level and subject matter experts - ‘space’ to work together without obliging them to look for artificial common causes. Creating this space can be eased by reconsidering the competence of the EU in light of the need for Internet readiness. In particular, the ability of the Internet to transcend and rewrite ‘market’ boundaries implies that a narrow interpretation of the ‘internal market’ discourse is no longer the sole reason or justification for European Union policymaking. At a less aggregate level, this entails changing internal and/or team geometries to create (perhaps temporary or issue-defined) *virtual units* that combine functions and expertise which are specialised along policy, domain or DG,

---

166 Examples include (to some extent) Intelligent Transport and Cybersecurity.
technological, commercial and research/innovation lines in order to provide a platform or incubator for ‘optimised’ initiatives.

**Sustaining engagement** – the networks, understandings, shared data resources, competences and issue ownership established in individual initiatives form the basis for a learning network of relationships between Internet ready individuals, institutions and issues. This in turn will make the Commission as a whole capable of a more agile, adaptive, proactive, nuanced and integrated approach to its policy obligations.

**Maintaining coherence** – the new challenges arising from the application of ICTs in ‘non-ICT’ domains cannot wholly pre-empt business as usual either within those domains or in light of DG CONNECT’s remit. Therefore, an Internet ready Commission will need to create methods for balancing these emergent or ‘wild card’ issues from those within the existing work programmes. This need for coherence extends to intervention mechanisms by embracing the “spirit of H2020” as well as that of REFIT and working through the associated policy processes and instruments to apply to toolkit.

**Framing** – at a more pragmatic level, this also means reinterpreting ‘successes.’ The results of Intelligence Gathering or even a Deep Dive may well be the identification of areas where less needs to be done or where others need to take action. The process would clearly separate areas of technological possibility from realistic prospects (where the market and the world are likely to respond to a bit of leadership) while respecting additionality and subsidiarity (even within the European institutions or the EC itself).

**Building understanding** - The cumulative effect should be a deeper understanding of institutional competencies and a meaningful and structured inventory of skills and knowledge. This would be supported and maintained by an expanding and structured repository of data, models, analytical methods and policy instruments as well as horizon challenges.

### 7.1.5. Specific jobs for the toolkit

The operation of the toolkit and the implementation of the processes illustrated in Chapter 6 do not take place in a vacuum, but depend on the experience and skills of individuals and teams contributing to developing these policies. The results of the recommended horizon scanning and issue identification gradually form a portfolio of potential issues, and the exercise of the toolkit will gradually lead both to their adaptation and to greater acceptance, skill and understanding in applying them. The collaborative nature of each application of the process will, moreover, lead to the formation of an extended network linking personnel and units across the DGs in ways that reflect the linkage of issues in Europe as a whole. This poses specific challenges such as those discussed below.

The continuing operation of the toolkit will create (at least by awareness and reference) a growing compendium of data, models, scenarios and issues. Potentially, this can serve as a stable platform for coordination and shared policy processes on an ongoing basis. However, data sharing and collection of data on behalf of others are not without cost and violate at least implicit organisational conventions. Thus it may be necessary to strengthen this by a

---

167 In particular, knowledge-sharing on its own is insufficient, esp. when it is assumed to mean sharing responsibility or liability.
combination of: op-level endorsement; formal requirements (e.g. in the Impact Assessment process); and/or dedicated resources for hosting the platform. By the same token, the time and efforts of the individuals involved in curating and maintaining these assets must be supported – ideally not as a dedicated role but at least in part through rotation on the basis of involvement with specific issues that draw on or feed into the ‘compendium’.

The collation of these data and models is not a mere matter of convenience or a way of forcing the separate institutions to share ownership of Internet Ready policy processes; rather it is a reflection of the evolution of the Information Society itself. Both “big data” and the identification of effective “small data” repackaging are based initially on agnostic (if not wholly unstructured) data collection and shared data access, on pattern-based\textsuperscript{168} analytics, and on collaborative modelling and scenario exploration in order to implement horizon-scanning and recognise emergent Internet readiness issues from a common base.

A related challenge concerns the ability of individuals with policy responsibility and understanding to dedicate their time and energy to applying the toolkit and to engage in the sort of collaborative responsibility-sharing envisaged here. One of the most pressing tasks for further work is the development of a suitable institutional basis that preserves existing lines of responsibility and accountability while facilitating Internet readiness.

By the same token, it is not intended that the recognition of Internet readiness should be seen as an attempt to rewire or merge the responsibilities of the different DGs or offices within them. While the interviews conducted revealed that collaboration was in a sense easier when the allocation of responsibility was less fine-grained and complex, the dynamic and complementary nature of Internet readiness issues dictates that differentiation of understanding and responsibility is necessary, just as interdisciplinarity trumps multidisciplinarity. This is reinforced for the legislative domain by the architecture of the EC; legislative proposals are essentially developed by the Commission as a whole, even when they are ‘driven’ by specific DGs. Thus a ‘Digital SecGen function’ could be established to provide a stable and neutral base for partnerships based on the toolkit processes.

A third challenge arises more directly from issue identification. As the range of issues expands, and as the complexities of any single issue are explored, it will be necessary to develop processes that adapt the prioritisation methodologies in the toolkit to enable the Management Team to prioritise and coordinate issues picked up by the horizon-scanning/alert identification tool in order to determine which to do first, free up necessary resources, negotiate power- and responsibility-sharing with other DGs and generate necessary understanding and buy-in. This can be facilitated by the creation – in the context of the compendium of successive horizon scans – of a database that maps the interdependencies and other characteristics of the issues. Over time, a market or bidding process could be implemented on the basis of an initial endowment of discretionary resources in order to identify the most promising portfolio or combination of issues to take forward from issue identification into further policy action.

These considerations lead to an initial set of specific tasks that can be accomplished using the toolkit and associate processes. Initially these would be taken within DG CONNECT.

\textsuperscript{168} These range from the correlation-based techniques of big data analytics to the more recent ‘deep learning’ approaches that are transforming machine intelligence.
It would be useful to develop and maintain a standards map to support other legislation. This would take the form of a classification of existing and new technologies that may need legislative action to limit or constrain, permit or encourage mandate or forbid their further development and deployment.

Associated with this is a responsibilities map\textsuperscript{169} to correlate i) technologies, ii) issues, iii) regulations and legislation and iv) responsible parties (at minimum by DG, but possibly office level). This can be used to: support assessment of emerging issues (who owns what?). It also helps in determining when new legislation or legislative processes are needed - e.g., when a Directive may need to be replaced with a Regulation (or vice versa), when legislation should be reviewed (what needs to be monitored) and modified or withdrawn; or when or whether new ‘digital by design’ rules can be issued under existing instruments (for example by asking whether the instrument makes room for the issues and/or implementation changes).

A further foundational step would be the establishment of Internet-ready policy option development criteria and procedures. These are necessary both for the formulation of policies for eventual implementation and to ensure that Impact Assessment (which necessitates comparison of a range of policy options) captures the full range of issues and possibilities arising from the Internet environment. The formulation of options may follow a variety of routes. It may merely entail modifying existing (non-ICT) rules to incorporate digital concerns (e.g. privacy) or means (e.g. automated traffic management, privacy by design). Conversely, it may mean changing existing (ICT-related) rules to incorporate sector-specific concerns or means. More ambitiously, it may be possible – through application of new procedures with suitable engagement mechanisms, checks and balances) to create new ‘horizontal’ or digital-specific instruments and/or develop and assess proposals for integrated or coordinated changes across multiple Directives and Regulations ‘owned’ within different DGs.

In the medium term, it may be useful to assess the scope for a Digital Secretariat-General function that could: serve as a platform for coordination between different DGs ‘connected’ by ICT-enabled developments; take responsibility for developing fully Internet-based rules; and assess the Internet-readiness of all legislation on a rolling basis (e.g. as part of REFIT) and develop methods for doing so.

Finally, we suggest re-examining (and possibly reviving) the European Interoperability Framework to support the operation of the Toolkit.

\textsuperscript{169} Currently, this mapping is carried out during annual (e.g. Impact Assessment road mapping) or multiannual planning (e.g. new initiative proposals for submission to a new College, multi-year evaluation plans, or REFIT planning) as well as during the development of the policy initiatives (e.g. by Impact Assessment Steering Groups, Interservice Consultations and, where necessary, in College “orientation debates.” This recommendation merely seeks to assure that these maps are futureScoped and help the recommended horizon-scanning rapidly and effectively to engage the most suitable parties in the most suitable (mutually-negotiated) ways.
References


CDC (US Centres for Disease Control and Prevention) (undated) “How many cases of foodborne disease are there in the United States?” at: http://www.cdc.gov/foodsafety/facts.html#howmanycases.


Choke Point Project homepage at: https://www.facebook.com/ChokePointProject.


DOT (US Department of Transport Research and Innovative Technology Administration (RITA)) homepage: http://www.its.dot.gov/.
Efficient Consumer Response European homepage at: http://www.ecr-europe.org/.
European Aviation Safety Agency Homepage at: http://www.easa.eu.int/.


Marsal-Llacuna, M., Colomer-Llinàs, J. and J. Meléndez-Frigola (2014) “Lessons in urban monitoring taken from sustainable and livable cities to better address the Smart Cities initiative” Technological Forecasting and Social Change


