37th Meeting of Senior Officials from Centres of Government

Leading the Digital Transformation from the Centre of Government

Dublin, Ireland, 8-9 November 2018

Session notes
The Centre of Government (CoG) is the body that provides direct support and advice to the Head of Government and the Council of Ministers. The CoG meetings began in the 1980s, and were consolidated into an annual event in the 1990s. CoG constitutes a forum for informal discussion and remain one of the OECD’s highest-level policy networks.

The meetings serve three main purposes:

- To review issues of how to make the centre of national government work more effectively;
- To achieve a more in-depth understanding of decision and policymaking systems in the host country.
- To work on broad governance issues fundamental to achieving economic and social public policy objectives.
The annual meeting of senior officials from Centres of Government is one of the highlights of the OECD calendar.

As one of the most high-level OECD networks, it offers a unique insight into strategic thinking at the top. We look to the Centres of Government to help us find new approaches to the unprecedented economic challenges that we face today.”

Angel Gurría
Secretary-General of the OECD
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Anticipating and guiding strategic digital transformation</td>
<td>9</td>
</tr>
<tr>
<td>Establishing a joined-up approach to collecting, using and protecting data</td>
<td>13</td>
</tr>
<tr>
<td>Addressing cybersecurity from a strategic perspective</td>
<td>17</td>
</tr>
<tr>
<td>References and further reading</td>
<td>22</td>
</tr>
</tbody>
</table>

### Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1. A significant share of jobs could be affected by automation</td>
<td>6</td>
</tr>
<tr>
<td>Figure 2. Digitalisation facilitates trade in counterfeit goods through the post</td>
<td>7</td>
</tr>
<tr>
<td>Figure 3. From vision to strategy</td>
<td>9</td>
</tr>
<tr>
<td>Figure 4. The centre of government-led model</td>
<td>11</td>
</tr>
<tr>
<td>Figure 5. Open-Useful-Reusable Government Data Index (OURdata), 2017</td>
<td>13</td>
</tr>
<tr>
<td>Figure 6. Global number of cyber security incidents from 2009 to 2015</td>
<td>17</td>
</tr>
<tr>
<td>Figure 7. Cyber crime: biggest online data breaches 2007-2018</td>
<td>18</td>
</tr>
<tr>
<td>Figure 8. Children experiencing cyberbullying</td>
<td>19</td>
</tr>
</tbody>
</table>

### Boxes

<table>
<thead>
<tr>
<th>Box</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box 1. Ten areas in which government needs to steer the digital transformation</td>
<td>10</td>
</tr>
<tr>
<td>Box 2. How much data?</td>
<td>14</td>
</tr>
<tr>
<td>Box 3. Trust in peer platform markets</td>
<td>20</td>
</tr>
</tbody>
</table>
Introduction

The digital transformation is well underway, characterised in OECD countries by almost universal, high-speed connectivity and the generation and use of vast amounts of data. Citizens, businesses and public authorities are constantly exposed to the sweeping changes that digitalisation is bringing. The arrival of constant mobile connectivity, combined with new products and apps, has created a digital ‘ecosystem’ that, through increasing use by individuals, firms and governments, is rapidly replacing traditional channels for many economic and social interactions. As this ecosystem grows, it becomes the normal way to access any product, information or service. Technologies continue to develop so rapidly that they are pushing the digital transformation in new and often unpredictable directions. Along with the obvious benefits and opportunities that it brings, the ‘dark side’ of the digital economy is also becoming more visible. As not only jobs, prosperity and well-being become ever more closely tied to digitalisation but also personal security and safety, our digital future has become a strategic and inherently political issue.

The need for a strategic and political response to digitalisation implies a leading role for the centre of government. The general role of the centre is to ensure that government decisions – made by politicians, often non-specialists, often working in conditions of extreme pressure – are not ad hoc, imprudent or inconsistent. Its objective is to promote evidence-based, strategic and consistent policies. Keeping a hold on the strategic direction of the government is a key task of the centre. As such, the centre needs to understand how the digital transformation will affect the lives of citizens, what they expect and what they are concerned about. This insight needs to guide government action from the centre out across the public administration and beyond in a credible, co-ordinated and visible way.

The starting point for a digital economy strategy should be, first and foremost, how to maximise the good things that digital can bring. The benefits from the digital economy are widely recognised. For example, job creation is increasingly linked to the spread of new technologies. According to a recent study, 56% of new jobs in advanced economies are in so-called “new professions” – specialists in cyber-security, social media, robotics, 3D printing, autonomous vehicles and so on. In these millennial industries, companies are expanding and demand for skilled labour and salaries is rising. The dynamism of these sectors underpins an increasing share of new growth.
At the same time, concern is growing that the digital economy could increase inequalities by putting pressure on wages at the low skill end of the labour market. With reports on the future of work suggesting that an average of 46% percent of jobs across the OECD area have high or significant potential to be displaced (see Figure 1), the social and, in turn, political stakes are very high. Governments need to have some idea of how to achieve (and communicate) a digital vision in which delivery drivers retrain as drone pilots or production line workers reskill as 3D printer managers and robot operators, rather than a bleak jobless future for the low skilled. The centre of government is already closely involved, along with key line departments, in reviewing and redirecting the levers of policy – investment, regulations and budget – across a wide range of policy areas including tax, education and skills, health, R&D and trade, in such a way that the digital economy generates growth and jobs without leaving large sections of the population behind.

**Figure 1. A significant share of jobs could be affected by automation**
Percentage of jobs at high risk of automation and at risk of significant change.

Source: (OECD, 2018b)

The process of designing a whole-of-government response to the digital economy is complicated by the uncertainties inherent in the way technologies develop. Emerging technologies such as artificial intelligence (AI) and blockchain pose huge challenges by virtue of their unpredictability. According to the OECD Digital Outlook, while we know that the number of connected devices in and around people’s homes in OECD countries is likely to explode (from 1 billion in 2016 to 14 billion by 2022), we do not yet know what policy implications this will have.
Devices and sensors that gather data and exchange information with one another to monitor the health, location and activities of people, the efficiency of city services and the condition of the natural environment all hold out enormous promise; but the ‘Internet of Things’ also creates concern about an unregulatable digital future. Similarly, the growth of e-commerce, which has overall led to an expansion of retail trade, also has a less positive side as it facilitates trade in illicit and counterfeit goods, including fake medicines and drugs, increasingly carried in individual small parcels through the post (see Figure 2). As an important actor in promoting regulatory quality, the centre of government is directly involved in steering public policy in these almost entirely uncharted waters.

**Figure 2. Digitalisation facilitates trade in counterfeit goods through the post**

Conveyance methods for counterfeits, as % of total customs seizures 2011-13

<table>
<thead>
<tr>
<th>Conveyance</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>63%</td>
</tr>
<tr>
<td>Air</td>
<td>21%</td>
</tr>
<tr>
<td>Sea</td>
<td>8%</td>
</tr>
<tr>
<td>Road</td>
<td>7%</td>
</tr>
</tbody>
</table>

*Source: (OECD, 2018d)*
The centre of government plays a dual role in policy: (1) to anticipate trends and develop a vision; and (2) to steer a strategic response. In essence, centres of government operationalise the political priorities (election manifesto or government programme) via policy development, co-ordination and monitoring mechanisms. The successful implementation of key policy agendas depends to a large extent on the centre’s ability to translate political objectives into instructions for departments that are realistic and clear. This includes some tasks that can make or break policy commitments, such as:

- preparing data and evidence on trends from diverse sources, including foresight and horizon scanning;
- ensuring that the budget preparation process reflects strategic priorities;
- ensuring that departmental work plans reflect priorities and include feasible, concrete actions to achieve them.

In the case of the digital economy, which can be seen as a means to an end rather than an objective in and of itself, an important point of departure for strategic thinking is to identify how the digital economy can support or even drive wider objectives. These wider objectives are often enshrined in a national development plan and might also be linked to an international agenda such as the Sustainable Development Goals. For example, if the key development challenge for a country is poverty reduction or social inclusion, the policy question for the digital strategy is ‘how can the digital economy serve the achievement of these objectives?’

**Figure 3. From vision to strategy**

![Diagram showing the relationship between International Agenda, National Economic or Development Strategy, Foresight, Strategic vision for digital transformation, Strategies for jobs, skills, etc., Subnational digital strategies, Strategies for innovation, industry, etc., and Strategies for broadband, digital security, etc.]

*Source: (OECD, 2018b)*
The breadth of activities that fall under the heading of a ‘digital strategy’ is extremely wide. Actions to promote the digital economy may imply trade-offs across sectors and the need to adjust policies in one sector in order to avoid negative externalities in another. This suggests the need for an ongoing process of negotiation among departments and with the business sector and civil society. Of particular note is the potential role of multinational technology companies in influencing the direction of policy in the digital area, with respect to technology diffusion, taxation of the digital economy, or technology-related norms and standards. The ten areas in which government needs to be active (see Box 1) all depend heavily on co-operation with the private sector.

Box 1. Ten areas in which government needs to steer the digital transformation

Digital transformation involves a large number of interlinked processes that need to be steered by government. According to OECD Digital Economy Outlook 2017, the top priorities are:

- Strengthening digital government services
- Further developing telecommunication infrastructure
- Promoting digital skills and competences
- Strengthening cybersecurity
- Enhancing access to data
- Encouraging digitalisation by small and medium-sized enterprises in particular
- Encouraging adoption of new technologies in specific sectors, e.g. healthcare, education
- Strengthening digital identities
- Promoting the ICT sector as an export industry
- Promoting e-commerce across the economy

In each of these areas, investment decisions across the administration and in individual organisations need to be made in a context in which new technology options are arriving almost daily.

Almost all OECD countries have already developed a national digital strategy, and governments have organised responsibilities for its development, co-ordination, implementation, and monitoring and evaluation in a variety of ways. In some countries, the head of government steers strategy development and strategic co-ordination, often providing personal leadership. Functions relating to strategic co-ordination and monitoring of progress are fulfilled by the centre of government, with line departments providing input for the design of the strategy and taking responsibility for aspects of implementation.
In other approaches, one or more lead ministries is assigned (or created) by the head of government to design and draft the strategy. Operational co-ordination is usually ensured by a dedicated co-ordination group of representatives from the implementing ministries and agencies. The latter also tend to monitor implementation in their respective areas and report back to the lead ministry and/or the ministerial council for the strategy’s overall evaluation. In these cases, the role of the centre of government is more arm’s length but nonetheless active. Whichever variant is adopted, the key challenge is to overcome some common obstacles to joined-up government, such as:

- Immediate economic and social pressures can crowd out strategic policy initiatives, particularly where the benefits from horizontal initiatives are likely to be felt beyond the electoral term.
- Public budgets and accountability systems are usually aligned with departmental structures and have difficulty tracking benefits that accrue in multiple policy areas, thereby reducing incentives to participate.
- Information sharing across departments and agencies is often poor, “daily” inefficiencies caused by incompatible IT systems, non-transfer of case histories, etc., slow down delivery and reduce the impact of individual actions in support of a strategy.

Efforts to improve co-ordination and align policies have sought to overcome these problems through different means, each with its own strengths and weaknesses, as shown below.
<table>
<thead>
<tr>
<th>Alignment tool</th>
<th>Strengths/weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation of “super ministers”</td>
<td>Success depends on the status of an individual and might not lead to effective integration at the policy level</td>
</tr>
<tr>
<td>Creation of “super ministries”</td>
<td>Internal silos often remain; merging two departments might not solve problem where policy has multiple dimensions</td>
</tr>
<tr>
<td>Policy “tsars”</td>
<td>Success depends on the status/personality of an individual</td>
</tr>
<tr>
<td>Inter-ministerial committees</td>
<td>Most common mechanism for &quot;routine&quot; coordination, but are less suited for ambitious, game-changing initiatives</td>
</tr>
<tr>
<td>Independent policy units</td>
<td>May face challenges in establishing legitimacy across departments</td>
</tr>
<tr>
<td>Inter-ministerial policy teams</td>
<td>Can work if departmental priorities and approaches are aligned; more difficult if inherent trade-offs are involved.</td>
</tr>
</tbody>
</table>

Based on past experience, an ambitious effort to align policies such as that required for the digital strategy needs a clear vision with measurable targets, an action plan with clear responsibilities and tasks for the different stakeholders and a system for monitoring progress. It would also need devices to keep senior government ministers and the head of government focused on the strategy and a process that has convening power and that draws on co-ordination as well as substantive expertise.

**Questions for discussion:**

- Are governments able to understand and stay alert to technology-driven changes on the horizon so that they can be more proactive rather than reactive (e.g. in regulation)?

- What capacities (foresight, technical...) are required at the centre to ensure that it can support this objective?

- What should be the specific role of the centre of government in ensuring a strategic approach to digital transformation?

- Should resources and capacity for digital transformation be located within the centre of government?

- What are the benefits of centralising? Are there potential drawbacks?

Session 2
Establishing a joined-up approach to collecting, using and protecting data

Government itself is, of course, a driving force for the digital transformation. “Digital government” – the adoption of digital technologies by government in the performance of its mandates – is therefore a crucial lever in getting the best out of the digital economy.

At first, digital government was seen as a way of driving efficiencies by reducing the cost of service delivery. Over time, it became clear that in order to improve the quality of services delivered online, rather than just reduce their unit cost, it could be necessary to join up some of the multiple databases held by government departments and use the data in a more integrated way. More recently, the emphasis in digital government has been on improving the interactions between government and citizens and using data gathered online as feedback to improve the design and targeting of policies. In turn, this has encouraged better use of data analytics and of digital tools to enhance public participation in policy development. The centre of government often plays a lead role in developing and piloting these tools.

As the amount of data collected expands, its (commercial) value is also becoming more apparent. Thousands of advertisement-generating apps to check the weather, find the best route to a destination or compare real estate prices and many other things use government data. Effective release of government data can improve the everyday lives of citizens, while promoting business innovation and generating revenue streams. At the same time, these opportunities bring a responsibility to maintain and control the quality of the data that is produced. Awareness that open government data has commercial and innovation value is helping to build a culture in which data is used as a resource, with an emphasis on innovative ways of using and reusing data rather than simply ‘data dumping’. The concept of “publish with purpose” is what best represents this emerging discussion (OECD, 2018c).

Figure 5. Open-Useful-Reusable Government Data Index (OURdata), 2017

Source: (OECD 2017d)
As open data policies mature, so does awareness of the need to establish adequate governance frameworks to deliver usable data at a reasonable price that maximises synergies across different government departments. Given the horizontal nature of government data and its uses, the design and implementation of joined-up data policies requires a high level of co-ordination of actors and decisions within and outside the public sector.

Countries’ experiences, and data from the OECD OURData Index, suggest that the governments achieving better results with open data are those that allocate responsibility to co-ordinate data policies close to the centre of government. This facilitates common platforms across the administration, borrowing the convening power and leverage of the centre of government to ensure that departments and agencies engage actively in data sharing initiatives.

When governments use data innovatively, they transform the process of policy-making, policy development and enforcement. Digital technologies enable real-time monitoring of outcomes that were previously unobservable. Armed with these data, policy makers and regulators can then better target existing policies in order to achieve policy outcomes with greater efficiency. For example, financial flows can be tracked at a higher level of granularity and periodicity than was previously possible, enabling the better enforcement of financial market regulations related to cartels, bid rigging or collusive behaviour, without necessarily needing to develop new legislation (OECD, 2017a).

Box 2. How much data?

By one estimate, 2.5 quintillion bytes of data are created each day, and the Internet of Things (IoT) is only accelerating that pace. Over the last two years alone 90 percent of the data in the world was generated (Marr, 2018). By the year 2020, about 1.7 megabytes of new information will be created every second for every human being on the planet.

Sharing data across government silos is crucial for digital transformation, but it is equally crucial that citizens trust government to protect their personal information from theft and misuse.

There is a risk inherent to keeping large amounts of sensitive data in a single database. Centralization can bring simplicity and ease of access – but also vulnerability to hacking or misuse. For instance, India’s Unique Identification Authority is designed to centralize the addresses and biometric data for the country’s 1.32 billion people. The database was hacked in January 2018, and 1 billion data records compromised (see Figure 6).
Some countries (France, UK, USA) have created a position of Chief Data Officer to help public organisations better manage data. Chief data officers are expected to improve how public institutions create, store, manage, use and share data and to strengthen evidence-based policy making (OECD, 2016a)

Questions for discussion:

• How can the centre help break down silos and promote a joined-up approach to the use of data to design regulations and deliver services more effectively and also more innovatively?

• What kinds of frameworks are being established to support a strategic and smart use of data, overcome obstacles to sharing data, and provide support for agencies to use data effectively?

Session 3

Addressing cybersecurity from a strategic perspective

The fear of online fraud or the misuse of personal data (identity theft, etc.) can prevent citizens from engaging in online transactions. For governments, the three most pressing digital security challenges affecting economic and social activities, according to an OECD survey, are cyber attacks against small firms, cyber attacks that disrupted or prevented economic and social activities and cybercrime/cyber espionage that involved the theft of digital intellectual property and assets (OECD, 2017b).

Digital security incidents, for both organisations and individuals, are increasing in terms of sophistication and impact. These incidents can disrupt the availability, integrity or confidentiality of information and information systems on which economic and social activities rely, and they can be intentional (i.e. malicious) or unintentional (e.g. resulting from a natural disaster, human error or malfunction).

Criminal organisations are increasingly active in the digital environment. As innovation is becoming more and more digital, industrial digital espionage is likely to increase. Some governments have also been suspected of carrying out online intelligence and offensive operations, perhaps for political motives or to damage an organisation or an economy. For example, a high-profile cyberattack in 2014 targeted Sony Pictures Entertainment, exposing unreleased movies, employee data, e-mails between employees, and sensitive business information like sales and marketing plans.

Figure 6. Global number of cyber security incidents from 2009 to 2015

“Hybrid risks” are a growing concern, and often have a digital element. These threats require minimal resources and often take advantage of the low cost, high impact influence of social media. They include disinformation campaigns on social and broadcast media, which can erode social cohesion, trust in public institutions by citizens, and the integrity of electoral processes.

With the Internet of Things (IoT) the risk of security incidents will most likely increase. Not only can the components of the IoT become the target of digital security incidents, with the consequence of disrupting physical systems, but IoT components can also be used to target digital systems, including through distributed denial of service attacks.

**Figure 7. Cyber crime: biggest online data breaches 2007-2018**

Number of compromised data records in selected data breaches as of September 2018 (in millions)

While concern about economic cybercrime and identity theft are high profile, there are other ways in which unsecure digital channels can have harmful effects. For example, the ease by which social networks allow negative information to be spread among groups is a cause for concern. About 8% of 11-15 year olds in OECD countries reported being subject to cyberbullying (Figure 7), although the share could be higher as victims are often reluctant to self-report. Governments have used information campaigns to raise awareness of the dangers associated with social networks among young people, but regulation or policing of social networks is difficult in practice.
Figure 8. Children experiencing cyberbullying
Percentage of 11, 13 & 15-year-olds being cyberbullied by pictures at least once, 2014

Conventional thinking about digital security assumes that it is possible to create a “safe and secure” digital environment. But digital “ecosystems” are constantly evolving due to technological change, threat adaptation, etc. Digital security risk thus cannot be eliminated, but it can be managed.

Risk management has become the recommended paradigm for addressing challenges related to digital risk and trust. A whole-of-government approach makes it easier to integrate digital security risk into national risk management. Also mechanisms are needed to allow risk-related information to flow across public-private sector boundaries, between large and small firms, along value chains, across sectors, across borders, etc. This sort of information sharing is not easy, particularly internationally and at scale. Obstacles include lack of trust and perception of unbalanced reciprocity, fear of further exposure and legal liability.

But these obstacles can be overcome, for example, by ensuring that two-way information sharing benefits all parties through mechanisms such as Information Sharing and Analysis Centers (ISACs). ISACs function best when encouraged and supported by public policy that encourages private sector many-to-many information sharing and collaboration. The centre can play an important role in building coalitions across stakeholders.

Source: (OECD 2018e)
Box 3. Trust in peer platform markets

Peer platforms, such as eBay, Airbnb or Uber, open up economic opportunities for the individuals supplying the goods or services (“peer providers”) and for the platforms making the connections (“peer platforms”). Platforms have developed a number of practical, innovative mechanisms to address concerns and inhibitors to consumer engagement. The most common trust mechanisms developed by these platforms are outlined below:

- Review and reputation systems: A central element in helping consumers to make informed choices are review and reputation systems, which can also help regulate behaviour through monitoring, feedback systems and the exercise of peer pressure.
- Verified identities: Some peer platforms take steps to verify the identity of peers, which can be particularly helpful in resolving disputes.
- Pre-screening: Some platforms offer pre-screening of peer providers, through verification of external databases (e.g. motor vehicle records or criminal background checks).
- Secure payment systems: Many peer platforms offer secure payment services, often in co-operation with established external payment systems.

Nonetheless, according to an OECD survey in 2017 of 10 000 consumers, less than half of PPM consumers have read the platforms’ terms and conditions or the privacy policies in detail, despite claiming that the privacy and security of their data are important to them.

Source: (OECD 2017c)

There is increasing convergence among countries’ privacy frameworks, notably through agreement on high-level guiding principles and good practices (the OECD Privacy Guidelines being the pioneer in this field, and the European General Data Protection Regulation (GDPR) being the most recent example) or enforcement fora (e.g. the Global Privacy Enforcement Network, and the recent opinion of the European Data Protection Supervisor on online manipulation and personal data). As the volume of data flows across borders grows, more international co-operation will be needed in terms of standard-setting and enforcement for data security.
Questions for discussion:

- What approaches do governments take to striking the right balance between safeguarding privacy and government information on the one hand, and allowing for the innovative use of data and information to create value on the other?

- What role can the centre play to promote international regulatory co-operation when a strictly domestic regulatory solution will not be sufficient to manage cross-border risks?
References and further reading


OECD (2018a), Centre Stage 2: The organisation and functions of the centre of government in OECD countries, OECD.


OECD (2018e, forthcoming), Well-being in the digital age: Understanding the opportunities and risks of the digital transformation for people’s well-being, OECD.


