WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

White Paper

Digital Policy Playbook 2017
Approaches to National Digital Governance

September 2017

World Economic Forum®

REF 310817

This white paper has been published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum, but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Contributors and Acknowledgements

The National Digital Policy Network Experts

Virgilio Almeida, Faculty Associate, Berkman Klein Centre for Internet and Society, Harvard University (Network Chair)

Doris Leuthard, President of the Swiss Confederation (Steward)

Luis Alberto Moreno, President of the Inter-American Development Bank (Steward)

Nabil Bukhalid, Co-Founder and President, Internet Society Lebanon (ISOC-LB), Lebanon

Demi Getschko, Director and President, NIC.br; Member of the ICANN Board (2005-2009), Brazil

Bassam Hajhamad, Partner and Consulting Market Leader, PwC, Middle East

James Johns, Visiting Senior Research Fellow, Policy Institute, King's College London; Director, Corporate Affairs, Hewlett Packard Enterprise (2015-2017), United Kingdom

Wolfgang Kleinwächter, ICANN Board Member; Professor for International Communication Policy and Regulation, University of Aarhus, Denmark

Maria Medrano, Director, Corporate Affairs, Latin America and Canada, Hewlett Packard Enterprise, USA

Miguel Porrua Vigon, Lead Specialist, e-Government, Inter-American Development Bank, USA

Thomas Schneider, Ambassador, Director of International Affairs, Swiss Federal Office of Communications, Federal Department of the Environment, Transport, Energy and Communications (DETEC), Switzerland

Randeep Sudan, Sector Manager, Information and Communication Technologies, World Bank, Washington DC

Stefaan Verhulst, Chief Research and Development Officer, Governance Laboratory, NYU, USA

Antonio Garcia Zaballos, Lead Specialist, Technology, Inter-American Development Bank, USA

At the World Economic Forum

Richard Samans
Head of the Global Challenges Team, Member of the Managing Board

Fadi Chehadé
Senior Adviser to the Executive Chairman

Derek O'Halloran
Head of Digital Economy and Society System Initiative, Member of the Executive Committee

Alex Wong
Head of Global Challenge Partnerships, Member of the Executive Committee

Mara Kelly
Project Collaborator, Digital Protocol Network on National Digital Policy

John Sumpter
Project Specialist, Digital Protocol Network on National Digital Policy

Alline Akintore Kabbatende
Project Collaborator, Digital Protocol Network on National Digital Policy

William Hoffman
Project Collaborator, Digital Protocol Network on National Digital Policy

Acknowledgements

Special thanks to PwC for their collaboration and professional services. Their expertise, engagement and resource support was vital for creating this White Paper.

Additional thanks to those who contributed to writing the case studies: Virgilio Almeida, Nabil Bukhalid, Glenn DeGama, Anurag Dua, Tal Goldstein, Bassam Hajhamad, James Johns, Wolfgang Kleinwächter, William Hoffman, Maria Medrano, Adriana Mendez, Bitange Ndemo, William Saito, Thomas Schneider, Tanya Stoianoff, Oliver Sueme, John Sumpter, Stefaan Verhulst, Livia Walpen and Antonio Zaballos. Special thanks to Nora Abusitta for her hard work in building the foundation for this unique endeavour to succeed.

Contents

Preface from the Network Stewards

DORIS LEUTHARD, President of the Swiss Confederation
LUIS ALBERTO MORENO, President of the Inter-American Development Bank

Digital technologies are quickly becoming the engine of change throughout all sectors of the global economy. By redefining the way in which industries, individuals, institutions and governments all interact, the Fourth Industrial Revolution holds unique promise to create a more inclusive, innovative and resilient society.

Yet with the promise comes a number of challenges in governing how these advanced and emerging technologies are used. The rapid pace of innovation, the threat of cyberattacks, the protection of human rights and the need for adaptive regulatory frameworks are top priorities for policy-makers to address. Balanced, inclusive and accountable digital policies will be fundamental for addressing the growing uncertainty and lack of trust seen throughout the world.

The Digital Protocol Network on National Digital Policy – launched by the World Economic Forum in 2016 – serves as the focal point for framing these emerging policy concerns arising from the digitalization of business and society. The Network's new White Paper, "Digital Policy Playbook 2017: Approaches to National Digital Governance", is an initial output and serves as a pragmatic tool that can contribute to the creation of a fair, accountable and inclusive Fourth Industrial Revolution.

The "Digital Policy Playbook 2017" is designed to help leaders understand the complex dynamics and difficult decisions they will face in managing their transition into the digital domain. With real-world insights on the implications of digitalization, the aim is to strengthen their confidence as they create new opportunities for all while lowering shared risks. By providing a richer understanding of the factors shaping our future, combined with pragmatic tools to drive the outcomes desired, this new playbook will serve to support the core mission of the World Economic Forum: improving the state of the world.

Introduction

RICHARD SAMANS, Head of the Global Challenges Team, Member of the Managing Board, World Economic Forum
FADI CHEHADÉ, Senior Adviser to the Executive Chairman, World Economic Forum

With its mandate to improve the state of the world, the World Economic Forum is embracing this challenge through its new Digital Protocol Network on National Digital Policy. Through this work, the Forum intends to catalyse the prototyping of agile digital governance solutions (i.e. digital protocols) so that the trustworthiness, accountability, fairness and inclusion of all stakeholders can be more fully addressed.

The Forum's Center for the Fourth Industrial Revolution will host and enable the formation and functioning of the Digital Protocol Networks. At its onset, there will be three initial classes of solutions (i.e. protocols) a network can choose from. One class will focus on tools and approaches for government policies, a second class on institutional agreements and codes of conduct, and a third on technical standards. By establishing informal, multistakeholder expert networks, such as the one responsible for creating this White Paper, the Forum will decouple the process of designing contextually relevant solutions from their subsequent implementation, maintenance, enforcement and adjudication. This inclusive approach will enable a more holistic understanding of dynamic issues as well as rapid prototyping at "internet speed".

The Digital Protocol Network on National Digital Policy – the community of experts who created this White Paper – was coalesced with two primary objectives: first, to expose national leaders from the public, private and civic sectors to innovative and practical mechanisms of national digital cooperation and governance; and second, to advance approaches that embrace the local context where adoption and impact can be most effectively realized – but without harm to the transnational nature of the digital space.

The Network has addressed these objectives by delivering a series of case studies exploring how a select number of national communities have addressed key digital challenges in a real-world context. The cases demonstrate different approaches to governance and offer insights on successes, failures and lessons learned in the process.

The outcomes of the National Digital Policy Network will be incorporated into the Forum's Digital Economy and Society System Initiative. This will impact digital cooperation and governance in a variety of ways:

- Provide a set of common principles applicable to core challenges of the Fourth Industrial Revolution
- Recognize and prioritize the importance of policy design and implementation, and the need for governments, businesses and civic groups to actively collaborate
- Discourage governments from implementing over-reactionary policies and regulations because of frustration over the inability to control transnational platforms
- Reduce the risk of digital policy fragmentation around the world
- Help companies understand that they have important global responsibilities, particularly in digital security – they may be transnational businesses, but they have obligations to the countries where they operate

Leadership from the highest levels of public, private and civic institutions will be vital for these new approaches to take root and have a positive impact. Clarity on how to balance complex and competing interests with transparency, trust and accountability will be essential for sustainable approaches to digital governance.

Along with the support and active engagement of global leaders, access to capital will also be required. Funding is needed to engage government officials, business leaders and civil society members to establish real-world pilots, and to enable continuous and active local engagement with impacted user communities. The cost of underinvesting in these key factors will be too great down the road.

Not only should innovative policies be financially resourced at the appropriate level, but recognizing the differences between urban and rural policies also needs to be addressed. As with so many issues, one-size-fits-all approaches are seldom effective, and the differences between rural and urban areas cannot be overlooked.

Alignment on the key performance indicators related to the transformative impact of digitalization is also vitally important. National digital strategies, particularly those focused on digital literacy and gender parity, need to be more than a declaration of good intentions. A list of defined, measurable and implementable indicators is central for sustained progress and investment.

Partner Introduction

SUPARNO BANERJEE, Vice-President, Public Sector Programmes, Hewlett Packard Enterprise, USA

The world is in the midst of a perfect storm. Demographic changes are shifting market boundaries. The Fourth Industrial Revolution is helping to create new products and services at an unprecedented pace, disrupting entire industries. Millennials and Gen Zs are bringing fresh ideas and new ways of working. Consumers and citizens are pervasively connected, and the voice of a single citizen has the reach to sway an entire nation. Yet, a significant percentage of our population remains on the wrong side of a digital divide, natural resources are coming under enormous pressure, and often our normal way of life is being upended by security threats.

These are complex times that often make it difficult to formulate policies and implement solutions that address the fundamental implications of these big, secular shifts, such as growth of new industries and national competitiveness, new business models, longer lifespans, the need for extended social services and trade-offs between improved security and individual rights. These are just a few examples of the multiple tensions that need to be dealt with.

The World Economic Forum "Digital Policy Playbook 2017: Approaches to National Digital Governance" is both timely and relevant, in that this compilation of case studies aims to provide policy-makers and practitioners with a pragmatic tool for prototyping and implementing digital governance solutions.

Aside from allowing unique insights into national approaches to governance, these case studies also perform another very valuable function: they articulate, either explicitly or implicitly, the strategic objectives and the public value of outcomes embodied in their respective national digital policies. These include:

- *Efficiency* in managing service delivery costs and ensuring efficient markets
- Improving *quality* of the services delivered
- Furthering *inclusion* to bridge digital and economic divides
- Enhancing *trust* in digital systems through privacy and security of information and systems
- Ensuring *sustainability* by taking the long view
- Fostering *agility as well as resilience* to allow policies and solutions to be implemented quickly and to respond to stresses, shocks, and citizen and business expectations

When developed comprehensively, integrated national digital policies can achieve these objectives by establishing both the policies and technology roadmaps to deliver shared outcomes. Providing clarity in the roles and responsibilities among government, the private sector, non-profits and individuals creates new forms of collaboration and is central to this Forum-inspired network.

Executive Summary

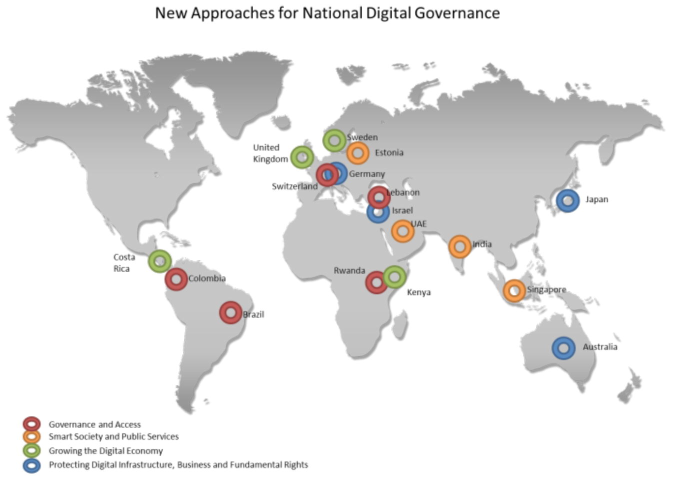
As the effects of the Fourth Industrial Revolution continue, there is a growing need to share pragmatic and practical insights in a more holistic manner to help guide the understanding and actions of digital policy-makers across silos. This White Paper presents case studies that reflect the different approaches countries have used to tackle the challenges of the Fourth Industrial Revolution.

The countries selected were chosen by the National Digital Policy Network to reflect a diversity of geographies and challenges. The four classes of challenges were based on the Open Systems Interconnection “stack”, starting with access and then examining the effects and results of the services leveraging that infrastructure.

The classes of challenges are:

1) Innovating in digital governance and access
2) Developing a smart society and public services
3) Growing the digital economy
4) Protecting digital infrastructure, business and fundamental rights

Source: World Economic Forum


New Approaches for National Digital Governance
Sweden
United Kingdom
Estonia
Germany
Switzerland
Lebanon
Israel
UAE
Japan
India
Costa Rica
Colombia
Rwanda
Kenya
Singapore
Brazil
Australia
Governance and Access
Smart Society and Public Services
Growing the Digital Economy
Protecting Digital Infrastructure, Business and Fundamental Rights

Prepared by a network of experts from more than a dozen countries in an open, collaborative and consensus-building manner, the report aims to be a playbook for government officials, civil society and business leaders. Envisioned as a living resource, the intention is to add new case studies over time as other countries share their experiences with national digital policies.

For those unfamiliar with the term “playbook”, it is a commonly used tool in many sports to provide potential strategies, or “plays”, which a team might execute in response to a set of circumstances during a game. This term was deliberately chosen in recognition of the nature of implementing digital policy: no single right answer exists for every country. The most applicable “play” will depend on the prevailing demographic, economic and political circumstances in each nation. The goal of this White Paper is to present a series of potential policy plays which have worked in specific circumstances, and from which other governments might choose to draw lessons.

Several core themes have emerged from the plays presented in this White Paper:

- Committed political leadership is vital for implementing digitalization strategies and initiatives.
- Agility is paramount to the success of digitalization. Countries are rewarded for creating governance solutions which are adaptable, innovative and collaborative in their implementation.
- The creation and implementation of a comprehensive digital development strategy should transcend the technology sector and embrace different sectors of society and the economy.
- Adequate government structures are needed to manage the digital transformation and to protect digital infrastructure, services and data.
- Multistakeholder digital governance models are unique in their ability to address the complexities of networked societies and economies.
- Partnerships are essential to accelerate positive socio-economic outcomes and to create enabling policy frameworks, particularly for improving communications infrastructure and creating digital public services.

Above all, agility is paramount. The goal of this work is to show the importance of national and transnational governance approaches which can adapt to changing circumstances – a system that mirrors the architecture of the internet itself.

1. Ensuring Innovation in Digital Governance and Access

Virgilio Almeida, Faculty Associate, Berkman Klein Center for Internet and Society, Harvard University, USA

Access and governance are the two fundamental pillars for the construction of national digital strategies that aim to provide access to an open, inclusive, secure and trustworthy internet. Countries in different geographical regions face a broad spectrum of challenges to implement digital policies. Access to the internet in many developing countries is limited by basic infrastructure problems. National digital governance policies and bodies address technical, economic, political and social issues, ranging over privacy, human rights, access to information, interconnection, and administration of protocols, internet names and numbers. This chapter presents case studies that show how different national digital policies have created innovative initiatives to deal with access and governance challenges.

Multistakeholder governance approaches are critical for sustainable digital strategies

The multistakeholder model's emergence is the result of a rather natural development of an unstoppable growing complexity of societies. As the impact of networked digital technologies continues to strengthen global socio-economic opportunities for all sectors of society, the importance of internet governance cannot be underestimated. Given the internet's open, distributed and transborder nature, stakeholders require new and innovative approaches in shaping its evolution. The internet's inherent complexity, velocity of change and lack of centralized control require stakeholders to align on shared principles and protocols which address an array of technical, commercial, social and political concerns with nuance and contextual relevance.

The emerging new capabilities which leverage the internet are opening extraordinary new horizons. From artificial intelligence to the internet of things to the adoption of blockchain, a new era of global development is emerging that represents a Fourth Industrial Revolution. But with this progress come many new challenges that require adaptive and agile governance. Central to this new approach for balancing competing interests on the internet is the adoption of multistakeholder governance models. Multistakeholder approaches are unique in their efficiency, the richness of their collaboration, inclusion and ways to balance competing interests. Brazil, in particular, stands out as a leading example with how it has embraced the concept of multistakeholder governance through its internet governance body, the Brazilian Internet Steering Committee (O Comitê Gestor da Internet no Brasil CGI.br). The innovative multistakeholder nature of CGI.br is unique in many ways.

World Economic Forum Internet for All Initiative

The multistakeholder approach is being applied to the problem of increasing internet access and adoption. Through the Internet for All initiative, the Forum, in close partnership with a national government, convenes a group of 100-200 actors working on the issue, representing all segments of the private sector (both global and local), as well as civil society and community organizations, academics, international organizations, charities and the government.

Through a structured process, these organizations define key barriers to increasing internet inclusion, and then form working groups that address each one. The groups meet regularly to share information on activities in their area of focus, and to develop new collaborative activities to accelerate progress against their goals. These efforts are coordinated by an on-the-ground secretariat that ensures cross-working group collaboration, and are guided by a national steering committee consisting of the leaders of the most active participating organizations.

This approach is yielding results. In Rwanda, the Digital Ambassadors Program, a collaboration between the government, the Digital Opportunity Trust and the Mozilla Foundation, trains 5,000 digital skills trainers who will be posted in rural areas to provide digital skills training to 5 million Rwandans. In South Africa, the Imbizo campaign of internet awareness has already reached thousands of non-internet users in its first months, providing email addresses and ensuring people understand how the internet can benefit their lives. Programmes are also running in Argentina and Jordan, where results are equally impressive, and more countries will join in 2018.

Additional information on the Internet for All initiative can be found at https://www.weforum.org/projects/internet-for-all

Balancing of competing interests

Multistakeholder decision-making, most importantly, represents a de facto system of checks and balances. With a wide range of backgrounds, interests and goals represented at the table, it is less likely that any one group will outweigh the interests of others. It also allows for input on policy issues from groups who, historically, may have been overlooked in decision-making. Opting for a multistakeholder strategy can have time and resource implications; however, when participants are aware of the impact of their decision-making, deliberations are thoughtful and informed; and, this model can increase accountability and legitimacy, and can outweigh the perceived "downsides". Public consultation is valuable only if the challenges of synthesizing large volumes of feedback are adequately resourced so that policy-makers have a clear overview of the range of views represented, and if the offer of consultation is not simply lip service paid in the wake of a predetermined outcome.

National digital strategies

Digital development strategies need to be broad and to address different sectors of the economy and society. The first step of a national strategy is access. Connectivity for all is a fundamental goal for most countries. The development of national digital strategies for broadband access, capacity building, e-government and governance has been proved as a useful initiative to accelerate the digital economy. To be effective, national strategies must include specific relevant targets that should be measurable, realistic and achievable. The national plan of Colombia, called Vive Digital, was key for the expanding access and use of the internet across the country. Rwanda developed in 2000 a National Information and Communication Infrastructure Plan that proposed a vision for 2020 that would ensure access for all citizens. The plan was regularly refreshed and updated, on a cycle of five years.

Promotion of public-private partnerships for improving connectivity

To tackle digital infrastructure challenges, many countries make use of public-private partnerships (PPPs). Effective regulation and PPPs are combined to encourage private investment to make access universal and affordable. Public investment in communication infrastructure usually concentrates on regions that are characterized by social or strategic needs. One secret to the success of Colombia and Rwanda in the implementation of digital policies was the use of PPPs. Through a PPP with initial investments of over $400 million, more than 19,000 kilometres of cable were laid across Colombia between 2010 and 2017. PPPs have been recognized as one of the key levers to foster internet access across Rwanda.

Additionally, another key contributor to the success of these policies was recognizing that the need for analysis should not only be at the national level, but also should address the differences between urban and rural areas. The scope and magnitude of the connectivity challenges can generally be linked to geographical considerations.

Along with the need to account for urban/rural differences and a commitment to provide universal access to the internet, it is also important to ensure the quality and speed of the internet connectivity is sufficient. It is important not only to have access and coverage to internet service, but also to ensure the quality, speed and reliability required by different types of real-time services can be deployed so that the intended end users actually reap the benefit. If there is access but the speed and quality is insufficient, the impact of digitalization within the economy will not materialize.

Federative Republic of Brazil

Play

Developing a multistakeholder internet governance model

Overview

Brazil has developed a multistakeholder internet governance model in a way that truly engages different sectors, including civil society, government, academia and business. Its model remains a concrete example for any country seeking to build an effective multistakeholder governance body.

Key Lessons

– Creation of the Brazilian Internet Steering Committee (CGI.br). Responsible for most internet-related issues in the country, including the coordination and integration of all Brazilian internet service initiatives, the CGI.br was created by a presidential decree in 1995. The Brazilian government established it as a multistakeholder, non-regulatory governance body. Two years later, Brazilian telecommunications legislation defined the internet as a “value-added service” that was different from the telecommunications infrastructure supporting it. This innovative approach allowed the internet to grow quickly in Brazil. The CGI.br board has 21 members: nine from government organizations, four from civil society, four from the private sector and four from the academic and technical communities. Government members are appointed, and all other members are elected by their respective communities. No single sector, even government, has a majority of votes on the board.

– Creation of the Brazilian Network Information Center (NIC.br). The executive arm of the CGI.br, the NIC.br was created to implement to implement CGI’s decisions and projects. Its mission involves certain rights and obligations, which include a) registering and maintaining “.br” domain names, as well as allocating autonomous system numbers and IPv4 or IPv6 addresses in the country; b) handling and responding to computer security incidents involving networks connected to the Brazilian internet (activities to be carried out by the Brazilian National Computer Emergency Response Team); c) projects that support and improve the country’s network infrastructure, such as the direct interconnection between networks and the distribution of the Brazilian Official Time (NTP.br); d) producing and publishing indicators, statistics and strategic information on the development of the internet in Brazil; and e) promoting studies and recommending procedures, regulations, and technical and operational standards that will improve network and internet service security, as well as ensure its increased and adequate use by society. The NIC.br invests in actions and projects that aim at improving the internet infrastructure services available in Brazil.

– Creation of the “Bill of Rights” for Brazilian internet users (“Marco Civil”). The Marco Civil Law is distinctive due to its substance and how it was created. Marco Civil applies to the internet’s key principles, such as freedom of expression, net neutrality and due process. How it was created and enacted are also important. Conceptualized in 2007, Marco Civil was drafted over many years, using an open multistakeholder process through which members of the public, government, global and local internet companies, civil society and others engaged in negotiations over the legislation’s text, largely mediated through an online platform passed in 2014.

– Creation of information infrastructure. PTT Metro (PTT is the Portuguese acronym for Internet Exchange Point [IX]) is composed of IXs in the main Brazilian cities. Begun in 2004, the project now has 12 IXs, with an aggregated peak in traffic of over 30 gigabytes per second (Gbps), and more than 200 participants. The biggest IX is PTT São Paulo, with more than 100 members and a peak in traffic of 25 Gbps. Participation is free of charge for all interested autonomous systems, except for the connection costs to some of the connection points of a given IX (the participant does not pay for the exchanged traffic).

– Creation of the Brazilian National Computer Emergency Response Team (CERT.br) within a multistakeholder governance body. Maintained by NIC.br, CERT.br is responsible for handling computer security incident reports and activity related to Brazilian networks connected to the internet. It serves as a focal point for incident notification in the country, providing the coordination and necessary support for organizations involved in incidents.

Description

Consensus building is a key activity for multistakeholder governance bodies. Stakeholder representatives present their views and positions on an issue, and then engage in a dialogue to achieve mutual understanding of problems. The quest for consensus in multistakeholder bodies is almost never an organized or orderly process. Because all stakeholders participate on equal footing, discussions are usually messy, with unpredictable developments. A basis of equal footing is an essential characteristic of multistakeholder models that aims to reduce groups' traditional influence and power, such as economic and political influence.

Some of the challenges associated with implementing multistakeholder governance bodies are:

- How can the most adequate set of stakeholders be identified to work on an issue?
- How can the mechanisms be defined for selecting representatives from different groups?
- How can influential non-governmental organizations and corporate power be prevented from capturing the multistakeholder process?

The central part of Brazil's internet governance ecosystem is the CGI.br. Created by Interministerial Ordinance 147 of 31 May 1995,[1] which was amended by Presidential Decree 4,829 of 3 September 2003,[2] its purpose is to coordinate and integrate all the country's internet service initiatives, as well as to promote technical quality, innovation and the dissemination of the available services.

The CGI.br constitutes an internet governance model for societies to effectively participate in decisions involving network implementation, management and use. Based on the principles of multilateralism, transparency and democracy, the CGI.br has been democratically electing representatives from civil society since July 2004 to participate in discussions and to debate priorities for the internet together with the government.

The CGI.br's main responsibilities are to: 1) establish strategic guidelines related to the use and development of the internet in Brazil; 2) recommend standards for technical and operational procedures for the internet in the country; 3) establish guidelines to orient the relations between the government and society in the execution of the Domain Name System registration activities, in the allocation of Internet Protocol (IP) addresses and in the administration of the country code top-level domain; 4) propose research and development programmes related to the internet; 5) promote statistical studies and recommend procedures, norms, technical and operational standards for network and internet services security, as well as for its growing and adequate use by society; and 6) participate in national and international technical fora for internet governance.

Resources

Brazilian Internet Steering Committee (CGI.br)
Brazilian Network Information Center (NIC.br)

Colombia

Play

Increasing internet access and the use of information and communications technology

Overview

Colombia's Vive Digital Plan is a comprehensive strategy with the goal of reducing poverty, creating jobs and boosting economic growth by leveraging the power of information technology (IT). The Plan's two phases (2010-2014 and 2014-2018) have focused on expanding the availability, accessibility and use of information and communications technologies (ICTs) across the country. With programmes ranging from digital literacy, local app development, and building trust and security in the internet, the Plan's first and most basic challenge was expanding the country's IT infrastructure while lowering the cost of access.

Key Lessons

- A comprehensive strategy reaps the benefits of the digital economy
- Access and affordability go hand in hand
- The availability of technology needs to be coupled with training and literacy programmes that encourage productive use of ICT

Description

Colombia's award-winning national digital strategy has been recognized for its vision and achievements in transforming the country's digital landscape. Launched in 2010, the Vive Digital Plan coupled the expansion of IT infrastructure across the country with policies and programmes that facilitated and ensured ICT adoption and use. These range from initiatives to build trust and confidence in the internet, to lowering the cost of ICT access and ownership, to digital literacy training for all citizens and specialized programmes for teachers and small businesses. The Plan also included measures to promote application development for the "base of the pyramid" – in other words, applications and online services that would provide value to the country's most disadvantaged socio-economic segments, thus bringing the benefits of technology to all Colombians.

Multiple organizations and international awards have recognized the Plan's comprehensive and strategic approach of bridging the digital divide and harnessing the power of ICT for economic development. But expanding IT infrastructure and access to ICT – the most fundamental aspect of the Plan – is a success story in and of itself.

Upon the Plan's launch, only 200 (17%) of the country's 1,122 municipalities had access to the optical fibre network. To expand the existing network to provide universal internet access, Colombia's Ministry of Information and Communications Technology (MinTIC) launched the National Optical Fiber Project in 2011. Several groups participated in the competitive process to build the country's optical fibre internet network. Through a public-private partnership with initial investments of over $400 million, more than 19,000 kilometres of cable were laid across the country between 2010 and 2017 – the most extensive network in Latin America. By the end of 2017, 95% of Colombia's municipalities will likely be connected to this network.

The remaining 5% of municipalities that cannot be reached via the optical fibre network due to rugged terrain or remoteness are being connected through the High Speed Connectivity Project. It uses a mix of high-speed satellite and terrestrial connections to reach about 445,000 Colombian citizens spread across 60% of the country's territory. The most remote and inaccessible of these areas – Colombia's Amazon region, for example – are being connected through wireless broadband. The Project is currently installing 142 towers that will complete the goal of internet coverage across Colombia.

The Vive Digital Plan also seeks to expand the availability of mobile broadband across the country. During the Plan's first phase (2010-2014), the government worked to transition from 3G to 4G by holding auctions for the 700 MHz band as well as the 900 MHz, 1.9 GHz and 2.5 GHz bands. As a result, Colombia now has six 4G operators and 770 municipalities on the 4G network. The Plan's second phase (2014-2018) continues to work towards efficient allocation of spectrum to promote innovative uses of technology. Initiatives include assigning an additional 245 MHz for 4G use, promoting the flexible use of both licensed and unlicensed spectrum, and freeing up additional spectrum for the internet of things.

Deploying this extensive network has put Colombia within reach of its goal of universal internet access for its municipalities, but challenges remain in extending the network into homes, schools and businesses. To fill the gap until the private sector connects the last mile, MinTIC committed to creating public or community access points across the country, with 6,926 Kioscos Vive Digital in rural and remote areas, and 894 Puntos Vive Digital in urban areas. The Kioscos provide at least one internet access point for villages and towns with more than 100 residents. These free public access points can be used for digital literacy training, internet access, and access to online government services by Colombians who don't own ICT devices or have internet connections at home. The country also has 645 free Wi-Fi hotspots, located mostly in parks, squares or tourist sites, with the goal of having 1,000 by 2018. Moreover, for a period of five years, the government will support free broadband service in 2,000 public institutions, usually in the education, health and cultural sectors.

In addition to expanding the infrastructure required to make IT and the internet accessible to its citizens around the country, the Colombian government has also implemented a comprehensive strategy to give all citizens the ability to harness the power of ICTs for their personal economic growth and development. First, it took steps to ensure that ICT services are affordable. Colombia signed on to the World Trade Organization's Information Technology Agreement, which eliminates tariffs on tech products, thus lowering costs for technology service providers as well as consumers. The government also eliminated taxes on the sale of computers. Following the elimination of tariffs and taxes, Colombia claimed to have the lowest-priced computers and tablets in Latin America. These two policy decisions have lowered the price of ICT hardware in the country, making it more affordable and accessible for a broader segment of the population. A study released in 2017 found that, for every 100 Colombians, there are 35 smartphones, 10 notebook computers, 8 desktop computers and 6 tablets.

In collaboration with the Ministry of Housing, MinTIC also subsidizes home internet access for lower-income households. These subsidized connections have benefited 140,000 homes, and the programme has contributed to internet access by reaching 41.8% of households. Beyond executing on the infrastructure and policy environment to make the internet and ICTs accessible to all Colombians, the government has training programmes to encourage the productive use of ICT that can lead to the Plan's goal of creating jobs and boosting economic growth.

At the most fundamental level, the En TIC Confio programme promotes trust and security in the use of ICT and the internet. It aims to build trust in technology while educating Colombians on how to use the internet productively and responsibly. In addition to the digital literacy training available for free at the Puntos and Kioscos Vive Digital, the government launched the Computadores para Educar [Computers for Schools] programme, which has delivered 1.9 million internet-enabled computers and tablets to schools. School teachers are being trained in ICTs so they can use these tools to improve the quality of education across the country.

Programmes also exist for training microenterprises on how to use the internet and ICTs to increase productivity and efficiency, and for training coders and application developers, among others. The MiPyme Vive Digital programme aims to bring Colombia's micro-, small and medium enterprises into the digital economy. By demonstrating the gains in productivity and efficiency that can come from using and adopting technology, the programme has helped to increase ICT adoption from 7% to 60% of these businesses. During the Vive Digital Plan's second phase, the goal is to have these enterprises go beyond internet connection to online presence and the use of e-commerce.

Through the Plan, Colombia is executing a vision to integrate the country in the global digital economy. Moreover, the government seeks to integrate all Colombians into the digital economy by eliminating the digital divide. Colombia has made great strides in laying the groundwork towards these goals and one of the foundational objectives of the Plan. Providing universal internet access is within grasp.

Resources MinTIC Plan Vive Digital (http://www.mintic.gov.co/portal/vivedigital/612/w3-channel.html)

Republic of Rwanda

Governance and Access

Play

Fostering internet access and use as a strategy for innovating and rebuilding a nation

Overview

As Rwanda rebuilds itself following the 1994 genocide, it looks towards 2050, when it plans to be a knowledge economy powered by technology.

Key Lessons

- The importance of good leadership and political will cannot be overstated. The story of Rwanda's transformation through access to technology is a testament to the pivotal role of good political leadership in the country's recovery and ascent as a rising success story over only two decades.

- Working closely with the private sector signalled the country's vision to deliver access to all. This included an enabling environment for business (Rwanda ranked 2nd in Africa in the World Bank's *Doing Business 2017* report), the prioritization of public-private partnerships (PPPs) for implementing national projects, and initiatives to cultivate a local innovation ecosystem.

- Rwanda's young population (median age of 19 years) holds great promise to leverage information and communications technology (ICT) for shaping the economy in the future. Building capacity and skills, and revising education curricula to prepare for the Fourth Industrial Revolution, are top national priorities.

Description

Rwanda, "the land of a thousand hills", lay in ruins at the end of the 1994 genocide. With the society's social fabric torn apart and infrastructure destroyed, the new leadership immediately began to drive reconciliation and reconstruction efforts across the nation.

In 2000, the government outlined its Vision 2020 to transform Rwanda into a knowledge economy.[3] Given that the country is landlocked with few natural resources, the government elected to tap into human capital to drive development and growth. Recognizing that ICTs are a linchpin to achieve this goal, efforts have been directed at increasing internet access for all Rwandans.

The key pillars of Rwanda's policy interventions to strengthen equitable internet access are:

Pillar I: Building foundations (ICT strategy and roadmap)

Adopted in 2000, the national ICT strategy and plan enumerated a four-phase approach to ensure access for all Rwandans and achieve Vision 2020. During the plan's Phase I, milestones were reached, which included establishing the Telecom and Utility Regulatory Authority, liberalizing the telecommunications industry in 2001 (the number of companies providing telecom and internet services increased from 1 to 12; and, mobile phone penetration in Rwanda stands at 79.2%, and internet coverage at 35.4%), and introducing the Rwanda Internet Exchange Point.

During Phase II (2006-2010), key infrastructure was put in place, including the national fibre optic backbone, the Kigali Metropolitan Network and the Tier-III National Data Center. With the institutions and infrastructure in place, four cross-cutting clusters were identified for Phase III (2011-2015) to continue the momentum towards Rwanda's policy goals:

- Skills development: In 2012, Carnegie Mellon University opened its first African campus in Rwanda. The presence of this world-class technology institution in Rwanda is already transforming the quality of technology education in the region.
- Private-sector development: Efforts have gone into developing the private sector, including the opening of kLab, the country's first tech innovation hub, in 2012.
- E-government: The government is part of a PPP with a private Rwandan technology company to transform government service delivery to citizens. Digitizing services (online and on mobile) takes services to the last mile, thereby reducing cost and time for citizens, and driving increased transparency and efficiency from government officers.
- Cybersecurity: The government established the National Computer Security Incident Response Center in 2015 and promulgated the first National Cybersecurity Policy to ensure the security and resilience of Rwanda's cyberspace.

From 2016 to 2020, Rwanda intends to consolidate its efforts to complete the country's ICT transformation. In addition to the national ICT strategy, policies and initiatives have been developed to stimulate internet adoption and the creation of an innovation ecosystem.

Pillar II: Fostering internet access, adoption and the development of local content

1. Broadband policy: Recognizing broadband as a utility, this policy sought to facilitate the increase of accessibility, affordability, reliability and usage of broadband services throughout Rwanda. The government has since entered into a joint venture with Korea Telecom for providing an open-access wholesale 4G-LTE network, the first in Africa. By the end of 2017, 97% of the population will have access to 4G.
2. Other policies and initiatives: These include the Smart Rwanda Masterplan (2015-2020), which outlines PPPs as a pillar for the success of public projects; the National Digital Talent Policy, with a Digital Ambassadors flagship initiative to have youths nationwide equip 5 million Rwandans with digital literacy skills; the National Innovation Policy to foster innovation through research; the Viziyo Initiative, in partnership with the private sector, to accelerate penetration of smart devices to underserved communities through loan schemes; and the Women Empowerment in Technology Strategy that is currently under development to bridge the gender divide in internet access and usage.
3. Smart Africa Initiative: Championed by the President of Rwanda, Smart Africa is an alliance of 21 African heads of state committed to accelerating socio-economic development through affordable access to broadband and usage of ICT. The alliance is already driving pan-African collaboration.

Efforts over the course of the past 17 years continue to yield results: internet penetration in Rwanda increased from 8% in 2012 to 35% in 2017. As usage and adoption continue to grow, the positive impact of increasing access for citizens is evident across all clusters of socio-economic development, including health, education and public service delivery.

Pillar III: Establishing internet governance

Along with its forward-looking policies on improving internet access to drive positive socio-economic gain, the Rwandan government has also recognized the importance of putting sound governance instruments in place to accelerate deployment of technology and inclusively serve the interests of all Rwandans.

Rwanda Utilities Regulatory Authority (RURA), the autonomous regulatory body overseeing internet governance, was created by law in 2001 with the mission to regulate telecommunications, information technology, broadcasting and internet technologies. It acts as the arbiter in ensuring fair competition and protecting consumers' interests and rights among policy-makers, licensed service providers (industry) and consumers in the aforementioned regulated sectors. RURA is also the accreditation and assessment body of certification authorities (CAs) for issuing digital certificates on the Public Key Infrastructure. RURA oversees the activities of the Rwanda Information and Communication Technology Association (RICTA). RICTA manages the Rwanda Internet Exchange (RINEX) and ".rw" registry:

1. The exchange's infrastructure is hosted at the neutral Virtual Landing Point. The introduction of RINEX had a significant effect on the internet's quality in Rwanda. Networks connected to RINEX exchange traffic directly with peers and no longer pay exorbitant transit fees to exchange data at hubs outside the country, resulting in faster internet speeds.
2. Given the high cost of Internet Protocol transit within Rwanda (because the nation is landlocked and not close to submarine cable landing points), RICTA is advocating for price differentiation between local content and content "fetched" from outside the country; this is expected to reduce the cost to end users.
3. RICTA engages content delivery network (CDN) service providers to host their caches at RINEX or within Rwanda (i.e. in a hosted network). In 2014-2015, RICTA successfully agreed with Akamai, one of the biggest CDN service providers, to host a cache in Rwanda.
4. Given the very low hosting fees available outside Rwanda (the offering of almost unlimited space and substantial computing capacity at a very low price), hosting content locally is comparatively expensive, making it difficult to compete with packages from providers outside Rwanda. RICTA is working on the Rwanda Web Hosting project to support the creation and, more importantly, the local hosting of local content. The project seeks to enable a local hosting business environment by working with local partners to build a subsidy model, with the aim to start bringing existing local content back to Rwanda from wherever it is hosted at the moment, and to create new content. RICTA is working closely with RURA and the Internet Society, among other stakeholders, on this project.

Resources

Rwanda Ministry of Youth and ICT (http://www.myict.gov.rw/home/)
Rwanda Utilities Regulatory Authority (http://www.rura.rw/index.php?id=23)

Lebanon

Play

Building out post-conflict internet infrastructure through multistakeholder efforts

Overview

In the absence of stable government in post-conflict Lebanon, multistakeholder partnerships have been critical to the buildout of the country's core internet infrastructure.

Key Lessons

– Creation of an engaged internet community helps to defend key internet principles.
The Lebanese internet multistakeholder community embraces and defends the internet's key principles, such as internet access for all, freedom of expression, net neutrality, no restriction on content and services, the safeguarding of privacy and security, fair access to public infrastructure and open access to cumulative commons data. The development of the community is inclusive, gradual and organic, leading to a self-renewing, healthy and sustainable ecosystem.

– Internalization of the open multistakeholder consultation process is critical to governance.
Over many years, Lebanese internet stakeholders engaged in long sessions of critical thinking on the outcome and effect of, as well as alternatives to, the governance structure. While acknowledging that multistakeholder governance will introduce complex processes with insecure outcomes, they made a conscious decision that multistakeholder governance is a strategic and preferred option for the country's internet governance. The Lebanese Academic and Research Network, Beirut-IX, the Lebanese Broadband Support Group, the Lebanese Internet Center (LINC), the E-Transaction Law and the Access to Information Law, to list a few, were all conceived, drafted, established and/or enacted using open multistakeholder processes. Members of the government, civil and academic communities, private sector and individuals engaged in open brainstorming and negotiating sessions, published their works openly and collected comments through online platforms.

– A declaration of principles regarding broadband can help enable economic growth and social development.
The Lebanese Broadband Manifesto is a declaration of deeds and principles that recognizes access to true broadband in the country as a right of each citizen, and a critical enabler of economic growth and social development. Government organizations, businesses, civil society, academia and individuals were invited to act in their personal and national interests by becoming part of an independent multistakeholder lobbying movement. The manifesto aims to give Lebanon the chance to be a competitive and prosperous contributor to the global knowledge economy, where true broadband connectivity is a main enabler.

– Community-managed information infrastructure is efficient and effective.
Ad hoc information infrastructure, created and managed by informal internet multistakeholders, is efficient, effective, resilient and sustainable, especially in the event of calamity or disaster. The Lebanese Domain Registry, Beirut-IX, Open Data Lebanon and the Lebanese Internet Center (LINC) are bottom-up multistakeholder ad hoc organizations created, governed, managed and operated by volunteers for the public interest. They all maintained and sustained quasi-normal operation and growth while faced with devastating wars and civil and political unrest. An engaged multistakeholder community proved to be the best safeguard, as well as an efficient and effective agent of risk mitigation and business continuity.

Description

Lebanon has spent much of the past four decades in a state of conflict. The Lebanese internet and digital industries developed organically within this deeply challenging context. For a country that some regarded as having the slowest internet speeds in the world, Lebanon is now slowly emerging as a thriving centre for young innovators, which is no small feat. Multistakeholderism has been at the core of digital development, allowing actors outside of government to take the lead.

Lebanon is a leading example of partners coming together in a challenging challenge, with industry, civil society and academia driving digital development. The multistakeholder model has been hailed as best practice for digital and internet governance. Lebanon illustrates that multistakeholderism may also be the most pragmatic internet governance model in post-conflict settings. Progress has not been without its problems, however. Although the Ministry of Telecommunications was the co-sponsor of work leading to LINC, political and administrative roadblocks held up LINC's operation as a public-private organization. Lebanon's broadband connectivity covers a large part of the country, but the average broadband speed of around 2 megabits per second needs to be dramatically increased. Openness is an important and positive aspect of the internet in Lebanon, where the country's constitution guarantees free speech and other principles of human rights.

Lebanon's internet (digital) governance issues are split between several government bodies: the Office of the Minister of Administrative Reforms (e-government issues), the Ministry of Telecommunications (including telecommunication, wired and wireless connectivity, broadband, mobile and duct access), the Ministry of Economy and Trade (business readiness), the Central Bank of Lebanon (technology start-ups) and the Telecommunication Regulatory Authority (representation at the International Telecommunication Union and the Internet Corporation for Assigned Names and Numbers).

Several partnerships between the Government of Lebanon and the private sector have sought to improve and expand access to the internet. The most significant was the Partnership for Lebanon, established in September 2006. According to Cisco in its 2010 "Corporate Social Responsibility Program Brief", the programme aims to "support post conflict reconstruction efforts and help the people of Lebanon find a path to stability and long term economic growth by leveraging public-private partnerships and collaborative technologies to create scalable, replicable, and sustainable solutions for country transformation. The Partnership was founded by Cisco, Intel, GHAFARI, Occidental Petroleum, and Microsoft."

BeirutIX, Lebanon's official internet exchange, was launched in April 2008 as a multistakeholder effort between the private sector, civil society and the academic community to stimulate economic growth, and the Lebanese Broadband Manifesto Support Group was established in October 2008. The Broadband Manifesto – Economic Growth and Social Development for Lebanon campaign, launched in 2006, gathered more than 8,000 signatures from businesses, civic and academic institutions and individuals demanding real broadband at affordable prices. The campaign was instrumental in pushing the government into offering Digital Subscriber Line (DSL) services, as well as initiating work on a national broadband strategy. The focal point of this multistakeholder endeavour was LINC, a bottom-up, non-profit PPP launched in 2014. LINC's alliance of civil society organizations, corporations, syndicates, universities, research organizations and the government aims to fill long-standing gaps in internet governance in Lebanon.

Various attempts have been made to coordinate Lebanon's digital policies, but no comprehensive strategic plan for the digital economy exists to date. The ICT Coordination Office, under the Office of the Prime Minister, developed the skeleton of the National ICT Strategy Action Plan in 2011, and the Ministry of Education developed the National Educational Technology Strategic Plan in 2012. However, the Lebanese government did not adopt the strategies, except for bits and pieces of the action plans executed in silos. The latest attempt was made in 2014 by the internet multistakeholder community to create LINC, which was mandated to govern and operate the .ib country code top-level domain registry.

Resources

Lebanese Internet Center (LINC) (http://www.isoc.org.lb/events/linc-launching-moet-june2014)
Lebanese Broadband Manifesto (http://www.isoc.org.lb//broadband-manifesto)

Swiss Confederation

Governance and Access

Play

Creating networked transformation processes through dialogue

Overview

In 2016, the Swiss government adopted its national Digital Switzerland strategy. It provides guidelines for government action and indicates where and how authorities, academia, the private sector, civil society and politics must work together to shape the digital transformation process for the benefit of all. A national dialogue with different stakeholders has been launched to discuss implementing and further developing the strategy.

Key Lessons

– Cooperation between all federal levels of the administration and the private sector, civil society and academia is crucial to seize the opportunities of digital transformation.
– Different stakeholders need to be included when implementing and assessing the national digital strategy, and when developing it further.
– Accessibility can be guaranteed through a universal service that provides broadband connections everywhere at an affordable price and a specified quality.
– The digital strategy needs to be embedded in the wider context of national policies, such as cybersecurity, energy policy and development cooperation.

Description

In April 2016, the Swiss government adopted a new overall strategy called Digital Switzerland. It focuses on the opportunities to use digital transformation for positioning the country as an attractive place to live and as an innovative, future-oriented location for business and research. The strategy provides guidelines for government action and indicates where and how authorities, academia, the private sector, civil society and politics must work together to shape the transformation process for the benefit of everyone in Switzerland.

Switzerland is generally in a very good position concerning telecommunications infrastructure and the use of information and communications technology (ICT). The Swiss Federal Council has had strategic guidelines since 1998 for an information society in Switzerland. However, the previous strategy documents concentrated mostly on the federal administration. For Switzerland to succeed in the digital arena, however, all stakeholders must work closely together. Digital Switzerland is therefore defined as an innovative umbrella strategy that, by following a multistakeholder approach, intends to coordinate the numerous activities and existing expert groups already in place, as well as the activities of the federal administration.

A key element is the national dialogue on Digital Switzerland, which the government launched in 2016 and where it assumes a moderator's role. Its objective is enhanced cooperation between all stakeholders and the exploitation of synergies between all federal levels of the administration and the private sector, civil society and academia. Switzerland is in a strong position, thanks to its multicultural nature and willingness to engage in dialogue and search for consensus, in addition to its pragmatic processes of direct democracy.

In the context of this dialogue, regular national conferences will be organized. The first one, in November 2017, will include topics such as digital political governance, education, innovation, digital transformation of the public sector, sustainability, the labour market in the digital age, cybersecurity and a framework for data policy. Together with external stakeholders, the government will take stock of and assess the necessity for new strategic objectives and measures towards a digital Switzerland.

Reliable, internationally competitive and affordable high-speed network infrastructure is the prerequisite for developing new ways of living and working, and providing new services and products. One of the key objectives of the Digital Switzerland strategy is therefore to guarantee equal opportunities and the participation of all in the information society: All Swiss inhabitants shall have low-cost, non-discriminatory access to high-quality network infrastructure and innovative services and applications.

In principle, the Swiss telecommunications market, liberalized in 1998, must prioritize meeting the needs of users. In some circumstances, and particularly in the peripheral and mountainous regions, users might not enjoy basic telecommunication services. Such cases are avoided through a universal service that guarantees a basic offering of services for the population throughout the country at an affordable price and a specified quality. The universal service to date includes telephony, telefax, data transmission, broadband internet connections, access to emergency services, public payphones and the provision of special services for the disabled. Its provision is guaranteed by a licence, which is awarded based on a public invitation to tender. The company Swisscom has provided the universal service since 1998.

The content of that service is updated regularly and has been redefined by the Federal Council from 2018 onwards. The new licence enters into force on 1 January 2018, and will run until 31 December 2022. Swisscom will continue to provide the universal service, with affordable telecommunications services available to all households in the country.

From 2018, the classic analogue and digital connections will be replaced by a multifunctional Internet Protocol-based connection. For the internet access included in the universal service, the Federal Council increased the minimum download/upload data transmission rate to 3,000/300 kilobits/second from 1 January 2018. Telefax and public payphones are no longer part of the universal service. Services for the disabled included in the universal service are being expanded: in addition to existing offerings, such as SMS transcription and the directory service, a sign-language relay service using video telephony for the hearing-impaired is now included in the universal service.

Based on Switzerland's federal constitution, the Digital Switzerland strategy is also embedded in the wider context of Swiss policies, and takes into account other existing government strategies. One example is cybersecurity. As current conflicts and tensions demonstrate, the digital space is increasingly being used for destabilization. Switzerland intends to counter this trend by campaigning for open, free and secure cyberspace, based on clear rules and mutual trust. The Digital Switzerland strategy emphasizes this and specifically refers to a national strategy for the protection of Switzerland against cyber-risks.

A link also exists between digitization and Switzerland's climate and energy policy objectives. The Digital Switzerland strategy recognizes the opportunities digitization offers to improve energy and resource efficiency, and calls for actively exploiting these opportunities. The strategy also acknowledges the importance of ICT as a critical resource for sustainable development in all areas of life. Switzerland therefore commits itself to equal access to the internet for the world's entire population, to fighting poverty using ICT and to linking the results of the World Summit on the Information Society (WSIS) with the United Nations Sustainable Development Goals.

The multistakeholder approach in Switzerland also entails some challenges. Firstly, as many different parties are involved, conflicts of interest may arise that need to be addressed. Definitions of clear rules and competences are also required. The Federal Council charged the Federal Office of Communications within the Department of the Environment, Transport, Energy and Communications with coordinating the activities linked to the Digital Switzerland strategy and bringing the different players together.

One policy challenge for Switzerland is to ensure that all its citizens can use ICT to participate competently in political, social, economic and cultural processes. The different federal levels in Switzerland (i.e. the confederation and the cantons) need to closely coordinate their strategies to safeguard and improve quality when integrating ICT into the educational system. To foster applied research and development is also crucial in this regard. To meet the needs of a digital society and economy, and to maintain Switzerland's leading position as a location for innovation and research, a targeted approach should be used to promote new education and training opportunities, university teaching positions and research centres, while considering the division of skills and university autonomy.

Another key policy challenge for Switzerland is the development of a coherent and future-oriented data policy, as stipulated by the Digital Switzerland strategy. This policy must ensure the potential of the growing collection and processing of data can be realized to Switzerland's advantage, without losing control of this data. Furthermore, Switzerland shall establish itself as a safe international location for data storage and as an ICT hub by establishing suitable general conditions.

Resources

Digital Switzerland strategy
(https://www.bakom.admin.ch/bakom/en/homepage/digital-switzerland-and-Internet/strategie-digitale-schweiz/strategy.html)

Universal service
(https://www.bakom.admin.ch/bakom/en/homepage/telecommunication/the-universal-service-with-regard-to-telecommunications.html)

2. Developing a Smart Society and Public Services

Bassam Hajhamad, Partner and Consulting Market Leader, PwC, Middle East

The smart digital era

The advent of smart societies led by digitally savvy governments is clearly apparent and here to stay. This begs the question of whether governments are ready, and how best to go about implementing digital change. Regardless of the political or economic conditions, and the sector or nation in which one lives, the pace and impact of digital technology is increasingly felt across every sphere. While the digital revolution has traditionally been attributed to the private sector and indeed owes a lot of its roots to it, forward-looking governments are taking on a new role in influencing this mix and, in many cases today, are leading innovative services through the public sector. A key driver for adoption has been improved service delivery at lower cost, contributing to more efficiency and to effective and collectively created public offerings. Successful governments should readily engage, adopt and indeed lead the digital technology transformation of their respective nations.

As this chapter shows, critical success factors contribute towards the development of smart societies, with mature governments playing a role at the forefront. It examines the drivers of digital government transformation and the typical process of national digital adoption, proven digital technologies and standards which have paved the way for other nations to leapfrog development, ecosystem imperatives and constraints, as well as leadership and governance matters which are central to realizing the benefits of this change. To derive tangible results, it is noteworthy to further cross-examine the above by applying a lens of centralization, national scale and political will.

Digital government models

To build sustainable digital societies requires adherence to dedicated planning and coordination, as well as phased implementation. From the outset, two broad digital government models exist. Acknowledging that each government has a unique setup, a hybrid of these two models is generally adopted in practice.

A centralized model usually applies for smaller governments, and a more decentralized version works for larger governments. For example, Singapore adopted the former model early on under its Smart Nation programme, which saw the central government authority – Singapore's Infocomm Development Authority – transform into a central regulatory arm (Info-communications Media Development Authority) and central enactment/activation arm (Government Technology Agency) with a dedicated Governing Council, Sector Committees and the Prime Minister's Office overseeing chief information officer (CIO)-specific protocol across sectors. Similarly, each ministry in Estonia has a dedicated CIO who coordinates with a central government CIO office. On the other hand, due to their sheer scale and thus implementation challenges in their digital journey, larger nations typically establish e-specific government authorities (e.g. the Unique Identification Authority of India). These digital authorities will rely on an ecosystem of multilayered and trusted networks which are fuelled by private-sector engagement.

In all cases, a cultural shift championed by specific leaders is an important trait for successful digital government transformation. To drive change, successful government programmes are steered by hand-picked private-sector technology pioneers who are positioned at the top of these new governing authorities. These leaders seek to change the traditional government culture of being risk-averse to inspire and promote a risk-taking culture within a secure environment. They apply innovative and entrepreneurial practices early on, such as test labs in Singapore. These platforms allow ideas to flourish and pay attention to the timeliness of implementation over excessive planning. Prioritizing the need for digital literacy, as well as addressing gender equity, is central for a smart society. Having a society that understands the benefits of the internet and knows how to improve quality of life is one of the main aspects of growth and development.

Digital government journey

Against the backdrop of different government models lies the digital journey. The first step in the digital government journey commences with computerizing and establishing common infrastructure to push all government services online.

The second step on the journey is that of moving to a single platform of public service delivery. This focuses on mobility and simplifying the citizen/user experience. Estonia and India both embarked on building a single digital identity system, whereby citizens utilize a single identity across numerous public (and later private) services. Albeit different in culture, scale and scope, the systems rely on interoperability and integration across technology atmospheres. This requires coordinated efforts across regulatory and legal domains, cross-sector collaboration and embracing an "open culture" (e.g. open standards, open source, etc.).

The final step in the journey is no better exemplified than by Singapore's GovTech initiative. It places citizens at the centre of service design and delivery, utilizing technologies such as artificial intelligence, robotics and blockchain to conduct predictive behavioural analytics to determine the most beneficial products and services for citizens, and the best means of end-to-end delivery. Here, a new cadre of digital leaders proactively drives initiatives through organic growth (rather than through a traditional top-down approach).

Digital public service success imperatives?

Building an integrated and sound set of efficient and effective public services through the adoption of digital technologies is no easy task. It demands sometimes very complex systems, capabilities and mindsets to cohesively operate in a dynamic manner. In all cases, support from the highest levels of government sponsorship is a prerequisite of digital government transformation for change. Instilling an "open culture", which adopts private-sector characteristics (e.g. Singapore's Technology Skills Accelerator [TeSA]) and sometimes challenges the traditional government model norms, pays remarkable dividends. Through this effort, good governance forms the backbone to successful end-to-end delivery, and, as can be seen in the case of Singapore, both national and sector-level active stakeholder participation is imperative.

A nation's infrastructure readiness, without which governments face the risk of rapidly losing benefits derived from investments, is also of paramount importance. For example, India's Aadhaar identification system relies on integrating frameworks across a number of core and peripheral socio-economic technologies, such as electronic Know Your Customer, digital locker, unified payment system and online authentication, to name a few.

A forward-looking regulatory and legal environment is a key enabler for bringing new digital services to market in a timely and concerted manner. This demands recognition of new technologies and clear guidance on usage of data, and an unrelenting focus on managing privacy protection and cybersecurity issues within this context, ensuring the right incentives are positioned in the right manner and to the relevant parties who have legitimate reason to collaborate, thus avoiding unwanted economic behaviour.

In all cases, engaging the private sector in public-sector digital schemes (through public-private partnerships) is generally cost-driven, such as in India's case, but it also provides the ideal platform to disseminate information and build systemic capabilities when rolling out a complex programme, such as that of Estonia or Singapore.

In summary, a rapidly growing global and digital society means an abundance of new technologies are increasingly impacting how governments can deliver creative and innovative public solutions and services to their citizens. The opportunity exists for all nations to embark on this journey in a well-conceived and planned manner, building on lessons learned from forward-looking digital governments in different scales and stages, such as those of Singapore, India or Estonia. This is a journey which is not immune to significant challenges. However, it offers greatest reward when citizens are placed at the centre of the digital government agenda and their views are creatively embedded within the core of the system. Today's governments have a number of lessons, practices and technologies which can be leveraged to leapfrog their digital agenda, ensuring citizens and communities are truly smart in design and results.

Republic of Singapore

Play

Empowering citizens in a smart nation

Overview

Singapore has become the world leader in delivering digital public service. It seeks to build citizen-centric and personalized digital services by analysing users' data and anticipating their behaviour, and drive stronger collaboration between government and citizens. Singapore's digital government programme has evolved rapidly in the past decade. The vision of Singapore becoming the first smart nation to grow its economy and empower citizens by its focus on connectivity, content and cybersecurity is becoming a reality.

Key Lessons

- Digital government is the main pillar for enabling the digital economy. Government should adopt a phased approach to implementation and focus on selected digital services in each phase that best align with overall strategy.
- Sponsorship from top leadership is critical to ensure success.
- An external and open innovation model should be empowered by a strong entrepreneurial environment.
- The regulatory framework must evolve to be applicable to new digital services and drive the digital economy.
- The governance structure must ensure collaboration among stakeholders at both national and sector levels.

Description

Singapore is widely seen as the global leader in developing a smart society and enabling digital government. It has topped the World Economic Forum Networked Readiness Index and the Huawei Global Connectivity Index two years in a row, and is widely seen as operating at the forefront of developing a smart society.

Singapore's Infocomm Development Authority (IDA), the main sponsor of Singapore Smart Nation initiatives, was restructured last year into the Info-communications Media Development Authority (IMDA) and the Government Technology Agency (GovTech) to better align strategic objectives with the required skillset. The IMDA acts as the regulatory and policy authority focusing on all telco and media regulations, including over-the-top (OTT) services. Their main plan is setting smart regulations around OTT without harming consumers. On the other hand, GovTech, made up of close to 2,000 people, is responsible for laying the foundations and delivering Singapore's Smart Nation/Digital Economy vision, in addition to digital government (chief information officer [CIO]) services, privacy protection and cybersecurity.

Singapore's success is partly the result of its early investments in information and communications technology (ICT), which includes the national broadband initiative Singapore ONE, and also the result of strong government commitment to the digital agenda, including its Smart Nation programme. Every government service is available online by default (around 1,600 services), and satisfaction rates are 95% for business and 97% for citizens.

More broadly, however, two important factors explain Singapore's digital success. First is the emphasis on user centricity – that is, starting from problems faced by citizens and using technology to find solutions. This may sound simple, but it's an important principle: it avoids governments going digital for the sake of doing so, and keeps policy focused on the right objectives. For example, the IMDA lab tested the use of drones to deliver mail to a remote island off Singapore, which would replace the need for boat crossings. Other programmes being run with IMDA support include using virtual reality both in the healthcare sector to train surgeons, and in classrooms to provide better experiences for schoolchildren.

The second factor critical to Singapore's success is the willingness of government to experiment and take risks. This is mainly led by GovTech focusing on government information technology (IT) to deliver citizen-friendly digital services and manage the government's IT infrastructure. It has attracted substantial engagement from industry by aiming to be a leader in applied technology, and by being prepared to trial, do proof of concept and experiment with artificial intelligence (AI), robotics, blockchain and other technological breakthroughs. GovTech builds and deploys products with industry; it is the only agency in government with the capability to take an idea all the way from development to final product. Private companies can then sell their products elsewhere in the world and capitalize further on the initial investment from GovTech.

Clearly, there are limitations to how far Singapore's success can be replicated. As a small city-state with a single layer of government, it can instigate and implement such innovations very quickly. Most countries have larger populations and more complex political systems, and are simply incapable of moving at this pace. However, Singapore's journey and the various stages of maturity for implementing digital government (below) provide many lessons:

Stage 1 – Automation and availability: where government is focused on digitizing its services and making them available on-line. The focus is mainly on citizens – their needs and engagement.

Stage 2 – Mobility and simplicity (single platform/portal): where government adopts a more integrated service delivery platform and portal for all online and mobile government services, simplifying the user experience and targeting both citizens and enterprise.

Stage 3 – Predictability, collaboration and personalization: where government becomes smarter about using customer data, relies more on AI to think ahead and anticipate things, and proactively provides personalized services. It also creates a fully open platform for citizens and enterprises to develop and customize their own services (digital communities).

Most emerging markets are still in Stage 1, focusing on short-term goals to automate services and engage citizens. Other markets, such as most countries of the Gulf Cooperation Council, have evolved to Stage 2. Singapore, Australia, the United Kingdom and Sweden are currently implementing Stage 3.

Based on the Singaporean experience, governments cannot build a digital nation without first maturing their digital government. Singapore started the digital government journey 35 years ago by focusing first on computerizing and building infrastructure to push all government services online (98% of those services went online by 2000). Then, it moved to another phase on a single mobile platform, where 300 services were mobile by 2010. The current phase is about building stronger collaboration between government and citizens, where all 1,600 government services are fully digitized (e.g. 95% of Singaporeans pay their taxes online in less than 10 minutes).

Various factors determine the success of digital government. This normally includes governance and leadership, infrastructure readiness, forward-looking regulations and an innovation ecosystem supported by an "incentivized" public-private partnership model. Singapore has enacted most of these enablers, as follows:

- Expanded broadband infrastructure (with enforced quality of service). Singapore is one of the most connected nations in the world, with 100% of homes connected (up to 10 gigabytes) and 150% device penetration.

- Continued to implement smart and converged regulations.

- Adopted an open innovation model through partnerships. This includes engaging and incentivizing start-ups in the innovation process, and creating a collaboration model (e.g. open key performance indicators).

- Upgraded internal capabilities to align with new technologies (e.g. AI, blockchain, augmented reality, big data, analytics, internet of things, sensors) and hired externally from other sectors. Singapore also launched a Technology Skills Accelerator (TeSA) programme in partnership with the private sector. This programme's main goal is to help fresh and mid-career ICT professionals get better jobs and grow in their careers by developing core ICT and business skills. Several private companies, including Singtel (the first firm to come on board), have committed to provide funding and training services, in their training centre as well as on the new TeSA portal. The IDA already has a Governing Council, Sector Committees and the Prime Minister's Office to run this programme, which will be part of the Singapore Smart Nation initiative. TeSA already launched 380 ICT training courses on its portal and secured a $120 million budget over three years

- Followed a more holistic process to coordinate activities across ministries and government layers (federal/municipalities), supported by CIO roles at municipal levels. Also, Singapore has learned from private business and mechanisms used to launch new services successfully (e.g. agile product development).

- Created an engineering culture focused on agile product development rather than a traditional government culture and processes (i.e. time should not be wasted on extra planning, with the focus on delivering success stories; a shift should be made from project to product approach; digital government leads should not be typical government employees).

In addition, the citizen has always been the centre of Singapore's digital economy and digital government efforts. The focus has always been on understanding and predicting citizens' needs to provide seamless experiences, rather than the traditional focus on citizen engagement. Government has relied on citizens' feedback and focus groups to create a citizen-centric view across all government services. The main objectives include:

- Making this service painless and less bureaucratic (e.g. paying taxes)
- Anticipating user requests ahead of time (e.g. sending a reminder when a passport is about to expire)
- Allowing citizens and enterprises to play a larger role in redefining and customizing digital services (digital communities)

As a small state with fewer than 6 million people and no natural resources to rely on, Singapore needed differentiation to prosper in the global economy. Now, it is a source of inspiration for all countries interested in developing digital public services. It should also be a source of inspiration through its ability to keep pace with technology for its citizens.

Resources IDA and GovTech (https://www.tech.gov.sg/)

Republic of Estonia

Play

Expanding digital identity and literacy for innovative public services

Overview

Estonia has fostered a long-term culture of supporting the development of information and communications technologies, emphasizing the need for legally cognizable digital identity services. The country has made tremendous gains, with strong determination to succeed and a long-term commitment to invest in distributed information technologies for delivering government services. It has invested in capacity building for all its citizens, as well as in the legal infrastructure that underpins and validates the use of digital identity technologies for financial services, healthcare and elections. In short, the country has a long-term commitment to identity, innovation and leadership.

Key Lessons

- Leadership support and sponsorship at the highest level (Prime Minister) is key to driving the digital agenda and making it a top priority. It goes beyond technology to include forward-looking economic capabilities.
- Early adoption of shared platforms is crucial.
- Digital capabilities are essential for building digital government services and enabling the digital ecosystem.
- Laws and regulations are powerful enablers (though considered by many countries as barriers), and must be utilized smartly to enforce data sharing and security.
- Privacy and cybersecurity are key drivers to digital adoption, and must be managed and designed carefully to be recognized by national legal frameworks.
- Partnerships with the private sector and joining forces early on will create powerful offerings.
- Adoption of a hybrid governance model is necessary to ensure alignment of digital services with the overall national digital agenda.

Description

Estonia's digital journey was focused on creating efficiency, from back office operations to service delivery. The country started implementing digital technologies from the late 1990s in the delivery of government services. Over time, the use of digital technologies as a key differentiator became a main pillar of Estonia's national economy and strategy. Its digital transformation was built on three pillars:

1. A focus on human-centred design to ensure widespread adoption and usage
2. The leveraging of digital ID and secure data exchanges across an array of sectors and applications
3. Coordinated cyber-risk management in a resilient and coordinated way (and not in silos)

From the start, Estonia was also keen to use technology to enable innovation and create simple digital interactions with entrepreneurs. This has evolved into a one-stop-shop model for service platforms, followed by a larger focus on data analytics to enhance service delivery and predict user behaviour.

One of Estonia's primary success factors for accelerating digital government services has been adopting the government as a platform model across the overall economy. This has translated into the adoption of secure and shared platforms and common data across public and private sectors, where digital services were built on top of these platforms.

A great example of Estonia's home-grown platforms is its national digital ID, built through a partnership model with the private sector. Secure, authenticated identity is the birthright of every Estonian; hospitals issue digital birth certificates before newborns arrive home, and their health insurance will have already started automatically. All residents of Estonia aged 15 or over have electronic ID cards, which are used in healthcare, electronic banking and shopping. With Estonia's national digital ID, individuals can sign contracts, encrypt email, get tram tickets and even vote. Estonia's digital identity was not merely an innovation in itself, but heralded the arrival of one of the most sophisticated e-governments in the world. Taxes can be filed in less than an hour, and payment of refunds occurs within 48 hours.

Three factors contributed to the success of Estonia's digital identity. First, it was mandatory; people could not simply opt out and rely on old paper systems, which meant nearly total uptake. Second, digital signatures represented a legal and secure way to sign anything, creating a plethora of conveniences and opportunities for the citizen. Finally, the system was developed through a series of public-private partnerships, and at a reasonable price.

Arguably the greatest success has been the system’s security. No major cyberattack, interruption or breach at any point has occurred, at least publicly. This is no small feat – especially considering what a target the system is – and is largely due to major investment and prioritization of cybersecurity.

The digital ID comes with challenges. The government had to organize digital training, especially in rural areas, to help elderly populations adjust to the new delivery of public services. Indeed, about 10% of the population is still not online. Outside of Estonia, several other countries have rejected this approach outright. The United Kingdom scrapped a planned £4.5-billion, much-criticized ID card scheme in 2010. And fundamentally, the use of information technology by Estonia’s private sector still lags the government’s success, despite such immense progress.

However, Estonia keeps moving forward, undeterred. This year, the hope is to add a level of automation to e-government services. In effect, rather than having to apply for a pension at the age of 63, for instance, the government will undertake the process instead and save the hassle – notification of an individual’s pension will simply appear. The country is also leading endeavours to embed the Digital Single Market across the European Union, signifying recognition of its leadership in this sphere.

Estonia relies on a very hybrid governance model where each ministry has its chief information officer (CIO) focused on digital development. In addition, the government’s CIO office was established to work with all ministries on setting the rules and experimenting with new technologies, working closely with the Prime Minister’s office to align on the national digital agenda.

The case of Estonia demonstrates how e-government is a path available and replicable to any country, especially small nations and not just the wealthiest ones. This major and secure innovation was achieved at comparatively low cost and with determination to succeed.

Resources Government CIO office (https://e-estonia.com/)

India

Play

Catalysing transformation through digital identity

Overview

In the absence of a nationwide accepted identity document, each sector created its own system of identification. A large portion of India's population still did not have a valid identity document. This was one of the main reasons the poor could not access benefits and subsidies provided by the government. In late 2009, India created Aadhaar, its identity programme that provides unique identity to each resident. The government has issued IDs to over 1.15 billion residents in India, and acts as a digital identity infrastructure used by various organizations to efficiently deliver services to residents. Aadhaar, one of the world's largest biometric-based digital identity systems, has created opportunities for the government and the private sector to transform citizen-centric services, and to provide innovative platforms for digital transactions.

Key Lessons

- An enabling legal and regulatory framework recognizing digital identity, data privacy and other important elements should to be established at the start of the programme.
- Citizen identity management needs sustained investments over a long time period and will require buy-in from the key policy-makers.
- The identity platform's role must be clearly stated, and the minimum information required must be defined and collected to deliver services in a cost-effective way.
- Biometric data collection enables highly accurate deduplication and the creation of unique identity for each individual.
- The government needs to collaborate with various ecosystem partners (including state government, registrars, enrolment agencies, authentication service providers, user agencies, logistics provider and project management unit [PMU], etc.) to successfully roll out a programme of this scale.
- The government should adopt a phased approach complimented by mid-term evaluations to fine-tune systems and update the rollout plan.
- The programme should focus on creating a robust identity infrastructure rather than dispensing expensive identity cards.
- Digital identity as a service offered by the government makes it easier for public- and private-sector organizations to adopt and use the identity services.

Description

Identification plays an important role in facilitating citizen interactions with government and private organizations. Robust citizen identification not only allows improvement in service delivery, but also has the potential to reduce the pilferage in government subsidies, enhance inclusion of right beneficiaries, increase tax collection, enhance the country's security posture and improve delivery of social programmes.

In the Indian context, the lack of a valid identity among most of the population contributed to social exclusion and created limitation for the beneficiaries to get access to basic government benefits, such as education, pensions, rations, subsidies, health and scholarships. It was important for the government to issue a unique identity to everyone in the country, enabling them to be formally recognized in the systems. Moreover, the unique identity could also help the government in effectively disbursing benefits and weeding out duplicates.

Growing expectations among citizens and advancements in information and communications technology (ICT) made the government rethink how it could leverage ICT to enable robust identification. India recognized the potential of digital identification and how it can be leveraged to enhance remote interactions with citizens in offering newer services in a more efficient manner.

In this context, the Government of India developed Aadhaar, the nationwide programme for issuing digital identity to each of the country's residents. Established in 2009, the Unique Identification Authority of India (UIDAI) was notified by the Planning Commission as an attached office to roll out Aadhaar. The programme was directly reviewed by a cabinet committee headed by the Prime Minister of India. To lead this massive programme, the government decided to invite Nandan Nilekani, co-founder of Infosys, one of the largest information technology organizations in India. Nilekani was given the newly created position of Chairman of the UIDAI, equivalent to a cabinet minister's rank. Various other industry experts were also invited to form the PMU that supported the design and development of the UIDAI.

The UIDAI's objective was to issue a unique identification number (UID), called "Aadhaar", to all residents of India that (1) is robust enough to eliminate duplicate and fake identities, and (2) can be verified and authenticated in an easy, cost-effective way. In 2016, the government enacted the Aadhaar Act, in which the UIDAI became a statutory authority responsible for Aadhaar, including operating and managing all stages of the Aadhaar life cycle; developing the policy, procedure and system for issuing Aadhaar numbers to individuals; and performing authentication. The authority is also mandated to ensure the security of identity information and authentication records of individuals.[5]

Designed as a foundational programme, Aadhaar was based on a de novo data collection exercise to register all residents in India. The mandate was to capture basic identity data (demographic details, fingerprints, IRIS recognition and photographs) and register 1.2 billion residents spread across multiple states and union territories. In view of the country's size, the scale of operations and desired speed, the UIDAI leveraged the private sector's entrepreneurial spirit and effectiveness. An ecosystem was created by engaging with private and public-sector partners who performed the enrolments in a decentralized manner. The entire enrolment exercise was meticulously planned, standardized and thoroughly field-tested prior to its launch. The ecosystem partners brought in the necessary field resources (hardware and manpower) and were remunerated by the UIDAI on every successful generation of unique identity, aligning the objectives of ecosystem partners and the UIDAI.

More than 100 registrars, 300 enrolment agencies and over 60,000 operators worked towards enrolling the masses. Since the first enrolment in 2010, the Authority has issued more than 1.15 billion Aadhaar numbers to residents. The UIDAI has also opened permanent enrolment centres for residents to register or update their details. More than 28,000 permanent centres are currently functional, and more are expected to be established in due course.[6] Once the data was collected as part of the enrolment process, it was submitted to the UIDAI for deduplication and processing of data to generate a 12-digit unique identification number called Aadhaar. The Aadhaar numbers issued by the UIDAI were accepted as a valid proof of identity and proof of address, and are ubiquitously used across the country.

In terms of service delivery, Aadhaar enabled the online authentication of individuals (through multiple methods) on a real-time basis. This is extremely useful for both the government and private sector to authenticate individuals without necessarily requiring individuals' presence in their offices. The UIDAI adopted a multilayered, trusted ecosystem approach allowing users across the public and private sectors to quickly onboard and use the authentication platform. Currently, more than 300 schemes are linked to Aadhaar, and around 3-5 million core authentications are occurring daily, with a plan to raise UIDAI's capacity to 35 million authentications a day in the near future.[7]

As the programme evolved, the government created a direct benefit transfer (DBT) platform alongside Aadhaar to directly disburse the benefits provided by the government to a citizen's Aadhaar-linked bank account. Aadhaar was leveraged to open bank accounts for 289 million individuals, and served as a natural place for all government subsidies and benefits to be credited to a beneficiary's bank account. The pilot rollout of the DBT was initiated in 2014 in 43 districts and 27 schemes. More than 357 million residents have benefitted from this scheme, and over $31 billion have been disbursed directly to the beneficiary's bank account. This has significantly improved the access and availability of funds for the beneficiaries, and has streamlined the government's benefit disbursal process.[8]

Aadhaar has made it easier for the beneficiaries to avail government services and subsidies, and to be part of social safety net programmes. It has also significantly helped to reduce the pilferage in government schemes. Through Aadhaar's implementation, the Government of India will save $1 billion annually. Through mid-2017, it is estimated that Aadhaar has helped save over $5 billion under various social benefit schemes. The government is introducing Aadhaar in various services, including income tax, civil registration, food subsidies, company registration, scholarships, pensions, healthcare and financial inclusion, among others. On one hand, the platform is helping to reduce pilferage/leakages, enhancing efficiency towards service delivery, establishing audit trails and easing identification, while on the other, it provides residents with convenience and enables them to access government benefits.

The identity infrastructure established by Aadhaar is also being used in various innovative frameworks, helping India transform into a digitally empowered society and economy:

- Electronic Know Your Customer (KYC): The framework has enabled a simplified digital (paperless) KYC process based on Aadhaar. The framework is extensively used in the financial sector and by telecom and government services to onboard customers.
- Digital locker: Digital locker facilitates paperless electronic governance for its citizens. It aims to provide a platform for secure issuance, storage and verification of digital documents, eliminating the use of physical documents.
- Unified payment interface: Established with the objective to give impetus to digital payments, this framework enables immediate money transfer through mobile phones.
- Online authentication: Various service providers are using Aadhaar authentication as a service to authenticate the Aadhaar holder for service delivery.
- E-signature: An online electronic signature service that can be integrated, with service delivery applications via an open application programme interface, to help an Aadhaar holder sign a document digitally.

Aadhaar's success can be attributed to various factors, including the innovative use of technology, the use of biometrics, field trials, open standards and framework, an ecosystem approach, collaboration with the private sector and an efficient procurement process. With effective planning, the government could roll out the Aadhaar programme at perhaps the lowest cost, an inspiration for those evaluating their national ID programmes and how to enable digital government transformation.

Resources

UIDAI (https://uidai.gov.in/), DBT Bharat (https://dbtbharat.gov.in/), National Institute of Public Finance and Policy (http://www.nipfp.org.in/home-page/)

United Arab Emirates

Play

Accelerating the digital dividend in government services

Overview

The United Arab Emirates (UAE) has traditionally been a regional pioneer in building new forms of citizen engagement, and is typically viewed as the leader in applying digital government transformations in the region. In recent times, the UAE has aimed higher and applied a dynamically accelerated, multi-tiered approach (federal and local), using clear and ambitious targets, strategic programme planning, design and execution through collective leadership to become a global benchmark in this field.

Key Lessons

– Success can be driven by a centrally led hybrid governance approach to programme implementation, with national leadership acting as a chief sponsor but fostering an enabling environment for each emirate to independently drive change internally.
– Leading cities (e.g. Dubai) adopt a sense of consistency and structure in e-government programme delivery through a multisector engagement model, based on setting ambitious targets, with clear methodologies and timelines to achieve them, and allowing flexibility in the model to adapt.
– A range of innovative drivers should be at the core of the government agenda, based on altruistic targets (e.g. happiness, or the customer experience), and working backwards to seek technological solutions through a participatory and open approach. This further promotes cross-sector collaboration (e.g. the arts and film) and does not allow technology itself to drive the change.
– An iterative and staged approach to long-term digital government deployment is imperative to ensure benefits are captured and disseminated in a timely manner through an entrepreneurial, lean-delivery model.
– Private-sector characteristics should be adopted in designing, implementing and promoting a performance-driven culture which is aligned and coordinated across entities and government layers.
– Trust is required as a key differentiator. The UAE pays close attention to how incentives and rewards are formulated to carefully promote rapid growth of digital government. It fosters a culture of being "ahead of the curve" and promotes constructive competition among government entities.

Description

The UAE is known for being a regional pioneer and a noteworthy global benchmark in the government innovation space (it is ranked 32nd in the United Nations E-Government Survey 2016). It is particularly focused on delivering high-end, customer-centric smart digital services across multiple platforms to government entities, businesses and individuals. Three separate streams of development took place along the UAE's journey, namely at a federal level and then, independently, at a local city level, primarily by Abu Dhabi and Dubai. This case study discusses the nation's accelerated journey in becoming a digitally savvy society and explores selective digital government cases, focusing mainly on Dubai (the leading emirate in this regard) to illustrate key success factors. It closes with what the future may hold for the UAE.

The UAE is based on a federal system, whereby the Supreme Council holds legislative and executive powers and operates in conjunction with a Council of Ministers (Cabinet), a parliamentary body in the form of the Federal National Council and the Federal Supreme Court, which is representative of an independent judiciary. Each emirate's ruler forms the Supreme Council and plays an active role in guiding the process of public participation, government transformation and, indeed, how national and local strategy is formulated and translated at the emirate level.

The UAE's digital government journey can be seen as having begun in 2001 through the e-Government initiative, which saw the Ministry of Finance and Industry launch the e-Dirham, issued to collect government fees. Over roughly the next decade, the UAE garnered efficiency initiatives mainly focused on government processes and cost reduction, along with some development of new revenue streams. In 2004, a memorandum of understanding was signed with Etisalat, the primary telecom provider, to supply infrastructure services for e-Government, and in 2006 the chief responsibility was transferred to the Ministry of Government Sector Development.

In May 2013, His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice-President and Prime Minister of the United Arab Emirates and Ruler of Dubai, announced the launch of an initiative that shifted the Dubai e-Government platform towards a “smart government” transformation agenda at the federal level. The UAE e-Government programme was launched with the more targeted intention to use mobile technology as the gateway to achieve more ambitious infrastructure and public service enhancements. The Telecommunications Regulatory Authority (TRA) was mandated to manage the implementation, including strategic monitoring and support under the guidance of a Supreme Committee chaired by the Minister of Cabinet Affairs. The Committee consisted of a range of government and industry members from the Prime Minister’s Office, the Ministry of Cabinet Affairs, the TRA, du, Etisalat and the Information and Communication Technology Fund. This top-down approach has proven critical in the UAE’s digital government story.

Detailed plans and roadmaps, such as the mGovernment Roadmap and the National Plan to Support Mobile Government Initiative, were released in 2015. They also operated in tandem with the Federal eGovernment Strategy 2012-2014. The Strategy provided the overarching legislation, infrastructure and institutional framework to catalyse specific programmes. This layer is essential to build trust in society, which allows creative ideas to come to fruition in an open environment (e.g. cloud computing infrastructure release during earlier years). The following set of initiatives are some examples where federal-level endeavours provided the needed integrated infrastructure to enable local government bodies to deploy successful solutions:

- Smart Pass: a service enabling unified data entry for online government transactions
- Government Service Bus (GSB): a linking platform for government service entities in a secure e-environment
- Federal Network (FedNet): a provider of internet services for 42 federal entities in the UAE
- Centre of Digital Innovation (CoDI): a central mobile app-testing laboratory for government

Programmes like these form the backbone of the TRA’s efforts to successfully establish its citizen-centric approach to public service delivery. It is driven by a continually expanding target/vision and builds on a collective approach steered by sound leadership. This occurs through a process of iteration, or continuous re-evaluation and subsequent relaunch of revised products and services. It is hinged on placing e-security and e-quality at the core to bolster public trust and active participation.

In fact, the TRA more recently announced the refreshment of the UAE government portal (government.ae) to better generate interest and enthusiasm among the public to engage in the mGovernment transformation. Here, the Centennial Plan 2071 programme, again launched by Sheikh Mohammed bin Rashid Al Maktoum, provides a map of how the government will enhance its reputation over the next few decades. It also sheds light on the UAE’s various plans, such as Dubai Integrated Energy Strategy and Abu Dhabi Economic Vision 2030. The UAE “Future” page on the portal is even more future-oriented, providing additional interest towards the Mars 2117 mission. The portal allows for greater public participation and control in developing content. Within these far-reaching ambitions lie foundational principles, including “simplicity, power and accuracy” of the customer experience. Given the diversity of the expatriate diaspora and the mix of backgrounds among the UAE public (constituting 88% of the population), these features are essential to a successful buy-in and adoption rate, which accelerated the e-Government’s success.

The UAE’s release in 2010 of its overarching Vision 2021 and the UAE Government Strategy 2011-2013 marked a turning point in how the government engaged with citizens through technological developments, and sought to deliver innovative value to its people through digital offerings. A key driver behind this change was visionary leadership to stay ahead of the curve. Rating and award schemes in government appeared, and a performance-led, meritocratic culture quickly emerged, using techniques such as “naming and shaming” that were quite contrary to traditional Arab culture. For example, the annual Best mGovernment Award applies to all government parties across eight categories (e.g. health, security, education) to encourage citizen- and business-focused innovative digital solutions in government.

A very structured hybrid governance model is clearly evident in the UAE's case. It is spearheaded by a common national strategic agenda (vision and strategy) and a cross-section of governmental and non-governmental institutions participating in different capacities (i.e. through different types of relationships). Committees, set up to provide fluidity in decision-making, are comprised of cross-sector entities at multiple levels of partnerships within a very organized and structured performance regime, all based on good private-sector practices. Arguably, this model has been successful due to the relatively small city size. Larger governments could face greater challenges in implementing it.

Each city subsequently pursued its own approach to implementation in this regard, with most momentum seen in the capital, Abu Dhabi, and perhaps more prominently in Dubai. While Abu Dhabi has relied on a traditional government approach to implementation, driven by the Abu Dhabi Systems & Information Centre, Dubai has adopted a few different routes to digitization in government.

Smart Dubai is a prime example of how this governance model has worked well. As the leading smart transformation government body in Dubai, the initiative aims to make Dubai the "smartest and happiest city" in the world.[9] Two differentiated bodies lead the change. The Smart Dubai Office (SDO) leads strategy and policy development, and the Smart Dubai Government Establishment (SDG) is the city technology execution arm. Several innovative programmes and platforms have been activated using high-tech blockchain solutions and big data analytics to achieve several objectives. They include Dubai Pulse, a central data host providing data to the public and private sectors; and, more recently, Dubai Now, a one-stop-shop app for all government services, providing more than 55 services in 11 categories (security and justice, public transport, payments and bills, visas and residence, driving, health, business and employment, education, housing, Islam, and miscellaneous) from 24 government departments, as well as semi-governmental and private entities in Dubai. One objective is to make the government paperless by 2021. In addition to tech platforms, Smart Dubai also provides the necessary institutional standards to ensure quality and consistency across initiatives in both virtual and physical domains (e.g. Happiness Meter, Smart Dubai Index and Smart District Guidelines). In fact, a new Ministry of Happiness was established in the UAE, signifying its importance at the federal level. Smart Dubai has achieved this by adopting a leading-practice balanced scorecard framework, engaging strategic programme management capability and forging 12 strategic partnerships and other partnerships with government and non-government entities.

In accordance with their mantra of continuous improvement through digital change, the Dubai government announced the Dubai 10X initiative in 2017, to be run under a council led by the highest authorities, sponsored by the Dubai Future Foundation (which acts as the conduit between government and businesses or the public in implementing many of these exciting and complex programmes) and run by the Dubai municipality. It aims "to place Dubai ahead of other cities in the next 10 years … and make Dubai the largest laboratory for future government experiences in the world". It places "disruptive innovation" at its core across all government entities by implementing a few organizational changes. One example is mandating each government entity to establish an independent "x-unit" department in charge, or providing disruptive solutions within their organizations. The Centre for Digital Innovation acts as a gatekeeper in this effort, leading "smart lab" solutions in mobile government services. This area is already seeing an uptick in activity, with teams having been formed, new ideas generated and partnerships forged with leading-practice entrepreneurial entities, including several in Silicon Valley. Prototypes are soon to be launched in government.

The UAE has proven to be a powerhouse in rapidly deploying digital solutions in government. Its exemplary vision (much of which several other nations have followed) and innovative capacity have placed it at the forefront of many digital government rankings; in fact, Accenture's Digital Government: Pathways to Delivering Public Services for the Future report ranks the UAE 3rd in the world in digital government. The UAE could face risks in possible duplication and inefficiencies: this would be due to the dichotomy in growth in digital government programmes coming on board, matched with the convergence of technologies. However, centralized leadership allows for clear oversight and an ability to quickly adjust the play. Another priority is upskilling the public sector to keep pace with digital escalation and adapt to this new mindset. Leading nations, such as Norway, are strongly attuned to driving a data-driven culture in public services. Achieving scale in digitally enabled participation and structuring inclusive policy-making should be top of mind in the UAE's journey. Lastly, the UAE must pay close attention to data governance excellence standards to realize untapped public-sector opportunities. All in all, the future of its government looks bright to say the least, and it is well on the way to achieving its Centennial 2071 goal of being the "best country in the world".

Resources

OECD (2017), Benchmarking Digital Government Strategies in MENA Countries, OECD Digital Government Studies, OECD Publishing, Paris

Government of Dubai (dubai.ae), Dubai Future Foundation (dubaifuture.gov.ae), Telecommunications Regulatory Authority (tra.gov.ae), Smart Dubai (smartdubai.ae) and Dubai 10X (dubai10x.ae)

3. Growing the Digital Economy

James Johns, Visiting Senior Research Fellow, Policy Institute, King's College London, United Kingdom; Director, Corporate Affairs, Hewlett Packard Enterprise (2015-2017), United Kingdom

A political imperative

Embracing digitalization offers profound benefits to governments looking to improve the productivity of the economies for which they are responsible, whether through better supporting growth in their native high-technology firms or through encouraging their traditional industries to adopt digital technologies in the transformation of their processes and business models. Although in some ways, a degree of laissez-faire is at the very heart of the innovation underpinning some of the world's leading digital companies, only the most ardent advocate of free market economics would suggest that doing nothing is an adequate or appropriate response from policy-makers to either challenge. At the very least (and as explored in the first chapter), governments have responsibilities to ensure that their countries have access to the necessary connectivity, and that citizens and businesses have the skills to participate safely in the digital economy.

This chapter examines the factors that have contributed to the creation of clusters of successful technology companies and the growth of digital economies in different parts of the world. The four case studies explore how policy-makers in different countries are shaping their nations' participation in the Fourth Industrial Revolution, creating the conditions necessary to drive growth and ensuring that their countries are well-positioned to capitalize on the benefits digitalization can bring. The case studies, from the United Kingdom, Sweden, Kenya and Costa Rica, illustrate how governments in countries with different economic, demographic and developmental circumstances have risen to this challenge.

The high-tech trinity: education, government and entrepreneurship

While it might be something of a cliché, the legend of Silicon Valley is a regular starting point in any conversation seeking the recipe for success in nurturing what is now called the digital economy. This story teaches us that a perfect storm of education, government and entrepreneurs came together to create a cluster of companies which, though many of their names are now consigned to the history books, still influence the global high-tech industry today.

In the legend, education is represented by Stanford University and its visionary professor, Fred Terman. Terman encouraged his students to start their own businesses, persuaded the university to give over part of its real estate (the Stanford Research Park) to house them and used his contacts to introduce them to potential clients. Government appears in the guise of the Naval Air Station at Moffett Field, initially home to the United States' airship programme and subsequently used as a base for maritime surveillance (even then a heavy consumer of electronic equipment) and the National Advisory Committee for Aeronautics, later subsumed into the National Aeronautics and Space Administration. All provided local, ready-made customers for Terman's protégés. Entrepreneurs complete the legend; individuals like Bill Hewlett and Dave Packard, who tossed a coin to decide the order in which their initials would appear in the name of the company they founded: HP. They include William Schockley, who took his work on the development of the transistor while at Bell Labs home to the West Coast so he could be near his ailing mother. When a group of Shockley's bright young researchers (the so-called "traitorous eight"), frustrated at his leadership style, left to form Fairchild Semiconductor in 1957, they gave birth to the industry from which the region takes its name: the design and manufacture of silicon chips. Silicon Valley remains one of most economically productive places on the planet, contributing more than 10% to California's gross domestic product and helping to ensure that the State of California sits alongside whole countries in the list of the world's largest economies. The area has the highest average salaries of any high-tech cluster in the world, and is home to the most millionaires and billionaires per capita in the United States.

That government can play a major role in driving the success of the digital economy is without doubt. Indeed, there are those who suggest that it is the principal actor. In her book *The Entrepreneurial State*,[11] Anglo-Italian economist and professor Mariana Mazzucato suggests that many of the inventions which underpin billion-dollar product lines, such as the iPhone, can trace their origins to publicly-funded research and development programmes, often with their roots in the military. Her argument is compelling and has resonated with many politicians around the world, as they seek to mimic the success of Silicon Valley in their own countries. The internet itself emerged from ARPANET, built by the US Department of Defense's Advanced Research Project Agency from its work on "packet-switching" networks, which could recover from military attack by rerouting communications through different nodes. The Global Positioning System (GPS), the platform that led to satellite navigation and enables place-based services such as Uber, was principally designed for military use. GPS is now a standard feature in any $100 smartphone. The research conducted by Larry Page and Sergei Brin that led to the "PageRank" algorithm – still the heart of Google's offering – was funded by US National Science Foundation grants. Originally intended to provide a tool for assessing the quality of academic literature, the patents it incorporates are still held by Stanford University. It could even be claimed that the electronic computer itself was the product of government activity, emerging from the work of the codebreakers at the UK Government Communication Headquarters at Bletchley Park during World War II. Notwithstanding this legacy and nearly 80 years on, governments around the world continue to hunt for the magic ingredient – the spark necessary to convert the trinity of education, entrepreneurship and public support into an innovation and economic powerhouse.

Sustaining success: the need for continuous reinvention

While the basic ingredients of Silicon Valley's success are well understood, the sustained success of the region has not always been easy to replicate elsewhere in the world. At its peak, "Silicon Glen", the collection of chip and computer manufacturing companies spread across Scotland's central belt, produced 30% of Europe's personal computers, 80% of its high-end workstations and 65% of its ATMs, but this largely manufacturing-based cluster has been in decline since the turn of the century. Similarly, the area along Route 128 in the northeastern United States saw the "Massachusetts Miracle", as a cluster of minicomputer manufacturers such as the Digital Equipment Corporation, Data General, Prime and Wang sprang up during the 1970s and 1980s. This legacy owed much to the high-tech trinity, with the role of education played by Harvard University and the Massachusetts Institute of Technology – their graduates our entrepreneurs, and government as a long-standing funder of research at both academic institutions and as a customer in the guise of the US Department of Defense and other federal bodies. During the early 1970s, "Route 128" employed more high-tech workers than Silicon Valley, but the number has declined since peaking in 1985, with most of the companies who contributed to its success having been acquired or simply gone out of business. It's important to note, however, that even Silicon Valley's success has not been linear; California lost its leadership in memory chip manufacturing to the Japanese in the 1980s. But that Silicon Valley still thrives, even though so many of the consumer electronics devices now associated with its leading companies are manufactured in China, illustrates how important it is to have continuous reinvention, and a willingness to move up the value chain for a cluster to survive across different generations of technology.

The global race for digital platforms and talent

A superficial examination suggests that one of the factors contributing to the success of US-based internet companies is the combination of the scale and relative homogeneity of their domestic market. Notwithstanding the variation in legislation which might be found across the 50 states, an American start-up can grow across a potential customer base of more than 300 million people that speaks a single language, without needing to open a second office. And once companies break free of their domestic market, their brands can be carried across the continents and promoted by a dominant popular culture embodied in music, films, television and other media which reach most of the world. The success of China's digital economy reflects a similar pattern, thanks to the size and homogeneity of its domestic market. China's internet giants Baidu, Alibaba, Tencent and Xiaomi all operate at a scale which rivals even the US giants. But except for Alibaba, whose portal into China's manufacturing industry attracts customers from around the world, these companies principally serve a domestic market of more than a billion people into which some of their American competitors have faced barriers to operating, and they have limited resonance outside their home region.

While market size and homogeneity are almost certainly a contributing factor in the growth of some larger firms, this is not something that smaller countries can easily replicate. Luckily, there is an important lesson in the dominance of global digital firms, which can be learned by understanding more about the technology that underpins them. Now, global internet companies are typically built using software platforms that can be consumed as asset-free, "as a service" models underpinned by open source software and open standards. The technologies are accessible to any business, whether existing or start-up, with the skills to embrace and integrate them into their operations. But because these technologies allow new companies to be created and to grow without many of the traditional barriers, such as the need to make capital investments in hardware or the physical challenges associated with operating a traditional bricks-and-mortar company across geographical boundaries, the leaders in these fields become very big very quickly, and often dominate the industries in which they operate. The emergence of this phenomenon was noticed more than five years ago by Silicon Valley legend Marc Andreessen, now an influential venture capitalist who founded Netscape, the company which first commercialized the web browser. In a seminal 2011 *Wall Street Journal* article,[12] he claimed that "software is eating the world" and observed that in most sectors of the global economy, the fastest-growing businesses were, in effect, software companies: Amazon in retail, Apple in music distribution, Facebook and Google in advertising, LinkedIn in recruitment, Netflix in video rental, and so on.

Although countries with a large domestic market do offer some advantages to digital companies, it is possible for smaller nations to harness these platforms and replicate the success of their stateside competitors if other conditions are present. The case study from Sweden illustrates how the country's political and economic culture contributes to a nurturing environment for entrepreneurs. This, together with the legacy of government programmes designed to increase Swedish citizens' access to personal computers during the late 1990's, has enabled this relatively small country to create a number of tech companies with a global reach rivalling those from Silicon Valley

So, the race for success in the digital economy is a global one, built on global networks and platforms. It is one in which talent moves to the locations where it can most easily fulfil its ambitions. Tellingly, immigrant founders started 52 percent of all new Silicon Valley companies between 1995 and 2005. When examining other countries or regions which have successful digital economies, there are many common factors. Access to skills, funding and connectivity are all critical. Collaboration between different sectors of the economy, including the role that government organizations play as a customer for technology, is a frequently mentioned theme. This is illustrated well in the case study from the United Kingdom, whose government has made extensive use of the power of public procurement to influence its domestic technology markets over the last seven years. The UK government has also used its funding and convening powers to help connect digital businesses with those in other sectors to accelerate the digitization of other industries through a series of "Catapult" centres, which help stimulate partnerships with start-ups and harness academic innovation.

Other countries have chosen a different route to countering the apparent disadvantage presented by a small domestic market. The Costa Rican case study reveals how the government, in a country of less than 5 million people, has used tax incentives and a longstanding commitment to free trade to make itself an attractive base for some of the world's digital firms, though, like Sweden, its domestic market alone would be unlikely to attract attention from the digital economies' giants. It nevertheless stands out as a success in the region in attracting foreign investment from technology companies. This, in turn, is driving growth in home-grown firms.

A success story from Africa is also examined. Successive governments in Kenya have taken steps to improve their country's digital infrastructure and promote its capital as a regional digital hub. Buoyed by the success of the innovative mobile payment platform M-PESA, Kenya's digital economy is now an attractive target for investors, and the growth of both multinational and home-grown digital companies is starting to deliver fascinating benefits to some of the East African nation's traditional industries.

If there is one key lesson from the case studies in this chapter, it is the importance for governments to understand they have a key role in setting direction and enabling the supporting infrastructure, but must not stifle entrepreneurial innovation. In an age when many of the barriers to accessing technology have been reduced, it is the creativity, imagination and drive of the people working in the digital economy which can serve as some of the biggest contributors to a nation's success in this field.

United Kingdom

Play

Developing the digital economy through careful targeting of government support

Overview

The United Kingdom has one of the most dynamic and fastest-growing digital economies in the world. The British government has played an important role in stimulating and sustaining this growth in recent years, but this has been carefully and sensitively targeted. Government support has been provided through ministerial championing of the sector, the application of public research and development (R&D) funding via innovative public-private partnerships, and public procurement policy.

Key Lessons

- Dedicated ministerial responsibility for the digital economy, supported by a high-profile team of civil servants working across government to develop and implement policy, can help achieve results in a short time.
- Carefully targeted use of public investment can stimulate market development through both public-private partnerships and building new institutions focused on new technologies or innovations.
- Government needs to play a significant role in supporting the digital economy by taking a lead in market shaping through public procurement policy.

Description

The United Kingdom has one of the world's leading digital economies, with the sector estimated to contribute 10% or £170 billion to the country's gross domestic product in 2016-2017, and to support more than 1.6 million jobs.[13] Between 2003 and 2013, the sector grew more than two-and-a-half times faster than the rest of the UK economy.[14] Though businesses operating in traditional information technology markets account for a significant portion of this (e.g. the manufacture of hardware and the development of software), the sector's scale is also supported by other areas of historical strength for the United Kingdom. This includes creative industries, much of whose content is now produced and distributed electronically, and financial services, which acts as a significant domestic customer for products of digital businesses.

To provide a focus for efforts to support this increasingly significant part of the British economy, the government created a team – the Digital Economy Unit (DEU) – within the Department for Digital, Culture, Media and Sport,[15] headed by the Minister for Digital and Culture (currently Matthew Hancock, Member of Parliament). Working under the broad remit to make the United Kingdom the best place to start and grow a digital business, the Minister and the DEU are responsible for a range of policy areas related to digital matters, including infrastructure (broadband and spectrum), cybersecurity, resilience and data protection, digital markets, consumer policy and digital skills. Given that many of these topics are cross-cutting, the DEU also works extensively with colleagues from other civil service departments to implement the policies, for example with HM Treasury in matters related to infrastructure, or the Department for Education for skills issues.

Another critically important government actor in driving the United Kingdom's digital economy has been the Cabinet Office, which has the lead responsibility for the government's own adoption of digital technologies to support the delivery of public services through the Government Digital Service. Collectively, public-sector organizations represent one of the largest markets for technology products and services in the United Kingdom. Since 2010, the Cabinet Office has executed a series of deliberately disruptive plays in technology procurement policy, which have been aimed at creating opportunities for smaller companies to bid for government contracts (historically the preserve of larger systems integrators) and driving the adoption of innovations such as cloud computing, technologies built on open source and open standards, and the adoption of open data as an underlying principle for public data sets. This twin-track approach, linking government's role as a supporter of the wider digital economy and a consumer of its products, has been a powerful influence on the market and the sector.

The British government has made targeted interventions to support the technology sector in recent years. The creation of Tech City is probably the one with the highest profile.[16] In London, a cluster of technology companies has grown up in Shoreditch in the East of the City, which is now the third-largest start-up cluster in the world after San Francisco and New York. The area is colloquially known as "Silicon Roundabout" after a traffic feature in the heart of the area. Shoreditch had historically been relatively run down, certainly in comparison to the City of London's financial district on which it borders. As a result, rents were relatively low, and the area had a reputation of being experimental in new ideas and having creative businesses and trendy bars, all of which helped to attract younger workers. In 2010, the cluster included about 85 companies, bringing it to the attention of the British government.[17] By 2011, the area had more than 200 companies, a number subsequently revised upwards to 5,000 in a survey by Wired magazine when the wider area was considered.[18]

In 2010, Prime Minister David Cameron appointed serial entrepreneur Eric van der Kleij to create a new public-private partnership, known as Tech City, with the aim of providing sympathetic support with a light touch to the cluster. The cluster has now grown not only to embrace local start-ups, but also, following determined courting by Cameron and his team, to serve as the home to global firms, with Google, Cisco, Facebook, Amazon and Intel operating facilities in the surrounding area. Alongside its original London-focused remit, the Tech City organization has similarly expanded to include nurturing more than 57 other technology clusters across the rest of the United Kingdom. They discharge this function through targeted programmes that fill market gaps across the lifecycle of digital businesses, including education for entrepreneurs and curating promising new companies. The programmes convene input from digital businesses and represent their interests with policy-makers, and promote the United Kingdom's digital sector within the country and internationally. Tech City discharges this last responsibility in part by publishing an annual report on the health of the United Kingdom's digital economy, called Tech Nation.[19]

The government has also directed part of the United Kingdom's national R&D funds (administered by Innovate UK[20]) into a range of other new institutions designed to stimulate private-sector investment in technology-driven innovation. This includes a series of Catapult centres,[21] each focused on a specific technology area. Though the Catapults' remit includes topics related to energy, biotechnology and pharmaceuticals, centres also focus on digital, satellite communications, future cities and advanced manufacturing, all of which are relevant to the digital economy. The centres provide a focus for late-stage R&D efforts and the commercialization of academic research. A related but separate body, also funded by Innovate UK, is the Open Data Institute (ODI).[22] It has the remit to promote the economic exploitation of open data sets via its associated web portal,including those published by government bodies as a result of the Cabinet Office's openness agenda. [23] The ODI, which has a remit to operate on a commercial basis and attract private-sector investment to match its public funding, has been internationally successful, having created more than 18 subsidiary "nodes" in other countries.

Notwithstanding the strength of the United Kingdom's digital economy, indications are that the United Kingdom is still lagging somewhat behind other nations when it comes to adopting digital technologies in its wider economy. The United Kingdom's domestic internet penetration is the highest in the G7, with 92% of individuals using the web,[24] and it ranks 5th (of 140 nations) on availability of technology, according to the World Economic Forum Global Competitiveness Report 2015-2016.[25] However, the country is only 14th in this ranking on company-level adoption, suggesting work remains in encouraging traditional businesses to embrace digitalization and address some of the wider issues associated with infrastructure and skills, which have the potential to act as barriers to this wider adoption.

The British government recognized this and, in March 2017, launched its first strategy[26] for the digital economy, based on seven pillars:

- **Connectivity –** building world-class digital infrastructure for the United Kingdom
- **Digital skills and inclusion –** giving everyone access to the digital skills they need
- **The digital sectors –** making the United Kingdom the best place to start and grow a digital business
- **The wider economy –** helping every British business become a digital business
- **A safe and secure cyberspace –** making the United Kingdom the safest place in the world to live and work online
- **Digital government –** maintaining the UK government as a world leader in serving its citizens online
- **Data –** unlocking the power of data in the UK economy and improving public confidence in its use

Though relatively little time has passed since the strategy was formally published, work on many of these policies has been underway for some time. In some respects, the document's publication represents the formalization of an existing programme of work. Nevertheless, with the investments it has already put in place to support digital businesses and to establish public-private institutions charged with driving collaboration between innovative digital companies and potential customers in other sectors, the United Kingdom is well placed to make a success of the new strategy.

Resources

UK Digital Strategy (www.gov.uk/government/publications/uk-digital-strategy)

Kingdom of Sweden

Play

Laying the foundations for a generation of technology entrepreneurs

Overview

Sweden's long-standing political consensus has created a supportive and low-risk environment for entrepreneurs. This, along with specific government intervention to support the availability of internet connectivity and to provide subsidies for purchases of personal computer (PC) hardware nearly 20 years ago, has helped the country become one of the most productive tech hubs in the world.

Key Lessons

- Measures to improve digital literacy need not be solely focused through traditional educational systems or institutions.
- Achieving significant and sustainable impact from taxpayer-funded investments in the digital economy should be considered a long-term play.
- Politicians should not worry much about accurately predicting how investments might generate a return in the short term, but rather on maximizing entrepreneurship.

Description

Unlike the United States, Singapore or Estonia, Sweden generally does not come first to mind as a digital success story. Overlooking Sweden, though, is a mistake; it is home to some of the global digital economy's most successful companies, including Spotify, King (the creators of the Candy Crush series of games) and Mojang (the creators of Minecraft), all hailing from Stockholm. Though not based in the country, Skype was co-founded by a Swede (Niklas Zennström). According to the investment firm Atomico, Sweden is the second-most prolific tech hub in the world on a per-capita basis, after Silicon Valley, with 6.3 billion-dollar companies per million people.[27] So how has this relatively small nation managed to compete so effectively as a leader in the global internet economy?

Sweden is among the world's leading adopters of the internet. It has a comprehensive state infrastructure, and the consensus domestically is that the entrepreneurial ecosystem is a direct consequence of high taxes and a generous cradle-to-grave welfare system. Schooling is free, and students can receive a stipend for attending university. As a result, Sweden is a somewhat "risk-friendly" place. Students from Sweden's universities do not graduate with high levels of debt before they start work. This, together with the country's robust social safety net, means that the risk of starting your own company is reduced. Sweden has other cultural and political strengths likely to have contributed to its success in creating competitive internet companies. English is widely spoken, and the country is a member of the European Union, which allows its businesses to benefit from the attendant market access. Furthermore, the country has a legacy of leadership in the traditional Scandinavian design principles of simplicity, minimalism and functionality, all of which are essential ingredients for successful online services.

These factors alone, however, cannot account for the success of Sweden's digital economy, which owes more to specific policy interventions made by the Swedish government during the period when the internet was first gaining widespread adoption in the late 1990s.

Sweden has long been among the leading adopters of the internet. It regularly appears in the top half-dozen countries in any study of internet uptake, with more than 90% of the population having access and 82% using it every day. The country was one of the first to liberalize its telecommunications industry in the 1980s with the removal of certain monopolies from the former state-owned provider, Telia. As demand for high-speed internet access increased in the late 1990s, frustration at the unwillingness of Telia to open its national fibre backbone led to community leaders across the country drawing up plans for local high-speed networks and collaborating to connect local networks to each other. The Swedish government began making public funds available to support such initiatives, using compliance (with an associated regulatory regime which mandated support for interconnection) as a condition for funding. An alternative national network backbone with openness at its core quickly arose. As a result, the market for high-speed internet access in Sweden today is extremely competitive, with consumers in some areas having the choice of nearly 20 providers and benefiting from some of the highest average connectivity speeds in the world.

Perhaps the most novel factor in the growth of Sweden's contemporary digital economy, though, concerns measures that gained broad political support during the late 1990s to provide subsidized access to PCs. During 1996 and 1997, various motions proposing such a measure were placed before the Swedish parliament from parties on both sides of the political spectrum. Furthermore, during this period both the Swedish Trade Union Confederation (Landsorganisationen i Sverige, or LO), which represents blue-collar workers, and the Swedish Confederation of Professional Employees (Tjänstemännens Centralorganisation, or TCO) operated similar schemes aimed at members of their affiliated trade unions. Using their purchasing power to negotiate favourable prices from vendors, they offered members the opportunity to rent a package of computer equipment. The LO scheme was launched in September 1997 and resulted in the purchase of 45,000 computers in its first six months, at a cost of about two-thirds of comparable retail prices.

Following an evaluation of proposals by the Ministry of Finance, a scheme was put before the Riksdag (national legislature) in October 1997 that would take effect from January 1998 and enable citizens to offset the purchase of a PC against tax. Collaboration between employers and hardware vendors led to schemes whereby employees could pay for their PCs in instalments. By the end of December 2001, 850,000 new PCs had been delivered through the scheme. The Swedish government estimated that, during this period, 1 million people gained access to computers for the first time through this initiative (reflecting multiple residents per household), and this in a country with a population of about 8 million at the time. The cost to taxpayers of the scheme during this period was estimated at SEK 3.9 billion (Swedish krona), or €40 million. Because of this intervention, a generation of young Swedes grew up with access to technology they might not have had otherwise. Research conducted on the success of the scheme suggests that nearly three-quarters of employers believed that their staff's literacy in information technology (IT) had improved, and that 57% believed the scheme had delivered consequential benefits to their company. In terms of individuals' views of the initiative, 71% stated that their computer skills had improved, and 54% believed their computer literacy had increased.

It would be unrealistic to claim that those supporting the scheme back in the late 1990's could have possibly predicted how the country's contemporary digital economy would have developed. At the time, the pressure to improve the population's digital literacy came more from traditional Swedish firms that could foresee the benefits of incremental adoption of IT in their operations. Nevertheless, Sweden's success as a significant player in the digital economy clearly owes much to the investments the nation made at the turn of the last century.

Resources

Government Offices of Sweden: Ministry of Enterprise and Innovation (www.government.se/government-of-sweden/ministry-of-enterprise-and-innovation/)

Republic of Kenya

Play

Harnessing digital technology to drive economic development and provide employment

Overview

At a time when many, ostensibly more developed economies are struggling to reconcile the adoption of digital technologies with their impact on traditional industries and jobs, the Republic of Kenya has achieved remarkable results from its efforts over the last decade to embrace information and communications technology (ICT) in pursuit of economic growth.

Key Lessons

- Investment in robust internet infrastructure is the foundation stone of effective digital policy.
- Digital technologies can support economic growth in developing nations by nurturing native ICT companies through the digitization of traditional industries, and by harnessing the foreign investments of existing large-scale internet platform companies.
- Success breeds success: governments will likely find it more effective to recognize where growth is being sustained through market effects and support this, rather than to risk stifling growth by seeking to over control.

Description

Kenya’s achievements in developing its digital economy have resulted both from implementing specific government policies and from innovation in the country’s private sector, particularly in its telecommunications industry. Deregulated in 1998, the industry gave birth to East Africa’s biggest company, Safaricom.[28] Kenya now has the highest internet penetration on the African continent, with an estimated 81.8% of its 48 million citizens online, considerably above the average (28.3%) for the rest of the continent.[29] Not only does the country’s digital economy surpass that of most of its African neighbours, but the innovations it has helped to develop, such as the M-PESA[30] mobile payments platform and the Ushahidi crisis-mapping application,[31] are increasingly being adopted internationally, including elsewhere in Africa and in parts of the Middle East, Asia and Eastern Europe. The country leads the developing world in mobile payment services, and has 18 million active users of M-PESA, the money transfer and microfinancing network estimated to handle 40% of the country’s gross domestic product.

Kenya’s Ministry of Information and Communication published its first ICT policy[32] in 2006, which set out a vision for “a prosperous ICT-driven Kenyan society” and committed to ensure “the availability of accessible, efficient, reliable and affordable ICT services”. This commitment to development through the use of digital technologies was later incorporated into the wider economic plan, Vision 2030.[33] Launched in 2008 by the government of President Mwai Kibaki, it has been continued under his successor, President Uhuru Kenyatta. Vision 2030 set a goal for Kenya to become a “globally competitive and prosperous nation with a high quality of life”, and aims to “transform Kenya into a newly industrializing, middle-income country providing a high quality of life to all its citizens by 2030 in a clean and secure environment”. [34] The vision is anchored in three key pillars (economic, social and political governance) and 10 sectors, which include infrastructure; science, technology and innovation; and business process offshoring and information technology (IT)-enabled services. Vision 2030 is being realized through a series of successive five-year medium-term plans, including updates to the original 2006 ICT policy.

The 2006 strategy defined five priorities: ICT infrastructure, leveraging of ubiquitous mobile platforms to build applications and local content, building of human resource capacity, development of public-private partnerships, and creation of employment opportunities for the growing youth population. A major foundation of the initial plan’s success was dramatically upgrading Kenya’s core internet bandwidth. Like other East African countries, Kenya had historically relied solely on satellite links for internet connectivity and international communication. With pan-African efforts aimed at delivering improved links subject to delay, the Kenyan government took unilateral action in 2006 and commissioned the first in a series of undersea fibre cables, which came ashore in the coastal city of Mombasa in 2009, linking Kenya to the United Arab Emirates (UAE). The East Africa Marine System (TEAMS), a joint venture between the Kenyan government, its national telecom operators and the UAE network operator, Etisalat, now provides broadband connectivity to Kenya and many of its neighbouring countries, supplemented by connections to other international undersea networks shared with other African nations.

Having secured a step change in the speed and cost of broadband connectivity, the Kenyan government was able to proceed with other aspects of its strategy, including subsidizing broadband for universities and schools, and creating start-up hubs where entrepreneurs had access to high-speed internet. Through these and other initiatives, the Kenyan ICT sector grew nearly 20% annually between 1999 and 2009. The resulting buzz surrounding Kenya's digital economy started to attract attention from established international technology companies and investors, from both inside the country and elsewhere. Facilities such as iHub[35] (launched in 2010) were among the incubators created to provide support for local technology start-ups. By 2016, more than 170 separate companies had passed through iHub alone.[36] In 2013, IBM Research announced that its first African Research Laboratory would be in the Kenyan capital of Nairobi,[37] the result of a public-private partnership with the Kenyan government. Dutch health technology firm Philips followed suit in 2014 with plans to locate its African innovation hub in Nairobi.[38] More recently in 2017, CSquared, an internet company with $100 million of backing from a range of investors including Google, announced that its operations in Sub-Saharan Africa would also be headquartered in the Kenyan capital, further cementing Nairobi's status as a global digital hub.

The Vision 2030 blueprint always included a more ambitious locus for Kenya's high-tech industries: the Konza Technopolis.[39] Following feasibility studies, 5,000 acres of land about 60 kilometres outside Nairobi were procured in 2009, and detailed designs for the new "tech city" were produced as part of the second five-year ICT sector plan,[40] with construction work starting in 2016. Though progress on this development has been slower than expected, Konza (dubbed "Silicon Savannah") is ultimately expected to grow into a community of over 200,000, supporting the development of the business process outsourcing/IT-enabled services, life sciences, telecom and education industries. Whether Konza can ever displace Nairobi as the principal destination for technology investment in Kenya remains to be seen.

In addition to the benefits arising directly from Kenya's ICT sector, digitization of traditional industries is helping to create economic value, even where the platforms are provided by the established internet giants of Silicon Valley. When the California-based taxi-hailing firm Uber started operating in Nairobi, it faced opposition from established operators similar to the resistance it has experienced elsewhere in the world. As part of its efforts to address such concern, Uber has formed a partnership with Kenya's Sidian Bank to offer unsecured loans to its drivers of up to 100% at favourable interest rates and with no down payment, allowing them to purchase suitable vehicles.[41] This scheme's novel feature is that a driver's eligibility to receive such a loan is based on data collected by the Uber app, rather than on traditional credit references, which are not widely available in Kenya. Eligible drivers are those who have undertaken at least 500 trips and secured a passenger rating of at least 4.6 out of 5. While the benefits of this scheme for Uber are obvious, it would be mistaken to disregard the move as simply a PR stunt. The partnership is expected to lead to loans of about KES 10 billion (Kenyan shillings), or roughly $100 million, over three years. Moreover, it clearly could create significant economic opportunity for individuals taking up the offer, which they would struggle to secure through other routes.

But the most compelling examples of the economic value from digitization of the Kenyan economy are in the synergies between contemporary information technologies, native technology companies and the most traditional businesses. Post-harvest losses are estimated to count for between 30% and 50% of the food grown in Africa, [42,43] and agriculture accounts for 77% of all self-employment in Sub-Saharan countries. Nairobi-based start-up Twiga Foods[44] is using a mobile platform linked to M-PESA and big data analytics to restructure the farm-to-market supply chains for fruit and vegetables. By aggregating data from their customers and organizing distribution to retailers based on their needs, Twiga's platform has helped to reduce waste and to more accurately match pricing to supply and demand. The platform also extends credit to retailers, helping with their liquidity. Currently employing 140 people, Twiga is one of the fastest-growing companies in Kenya. It seeks to move beyond farm produce and become a full-service M-commerce platform, offering the potential to deliver the same benefits it has already provided to food stallholders to other small businesses.[45]

Despite the successes of Kenya's digital economy, some suggest it is overhyped. Entrepreneurs complain that funding from local backers is still hard to secure for technology companies, and that potential investors do not understand digital business well enough. Critics have suggested that the support for start-ups from non-governmental organizations is greater than that from true investors, and other African cities are starting to make inroads into Nairobi's lead. Many of these issues and criticisms will be familiar to technology clusters elsewhere in the world. Regardless of the validity of any such criticism, the building blocks established in Kenya look to be a robust platform for continued growth of its digital sector for some years to come.

Resources

Kenya Ministry of Information, Communications and Technology (http://www.ict.go.ke/)

Republic of Costa Rica

Play

Establishing tax incentives and a commitment to free trade to attract foreign investment in high-tech

Overview

Costa Rica has successfully transformed itself from a largely agricultural economy into one where information and communications technology (ICT) services play an increasingly significant role, largely through attracting foreign investment from multinational technology companies. As one of the strongest champions of the World Trade Organization's Information Technology Agreement, Costa Rica credits this as a significant factor in attracting ICT investment.

Key Lessons

– Countries with small populations can go beyond expectations when encouraging investment in ICT by offering investors efficiencies rather than market access.

– Though tax breaks, free trade and labour arbitrage are powerful incentives for foreign investment, governments seeking to exploit this approach to develop their digital economies must ensure they also take steps to build human capacity and skills, and to ensure that wage inflation does not diminish their appeal over time.

– Governments of countries from which overseas firms are exporting goods or services using nearshoring or offshoring models, and which provide limited or no customers in the local market, must nurture a balanced portfolio of investments to avoid being overdependent on any single employer. Hence, they will be able to cushion their workforce and economic performance against decisions to withdraw investments.

Description

With a population of 4.6 million people, Costa Rica is a relatively tiny country compared to some of its Latin American neighbours. However, it has established an enviable record of attracting foreign direct investment within the region, much of which has been generated from American-headquartered multinational technology companies. As shown in some of the other case studies, a combination of two factors helps to drive Costa Rica's attractiveness to investors in the digital sector. First, the country offers a generally favourable environment to locate a business. It has a more than 120-year history of democratic government, and is one of the most politically and economically stable nations in the region, as well as one of the safest in which to live. Second, since 1985 the government has made explicit efforts to promote the country as an attractive location for foreign direct investment and in trade liberalization.[46] With close to a third of its territory reserved for nature conservancy, finding new sources of income and economic growth have been a national imperative.

A combination of government-run bodies and non-governmental organizations are explicitly focused on promoting investment in Costa Rica, and include the Ministry of External Trade, COMEX (Ministerio de Comercio Exterior de Costa Rica), PROCOMER[47] (Promotora del Comercio Exterior de Costa Rica) and CINDE[48] (Coalición Costarricense de Iniciativas de Desarrollo). Created in 1982 with the funding assistance from the US government's USAID programme, CINDE is now independent and self-funding. Since its inception, it has helped to attract more than 280 high-tech companies to invest in Costa Rica. Both PROCOMER and CINDE are recognized as some of the most effective organizations of their type in South America.[49,50] In 2016, their efforts saw 40 new investment projects in the multinational services, life sciences, advanced and light manufacturing, and food industry sectors. Moreover, 94% of the foreign companies already established in Costa Rica either expanded or maintained their level of operations in the country. Collectively, these initiatives were responsible for creating 12,307 new formal jobs and contributed to the country's 4.3% growth in gross domestic product (GDP) in 2016.[51]

Though other electronics companies had made limited investments prior to the mid-1990s, Intel, after determined courting by CINDE, decided in 1997 to locate a new $300 million microprocessor plant in Costa Rica. This stands out as a tipping point in the story of the country's digital economy. Prior to the plant's opening, Costa Ricans had limited opportunities to work in the electronics or technology industries. Thereafter, direct and indirect employment opportunities were created in the ecosystem arising from Intel's investment.[52] The facility accounted for 4.9% of the country's GDP by 2006, and 20% of its exports.[53] Though manufacturing ceased at the plant in 2014 with the loss of about 1,500 jobs, it remains a design and test location for Intel and still employs nearly 2,000 people.[54] Currently, many other leading technology companies have significant operations in Costa Rica, including Accenture, Akamai, Cisco, Computer Associates, DXC Technology, Hewlett Packard Enterprise, Microsoft and VMWare.[55] The ICT sector accounts for 32% of Costa Rica's exports.

A principal reason for Costa Rica's ability to attract these organizations is the generous tax breaks it offers them through its Free Trade Zone regime.[56] A range of taxes are waived for companies meeting certain obligations as to the scale of their investments over a specific period, the number of jobs created and their commitment to export goods or services. This includes full or partial exemption from corporate income tax, and full exemption from customs duties on imports and exports, and from local taxes and withholding taxes for overseas remittances. The criteria and package of tax exemptions vary depending on the type of company and the companies' preferred location, with different municipalities able to offer different incentives by varying local taxes. Costa Rica acceded to the General Agreement on Tariffs and Trade in 1990, and was a founding member of the World Trade Organization in 1995. The country has had a bilateral free trade agreement with Canada since 2002 and, after initial delays in ratification, has been a participant in the Dominican Republic-Central American Free Trade Agreement (CAFTA-DR) with the United States since the beginning of 2009,[57] which significantly boosts its attractiveness for companies servicing North American markets.

Such financial benefits would be of little value if Costa Rica could not provide the skilled labour necessary to staff the facilities that companies invest in. In this regard, the country is reaping the benefits of long-standing policy decisions. Education has been free and compulsory in the country since 1869. The teaching of English begins in elementary school, and a large percentage of its citizens speak English fluently. Increasingly, Costa Rica is also incorporating skills relevant to a career in technology into the curriculum. CINDE and CAMTIC (Cámara de Tecnologías de Información y Comunicación), the Costa Rican technology trade association, have helped to develop specialist programmes aligned to the sector's needs, combining soft skills, language and technical expertise in certifications such as Six Sigma or Information Technology Infrastructure Library (ITIL). Costa Rica was rated first for innovation in the Latin America and Caribbean region in the last World Economic Forum Global Competitiveness Index.[58] Another important actor in driving educational programmes in ICT is the country's Omar Dengo Foundation (Fundación Omar Dengo).[59] Founded in 1987, this far-sighted, non-profit organization works to design and implement innovative educational programmes.[60] Such programmes encourage the development of skills and promote the use of digital technologies as tools for learning, and the development of children, youth and adults to mitigate social, educational and digital gaps. The Foundation works closely with the Ministry of Public Education and the Ministry of Science, Technology and Telecommunications to improve the quality of the Costa Rica educational system and to implement the required ICT infrastructure. Its initiatives have been particularly effective in supporting children from the country's rural population to use ICT in their education.

Though dominated by international companies, Costa Rica's digital economy is increasingly producing its own native successes. The country has a growing start-up and developer culture,[61] and steps are being taken to support greater participation of women in the technology sector through mentoring networks.[62] CAMTIC's map[63] of the country's ICT sector, produced in partnership with PROCOMER in 2015, provided comprehensive insight into the depth and breadth of Costa Rica's digital economy.

Given the country's small population, the merit in the longstanding strategy of driving Costa Rica's economic growth by attracting foreign investment and encouraging the export of goods and services is clear. However, the opportunities for labour arbitrage within the ICT sector are likely to even out over time, as participating economies start to "level up". Thus, investment decisions will likely shift towards the question of quality and capability rather than solely of cost. Costa Rica must therefore build on the work it has already done to grow the digital skills of its citizens if it is to continue to compete successfully for technology investments. One further issue likely to concern countries that adopt this model is whether the nations served by their overseas investors continue to fulfil their obligations to comply with existing free trade agreements. Threats to impose border-adjusted taxes or other measures which would undermine the offshore/nearshore model are a potential risk in this regard.

Nevertheless, the transformation of Costa Rica's economy from one focused on agricultural produce to one where high-tech and services play such an important role is an impressive story. It owes much to the consistency of relevant policies in education, taxation and free trade over the long term, and to the quality of execution of its trade promotion activities.

Resources

COMEX (Ministerio de Comercio Exterior de Costa Rica) (http://www.comex.go.cr/)

4. Protecting Digital Infrastructure, Business and Fundamental Rights

Wolfgang Kleinwächter, ICANN Board Member; Professor for International Communication Policy and Regulation, University of Aarhus, Denmark

An open, secure and trustworthy internet is a precondition for the development of a robust digital economy. In developing a national digital policy, governments must treat security and trust as foundational. It goes without saying that security and privacy do not contradict each other, but they are essentially two sides of the same coin. It is not a zero-sum game where security can only be enhanced at the cost of privacy.

The multistakeholder approach is essential for effective security policies given how the private sector, technical community and civil society all have their unique roles and responsibilities. In a more specific sense, there are four main things for stakeholders at the national level to focus on in terms of data security:

1. Develop a comprehensive **national cybersecurity strategy** which includes measures to protect national critical infrastructure against cyberattacks, deter all forms of cyberaggression against national assets and enhance the awareness of potential cyberthreats, in both the public and private sectors

2. Adopt specific **cybersecurity and data protection legislation** which has to include, inter alia, definitions of categories of cybercrime, adequate reporting duties for state and non-state actors about cyberattacks, and the establishment of clear, pragmatic and legally enforceable approaches for upholding harms related to privacy and data discrimination

3. Establish **institutional mechanisms to react against cyberattacks** as computer emergency response teams (CERTs)/computer security incident response teams (CIRTs)

4. Engage in broad-based **cybersecurity capacity building and awareness raising programmes** for state actors, businesses (in particular small and medium businesses) and individual users

4. Along with a focus on enabling policy frameworks for data security, it is also vitally important to establish agile and adaptive policies for the use of data. Most important is the need for shared principles combined with agile and adaptive enforcement mechanisms on a transnational level. Key themes for leaders to focus on include:

Deliver meaningful transparency

Transparency practices need to be reframed to be more meaningful, actionable and relevant for individuals. Greater emphasis is needed on presenting individuals with understandable and relevant information on how data is being used. Organizations need to simplify the ways in which they communicate their data practices to reduce the complexity of transparency for individuals. Also needed are policies and tools for understanding how data flows “out the back door” of institutions. The forward transfer of data throughout the ecosystem is complex, opaque, and drives uncertainty and suspicion.

Strengthen accountability

As the calls increase for shifting the primary focus of governance to be more usage-based and contextual, holding relevant stakeholders of all sizes accountable in a defined and measurable way is a priority. Trust networks and holistic incentive structures are needed to ensure principled and enforceable use of data.

Empower individuals

As the value and volume of data originating from sensors and analytics increase, individuals are increasingly unaware of and distanced from the decisions on how all this data is being used. Individuals need to be empowered in two ways: having a say in how data about them is used by organizations, and having the capacities to use data for their own purposes. Additionally, as the predictive power of algorithms increases, individuals need to more effectively engage in understanding (and managing) the intended impact of data usage.

Commonwealth of Australia

Play

Strengthening national cybersecurity in pursuit of innovation, growth and prosperity

Overview

Australia’s federal government has put in place a comprehensive new strategy, created new political and civil service roles, allocated new funding and executed a series of machinery of government changes to raise cybersecurity up the political agenda and improve capability.

Key Lessons

- Comprehensive improvements in cybersecurity require political leadership.
- Political leaders should be prepared to revisit historical organizational models to ensure the machinery of government is properly aligned against cyberthreats, and to consider new roles to coordinate and lead the whole-of-government response.
- In the face of an evolving and dynamic threat environment, governmental structures and policies need to similarly evolve to avoid the false confidence arising from a tick-box approach to security.

Description

Though politicians of all nations increasingly need to engage on digital policy to a much greater degree than before, Australia is an interesting example of a country that has benefitted from a Prime Minister with in-depth knowledge of the topic, gained not only through previous ministerial portfolios but also in his life outside politics. Prime Minister Malcolm Turnbull served as the country’s Minister for Communications from 2013 to 2015, during which he steered through significant change to the programme to deliver the country’s national broadband network. Prior to entering politics, he had been an investor in a range of internet and e-commerce companies; indeed, his appointment as Prime Minister in 2015 was welcomed by many in the country’s technology sector,[64] with one entrepreneur stating, “People in the tech sector know that he gets it.”[65]

Australia occupies a distinctive geopolitical position. One of the world’s most advanced economies and most stable democracies, it has, however, a relatively small population (about 25 million). Nevertheless, as a long-standing participant in the United Kingdom–United States of America Agreement, Australia is a member of the Five Eyes community, along with the United States, United Kingdom, Canada and New Zealand, and therefore plays a significant role in international intelligence matters. It is perhaps no surprise then that under Prime Minister Turnbull’s leadership, the issue of cybersecurity has risen up the political agenda. This has not, though, been solely the product of personal interest and a legacy of the country’s historical relationships: a series of internal and external events have also contributed to the larger profile that cybersecurity has in contemporary Australian politics.

First, like many countries with similar systems of government, Australia’s political class is increasingly concerned about the potential for interference by other nations in their country’s democratic processes. Second, they have noted the large-scale cybersecurity incidents affecting other countries, in particular the WannaCry ransomware attack in May 2017 which caused significant disruption to parts of the UK National Health Service, and questioned how their institutions might cope in a similar situation. Finally, and perhaps most directly, the Australian government itself experienced a major cybersecurity incident in 2016, when it was forced to temporarily shut down the internet site, through which citizens were submitting responses to the Australian Statistics Bureau’s quinquennial census, following a series of distributed denial-of-service (DDoS) attacks. Though the service was recovered within two days, what should have been a preventable incident was an embarrassment, given Australia’s commitment to the digitalization of public services (see the second chapter), and has further catalysed the government’s determination to improve its capability to prevent and/or withstand similar incidents in the future.

The roots of Australia's revised approach to cybersecurity lay in a review commissioned by Turnbull's immediate predecessor, Prime Minister Tony Abbot (2013-2015), towards the end of 2014. The resulting strategy, published in April 2016, was a comprehensive attempt to raise the profile of the topic and enhance the capacity of both the Australian government and Australian businesses. The strategy contained 33 measures across five themes:

1. **Creating a cyberpartnership** – engaging government bodies, business and the research community to work together to advance Australia's cybersecurity
2. **Strong cyberdefences –** making Australia's networks and systems hard to compromise and resilient to cyberattacks
3. **Global responsibility and influence –** actively promoting an open, free and secure cyberspace
4. **Growth and innovation –** enabling Australian businesses to grow and prosper through cybersecurity innovation
5. **A cybersmart nation –** ensuring that Australians have the cybersecurity skills and knowledge to thrive in the digital age

Many of the measures centred on making better use of the undoubted existing strengths of the Australian defence, justice and intelligence apparatus by turning it outwards to better support engagement with stakeholders beyond its traditionally closed environment. For example, of the A$230 million (approximately $182 million) funding over four years to support the strategy, the most significant individual item related to relocating the Australian Cyber Security Centre. The Centre shared a classified office with the Australian Security Intelligence Organisation, but will move into a more open and accessible facility to facilitate its growth (through the recruitment of staff with less stringent security clearances) and improve collaboration with business

The remainder of the funding is spread across all five themes outlined in the strategy and allocated across different ministries, including Defence and the Attorney-General's Department, as well as the Industry, Innovation and Science, and Foreign Affairs and Trade portfolios. Notable other investments included funding to improve the capability and capacity of Australia's Computer Emergency Response Team, as well as to establish a network of joint cyberthreat sharing centres and a campaign to raise national cybersecurity awareness. Also of note was the allocation of significant funding to establish a national cybersecurity innovation network and Cyber Security Growth Centre, an industry-led, non-profit organization intended to take advantage of the growing global market for cybersecurity products and services. The last major item of expenditure relates to additional funding for the Australian Federal Police to strengthen cybercrime investigation and response capability and capacity.

Alongside the launch of the strategy, the Australian government also made a series of new and, in some cases, novel appointments to support its implementation. At the political level, Daniel Tehan, Member of the Australian House of Representatives, was appointed to the new post of Minister Assisting the Prime Minister for Cyber Security in July 2016.[66] Within the Australian Public Service, Alastair MacGibbon was appointed as the Prime Minister's Special Adviser on Cyber Security in May 2016.[67] A former Australian federal police officer, MacGibbon was founder of Australia's National High-Tech Crime Centre, and had most recently been the country's first e-Safety Commissioner.[68] Finally, within Australia's diplomatic service, Tobias Feakin, a member of the committee whose review led to the new strategy, was appointed as Australia's first Ambassador for Cyber Affairs,[69] with the responsibility for "whole of government international engagement to advance and protect Australia's national security, foreign policy, economic and trade, and development interests in the internet and in cyberspace". These appointments, together with the personal interest shown by the Prime Minister, have significantly strengthened the representation of cybersecurity issues within the political class, and within the Australian Public Service and its diplomatic corps. They have also contributed to ensuring that cybersecurity matters are addressed at the Council of Australian Governments, the forum that brings together elected representatives from the federal and state governments.

In April 2017, on the first anniversary of the publication of the new strategy, the Australian government published an update on progress against each of the five themes.[70] Inevitably, given that the strategy is intended to be realized over a four-year period, good progress has been made in some areas, with others are still lagging. Though the DDoS attack affecting the Australian census occurred after the publication of the strategy in 2016, lessons from the two enquiries into the incident by the Senate[71] and the Office of the Prime Minister[72] have clearly provided additional evidence of what needs to change within the Australian Public Service, and further strengthened the government's resolve to address these issues. One novel recommendation from the second of these reports was that ministers should attend a "boot camp" to improve their knowledge of cybersecurity and enable them to understand the role that they must play, as the political leaders of their departments, in understanding and managing these risks.

Nevertheless, Australia's cybersecurity stance has clearly improved due to the government's intervention. Minister Tehan's introduction to the progress report, however, notes: "In the world of cybersecurity, if you are standing still you are going backwards." Building on the existing momentum in security matters, Prime Minister Turnbull announced a further and more radical set of machinery of government changes in July 2017. This will establish a new Home Affairs "super-ministry" to oversee all of Australia's domestic security agencies, including the Australian Security Intelligence Organisation, Australian Federal Police, Australian Border Force and Australian Criminal Intelligence Commission. Modelled on the United Kingdom's Home Office, the intention is to create an environment in which agencies work together as closely as they can. As part of these changes, MacGibbon will take on leadership of the revised Australian Cyber Security Centre in its new, more outwardly-facing role. He has commented that, through the latest strategy and with the recent machinery of government changes, he expects Australia to move "to the front of the pack" in terms of its ability to exploit cybersecurity as a driver of economic growth, but warned that the country must continue to challenge itself if it is to maintain this standing.

Resources

Commonwealth of Australia, Department of the Prime Minister and Cabinet, Australia's Cyber Security Strategy, 2016 (https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf)

Israel

Play

Delivering a national cybersecurity initiative

Overview

The Government of Israel has set a vision for the country to be a leading nation in its capacity to harness cyberspace as an engine of economic growth, social welfare and national security. Israel's cybersecurity strategy is meant first and foremost to realize the Israeli cybervision by maintaining cyberspace as a safe sphere, investing state efforts in confronting cyberthreats and reducing the overall risk inherent in this sphere. The strategy also looks to continue establishing Israel as a dominant player in the international arena, a leader in technological innovation and a partner affecting the processes that shape cyberspace. Israel's cybersecurity strategy is the conceptual and practical foundation for the nation's efforts and activities in the field, designed to establish order in national efforts and ensure a stable, long-term solution. Moreover, the strategy is intended to provide an inclusive response to all threats and risks according to national interests and the state's responsibility, while ingraining new concepts and approaches adapted to the distinctive features and challenges that "cyber" poses.

Key Lessons

– State-wide effort is required to ensure the construction of Israel's cyberspace as a safe and lasting sphere of growth (based on Israel Government Resolution 2443, 15 February 2015) through various efforts to support organizational security efforts (e.g. best practice, guidance, regulations, incentives), regulate the cybersecurity market, set a high bar for government cybersecurity processes and implement solutions, processes and technological infrastructures at the national level.

– Establishing the National Cyber Security Authority (NCSA) to lead national security efforts and preparation for managing an integrated national campaign of security and law enforcement (based on Israel Government Resolution 2444 of 15 February 2015) was crucial. Setting up a central body for cybersecurity, with cybersecurity its sole concern, was important to serve as a hub of national knowledge and lead the defensive efforts against cyberattacks on the nation, as well as to conduct an integrated campaign with security and law enforcement agencies to deal with the sources of the threats.

– Research, development and implementation of state-level security capabilities and technologies can establish solutions specifically designed to strengthen cyber-resilience at the national level.

– Construction of a national scientific and technological cyberforce helps to continue strengthening Israel's scientific and technological foundations in cyberspace (industry, academia and human capital). This also helps to maintain the state's relative advantage and operational capabilities in the technological field, now and in the future, as part of the global effort to meet the challenge.

Description

The first major milestone in the development of the Israeli national cybersecurity efforts was taken in 2002, when the government authorized the National Information Security Authority (NISA) of the Israel Security Agency to instruct and protect vital computerized systems of selected public and private civilian organizations. Consequently, a supreme steering committee headed by the National Security Advisor was established to synchronize and observe the overall efforts of state-related cybersecurity. NISA's security efforts and the formation of the committee were a globally groundbreaking, national initiative of cybersecurity, as well as a significant contribution towards critical infrastructure security and the development of knowledge and capabilities in Israel.

The next milestone, following a recommendation of a broad expert committee, was presented in Government Resolution 3611 ("Advancing the National Capacity in Cyberspace") on 7 August 2011, to establish the Israel National Cyber Bureau (INCB), directly under the Prime Minister's Office. The INCB was charged with articulating the state's national cyberpolicy and strategy, promoting national processes and developing national cybercapabilities, while strengthening Israel's status as a world leader in the field.

On 15 February 2015, the Government of Israel adopted the major components of its national cybersecurity strategy, developed by the Bureau through two government resolutions: G.R. 2443 ("Advancing National Regulation and Governmental Leadership in Cyber Security") and G.R. 2444 ("Advancing the National Preparedness for Cyber Security"). One of the main decisions was to establish the NCSA, a new, designated agency responsible for leading the nation's cybersecurity. Together, the INCB and NCSA form the Israel National Cyber Directorate (INCD).

The Israeli cybersecurity strategy is based on a groundbreaking concept of operation for national cybersecurity. This concept is generic and thus relevant to other nations. It provides a conceptual framework for all national efforts and functions in the context of national cybersecurity, both the direct state actions to confront the threat and the indirect actions aimed at helping security activities within the market. The concept covers three operational layers defining state action as well as relations between the state and private-sector organizations:

- Market robustness: Ensuring the ability of organizational process as well as interorganizational and economic processes to continue operating under the routine of cyberthreats, by reducing networks' attack surface and thus lowering the potential that attacks will succeed. The state promotes this ability by providing support and motivation for organizational security efforts and handling market failures in the cybersecurity market.

- Systemic resilience: Establishing a systematic ability to confront cyberattacks and reduce the cumulative damage to the economy before, during and after incidents, particularly attacks that expand and have lateral implications. System resilience may be achieved by state processes encouraging information sharing, creating and disseminating valuable information, and assisting attacked organizations.

- National defence: Managing a state-level campaign against severe threats of determined, resource-rich attackers representing a clear and present danger to national security. Concurrently, defensive efforts contain attacks and their ramifications with active efforts to confront the threats' sources.

Finally, the strategy sets out Israel's commitment to partnerships in international efforts shaping cyberspace. The country will participate in the international discourse to shape this sphere, develop international partnerships to strengthen its own security capabilities and those of its allies, and harness national capabilities for building global cyberspace as a safe and secure sphere.

Resources

Israel, Prime Minister's Office, National Cyber Bureau (http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx)

National Cyber Security Authority (https://www.gov.il/en/Departments/national_cyber_security_authority)

Adamsky, D., 2017. "The Israeli Odyssey toward its National Cyber Security Strategy", The Washington Quarterly, 40:2, pp. 113-127 (https://twq.elliott.gwu.edu/israeli-odyssey-toward-its-national-cyber-security-strategy)

Japan

Play

Promoting security by design in policy and practice

Overview

Japan has promoted cybersecurity as an economic investment for companies, and cross-sector bilateral and trilateral collaboration as a means of strengthening cybersecurity and increasing intelligence sharing.

Key Lessons

- A key feature to crafting national cybersecurity policy is collaboration. Cyberthreat intelligence and public-private partnerships are critical for protecting infrastructure.
- A vision for cybersecurity (Japan 2020) should include internet-of-things (IoT) security and encourage business executives to consider cybersecurity as an investment opportunity for sustainable economic growth and innovation.
- International collaboration is crucial. Japan has expanded and strengthened its collaboration with other countries in cybersecurity, and is active in multilateral and bilateral cybersecurity dialogues with various countries.

Description

Since Tokyo was selected in September 2013 to host the 2020 Summer Olympic Games (Tokyo 2020), Japan has been making greater efforts to enhance its security in both the physical and cyber domains to ensure the event's success. In November 2014, the first Basic Act for Cybersecurity was enacted to define cybersecurity and the scope of the responsibility for the government, local municipal government, critical infrastructure companies and citizens. The Act declared that cybersecurity is essential to ensure the free flow of information and freedom of speech, and to create innovations and socioeconomic growth. It also gave legal authority to the National Information Security Centre (NISC) under the Cabinet Secretariat to craft a national cybersecurity strategy and policy; to serve as a point of contact for bilateral, trilateral and global cybersecurity collaboration; to gather and analyse cyberthreat intelligence; and to promote public-private partnerships for critical infrastructure protection. (NISC subsequently changed its name to the National Centre of Incident Readiness and Strategy for Cybersecurity, but is still known as NISC.)

Under the newly empowered NISC, the Japanese government issued the Cybersecurity Strategy in September 2015 to provide the country's cybersecurity vision in the run-up to Tokyo 2020. The strategy included IoT security and encouraged business executives to consider cybersecurity as an investment opportunity for sustainable economic growth and innovations, rather than as a cost centre. Based on the strategy, the Japanese government published the Cybersecurity Guidelines for Business Leadership in December 2015 to encourage companies to invest in cybersecurity and share cyberthreat intelligence to prevent successful cyberattacks. It also worked with companies and universities, and issued the IoT Security Guidelines in July 2016 to pursue security by design.

The pressure of Tokyo 2020, along with worries about IoT security, have prompted Japan to do more to promote cyberthreat intelligence sharing, which includes encouraging additional Information Sharing and Analysis Centres (ISACs). Japan already has the Information and Communication Technology ISAC and Financials ISAC, and in 2017 launched the Electricity ISAC that will collaborate with its European and US counterparts. Also, car manufactures initiated a framework in April 2017 to share cyberthreat intelligence to protect connected cars. Since Prime Minister Shinzo Abe stated in October 2015 that Japan will make driverless cars available by the Tokyo 2020 games, car cybersecurity has attracted substantial interest in the country.

Another major cyberthreat intelligence sharing framework is the Initiative for Cyber Security Information sharing Partnership of Japan, which was established by the Information-Technology Promotion Agency (IPA) under the Ministry of Economy, Trade and Industry. IPA works with critical infrastructure sectors such as electricity, gas and oil, as well as the Japan Computer Emergency Response Team/Coordination Centre (JPCERT/CC) and NISC, to share cyberthreat intelligence under their non-disclosure agreement and respond to any incident as soon as possible.

Prime Minister Abe's administration has actively expanded and strengthened security collaboration with other countries, including in cybersecurity. Japan has bilateral cybersecurity dialogues with various countries, such as Australia, Estonia, France, India, Israel, the United States and the United Kingdom, as well as trilateral ones where the countries mutually update each other on their national cybersecurity policy efforts, and share what they see in the threat landscape.

The Japanese government is also active in multilateral cybersecurity collaboration. It has been helping countries of the Association of Southeast Asian Nations over the past decade with cybersecurity capacity building by providing policy-making advice, technical skills and cyberthreat intelligence sharing. Furthermore, Japan has been participating in the United Nation's Group of Governmental Experts and Global Conference on Cyberspace, with the goal of contributing to the establishment of international norms and confidence building.

Resources

Initiative for Cyber Security Information Sharing Partnership of Japan (J-CISP): Annual Activity Report FY 2012 (https://www.ipa.go.jp/files/000032417.pdf)

JPCERT/CC (www.jpcert.or.jp/english/)

Federal Republic of Germany

Play

Enabling a trustworthy digital agenda

Overview

In August 2014, the German Federal Ministry for Economic Affairs and Energy, the Federal Ministry of the Interior and the Federal Ministry of Transport and Digital Infrastructure introduced a Digital Agenda for the legislative term of 2014 to 2017. By doing so, the federal government aimed to actively assist and foster the development of a digital transformation to strengthen Germany's economic future. Furthermore, the Federal Ministry of the Interior presented a new Cyber Security Strategy for Germany, amending the Cyber Security Strategy of 2011 to concentrate strategic approaches and objectives already elaborated into one interagency strategy that captures the relevance and broadness of this topic.

Key Lessons

- Germany's success in digital infrastructure is enabled by its regulatory framework that supports investment and innovation of companies. Enacted in 2016, it establishes legal and planning certainty for all stakeholders.
- Germany's Cyber Security Strategy is focused on a future-oriented cybersecurity policy to ensure freedom and security. Cyberattacks are increasing, and most of these attacks strike insufficiently protected information technology (IT) systems.
- The IT Security Law has enlarged the protection of critical infrastructure by establishing resilient IT against (terroristic) cyberattacks, where operators of critical infrastructure are obliged to report cyberincidents.
- To build protection and trust within society and the economy, the government adopted data processors to confirm they have adequate technical and organizational measures that ensure sufficient levels of data protection.
- To advance the digital workplace and economy, German policy-makers are focused on enabling policy frameworks for small and medium-sized enterprises to recast their value chains and redefine business models to reflect the Industry 4.0 agenda.

Description

Germany's digital transformation is an example of a multifaceted and coordinated strategy that focuses on investing in internet infrastructure, cybersecurity and trust, along with using fit-for-purpose data protection measures and strengthening capacities of the digital workplace. It comprises the following initiatives:

Digital Infrastructure
A core focus in Germany has been to provide a broadband infrastructure that delivers download speeds of at least 50 megabits per second until 2018, not only in urban but also in all rural areas. For this goal, adequate spectrum has been made available, and intelligent mobile services are helping to accelerate penetration rates. A key enabler of this success has been a regulatory framework enacted in 2016 that established legal and planning certainty for all stakeholders (DigiNetzG) and the Network Alliance for a Digital Germany (Netzallianz Digitales Deutschland), which supports both the investment in and innovation of companies.

Cyber Security Strategy
With the growing digitalization of modern society, the vulnerability and risks of IT also grow. The number of cyberattacks are constantly increasing, and most of them strike insufficiently protected IT systems. Against this background, Germany has initiated a future-oriented cybersecurity policy to ensure freedom and security. The Federal Office of Information Security is empowered to fight threats and prioritize the importance of information and communications technologies. It was broadly amended in 2015 to reflect the current nature of IT security risks.

IT Security Law
The Law entered into force in July 2015, with its main goal to enlarge the protection of critical infrastructure by establishing resilient IT against terroristic cyberattacks, where operators of critical infrastructure are obliged to report cyberincidents. The Law also brought changes to the Telecommunications Act, the Energy Industry Act and the Atomic Energy Act. National regulations are required to implement the IT Security Law to concretize the critical infrastructures. A first regulation entered into force in May 2016 to cover the energy, communications technology, water system and nutrition sectors. A draft for the second regulation, enacted in April 2017, also covers the finance, transportation and health sectors.

Cyber Security Strategy
The strategy includes measures of the Federal Office of Information Security in the following areas:
- Protecting critical information structures
- Securing IT systems in Germany
- Strengthening of IT security within the public authorities
- Developing a National Cyberdefence Centre (established 2011). The Centre, a facility between federal security bodies, enables better cooperation between security agencies and is part of the Federal Office for Information Security
- Installing computer emergency response teams (CERTs) that can react to cyberincidents on-site
- Establishing a national Cyber Security Council
- Establishing a central body for IT in the safety sector
- Using reliable and trustworthy IT

Building protection and trust within society and the economy
The Federal Parliament recently adopted a draft for a new Federal Data Protection Act (BDSG-E) to implement specifications of the General Data Protection Regulation (GDPR). In general, the BDSG obliges data processors to ensure adequate technical and organizational measures that guarantee a sufficient level of data protection.

Digital workplace and economy
Along with deploying a high-performing and highly reliable Internet Protocol infrastructure, German policy-makers also focused on enabling policy frameworks for small and medium-sized enterprises to recast their value chains and redefine their business models to reflect the Industry 4.0 agenda.

Innovative public administration
Germany seeks to ensure the efficiency and security of IT systems of authorities. Digital access to public authorities is relevant for having a strong connection to citizens and ensuring their confidence in the government.

Shaping digital environments in society
Germany will continue An Internet for Children, an initiative that prepares children for digital devices and improves opportunities for citizens to participate online.

Education, science, research, culture and media
The Council for Information Infrastructure will coordinate and advise on building a science and research information infrastructure. The Digital Media in Vocational Education and Training project aims to improve the use of digital tools.

Resources DigiNetz-Gesetz (http://www.bmvi.de/DE/Themen/Digitales/Breitbandausbau/DigiNetzG/diginetzg.html)

Conclusion and Next Steps

As the Fourth Industrial Revolution begins to affect the economic and societal layers of the digital economy, the challenges related to ensuring fair and accountable outcomes for that economy are complex. Uncertainty, opacity and the velocity of change demand new approaches for strengthening trust and inclusion. Some of the central themes of these new approaches, distilled from the various case studies shared in this White Paper, are listed below:

Ensuring innovation in digital governance and access

- Internalize the multistakeholder consultation process, given its efficiency and flexibility to address the complex balancing of interests required for a country's digital transformation.
- Establish an enabling environment for business that prioritizes public-private partnerships and cultivates a local innovation and content-creation ecosystem to ensure sustained usage.
- Couple investments in the availability of access technologies with training and literacy programmes that encourage the productive use of digital technologies. Particular attention should be paid to the needs of youth. Collecting separate statistics in rural areas can help to better identify needs and track progress on closing the digital divide.

Developing a smart society and public services

- Curate a community of leaders (from a variety of public- and private-sector actors) to change the institutional culture of both governments and businesses from being risk-averse to being inspired, innovative and entrepreneurial.
- Establish collaborative platforms that allow ideas to flourish, with particular attention paid towards action and disciplined execution versus excessive planning and circular dialogue.
- Ensure a forward-looking regulatory and legal environment is in place, with balanced incentives to bring new digital services to market in a timely manner. Recognize that new technologies require change and, as such, demand clear guidance on issues related to data protection, privacy, human rights and cybersecurity.
- Prioritize the need for digital literacy and for addressing the gender inequalities within the larger digital divide.

Growing the digital economy

- Seek to play a more active role in preparing an economy to harness the benefits and tackle the challenges associated with adopting digital technologies.
- Ensure government policy-makers recognize their role in setting direction and enabling the supporting infrastructure without stifling entrepreneurial innovation.
- Foster the creativity, imagination and drive of the individuals working in the digital economy. This can serve as one of the biggest contributors to a successful digital transformation.

Protecting digital infrastructure, business and fundamental rights

- Develop a comprehensive national cybersecurity strategy that includes measures to protect national critical infrastructure against cyberattacks, deter all forms of cyberaggression against national assets, and enhance the awareness of potential cyberthreats in the public and private sectors.
- Adopt specific cybersecurity and data protection legislation to include, inter alia, definitions of categories of cybercrime, adequate reporting duties for state and non-state actors, and the establishment of clear, pragmatic and legally enforceable approaches for upholding harms related to privacy and data discrimination.
- Empower individuals on how data about them is used by organizations, and how they can use data for their own purposes and to more effectively engage in understanding (and managing) the intended impact of data usage.

Appendix

Embracing the adoption of digital protocols and the digital policy model canvas

Policy leaders need to more effectively identify emerging needs, prioritize critical issues and design conceptual prototypes of what an implementable and repeatable governance solution would entail.

For example, by establishing a protocol for collecting relevant and meaningful case studies on innovative national digital policies, knowledge exchange could be enhanced throughout the digital ecosystem.

One initial notion of such a protocol could be the use of a digital policy canvas for identifying meaningful case studies. Key steps in implementing this approach would include the following:

- Start with a well-developed problem or definition of an opportunity, mostly informed through public consultation and due diligence
- Have a clear sense of the beneficiaries (whether business or individuals) and their needs, applying user-focused design methodologies at times
- Map, curate and engage with key stakeholders who are crucial to developing and/or implementing the policy or approach
- Be sensitive to the context – cultural, political or social – of the topic at hand, and stay informed about what was tried elsewhere
- Adopt an inclusive process and coordinate with global actors
- Assess existing solutions or engage different people/ constituencies to ideate new approaches
- Be aware of budget and time constraints, and the possible risks associated with certain approaches

Using this process and following these questions (see the example on Rwanda's broadband policies), create an evidence-based "canvas" that pragmatically serves the needs of each issue and the relevant community of policy-makers.

Applying the Digital Canvas: A Review of Rwanda's National Broadband Policy

Definition of the issue/opportunity

What is the specific issue or opportunity?
In 2000, Rwanda outlined a vision to become a knowledge-based economy by 2020 (this has since been revised to 2050).

In 2000, a national ICT strategy (2000-2020) was promulgated, highlighting priority areas every five years and underpinned by universal access for all. Broadband was identified as an enabler for the growth of an innovation ecosystem, and one that would surely serve as a main driver in achieving Rwanda's goal to become a knowledge economy.

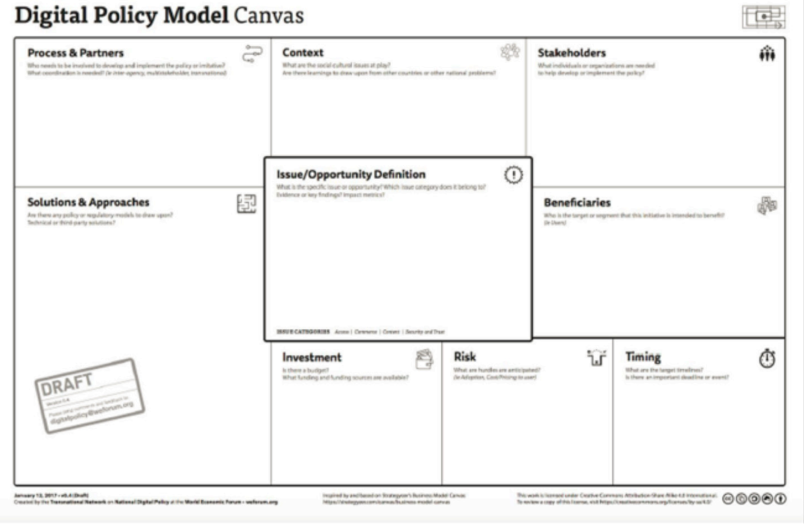
One of the limiting factors for telecom carriers to rollout broadband was the cost of deploying infrastructure in remote and underserved areas (inhabited by markets with low purchasing power).

To drive universal access while sustaining fair competition in the industry, the government made a strategic decision to foster an infra-sharing regime with an open-access wholesale network to preclude duplication of investments while driving the rollout and adoption of broadband services.

To encourage investment by a wholesale partner, a broadband policy needed to be established.

Which issue category does it belong to?
Access

Evidence of key findings supporting the definition of the problem or opportunity?
Mobile penetration = 60%
Internet market penetration = 8.5%
10% increase in broadband penetration = 1.38% per-capita growth in gross domestic product



Digital Policy Model Canvas

Process & Partners
Who needs to be involved to develop and implement the policy or initiative?
What coordination is needed? (ie inter-agency, multistakeholder, transnational)

Context
What are the social cultural issues at play?
Are there learnings to draw upon from other countries or other national problems?

Stakeholders
What individuals or organizations are needed to help develop or implement the policy?

Issue/Opportunity Definition
What is the specific issue or opportunity? Which issue category does it belong to?
Evidence or key findings? Impact metrics?
ISSUE CATEGORIES Access | Commerce | Content | Security and Trust

Solutions & Approaches
Are there any policy or regulatory models to draw upon?
Technical or third-party solutions?

Beneficiaries
Who is the target or segment that this initiative is intended to benefit?
(ie Users)

Investment
Is there a budget?
What funding and funding sources are available?

Risk
What are hurdles are anticipated?
(ie Adoption, Cost/Pricing to user)

Timing
What are the target timelines?
Is there an important deadline or event?

DRAFT
Version 0.4
Please send comments and feedback to digitalpolicy@weforum.org

January 13, 2017 • v0.4 (Draft)
Created by the Transnational Network on National Digital Policy at the World Economic Forum • weforum.org

Inspired by and based on Strategyzer's Business Model Canvas
https://strategyzer.com/canvas/business-model-canvas

This work is licensed under Creative Commons Attribution-Share Alike 4.0 International.
To review a copy of this license, visit https://creativecommons.org/licenses/by-sa/4.0/

Impact metrics
Broadband coverage of 97% of the population by end-of-year 2017, with all schools, hospitals and local administrative centres connected to broadband, and multiplier effects such as the creation of an innovation ecosystem

Canvas review
The issue and opportunity were clear and well-defined during the formulation process. The canvas is useful in highlighting the need for stakeholders to outline clear, specific and measurable impact metrics – for example, around the use by the beneficiaries (underserved communities). This translates into maximization of costs.

Beneficiaries
What is the target or segment of society (demographically, geographically, or type of company [e.g. small to medium-sized enterprise]) that this initiative is intended to benefit (i.e. users)?

Underserved Rwandans: They would benefit from coverage and complementary initiatives by government to drive up adoption of broadband nationwide (e.g. Viziyo loan programme providing smart devices) and the deployment of smart centres at hospitals, schools and administrative offices.

Telecom Carriers: The cost burden of investing in infrastructure to provide broadband would be addressed by this policy.

Canvas Review
The canvas stresses the importance of a "value proposition", reminiscent of the business canvas. This ensures that policy-makers understand needs, and address the value to and concerns of all relevant stakeholders. It also emphasizes a need for concrete evidence, thus reducing the risk of subjective perspectives in decision-making.

Stakeholders (Constituency mapping)
What individuals or organizations will be affected, or are needed to help develop or implement the policy?

Ministry of Youth & ICT (MYICT): ICT policy arm of the government

Rwanda Utilities Regulatory Authority (RURA): Autonomous body charged with licensing and regulation of the telecom industry

Rwanda Development Board (RDB): Investment promotion and engagement with potential private wholesaler partners

Private Sector Federation: Umbrella organization for private companies (including telecom carriers, internet service providers and mobile virtual network operators that are members of the Rwanda ICT Chamber)

Context
Are there learnings to draw upon from other countries or other national problems? What are the social and cultural issues at play?

Many African nations are concerned about universal access, especially given the size of underserved communities. Some countries have tried to engage telecom carriers to invest in expanding infrastructure to underserved communities to increase access, but given the cost, this has mostly been in vain. In Rwanda, the urgency to tap into human capital through innovation meant exploring new approaches.

The model of wholesale-only Radio Access Networks for mobile broadband is new in Africa (and countries similar to Rwanda in, for example, economic status and demographics). However, a few countries, such as the United Kingdom and New Zealand, have explored similar models, and lessons could be learned from their experiences.

Nevertheless, after consultations and engagement with all stakeholders in the public, private and civil society sectors, this was a bold and ambitious move by the government to provide access to all citizens.

Process and partners
Who needs to be involved and at what stage (setting the agenda, identifying solutions, implementing, evaluating)? What coordination is needed (interagency, multistakeholder, transnational)?

Multistakeholder coordination was required. MYICT led this during the policy formulation process; thereafter, and in line with the policy, a joint government-private sector steering committee, co-chaired by MYICT and PSF, led the process.

Canvas Review
N/A

Investment
Is there a budget?
Yes

What funding and funding sources are available?
Government budget lines and private investment through wholesale partners were both made available. A feasibility study had been carried out, prior to the policy development exercise, to assess the viability of the open access model. Therefore, the investment needs were well thought-out and very clear from the beginning.

Risks
What hurdles are anticipated?

Canvas Review
A risk assessment is not documented in the policy. This is a great recommendation from the canvas as it ensures that mitigation strategies are clearly outlined. The canvas should include a pointer on mitigation plans beyond an assessment of the risks.

Timing
What are the target timelines?

Entry of wholesale partner in the market; issuance of the licence, including negotiation of terms and conditions of the wholesale licence, is six months

Network rollout: three years

Digital literacy programme and schemes to support adoption of smart devices: three years

Connect all public entities in rural areas (schools, hospitals, local administration institutions): 18 months

Canvas Review
During formulation, an implementation timeline was outlined. In this section, the canvas could probably explicitly highlight a link between impact metrics and timelines to ensure they are concretely outlined and that the linkage is not lost.

Overall Input
The policy canvas, like the business canvas, would definitely facilitate policy-makers' thinking through interventions for identified issues and/or opportunities.

One of the challenges with policy formulation and implementation is the ability to bring stakeholders to work on a common goal in a timely, responsive manner. An iterative, agile process to formulate a policy may be worth exploring – one that fosters the concept of "piloting" to allow policies to be tried and tested, after which feedback and lessons learned can be used to draft a final policy paper for legislative (or similar) action. The canvas could serve to highlight this.

Additional Information

For additional information on the case studies identified in this White Paper, please contact the individuals listed below.

Ensuring Innovation in Digital Governance and Access

Federative Republic of Brazil
Virgilio Almeida (valmeida@cyber.law.harvard.edu)

Colombia
Maria Medrano (maria.medrano@hpe.com)

Republic of Rwanda
Alline Akintore Kabbatende (allineakintore.kabbatende@weforum.org)

Lebanon
Bassam Hajhamad (bassam.hajhamad@pwc.com)

Switzerland
Thomas Schneider (thomas.schneider@bakom.admin.ch)

Developing a Smart Society and Public Services

Republic of Singapore
Bassam Hajhamad (bassam.hajhamad@pwc.com)

Republic of Estonia
Bassam Hajhamad (bassam.hajhamad@pwc.com)

India
Bassam Hajhamad (bassam.hajhamad@pwc.com)

United Arab Emirates
Bassam Hajhamad (bassam.hajhamad@pwc.com)

Growing the Digital Economy

United Kingdom
James Johns (jamesandrewjohns@gmail.com)

Kingdom of Sweden
James Johns (jamesandrewjohns@gmail.com)

Republic of Kenya
James Johns (jamesandrewjohns@gmail.com)

Costa Rica
James Johns (jamesandrewjohns@gmail.com)

Protecting Digital Infrastructure, Business and Fundamental Rights

Commonwealth of Australia
James Johns (jamesandrewjohns@gmail.com)

Israel
Tal Goldstein (talgol@pmo.gov.il)

Japan
William H. Saito (william@saitohome.com)

Federal Republic of Germany
Wolfgang Kleinwächter (wolfgang.kleinwaechter@medienkomm.uni-halle.de)

Digital Policy Model Canvas
Stefaan G. Verhulst (sverhulst@nyu.edu)

Internet for All
Alex Wong (awong@weforum.org)

Endnotes

1. Brazilian Internet Steering Committee (Comitê Gestor da Internet no Brasil – CGI.br), Interministerial Ordinance 147 of 31 May 1995. Available at http://www.cgi.br/portarias/numero/147.
2. Brazilian Internet Steering Committee (Comitê Gestor da Internet no Brasil – CGI.br), Presidential Decree 4,829 of 3 September 2003. Available at http://www.cgi.br/pagina/decretos/108.
3. Since revised to Vision 2050.
4. The Economist, "Estonia takes the plunge: A national identity scheme goes global", 28 June 2014. *Available at* https://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge.
5. Unique Identification Authority of India, Government of India. See www.uidai.gov.in.
6. Government of India, Ministry of Electronics & IT, Press Information Bureau, "UIDAI Achieves 111 Crore Mark on Aadhaar Generation Unique Identity Covers to Over 99 Percent Adult Residents of India", 27 January 2017. Available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=157709.
7. The Economic Times, "Aadhaar authentications hit record high of 94 crore in July", 1 August *2017. Available at* http://economictimes.indiatimes.com/news/economy/indicators/aadhaar-authentications-hit-record-high-of-94-crore-in-july/articleshow/59853131.cms.
8. Government of India, Direct Benefit Transfer. See www.dbtbharat.gov.in.
9. A statement by Sheikh Maktoum on launching the 10X initiative under the Dubai Future umbrella. See http://www.dubaifuture.gov.ae/our-initiatives/dubai-10x/.
10. Ibid.
11. Mariana Mazzucato, The Entrepreneurial State. See https://marianamazzucato.com/entrepreneurial-state/.
12. "Why Software Is Eating the World" by Marc Andreessen, article originally published in The Wall Street Journal on 20 August 2011. Available at https://a16z.com/2016/08/20/why-software-is-eating-the-world/
13. Tech Nation 2017, "At the forefront of global digital innovation". See http://technation.techcityuk.com/.
14. UK Government, House of Commons, Business, Innovation and Skills Committee, The Digital Economy, Second Report of Session 2016-17, HC 87, 18 July *2016. Available at* https://publications.parliament.uk/pa/cm201617/cmselect/cmbis/87/87.pdf.
15. UK Government, Department for Digital, Culture, Media & Sport. See www.gov.uk/government/organisations/department-for-culture-media-sport.
16. UK Tech City. See www.techcityuk.com.
17. Wired, "London's Silicon Roundabout", 29 January 2010. Available *at* http://www.wired.co.uk/article/silicon-roundabout.
18. Search Office Space, "Tech-City, London's Silicon Valley", 17 March 2011. Available at http://www.searchofficespace.com/news/tech-city-londons-silicon-valley.
19. Tech Nation 2017. op. cit.
20. UK Government, Innovate UK. See www.gov.uk/government/organisations/innovate-uk.
21. Catapult, The Catapult Programme. See www.catapult.org.uk.
22. Open Data Institute (ODI). See www.theodi.org.
23. UK Government, Find data published by government departments and agencies, public bodies and local authorities. See www.data.gov.uk.
24. International Telecommunication Union (ITU), Statistics, ICT Facts and Figures 2017. See www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
25. World Economic Forum, The Global Comp*etitiveness Report 2015-2016. Available at* http://reports.weforum.org/global-competitiveness-report-2015-2016/.
26. UK Government, "UK Digital Strategy", Policy Paper, 1 March 2017. Available at www.gov.uk/government/publications/uk-digital-strategy.
27. Atomico, "Supercharging our commitment to Sweden", 26 March 2015. Available at http://news.atomico.com/supercharging-our-commitment-to-sweden/.

28. Safaricom. See https://www.safaricom.co.ke/.

29. Miniwatts Marketing Group, Internet World Stats, Usage and Population Statistics, “Internet Penetration in Africa”, 31 March 2017. See http://www.internetworldstats.com/stats1.htm.

30. Safaricom, M-PESA. See https://www.safaricom.co.ke/personal/m-pesa.

31. Ushahidi. See https://www.ushahidi.com/.

32. Republic of Kenya, Ministry of Information & Communications, National Information & Communi*cations Technology (ICT) Policy, January 2006. Available at* https://www.researchictafrica.net/countries/kenya/National_ICT_Policy_2006.pdf.

33. Kenya Vision2030. See http://www.vision2030.go.ke/.

34. Kenya Vision2030, “About Kenya Vision 2030”. See http://www.vision2030.go.ke/about-vision-2030/.

35. iHub Nairobi, “Hello, We are iHub”. See https://ihub.co.ke/.

36. Forbes, “Kenya’s iHub Enters a New Chapter”, 11 March 2016. Availab*le at* https://www.forbes.com/sites/tobyshapshak/2016/03/11/kenyas-ihub-enters-a-new-chapter/#1d9247ee4f6a.

37. IBM, IBM Research – Africa, “Developing solutions in Africa, for Africa and the world”. See http://www.research.ibm.com/articles/africa.shtml.

38. Philips, “Philips to establish Research & Innovation Hub in Africa”, 20 March 2014. Available at http://www.philips.com/a-w/about/news/archive/standard/news/press/2014/20140321-Philips-to-establish-Research-and-Innovation-Hub-in-Africa.html.

39. Konza Technopolis. See http://www.konzacity.go.ke/.

40. Republic of Kenya, Ministry of Information, Communications and Technology, Ministerial Str*ategic Plan 2013-2017. Available at* http://www.ict.go.ke/wp-content/uploads/2016/04/MinistryStrategic.pdf.

41. Sidian Bank, Uber and Sidian Bank announce a partnership to launch the Uber Vehicle Solutions Programme, 25 May 2016. See https://www.sidianbank.co.ke/products/loans/uber-and-sidian-partnership.

42. Standard Digital, “How ready food goes to waste in Kenyan towns”, 29 March 201*7. Available at* https://www.standardmedia.co.ke/article/2001234463/how-ready-food-goes-to-waste-in-kenyan-towns.

43. World Food Preservation Center, “First Ever Africa-wide Post-Harvest Congress Ends in Nairobi with a Call for Increased Investment in the Sector”, 29 March 2017. Available at http://www.worldfoodpreservationcenter.com/1st-all-africa-postharvest-congress-and-exhibition.html.

44. Twiga Foods. See http://www.twigafoods.com.

45. TechWeez, “How Grant Brooke’s Startup Twiga Foods Is Using Tech to Transform Food Retail, 20 September 2016. Available at http://www.techweez.com/2016/09/20/twiga-foods-grant-brooke-interview/.

46. Working Group on Development and Environment in the Americas, “Foreign Investment and Economic Development in Costa Rica: The Unrealized Potential”, Discussion Paper No. 13, April 2008. Available at https://ase.tufts.edu/gdae/Pubs/rp/DP13Paus_CorderoApr08.pdf.

47. PROCOMER, Costa Rica exporta. See http://www.procomer.com/.

48. Costa Rican Investment Promotion Agency (CINDE). See http://www.cinde.org/.

49. Site Selection Magazine, “Costa Rica: A spot where productivity & sustainability meet to reach true ROI”, *May 2017. Available at* https://siteselection.com/issues/2017/may/costa-rica-a-spot-where-productivity-and-sustainability-meet-to-reach-true-roi.cfm.

50. International Trade Centre, “Costa Rica’s TPO, PROCOMER, is model of good practice”, 28 October 2014. Available at http://www.intracen.org/article/Costa-Ricas-TPO-PROCOMER-is-model-of-good-practice/.

51. World Bank Group, Costa Rica Data. See http://data.worldbank.org/country/costa-rica.

52. World Bank Group, The Impact of Intel i*n Costa Rica: Nine Years After the Decision to Invest, 2006. Available at* http://siteresources.worldbank.org/EXTEXPCOMNET/Resources/2463593-1213887855468/44_The_impact_of_Intel_in_Costa_Rica.pdf.

53. elEconomista.es, “Intel supone el 4,9 por ciento del PIB de Costa Rica”, 6 October 2006. Available at http://www.eleconomista.es/empresas-finanzas/noticias/81837/10/06/Intel-supone-el-49-por-ciento-del-PIB-de-Costa-Rica.html.

54. Intel Corporation, “Intel in Costa Rica”. Available at https://www.intel.com/content/www/us/en/corporate-responsibility/intel-in-costa-rica.html.

55. Costa Rican Investment Promotion Agency (CINDE), Services Sector, Success Stories. See http://www.cinde.org/en/sectors/services/success-stories.

56. PROCOMER, Why Costa Rica?, Free Trade Zones Regime. See http://www.procomer.com/en/freetradezone-investor#1.

57. Office of the United States Trade Representative (USTR), "CAFTA-DR (Dominican Republic-Central America FTA)". See https://ustr.gov/trade-agreements/free-trade-agreements/cafta-dr-dominican-republic-central-america-fta.

58. World Economic Forum, Global Competitiveness Index, "Regional highlights: Latin America and the Caribbean", 2016. Available at http://reports.weforum.org/global-competitiveness-index/regional-highlights-latin-america-and-the-caribbean/.

59. Omar Dengo Foundation. See http://www.fod.ac.cr/index.php.

60. Omar Dengo Foundation, "The Program of Educational Informatics MEP-FOD: A Contribution to the Development of Costa Rica". Available at http://www.oas.org/udse/caribworkshop/Omar%20Dengo%20Foundation.pdf.

61. PulsoSocial, "Startup Ecosystem Canvas presenta los recursos para emprendedores en Costa Rica", 30 July 2015. Available at http://pulsosocial.com/2015/07/30/startup-ecosystem-canvas-presenta-los-recursos-para-emprendedores-en-costa-rica/.

62. MenTe en Accion. See http://www.menteenaccion.org/.

63. CAMTIC, "Mapeo Sectorial de Tecnologias Digitales 2014". Available at http://www.camtic.org/wp-content/uploads/2017/06/CAMTIC-Mapeo-Sectorial.pdf.

64. The Australian, "Malcolm Turnbull primed for technology disruption", 15 September 2015. *Available at* http://www.theaustralian.com.au/business/technology/turnbull-primed-for-disruption/news-story/b4eaa98813ab8b4f7c9252fc59dd7cc8.

65. The Sydney Morning Herald, "Technology start-ups thrilled for Malcolm Turnbull as Prime Minister", 15 Septe*mber 2015. Available at* http://www.smh.com.au/it-pro/government-it/technology-startups-thrilled-for-malcolm-turnbull-as-prime-minister-20150915-gjn6y7.html.

66. Australian Government, Department of the Prime Minister and Cabinet, "The Hon Dan Tehan MP, Minister Assisting the Prime Minister for Cyber Security", 20 July 2016. Available at https://www.pmc.gov.au/news-centre/cyber-security/hon-dan-tehan-mp-minister-assisting-prime-minister-cyber-security.

67. Australian Government, Department of the Prime Minister and Cabinet, "Alastair MacGibbon in new role of Cyber Security Special Adviser", 30 May 2016. Available at https://www.pmc.gov.au/news-centre/cyber-security/alastair-macgibbon-assumes-new-role-cyber-security-special-adviser.

68. Australian Government, Ministers for the Department of Communications and the Arts, "Leading online safety expert Alastair MacGibbon appointed Children's e-Safety Commissioner", 19 March 2015. Available at http://www.minister.communications.gov.au/paul_fletcher/news/leading_online_safety_expert_alastair_macgibbon_appointed_childrens_e-safety_commissioner#.WXZVzumQw-U.

69. Australian Government, Department of Foreign Affairs and Trade, Australian Ambassadors and other representatives, "Australian Ambassador for Cyber Affairs: Dr Tobias Feakin". Available at http://dfat.gov.au/about-us/our-people/homs/Pages/ambassador-for-cyber-affairs.aspx.

70. Australian Government, Australia's Cyb*er Security Strategy: Enabling innovation, growth & prosperity, First Annual Update 2017. Available at* https://cybersecuritystrategy.pmc.gov.au/cyber-security-strategy-first-annual-update-2017.pdf.

71. Parliament of Australia, 2016 Census. See http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/2016Census.

72. Parliament of Australia, Department of the Prime Minister and Cabinet, Review of the events surroundi*ng the 2016 eCensus: Improving institutional cyber security culture and practices across the Australian government—Alastair MacGibbon, Special Adviser to the Prime Minister on Cyber Security, 13 October 2016. Available at* http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A"publications%2Ftabledpapers%2Fa41f4f25-a08e-49a7-9b5f-d2c8af94f5c5%22.

WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org