Short term high quality studies to support activities under the Eastern Partnership
HiQSTEP PROJECT

Harmonisation of the Digital Markets in the Eastern Partnership

SUMMARY OF KEY FINDINGS

Kantor Management Consultants

ibf INTERNATIONAL CONSULTING

ICMPD 20 YEARS

eptisa

This Project is funded by the European Union

The Eastern Partnership (EaP) is a joint initiative of the EU and its Eastern European partners: Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova and Ukraine. Eastern Partnership promotes smart, sustainable and inclusive development of a free market economy in the Partner Countries.

Multilateral cooperation in the Eastern Partnership takes place across a wide array of issues. This work is guided by four thematic platforms, supported by various expert panels, several flagship initiatives and projects. Among the areas of information society, media and the Network of Electronic Communication Regulators, Platform 2 – «Economic Integration and Convergence with EU Policies» includes important aspects of the Harmonisation of the Digital Markets (HDM) between the EU and the Eastern Partnership Countries.

The presented HDM study examines the state of play of digital markets in the six Partner Countries, comparing it with the best practices in EU countries. The study focuses on six priority areas, namely: Network and Information Security and Cyber–security, Electronic Identification and Trust Services, Electronic Customs, Electronic Commerce for SMEs, Digital Skills and Telecom Rules. The study is co–chaired by the European Commission Directorate General for Neighbourhood and Enlargement Negotiations (DG NEAR) and Directorate General for Communications Networks, Content & Technology (DG CONNECT).

The specific objectives of the study were the following: a) to lay the foundation for the development of Digital Market Agendas for the Eastern Partnership countries; b) to analyse the benefits that would result from harmonisation between the Partner Countries and the EU, and; c) to identify follow–up actions in the form of a roadmap for the priority areas under the HDM and for each Partner Country.

This cross–country report on the HDM in the Eastern Partnership is part of the project 'Short term high quality studies to support activities under the Eastern Partnership – HiQSTEP, EuropeAid/132574/C/SER/Multi', carried out by an international consortium under the leadership of Kantor Management Consultants.

The HDM study was implemented by a team under the leadership of Vladimir Abramytchev (Study Team Leader, eCustoms, eCommerce), and composed of senior international experts Yuri Misnikov (Network and Information Security and Cyber–security, Electronic Identification and Trust services) and Peter Lundy (Digital skills, Telecom Rules) together with national experts: Gohar Malumyan (Armenia), Vusal Abbasov (Azerbaijan), Anna Pobol (Belarus), Ana Nakashidze (Georgia), Olga Demian (Moldova) and Sofia Belenkova (Ukraine).

The overall supervision was carried out by Przemyslaw Musialkowski, Team Leader of the HiQSTEP Project. Vassilis Kopanas (DG CONNECT), Simone Rave (DG NEAR), Isabelle Pellier (DG NEAR), and Valery Virkovski (HDM Working Group) assured the methodological direction of the study. Alessandra Falcinelli (DG CONNECT), Alessandra Sbordoni (DG CONNECT), Zahouani Saadaoui (DG TAXUD), Tamas Kenessey (DG CONNECT), Marietta Grammenou (DG CONNECT) and Vassilis Kopanas (DG CONNECT) advised to define the EU baseline[1].

Sincere gratitude is expressed by the entire team to all contacted stakeholders in the six Partner Countries who provided information during interviews and responded to questionnaires. Thanks is given to the participants of HDM Workshop and the members of the HDM Working Group for their highly valuable feedback and information, and to Dimitra Malandraki (Kantor) for efficient administrative and back–up support. Finally, yet importantly, appreciation goes to all staff members of the European Commission and specialists in the Eastern Partnership countries who directly or indirectly helped to complete this study.

November 2015

[1]For any request about the study, please contact Vassilis Kopanas (Vassilis.Kopanas@ec.europa.eu), Isabelle Pellier (Isabelle.PELLIER@ec.europa.eu) and Vladimir Abramytchev (vladimir@archev.net)

TABLE OF CONTENTS

ASSESSMENT METHODOLOGY

The HDM assessment methodology provides a framework to measure the extent of harmonisation in 6 priority areas of the digital markets between the Partner Countries and the EU. The key benefits of the harmonisation are defined from a set of unique assessment benchmarks per priority area. They characterise the most impactful aspects – from economic, technical, legal and regulatory perspectives – required to align the level of development of the digital markets in the Partner Countries with those of the EU. The input benchmarks for each priority area are combined into some key indicators that jointly constitute an overall harmonisation score – the state of play of a country in a priority area.

The baselines for each of the 6 priority areas describe the state of play in the relevant EU legislation, policies, strategies, best practices, standards, ICT platforms and information services. The baselines also links to the key actions and the three pillars of the Digital Single Market Strategy for Europe.

The data for benchmarks is primarily obtained from stock-taking in the Partner Countries using questionnaires for each priority area completed by desk research and interviews. Interviewees choose scores that they consider most appropriate to describe the current state of play in a country. The comparison of obtained scores with the EU baseline reveals gaps between the state of the digital markets in the Partner Countries with the EU digital market in the 6 priority areas.

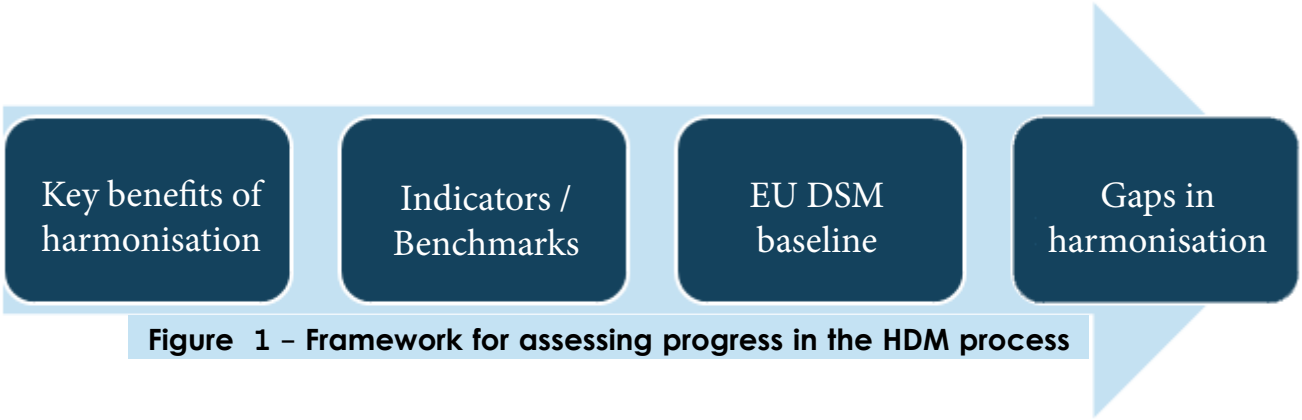


Figure 1 – Framework for assessing progress in the HDM process

The gap analysis results in a road map containing priority areas for the harmonisation and proposals for concrete follow-up actions in each priority area and for each Partner Country. Priority projects are formulated to address the common gaps across all 6 Partner Countries.

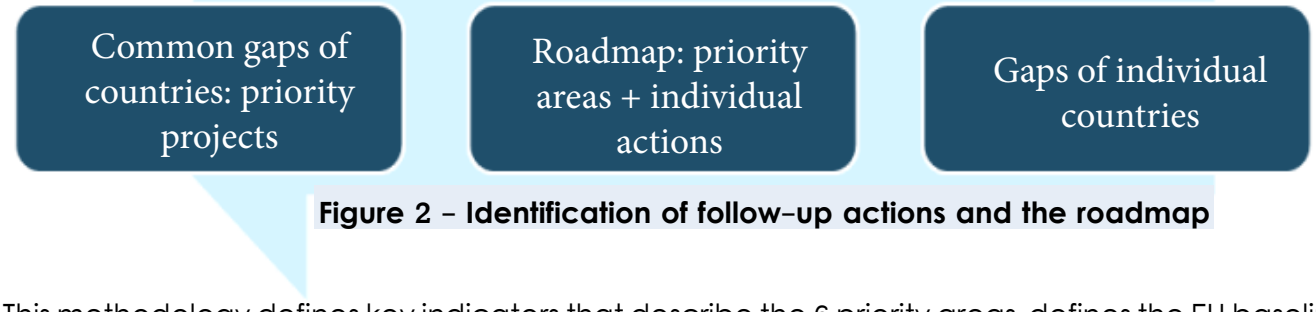


Figure 2 – Identification of follow-up actions and the roadmap

This methodology defines key indicators that describe the 6 priority areas, defines the EU baseline, provides a foundation for the development of digital market agendas for the Partner countries. The study reflects benefits that would result from an HDM between the Partner Countries and the EU, identifies a roadmap of follow-up actions for the priority areas under the HDM for each Partner Country and for the Region.

RESULTS

Network, Information Security and Cyber-security

Network, information and cyber security (NIS) refers to the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies. At the EU level, it is governed by common cybersecurity strategies and regulation (e.g. the Network and Information European Agenda on Security, Security Directive, European Cybersecurity Strategy). The EU baseline also includes personal data and privacy regulation (Articles 7 and 8 of the Charter of Fundamental Rights, the General Data Protection Regulation and the ePrivacy Directive).

All Partner Countries demonstrate strong political will to address the constantly evolving NIS-related challenges, including the willingness to cooperate with the EU and internationally. Whereas there is a minimally sufficient legal certainty on Cyber Security – supported in some cases by the availability of strategic national plans and programmes – the Region substantially lags behind the EU. Only Georgia and Moldova have fully-fledged national Cyber Security strategies, although other EaP countries have plans to develop ones. On the other hand, the Region is technologically well advanced, using the latest software of high international standard.

Overall, the NIS area in the Region is still regulated by fragmented and disparate (and sometimes outdated) frameworks, mainly by secondary legislation rather than consolidated laws. Internet openness, confidentiality of personal data and online privacy are protected by law in all Partner Countries. However, the legal basis of such protection is not sufficiently streamlined and does not adequately address all challenges related to internet safety, while technology is advancing and societies are becoming more concerned about such challenges.

The Partner Countries share a number of common problems that need to be addressed in a coordinated manner in order to harmonise with the EU. The Association Agreement (AA) countries are more advanced in terms of harmonisation. The largest gaps are those caused by the absence of dedicated national cyber-security strategies; lack of services provided to the National Regulatory Authority (NRA); inadequate technical, human and financial resources available for managing security threats; insufficient transparency and openness in reporting on security breaches; and existing vulnerabilities of private sector critical infrastructures. Most countries do not practise cyber-attack simulations on a regular basis. Action is required for ensuring well-functioning alert platforms, hotlines for both experts & the public. The recommended actions below are intended to (a) harmonise the existing legal and regulatory environment in the Partner Countries with relevant EU-level cybersecurity strategies and regulation, and (b) enhance national Computer Emergency Response Teams' (CERTs) capacities to better protect electronic communication networks, digital content and privacy, as well as to respond effectively to cybersecurity threats. The implementation of the recommended actions should take full account of the European Digital Single Market (DSM) Strategy provisions. Better protection of the critical information infrastructure will help reinforce trust and security in digital services and in the handling of personal data, reduce cyber threats across borders to minimise their negative impact on the economy, on citizens' fundamental rights and on society at large as envisaged by the DSM Pillar 2: "Create the right conditions for digital networks and services to flourish in order to have secure and trustworthy infrastructures and electronic public services".

RECOMMENDED ACTIONS :
Network, Information Security and Cyber-Security

1. Identify the legal/regulatory and organisational/institutional barriers in the Partner Countries to closer harmonisation with EU-level cyber security strategies/regulation and the DSM Strategy; prepare common and country-specific recommendations (roadmaps) for improving national legislation to protect digital networks/critical infrastructures and respond effectively to cyber-threats including threats to personal data and privacy.

2. Formulate common principles for developing national Cyber Security policies/strategies; specifying common requirements for establishing minimal security levels in the field of critical information infrastructure, including in the private sector, and guaranteeing internet safety while maintaining its openness.

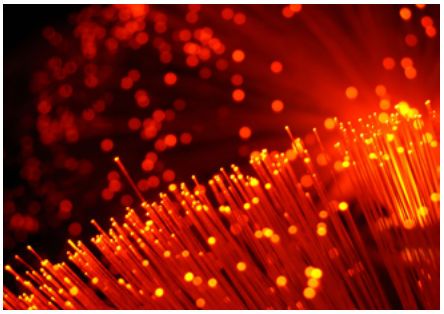
3. Develop a common capacity-building plan to empower national Computer Emergency Response Teams (CERTs) to enhance their competencies through cooperation with CERT-EU and the European Network and Information Security Agency (ENISA).

Electronic Identification and Trust Services

Electronic identification (eID) and electronic trust services (eTS) encompass electronic signatures, seals, time stamps, electronic delivery services and website authentication. These are key enablers for secure cross-border electronic transactions and are central building blocks of the Digital Single Market.

Cross-border interaction demands better understanding of the conditions to be met by public service and trust service providers to guarantee the required security levels for accessing services of other countries and granting access to local services. The HDM cooperation framework seeks to harmonise the rules for electronic trust services with the relevant provisions of the eIDAS regulation in order to enable the mutual acceptance of electronic signatures across borders (which is not possible at present for the Partner Countries), and thus facilitate the free movement of goods and services between the Partner Countries and the EU Member States.

Partner Countries demonstrate rather similar results in the field of eID/eTS. In general, e-Government development (including eProcurement as well as eCommerce) has been the main driving force in building national certification infrastructure and related services.



The best progress has been achieved in the creation of the eID/eTS infrastructure and in the implementation of eSignatures. Legal certainty about eID is largely sufficient and leadership is fairly strong. Achieving the EU baseline is in the national interest of each country of the Region, given the new commercial opportunities that may emerge as a result of making digital signature operational across borders. Some Partner Countries have already significantly aligned their national legislation and real-life practices with those of the EU (Georgia and Moldova). Moreover, Moldova and Azerbaijan have created mobile identification infrastructure and services. However, the European experience and best practices are not sufficiently known in the Region, except for the Estonian x-Road secure interoperability solution that is currently tested and applied in Georgia, Moldova, Azerbaijan and Ukraine.

The access to European knowledge in eID/eTS is still rather restricted. At the moment, the Region's digital markets are still closed. Yet, all Partner Countries express readiness to change their legislations in order to enable cross-border electronic signatures and related certification services. All Partner Countries are advised to align with the provisions on electronic identification and trust services for electronic transactions in the EU internal market (eIDAS regulation). In addition, an opportunity of joining the large-scale project STORK on a pilot basis should also be considered.

Legally and technically, each Partner Country has a sufficiently developed eID/eTS infrastructure. However, its actual usage remains inadequate. Digital signatures are not used widely as the main tool of electronic identification and are not interoperable across borders. Interoperability of state and private sector information systems (technical, organisational and legal) and inter-agency coordination are still weak, which is manifested by the overall lack of well-integrated and secure e-Government architectures based on the whole-of-government principle. There is a clear lack of e-services requiring secure electronic identification.

Until now, electronic signatures have served the business community better than citizens. Public procurement is steadily moving online (this has already been done in Armenia), but digital signatures are not fully integrated into eProcurement processes and platforms. This undermines security and also puts limits on the full automation of the award and post-award stages where strong identification is needed.

The recommended actions below are intended to (a) harmonise the existing legal and regulatory environment in the Partner Countries with relevant European eIDAS principles and provisions, and (b) enable secure cross-border interoperability of electronic transactions, content and services. The implementation of the recommended actions – aimed at making national Public Key Infrastructures more reliable and secure – will take full account of the European Digital Single Market (DSM) Strategy provisions. The harmonisation of rules for trust services will facilitate lowering and removing barriers that hamper the exchange of cross-border online activities and create better eCommerce rules of cross-border online access that consumers and business can trust, as envisaged by the DSM Pillar 1: "Better access for consumers and businesses to online goods and services across Europe". The development of eGovernment services and other digital content accessible across borders, especially aimed at SMEs, will be aligned with the DSM Pillar 2: "Create the right conditions for digital networks and services to flourish" and Pillar 3: "Maximising the growth potential of our European Digital Economy to have secure and trustworthy infrastructures & electronic public services."

RECOMMENDED ACTIONS: Electronic Identification and Trust Services

4 Identify the legal/regulatory and organisational/institutional barriers existing in the Partner Countries for closer harmonisation of rules for electronic trust services with eIDAS Regulation and the DSM Strategy; prepare common and country-specific recommendations (roadmaps) for improving national legislation to make digital signature interoperable across borders.

5 Identify a list of digital services in each Partner Country as candidates for cross-border interoperability aligned with the DSM priority pillars, areas and actions; develop a regional roadmap for further implementation.

6 Identify the range and scope of priority issues that require express sharing of European knowledge and good practices in eGovernment services to citizens and businesses to raise their reliability, utility and security; align such services with the DSM Strategy and propose instruments/mechanisms of access to relevant knowledge accumulated in the EU and individual Member States to replicate good practices.

7 Establish a fast-track initiative to enable Partner Countries to benefit quickly from EU approaches and experiences in cross-border interoperability of digital services; undertake feasibility studies to explore joining successful EU large-scale pilots, such as STORK 2.0 and e-SENS.

Electronic Customs

Electronic Customs (eCustoms) initiatives aim to replace paper format customs and trade procedures with electronic ones, thus creating a more efficient customs environment.

Implementation of the legal framework related to eCustoms in the Partner Countries is the most advanced aspect towards harmonisation with the EU in this area. The overall legal framework and several major regulatory provisions related to eCustoms, such as paperless environment for customs and trade, risk management framework, status of authorised economic operator are already in line with the EU baseline. Main customs procedures have been automated. In contrast, only three Partner Countries have extended them into national single window systems (Armenia, Azerbaijan and Georgia) and the overall automation of trade procedures is low.

The main challenge for the HDM in eCustoms is to ensure interoperability of electronic customs and single window systems (at legal, infrastructure and information services levels) between the Partner Countries, and with relevant systems of the EU member states and those of the European Commission. The lack of interoperability significantly obstructs the creation of a paperless trade environment.

The most significant gaps in eCustoms harmonisation for the Region relate to the implementation of information services. While the electronic submission of summary electronic declarations is widely implemented, some key information services have not yet been realised in most of the Partner Countries. These are systems for the registration and exchange of data about authorised economic operators, anti-counterfeiting and anti-piracy systems, and management of registered exporters. Automated data exchange with the EU or even with other neighbouring countries remains very limited.

With regard to infrastructures, little has yet been done to implement electronic interfaces for enabling economic operators to handle all customs-related issues and formalities in international business transaction with the customs authorities of the country where they are established. With the exception of Azerbaijan and Ukraine, there is no infrastructure in place allowing traders from the Partner Countries to transmit electronic documents to the customs authorities of other countries.

RECOMMENDED ACTIONS: Electronic Customs

8 Implement the key infrastructure and information services at the level of individual Partner Countries: economic operators' registration and identification system; national anti-counterfeiting and anti-piracy system; and creation of national segments of Registered Exporters System.

9 Harmonise the legal frameworks with the EU in the following aspects: Authorised Economic Operator (AEO) status; regulatory basis for lodging summary customs declarations for pre-arrival and pre-departure information.

10 Implement infrastructure and develop information services for cross-border eCustoms with the EU: exchange of national data on Authorised Economic Operators; exchange of summary electronic declarations; automated exchange of export/import/transit data (through the EU SPEED portal); submission of national data to the EU Registered Exporters system (REX); exchange of electronic trade certificates.

11 Set up a common anti-counterfeiting and anti-fraud information system for the Partner Countries and connecting it with the EU Central Anti-Counterfeiting and Anti-Piracy System (COPIS).

eCommerce for Small and Medium Enterprises

Electronic Commerce for Small and Medium Enterprises (eCommerce for SMEs) is trading in products or services using computer networks, such as the Internet.

The Region has achieved on average around half the compliance with the EU baseline for eCommerce for SMEs. The Partner Countries have defined their legal frameworks and facilitated the deployment of basic infrastructures and services for eCommerce.

A good degree of harmonisation with EU best practices has been achieved in openness of the Partner Countries to competition. In Internet security and privacy, Belarus, Moldova and Ukraine put no obligation for service providers to monitor transmitted or stored information. In measures for consumer rights protection, the legislation of Azerbaijan and Belarus explicitly defines transparency requirements of commercial communications information to be lawfully provided by eCommerce traders. Establishment of equal validity between electronic and paper contracts facilitates eLogistics.

The aspect of competition in eCommerce for SMEs in the Partner Countries is the most advanced from the point of view of harmonisation with the EU. Partner Countries are open for competition in the eCommerce market and have little or no obstacles for market access by SMEs from other countries. The regulatory framework in eCommerce is business friendly and open to the free movement of information society services. None of the Partner Countries requires explicit authorisation to pursue the activity of an eCommerce service provider.

Most of the countries have introduced only some basic aspects of national legal frameworks specifically related to eCommerce. Electronic payment for eCommerce transactions is the biggest gap with EU practices. In most of the Partner countries there are no regulations that limit service fees for the use of means of eCommerce payment (credit card, electronic valets, banking transfer etc.). This obstructs the implementation of a seamless approach to cross–border payments. Even if most of countries explicitly legalise equal treatment between paper and electronic invoices, none of the countries have implemented national semantic data models and standardised formats of electronic invoice.

Some common gaps in the Partner Countries are related to legal provisions securing the protection of consumer rights within eCommerce transactions. This notably includes almost absent international cooperation mechanisms for consumer protection (with exception of Belarus and Armenia), missing out–of–court dispute settlement mechanisms for eCommerce transactions. None of the Partner Countries has established an on–line dispute resolution system for participants of eCommerce transactions. There are no national schemes of online trustmarks for eCommerce retail websites in the Region. In most of the Partner Countries, there are no legislative provisions that would define specific liability regimes for providers of three categories of essential services assuring the functioning of eCommerce: transmission temporal storing of data and hosting services.

Only Armenia and Belarus have introduced in their national legislations the provisions specifying terms and conditions related to the risk of loss of or damage to the goods purchased through eCommerce and to the responsibilities of the parties involved in case of loss or damage of goods. The same applies to the definition of the rights on delivery of goods.

RECOMMENDED ACTIONS: eCommerce for Small and Medium Enterprises

12 Create a common eCommerce trustmark scheme for retail websites in the Region by joining the work in progress on EU–wide trustmark schemes. These aim to reassure consumers on the reliability of accredited eCommerce traders from the Partner Countries.

13 Set up national online dispute resolution systems for parties involved in eCommerce, enhance international cooperation mechanisms on consumer protection within the Region and with the EU.

14 In ePayment, harmonise the rules on fees for the use of means of eCommerce payment between the EaP countries and the EU. Based on the EU best practices, develop a unified approach for national semantic data models and standardised formats of electronic invoice and contract.

15 Harmonise national legal frameworks with the EU best practices in the following aspects: requirements of minimum general information presented by eCommerce providers; transparency requirements for on-line commercial communications; rights on delivery of goods purchased on-line; rules on the conditions for risk of loss or damage to goods shipped within eCommerce.

16 Develop eCommerce platforms that assist SMEs in their digital activities of on-line trade of products and services, electronic contracting and invoicing, fulfilment of customs and trade procedures in electronic form. The design of such platforms would need application of most of the EU eCommerce baseline requirements such as consumer rights protection measures, ePayment, and eLogistics.

Digital Skills

Digital Skills are broadly defined as ICT-related skills for the labour force, including ICT professionals, digital learners and citizens). The role of ICT in raising productivity and living standards is critical. The largest obstacle to harnessing the power of ICT is the shortage of digital skills. By 2020, Europe might face a shortage of almost 825,000 ICT professionals. This is what is termed the "digital skills gap".

The Region faces shortages of the same critical skills, but unlike in the EU, the digital skills gap has not yet been systematically measured and monitored. Although some good progress has been made across the Region in bringing better ICT into education, there is still a lack of awareness at policy level and a lack of coordination of initiatives at regional, national and local levels.

The development of Digital Skills requires a co-ordinated policy approach, within the context of national policies for uptake of ICT for competitiveness, growth, employment, education, lifelong training and social inclusion. Digital Skills must be elevated to have an important place in long-term national policy. Harmonisation efforts should play a central role in developing these national policies and actions, within which a long-term Regional Digital Skills agenda is launched, to improve cooperation and mobilisation of all stakeholders and to adopt best strategies and practices in order to better face global competitive challenges.

Policy makers across the Region generally recognise the importance of ICT in economic and social development, but the focus on Digital Skills is insufficient, especially in the context of creating growth and jobs. Moldova has already made good progress in creating a policy context for Digital Skills under its "Digital Moldova 2020" initiative. All countries of the Region are already implementing projects to bring ICT learning into schools and universities.

Working with companies in national and local coalitions, using the same model as the Europe's Grand Coalition for Digital Jobs, should focus particulary on the young workforce. This can be done by training individuals and seeking to reduce youth unemployment, helping business "start-ups" grow by giving them bigger markets to sell to from Day 1, and supporting labour force changes in companies which have not adapted to new digital, data-driven business models.

RECOMMENDED ACTIONS: Digital Skills

17 Measuring the skills gap. The earliest need is the systematic measurement and monitoring of the digital skills gap. Without this measurement, awareness of the need to match demand and supply is missing.

18 Co-ordination of Digital Skills initiatives. Policy development and implementation of initiatives would be greatly leveraged by welcoming the Partner Countries into Europe's Grand Coalition for Digital Jobs. Initiatives could follow to form national & local coalitions that would coordinate participation, awareness raising and resources facilitation.

Telecom Rules

Telecom Rules consist of the policy, legal, regulatory and implementation frameworks, which are necessary for effective electronic communications' markets to operate. Harmonisation of Telecom Rules would bring about benefits for all market participants. There can be positive impacts across digital markets by improving broadband investment and access for market participants, particularly through greater connectivity. Benefits from increased broadband penetration occur at the macro–economic level, as well as via providing the access platform for digital single market growth, for example through cloud computing, enhanced cross–border payments and increased physical delivery services. Harmonisation of Telecom Rules has already progressed within the EU and will continue to be developed in 2016, through the Digital Single Market strategy.

There are significant gaps in Telecom Rules both within the Region and between the six Partner Countries and the EU. There is no unified policy in the Region that encapsulates the EU's "Digital Agenda" target for universal access to high speed (>30Mbps) broadband by 2020. The average broadband penetration in the Region currently lags well behind the EU for both fixed and mobile broadband services. Fixed broadband penetration per capita in the Region stands at 13% compared with 30% in the EU. For mobile broadband, the gap is even wider – at 21% for the Region compared with 61% for the EU. The gap is still wider outside urban areas, with rural broadband penetration typically being only one tenth of urban penetration across the Region. The closing of this "broadband connectivity gap" is of vital importance, not just in terms of the potential to boost GDP growth (estimated in the report at between 2.9Bn and 4.3Bn in the Region for fixed broadband alone), but also in terms of providing the essential connectivity platform for other areas of digital market progress including the priority topics studied in this report.

Azerbaijan and Belarus have already committed significant state funding to broadband infrastructure. In harmonising policy with the EU, better competitive conditions in both these countries will lead to more efficient markets with greater consumer choice and improved private sector confidence. In the other four countries, existing broadband service provision has been left almost entirely to the private sector. Although this has already given good broadband coverage in urban areas, rural areas are left relatively unserved due to less attractive investment returns.

The legal and regulatory frameworks in the six Partner Countries are all different. Gaps are particularly evident in the Region's Telecom Rules that impact broadband connectivity, including the regulatory enablers to market entry, the necessary competitive market safeguards for private investors and in the state–aid rules applied to public investments. The alignment process has already begun in Georgia, Moldova and Ukraine. Full alignment embraces not only the key enablers to fixed infrastructure investment, but also requires the harmonisation of spectrum management procedures, particularly with respect to the "digital dividend" spectrum which is especially useful for deployment in rural areas.

RECOMMENDED ACTIONS: Telecom Rules

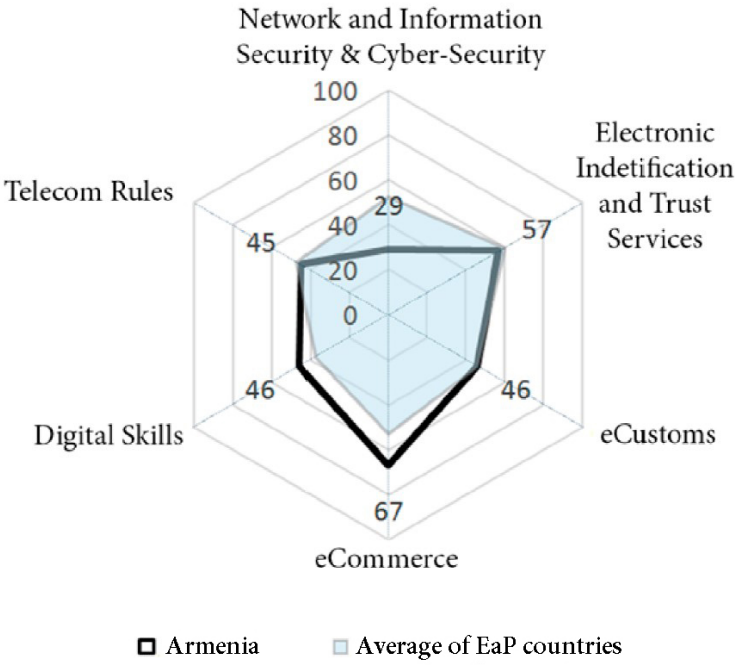
19 Harmonisation of policy for broadband access. There is a pressing need for the creation of a common policy across the Region to close the "broadband connectivity gap". Policy in the Partner Countries should mirror the ambitious targets for universal high–speed broadband access across the EU. This will give a significant boost to investors' confidence in the Region, because investors could expect the same enabling conditions that are already in place in the EU.

20 Closing the broadband connectivity gap will require further significant investments, particularly in the outreach of infrastructure to rural areas. The legal and regulatory frameworks across the Region need to be adjusted to ensure that the investment–enabling provisions for high–speed broadband infrastructure already contained in the EU are adopted by the six Partner Countries.

OVERVIEW OF THE INDIVIDUAL PARTNER COUNTRIES

The graphs represent the state of play of the respective EaP countries' digital markets in the six priority areas. 100% represents the EU baseline, the shaded area represents the EaP regional average.

Armenia



In the field of **network, information and cyber security**, Armenia displays the largest gap in relation to the EU baseline, therefore its score is significantly below the average for the Region. Armenia is the only Partner Country that has not established a Computer Emergency Response Team although it joined the Cyber Crime Convention in 2001 and ratified it in 2006. Narrowing the gap requires preparing a national cyber-security strategy, developing procedures for reporting on security incidents in an open and transparent manner, defining minimal security levels and regularly practising cyber-attack simulations.

For **electronic identification and trust services**, Armenia has reached average for the Region. The biggest gaps with the EU baseline are found in the area of e-services for businesses and citizens (provided at lower maturity levels) and in the insufficient legal certainty about licensing in the area of Public Key Infrastructure (PKI). It is important that electronic identification and trust services become interoperable across borders and are recognised in other countries. While Armenia's eProcurement system is almost on a par with the EU baseline, digital signatures should be integrated into the entire tender process.

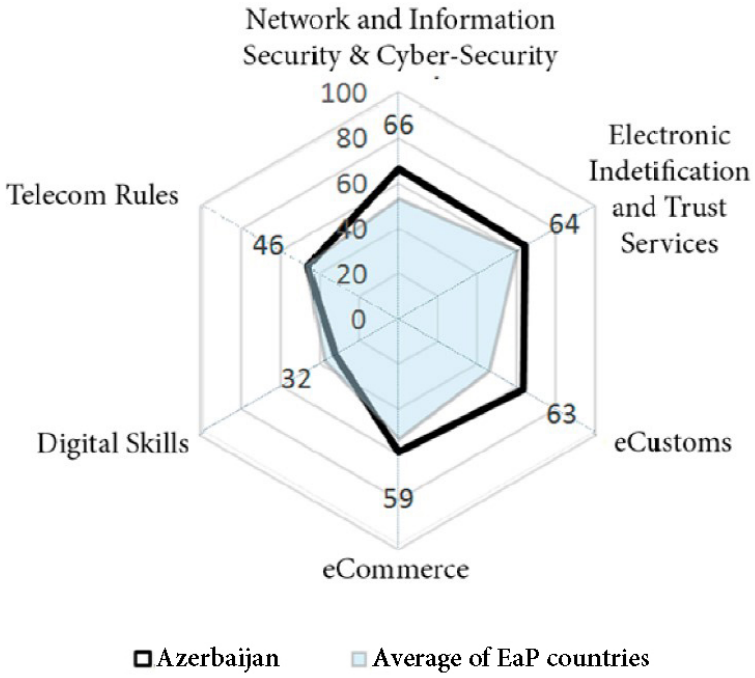
For **eCustoms**, Armenia's score is at the average of the Region. A good level has been achieved in the aspects of eCustoms legal framework and infrastructure. Further harmonisation with the EU requires implementation of advanced information services. Specifically, priority aspects include management the status of Authorised Economic Operator (AEO), setting-up registration systems and organising exchange of AEO data within the EU, creating an anti-counterfeiting & anti-piracy system, administration of registered exporters status, and data submission to the Single Point for Entry or Exit of Data portal (SPEED) of the EU.

Armenia's score in **eCommerce for SMEs** is above the average for the Region. The country has achieved significant progress in the aspects of openness to competition in eCommerce and electronic payments, but more needs to be done in the areas of internet security and privacy, as well as in consumer rights protection. Specific follow-up activities are needed for setting-up a national trustmark scheme for eCommerce websites, defining out-of-court dispute settlement mechanisms, online dispute resolution system for consumers for eCommerce transactions and anti-spam legal regulation.

For **Digital Skills**, Armenia's score is above the average for the Region. Progress has been made especially in introducing ICT for better education and there have been some independent initiatives for the development of ICT user skills for targeted groups. The Enterprises Incubator Foundation of Armenia published a report on the Digital Skills Gap in 2014 which should lead to increased awareness. Though the Government has announced that ICT is a priority sector for the country's economic development and for the creation of a knowledge-based economy, the strategies for the development of digital skills are not yet coordinated. Responsibilities are distributed among a number of institutions – notably the National Centre of Educational Technologies (NCED) (in education), the National Quality Assurance Organisation and the Ministry of Economy. Action has been led mainly by initiatives in the private sector, using professional organisations and NGOs. These are not part of any special national agenda. Clear and coordinated policy is required and key components of action should be defined – awareness raising, long term co-operation, human resources investment, making ICT attractive, developing digital literacy for employability and e-inclusion and lifelong acquisition of digital skills. Progress can be made by forming a national coalition for digital jobs, as well as local coalitions to share best practices and link with Regional and EU initiatives under the "Grand Coalition for Digital Jobs".

For **Telecom Rules**, Armenia's score is slightly lower than the average for the Region. Good progress has been made in exploiting the spectrum to achieve universal mobile coverage. Even so, overall penetration for broadband services remains significantly below the EU average. The policy, legal and regulatory framework for the electronic communications sector is not well aligned with the EU Telecoms Rules. The lowest score are in the elements that ensure competitive broadband markets, give better information to consumers and increase attractiveness for infrastructure investors. There is no clear policy for universal access to high speed (>30Mbps) broadband within an achievable deadline. The EU baseline contains this "Digital Agenda" target for 2020. Furthermore, the regulatory capacity in the sector is very limited and remains part of the Public Utilities Regulatory Commission which is dependent on state funding. The EU baseline requires far greater independent focus on this market sector. More resources are required to regulate this fast changing and dynamic market which is vital to the economy. Legal and regulatory change is required to improve competition in the market and to provide more favourable conditions for infrastructure investors leading to better broadband choices for consumers.

Azerbaijan



For **network, information and cyber security** Azerbaijan's score is higher than the average for the Region. The largest remaining gap with the EU baseline is the availability of strategic documents that spell out priorities and actions, especially regarding minimum security levels. There are also gaps in human resources capacity, lack of regular training and the persistent challenge of ensuring transparency in security issues. The country needs a comprehensive national cyber-security strategy to specify minimal security levels, define rules for reporting and disclosure in security breaches and risks, enhanced capacities.

Azerbaijan has made good progress in building infrastructure for **electronic identification and trust services**. Its state of play is higher than the average for the Region. The largest gaps are observed in the areas of eProcurement, public confidence in eID, eGovernment interoperability and standards. The most important priority is to improve legal certainty (possibly with a new law) to make electronic identification services interoperable across borders and digitise public procurement at all stages of the tender process.

For **eCustoms**, the achievement is significantly above the average for the Region. While Azerbaijan has implemented a relevant eCustoms legal framework and technical infrastructure, further harmonisation is particularly required in deployment of information services. Specifically, the priority aspects are setting-up a registration system of Authorised Economic Operators and organising exchange of AEO data with the EU and within the Region, creating anti-counterfeiting and anti-piracy system and creating interfaces to conduct all customs-related procedures in electronic format.

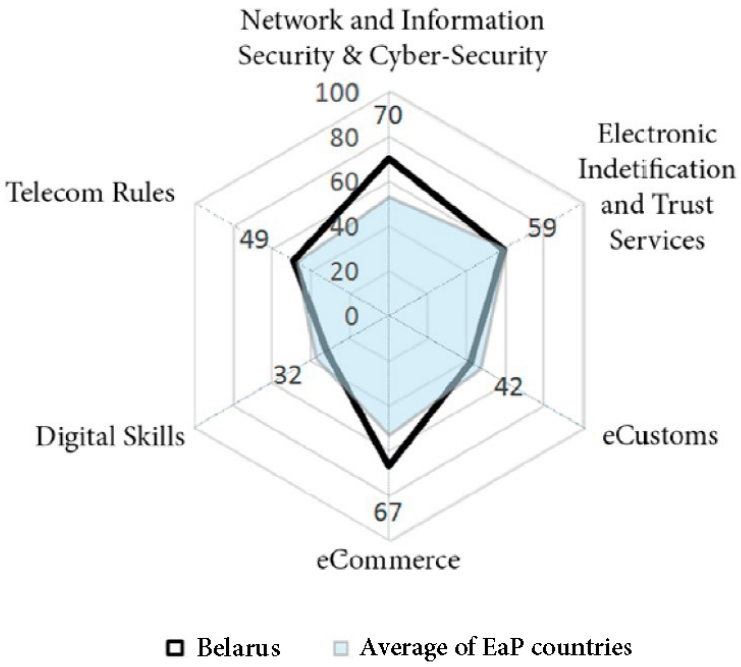
In **eCommerce for SMEs**, Azerbaijan scores higher than the Region's average. The country has achieved significant progress in opening eCommerce for international competition, in consumer rights protection and in eLogistics. Larger gaps with the EU are observed in the areas of electronic payments, internet security and privacy. Specific follow-up activities are required in setting-up an online dispute resolution system for consumers for eCommerce transactions, assuring equal treatment between paper and electronic invoices, defining a specific liability regime for intermediary eCommerce service

providers, and securing consumer protection through enhancement of international cooperation mechanisms.

For **Digital Skills**, Azerbaijan's score is lower than the average for the Region. Progress has been made especially in introducing ICT for better education, but there are still significant gaps in comparison with the EU in policy formulation and in the levels of coordination required to ensure an adequate supply of the necessary skills to create growth and jobs. As a vital first step, the extent of the "digital skills gap" should be systematically measured and monitored so that awareness of the need for action across all sectors can be raised. Clear and coordinated policy is required and key components of action should be defined – long term co-operation, human resources investment, making ICT attractive, developing digital literacy for employability and e-inclusion and lifelong acquisition of Digital Skills. Progress can be made by forming a national coalition for digital jobs, as well as local coalitions to share best practices and link with Regional and EU initiatives under the "Grand Coalition for Digital Jobs".

For **Telecom Rules**, Azerbaijan's score is around the average for the Region. Good progress has been made using state investment to build infrastructure for broadband services. However, the policy, legal and regulatory framework for the electronic communications sector is not well aligned with the EU Telecom Rules, particularly in the elements that ensure competitive markets and attractiveness to private investors. Furthermore, the regulatory capacity is very limited and remains part of the ministry structure, whereas the EU baseline requires far greater independence and separation. More resources are required to regulate a fast changing and innovative sector which is vital to the economy. Legal and regulatory change is required to improve competition in the market and to provide more favourable conditions for private investors and more consumer choice.

Belarus



Belarus has not yet joined the Convention on Cybercrime[1]. Yet its legislative and regulatory framework is generally adequate to respond to existing challenges. Belarus exhibits the smallest gap with the EU baseline. The legal and regulatory framework still needs improvement, especially in the formulation of a national Cyber Security Strategy to address numerous challenges in a comprehensive way. Also, the country requires better legal protection of personal data and online privacy and thus better balance Internet openness with safety.

Belarus' score in **electronic identification and trust services** is at the level of the Region's average measured against the EU baseline. The country does not have any clearly weak area, with the largest gap measured for e-services for citizens. eProcurement, common infrastructure and eGovernment interoperability, the use of ICT standards and interoperability are at the medium level. While technically and legally it is not possible to use digital signature across borders, there are plans to overcome the existing obstacles. Belarus would benefit from making its national legislation more compatible with Europe's eIDAS Regulation, raising security of electronic transactions and making eSignatures interoperable with the EU.

Belarus achievement in **eCommerce for SMEs** is above the average for the Region. Compared with the EU best practices, the country has achieved significant results in openness of eCommerce for international competition, consumer rights protection and eLogistics. The biggest gaps with the EU are in the areas of electronic payments, Internet security and privacy. The required priority follow-up activities are the introduction of a specific liability regime for eCommerce intermediary service providers, the setting-up of online trustmark schemes for eCommerce websites, the setting-up online dispute resolution system for participants of eCommerce transactions, and the introduction of the rights on delivery of goods into the regulatory framework.

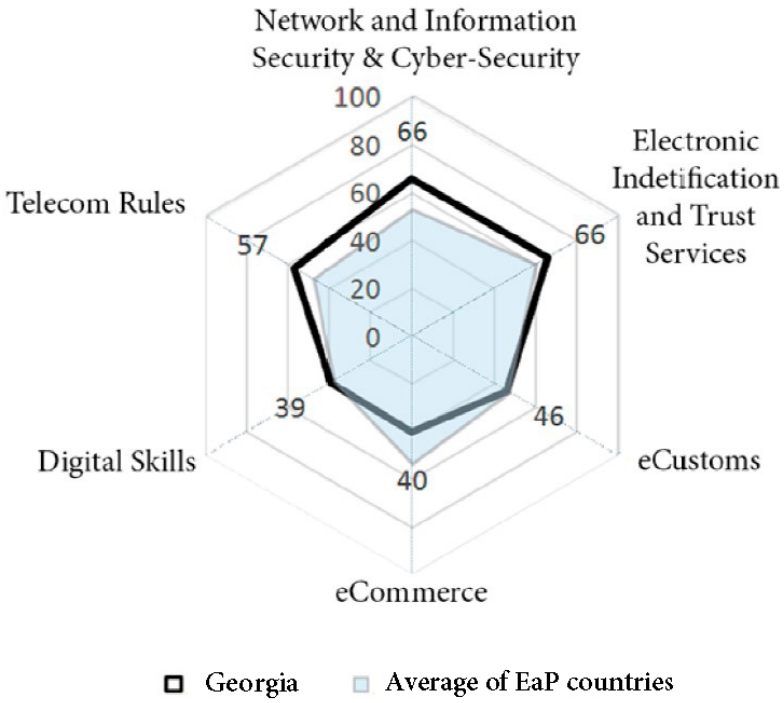
[1]Council of Europe Convention on Cybercrime of 2001 (CETS 185) is the key international agreement in the field of network, information and cyber security.

For **eCustoms**, the achievements are slightly below the average of the Region. While Belarus has established an appropriate legal framework aligned with the EU best practices, major gaps are observed in the availability of technical infrastructures and information services. The priority harmonisation actions require automating exchange of customs–related data (pre–arrival and summary declarations) with the EU through Single Point for Entry or Exit of Data (SPEED) portal, creating electronic interfaces to conduct all customs–related business, and implementing a comprehensive national single window system for trade. Information services include setting up a national registered exporters' system and a registration system of Authorised Economic Operators with exchange of data with systems the EU member states.

For **Digital Skills**, Belarus scores lower than the average for the Region. Progress has been made especially in using ICT for better education, and some policy context has been created, for example, using a formalised classifier for professions. There are still significant gaps with the EU in policy formulation and in the levels of coordination required to ensure an adequate supply of the necessary skills to create growth and jobs. As a vital first step, the extent of the "digital skills gap" should be systematically measured and monitored so that awareness of the need for action across all sectors can be raised. Neither the Ministry of Education nor the Ministry for Labour have a department in their structure that are responsible for IT education and digital skills in general. Clear and coordinated policy is required and key components of the action should be defined. Short–term priorities are to develop a curriculum and educational content standards for ICT skills based on the European e–Competence Framework, create the system of user–generated electronic content to be used for distance learning. Progress can be made by forming a national coalition for digital jobs, as well as local coalitions to share best practices and link with Regional and EU initiatives under the "Grand Coalition for Digital Jobs".

For **Telecom Rules**, Belarus scores slightly higher than the average of the Region. Particular progress has been made using state investment to build infrastructure for broadband services, giving Belarus the highest level of broadband penetration in the Region. However, there are no "state–aid rules" in place to ensure that this infrastructure provides the required competitive safeguards, including open access to alternative operators. The policy, legal and regulatory framework for the electronic communications sector is not well aligned with the EU Telecom Rules, particularly in the elements that ensure competitive markets and attractiveness to private investors. The electronic communications regulatory function remains part of the ministry structure, whereas the EU baseline requires far greater independence and separation. More resources are required to regulate a fast changing and innovative sector which is vital to the economy. Legal and regulatory change is required to improve competition in the market and to provide more favourable conditions for private investors and more consumer choice. In particular, ex–ante market analysis procedures need to be introduced and market entry made easier by the simplification of the currently complex licensing regime.

Georgia



Following the cyber-attacks on its electronic infrastructure and networks in 2008, Georgia takes **network, information and cyber security** seriously. After joining the Cybercrime Convention in 2008, the country has steadily advanced in applying European principles. More progress needs to be made in the field of private sector infrastructures, management of security breaches and reporting in a transparent and open manner. The country should continue aligning national legislation with that of the EU (e.g. by formulating a new national Cyber Security Strategy in line with the European Cyber Security strategy).

For **electronic identification and trust services** Georgia achieves the highest mark within the Region. Adopting EU policies and practices has been the main driver of the country's progress across the board. The current legal framework provides sufficient conditions for the secure exchange of information between certification service providers, consumers and businesses. There is a plan to start international cooperation in the field of mutual recognition of electronic trust services across borders. The main attention should be devoted to e-services, a common eGovernment architecture and interoperability.

For **eCustoms**, Georgia's score is just below the average of the Region. While Georgia has defined the relevant legal framework corresponding to EU standards, the biggest gap is in availability of information services. The priorities for follow-up actions are setting-up a registration system of Authorised Economic Operators and organising data exchange with the EU and the Region, creating anti-counterfeiting and anti-piracy systems, creating electronic interfaces to conduct all customs-related business in electronic format and the implementation of uniform user management and digital signatures.

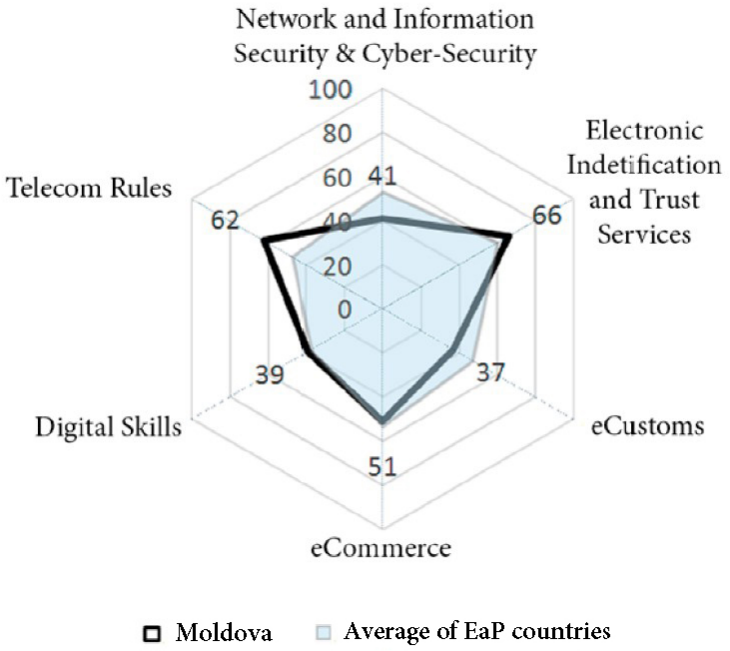
Georgia's score in **eCommerce for SMEs** is below the average of the Region. The country has achieved a significant level of harmonisation with the EU best practices in openness for competition in eCommerce, in Internet security and privacy. The biggest gaps are in the protection of consumer rights and eLogistics. Priority follow-up activities are needed to define online trustmarks for retail websites. Amendments of the legislation are required to ensure the transparency of on-

line commercial communications, to define requirements for contracts concluded on–line, and to define conditions for the risk of loss of or damage to the goods purchased on–line. In information services, the country needs to set–up an online dispute resolution system for parties involved in eCommerce transactions.

For **Digital Skills**, Georgia's score is around the Regional average. Progress has been made especially in introducing ICT for better education and some policy development has been initiated, together with actions on growth of digital skills and jobs. Georgia has not yet carried out a thorough survey to measure the "Digital Skills gap". The overall understanding of the importance of digital economy is in place and the government has initiatives to promote innovation and technology, including the creation of the Georgia Innovation and Technology Agency plus a technological park, with a planned opening in 2015. The E–Georgia initiative – including e–inclusion and ICT skills development policies– is not yet adopted. Clear and coordinated policy is required and key components of the action should be defined. The challenge is to unify the stakeholders and gather commitment to the idea of digital skills development coalitions. Cooperation between Government and the private sector on these issues would increase trust and would have long term benefit. Progress can be made by forming a national coalition for digital jobs, as well as local coalitions to share best practices and link with Regional and EU initiatives under the "Grand Coalition for Digital Jobs".

For **Telecom Rules**, Georgia scores higher than the average of the Region. Good progress has been made in adopting the EU legal and regulatory framework by the well–resourced, independent regulator for electronic communications. Significant steps include spectrum liberalisation, the removal of licensing in favour of a simple notification procedure and the use of ex–ante regulatory procedures based on market analysis to improve sector competitiveness. Even so, the overall penetration of broadband services remains significantly below the EU average. There is no clear policy for universal access to high speed (>30Mbps) broadband within an achievable deadline. The EU baseline contains this "Digital Agenda" target for 2020. Investment in infrastructure has been left largely to the private sector and the penetration of broadband services in rural areas is still very low. The legal and regulatory framework requires updating to include the latest ex–ante wholesale market and infrastructure enablers, co–ordination of civil works and simpler access to rights of way. Georgia has already used the EU Telecoms Rules model to create a competitive market for electronic communications and now the key challenge is to bring investment in high–speed broadband infrastructure out to the rural areas. Full support should therefore be given to the required analysis and planning for universal high–speed broadband, with public and private sector involvement to define and implement the required investments.

Moldova



Since joining the Convention on Cybercrime in 2009 the country's leadership has demonstrated strong political will to address new challenges of **network, information and cyber security** by aligning closely with Europe. The government has adopted a law to prevent and fight cybercrime, as well as to establish CERT. The National Strategy for Information Society Development 'Digital Moldova 2020' contains direct references to cyber-security in alignment with European principles. Yet the country needs to intensify its efforts to diminish the gap with the EU baseline which is significant. Management of critical information infrastructure, alert platforms, minimal security levels and cyber-attack simulations are particular weaknesses.

Moldova is one of the best performers in creating and using the **electronic identification and trust services** infrastructure, scoring above the average of the Region. The government common technology platform M-Cloud, which is built on open architecture and European principles of eGovernment interoperability, is already at the level of the EU baseline. A number of mobile identification tools have been successfully implemented. Other required actions are the closing of the existing gaps in eProcurement and public confidence in eID, interoperability and digital signature.

For **eCustoms**, the state of play is significantly below the average of the Region. While Moldova has achieved progress in creating a relevant legal framework, there are gaps with the EU baseline in the implementation of related infrastructures and the setting-up of information services. The priority aspects for follow-up actions are creating electronic interfaces to conduct all customs-related business on-line, setting-up an integrated tariff information system, implementing national registered exporters' system and data exchange with the EU, and creating anti-counterfeiting and anti-piracy systems.

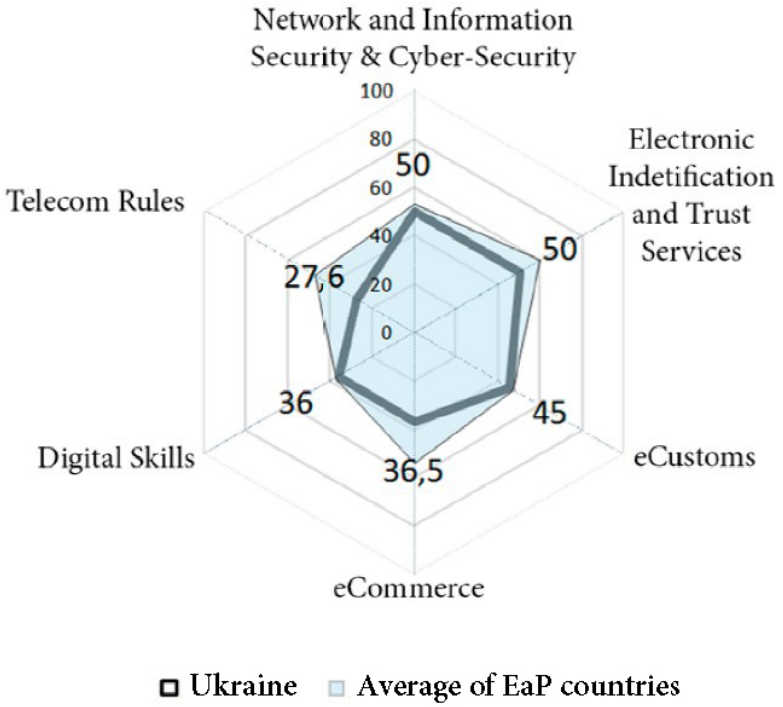
Moldova's score in **eCommerce for SMEs** is slightly below the average of the Region. The country has achieved significant progress in opening its eCommerce market to international competition, in assuring Internet security and privacy. The main gaps with the EU are in the areas of eLogistics and in protection of consumer rights. Specific follow-up activities are needed for defining regulatory framework for the conditions for the risk of loss of or damage to the goods purchased through eCommerce, introducing out-of-court dispute settlements for eCommerce cases, setting-

up online dispute resolution system for participants of eCommerce transactions, defining specific liability regime for eCommerce intermediary service providers and securing consumer protection international cooperation mechanisms.

For **Digital Skills**, Moldova scores slightly higher than the average for the Region. Progress has been made especially in introducing ICT for better education. Awareness has been raised following a study on ICT industry skill requirements and actions have been defined for developing digital skills under "Moldova 2020" strategy. Clear and coordinated policy is required and key components of the action should be defined. The challenge is to unify the stakeholders and gather commitment to the idea of digital skills development coalitions. A clear institutional framework needs to be put in place and cooperation between the Government and the private sector needs to be initiated. Progress can be made by forming a national coalition for digital jobs, as well as local coalitions to share best practices, link with Regional IIII EU initiatives under the "Grand Coalition for Digital Jobs".

For **Telecom Rules**, Moldova's score is higher than the average for the Region. Good progress has been made in adopting the EU legal and regulatory framework by the well–resourced, independent regulator for electronic communications. Significant steps include spectrum liberalisation, the removal of licensing in favour of a simple notification procedure and the use of ex–ante market analysis in regulatory procedures to improve sector competitiveness. The overall penetration of broadband services remains only at half of the EU average. Investment in infrastructure has come from both private sector and the state–owned operator, but there is no universal access policy for high–speed (>30Mbps) broadband, nor "state–aid" rules. The EU baseline contains this "Digital Agenda" target for 2020. Penetration of broadband services in rural areas is still very low. The legal and regulatory framework in Moldova requires updating to include the latest ex–ante wholesale market and infrastructure enablers, co–ordination of civil works and simpler access to rights of way. Moldova has already used the EU Telecoms Rules model to create a competitive market for electronic communications and now the key challenge is to bring investment in high–speed broadband infrastructure to the rural areas. Full support should therefore be given to the required analysis and planning for universal high–speed broadband, with public and private sector involvement to select and implement the required investments.

Ukraine



Ukraine's state of play in the area of **network, information and cyber security** is close to the average for the Region. The government has been pro-active in adapting to European principles and practices. There is a strong national CERT, well-developed and applied security standards, identified minimal security levels and an open and free internet (the gaps are minimal in these areas). The weakest aspects are inadequate legal and regulatory frameworks, defining the process of reporting on security incidents and breaches (including interaction with Telecom Regulator), vulnerable private sector critical infrastructure (its assessment and identification needs improvement), an absence of a single national alert platform and lack of regular cyber-attack simulations.

Ukraine's score on **electronic identification and trust services** is below the Region's average. Significant improvements are required in the provision of e-services that involve secure electronic identification and authentication. Particular attention is needed in developing eProcurement as this area is currently weak.

For **eCustoms,** the state of play is close to the average for the Region. Progress towards the harmonisation with EU best practices has been made in implementation of a relevant legal framework and in eCustoms infrastructure. More needs to be done in setting-up a legal and regulatory framework defining the status of an authorised Economic Operator, in uniform user management and in wider usage of electronic signatures by government organisations. Other priority actions include the creation of a national single window system for external trade, defining the status of registered exporters and the implementation of information systems for their management and data exchange with the EU countries, the setting-up national anti-counterfeiting and anti-piracy system.

Ukraine's score in **eCommerce for SMEs** is below the average of the Region. While the country has achieved progress in implementing measures to ensure internet security and in opening the eCommerce market to competition, the biggest gaps with the EU baseline are notably in the areas of eLogistics, ePayment and consumer rights protection. The priority aspects for specific follow-up actions are defining equal validity of electronic and offline contracts, defining the rights on delivery of goods purchased through eCommerce, introducing equal treatment

between paper and electronic invoices, limiting fees for the use of means of eCommerce payment, and setting-up national trustmarks schemes for retail eCommerce websites.

For **Digital skills**, Ukraine's score is close to the average for the Region. Action is required to increase awareness on the digital "skills gap" and to develop a strong political will for prioritisation, co-ordination and support of relevant initiatives to promote digital skills and jobs. Clear and coordinated policy is required and key components of the action should be defined. The challenge is to unify the stakeholders and gather commitment to the idea of digital skills development coalitions. A clear institutional framework needs to be put in place and cooperation between the Government and the private sector needs to be initiated. Progress can be made by forming a national coalition for digital jobs, as well as local coalitions to share best practices, link with Regional & EU initiatives under the "Grand Coalition for Digital Jobs".

For **Telecom Rules**, Ukraine scores much lower than the average of the Region. Broadband services penetration stands significantly below the EU average. Closing this significant "broadband gap" could add between EUR 2.9 billion and EUR 4.3 billion per annum to Ukraine's GDP. The harmonisation of spectrum exploitation would bring further economic benefits. This will require additional policies and Telecoms Rules to accelerate investments in high-speed broadband infrastructure, both in the private sector and using state-aid. The legal and regulatory framework for the electronic communications sector is not well aligned with the EU Telecom Rules, particularly in the elements that ensure competitive markets and attractiveness to private investors. This includes the latest ex-ante wholesale market and infrastructure enablers, co-ordination of civil works and simpler access to rights of way. Full support should therefore be given to the required analysis and planning for universal high-speed broadband, with public and private sector involvement to define and implement the required investments.

Find out more about the Eastern Partnership:
European Commission, Directorate-General for
Neighbourhood and Enlargement Negotiations:
http://ec.europa.eu/enlargement/neighbourhood/eastern-partnership
Facebook:
EU neighbourhood & enlargement
Twitter:
@eu-near
EU Neighbourhood Info Centre:
http://www.enpi-info.eu/indexeast.php