Government of the Republic of Estonia

DIGITAL AGENDA 2020 FOR ESTONIA
Updated 2018 (summary)

EXECUTIVE SUMMARY

Information and communication technology (ICT) has become one of the main tools for raising the competitiveness of every economic sector and walk of life. Therefore, the possibilities of ICT and challenges stemming from technology must be taken into consideration in preparing any national strategy as well as in developing services and products.

In light of the above, the **strategy does not deal with the uptake of ICT in different walks of life and policy areas** such as implementation of ICT in healthcare or private enterprise. Instead, the point of departure and **general objective is the development of a mature and secure environment for the widespread use and development of smart ICT solutions.** The overarching aim is to use ICT to support economic competitiveness and to achieve a rise in people's well-being and effectiveness of public governance.

The Digital Agenda includes more detailed **sub-objectives in two fields: development of information society** and **increasing cyber security** (see figure 1). The cyber security strategy can be found as a separate full-length document in Appendix II of this strategy.

The **most important activity areas** in the Digital Agenda are the following:

- By 2020, the **ultra-fast broadband fibre optic cable network** will be completed and steps will be taken for growth in the availability of last-mile connections.

- The **Estonian 5G activity plan** will be developed and implemented to stimulate the establishment and uptake of next-generation wireless communication networks in Estonia.

- As the next leap in the quality of public e-services and user experience, "**invisible**" **and proactive event services** will be developed to make public services as simple and efficient as possible for users. People must be able to get things done in one interaction, intervening only if prompted by the government, if at all.

- The plan is to raise the **capability of the public sector for using data analytics and research**, including upgrading the relevant awareness and skills**.**

- The **adoption of artificial intelligence applications** in the public sector will begin: a relevant activity plan will be developed and implemented and pilot projects of **so called "kratt" will be carried out**.

- With data volumes increasing and widespread cross-use of data, people must have control over the use of their data. Technological and organizational and legal conditions will be created so that **people will know and be able to specify who uses the data in the hands of the state, when it is used, and for what purposes**, so that among other things, they can allow their data to be used more easily (e.g. for research and developing new services).

- New measures and initiatives will be launched for ensuring the supply of **ICT specialists** (including broadening in-depth ICT studies at general educational schools) **and acquisition of higher ICT skills** in traditional sectors of the Estonian economy.

- **The main pillars of national cyber security capacities will be strengthened and the readiness of the state and private enterprises to cope with cyber incidents will be increased**: the cyber security baseline standard will be updated, the state's competencies in the field will be consolidated, more effort will be placed into raising cyber awareness of citizens, steps will be taken for early detection of data security needs in service development and IT development (the so-called security-by-design and privacy-by-design principles).

- **Innovation in the field of e-governance and cyber security will be accelerated**: more piloting of projects will be carried out, and new ways of involving private companies in product development; re-use of data and existing solutions will be developed, and greater support will be given to research and development (especially in the field of cyber security), among other activities.

- The uptake of digital identity and services among foreign nationals will be promoted – the **e-Residency programme will be expanded**.

The **general responsibility for implementation** of all activity areas will lie with the **Ministry of Economic Affairs and Communications**. Other ministries and institutions, including agencies in the jurisdiction of the Ministry of Economic Affairs and Communications, will be responsible for specific activities contained in the activity areas. Relevant roles and division of labour is covered in the strategy's implementation plan and will be set forth in the strategy programmes.

The steering body for implementing the strategy is the **e-Estonia Council**, and with regard to the cyber security sub-area and strategy, the **Cyber Security Council.**
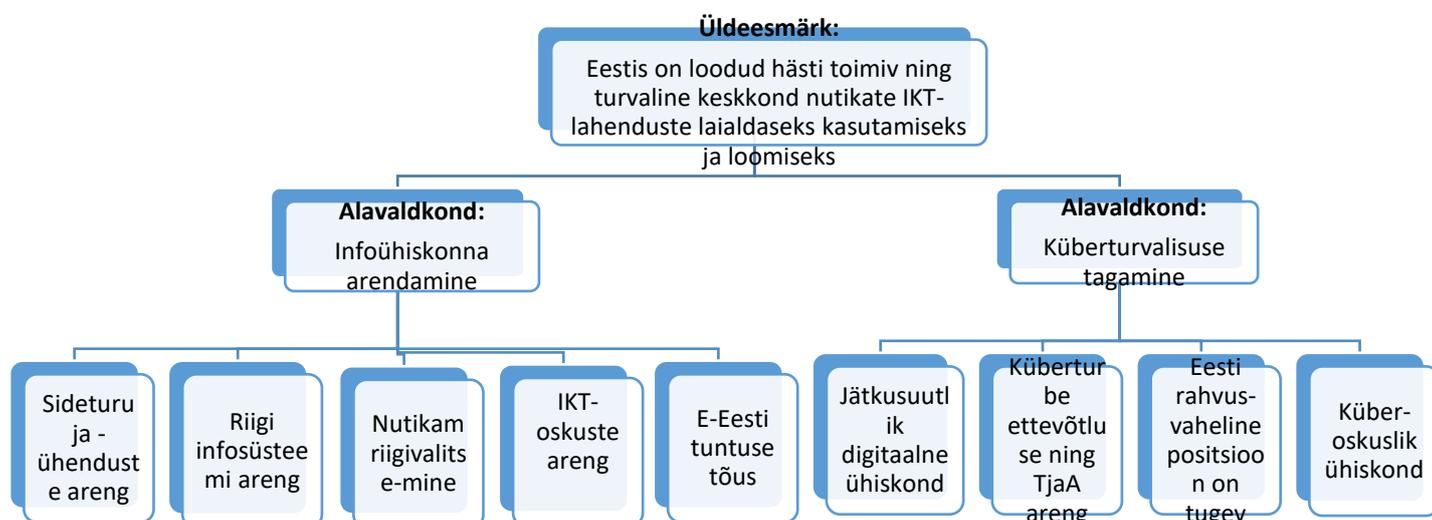
Figure 1: General objective, sub-fields and sub-objectives of the Digital Agenda 2020 for Estonia.

INTRODUCTION

This document, updated in 2018, is a strategy for developing information society and ensuring cyber security.

The impact of information and communications technology (ICT) on economic competitiveness, well-being of people and the functioning of public administration cannot be overestimated. According to data from an analysis conducted by McKinsey[1], the Internet alone generates 21% of growth in the gross domestic product, with 75 percent of benefits captured by companies in traditional industries.

According to an analysis conducted by the Estonian Development Fund (Arengufond), the economic growth attributable to the ICT sector could be projected to be within the range of 0.9–1.3%[2] in this decade. In the European Union, ICT is a key area[3], the introduction of which helps the community to move toward the objective set forth in the competitiveness strategy – to bring Europe to smart, sustainable and inclusive economic growth by 2020. ICT has become one of the main catalysts for changes in all walks of life, including, to an increasing extent, in ensuring people's personal well-being.

For companies, the uptake of ICT allows them to optimize current business processes and also create completely new and innovative goods and services. For individuals, ICT gives access to endless information resources, such as world cultural heritage and learning materials that broaden possibilities for self-development and increase well-being. Organizing and providing public services using ICT solutions allows taxpayer money to be redirected from administrative tasks to substantive functions, thus creating possibilities for simplifying communication for citizens and companies. These are just a few examples of the many benefits ICT can offer.

From autumn 2012 to spring 2013, experts from the private, third and public sectors gathered at the behest of the Ministry of Economic Affairs and Communications and the Government Office to set forth the future aims of Estonia's ICT policy and to prepare the Digital Agenda 2020 for Estonia."[4] Led by the Ministry of Economic Affairs and Communications, the first half of 2018 saw an interim review of the Digital Agenda, where experts proposed updates to the strategy. In addition, the national cyber security strategy – which had thus far been a separate strategy – was incorporated into the strategy. Its predecessor was the Cyber Security Strategy 2014-2017. To develop the latter, stakeholders, partners and experts from various sectors were engaged in parallel efforts, complementing the process of updating the strategy. Experiences to this point have led to the understanding that the creation and development of a successful digital government require both: the development of information society and guaranteeing of cyber security to proceed strategically, hand in glove. The role of cyber security in an information society is to ensure conditions for using the possibilities of ICT in an efficient and secure manner. In the planning process, we must inevitably proceed from the principle of security by design: a digital environment cannot be planned separately from security; rather, the security component must be a natural part of the network, services and basic infrastructure, planned based on the holistic view of developing a digital society, not narrowly from the aspect of ensuring data security.

The basic idea for setting aims has been the realization that ICT continues to be an important tool for increasing economic growth and improving people's quality of life. Realizing the full potential will require a coordinated

---

[1]"Internet Matters: The Net's sweeping impact on growth, jobs, and prosperity".
http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters
[2]Analysis conducted by the Estonian Development Fund, "Smart specialization – analysis of limitations" (2013).
[3]The EU information society policy "Digital Agenda for Europe" was one of the seven flagships for achieving the EU's competitiveness plan "Europe 2020". http://ec.europa.eu/digital-agenda. In 2015, the European Commission initiated the Digital Single Market Strategy https://ec.europa.eu/commission/priorities/digital-single-market_en
[4]The list of workshops and the list of the agencies, companies and organizations that took part can be found in Appendix 3 to this document.

effort from multiple parties. It was therefore necessary in preparing and conducting the interim review of the strategy to jointly discuss and agree on how we will address the major nationwide challenges involved in the smart uptake of ICT in Estonia by 2020.

The means and opportunities of ICT policy were a particular focus. As stated earlier, this document does not cover the uptake of ICT in different walks of life and policy areas such as implementation of ICT in healthcare or entrepreneurship. Right from the beginning, the main content of the Digital Agenda was the **creation and development of general prerequisites for the development of information society and the use of ICT**, and the only specialized focus theme is the general improvement of public governance through the use of ICT.[5]

Above all, planning of the areas in the Digital Agenda for Estonia were based on the two key strategic objectives established in the competitiveness strategy "Estonia 2020": **to achieve growth of productivity through higher value-added goods and services, to increase total employment.**

In addition to the competitiveness strategy, there was a search for ways of using smart ICT to propose answers to the challenges set out in the "Sustainable Estonia 21" strategy: environmental protection, preservation of culture, greater cohesiveness and growth of well-being. Although the attainment of these objectives is largely related to the overall improvement of the economy (i.e., the rise of productivity and employment), ICT can be used to better preserve culture and language.

To achieve competitiveness and sustainable development, we need a state that functions effectively and efficiently. For this reason, we proceeded not only from the two aforementioned horizontal strategies, but also from the recommendations proposed in the OECD's 2011 and 2015 reports[6] for developing Estonian public governance. Above all, these address the need to make the provision of public (e-) services more efficient and improve cooperation between government institutions.

On the basis of discussions and analyses, a broad future vision for information society was put together in cooperation between representatives from the government and the Estonian Association of Information Technology and Telecommunications. It describes what will have changed for the better in the Estonian ICT sector by 2020, and how. This is a broader vision for information society, meant as a common basis for the various sectoral strategies and the ICT sector's own development strategy. That means the government's different policy areas and the ICT sector will work together to realize the broader vision for development of Estonian information society.

This document sets out the steps planned in the context of national ICT policy for implementing the information society vision for 2020, along with its activity areas. The objectives and activity areas are planned as two broader sub-fields: development of information society (including furthering telecommunication, state information system, e-governance and services, ICT skills and the reputation of e-Estonia) and increasing cyber security. The more detailed cyber security strategy can be found as an appendix to this strategy.

The preparation and implementation of the strategy is guided by the core Principles of Estonian Information Policy, adopted by the Riigikogu in 1998 and updated in 2006[7], which set forth the principles for the functioning of the public sector in developing information society. Appendix 1 provides a more detailed elaboration of these principles for the years 2014 to 2020, which will be taken into account throughout the implementation of the strategy.

In addition, the document was prepared in consideration of lessons learned in implementing the previous strategy, Estonian Information Society Strategy 2013" and the results of discussions held with various parties

---

[5]See the Government of the Republic order and related documents regarding the approval of the proposal to compile the Estonian Information Society Strategy 2020. http://infoyhiskond.eesti.ee/eesti-infouhiskonna-arengukava-2020/dokumendid
[6]https://riigikantselei.ee/et/valitsuse-toetamine/oecd-riigivalitsemise-raport
[7].The basic principles of Estonian information policy, adopted in 1998: https://www.riigiteataja.ee/akt/75308.
. The 2006 updated principles for developing information society are set forth in Appendix 1 to this document.

and background studies and analysis of trends[8], along with the European Union's information society objectives, Digital Agenda for Europe[9].

The strategy was prepared in close cooperation with different partners from all three sectors. In May 2013, a public consultation was held on the topic of the strategy and in the first half of 2018, suggestions were elicited from key partners in the course of the interim review and public consultations were held. The drafts were discussed and approval received from the Information Society Council at sessions of the Government of the Republic and its successor, the e-Estonia Council and in the case of the cyber security sub-field and the cyber security strategy, at sessions of the Cyber Security Council. The Research and Development Council of the Republic of Estonia gave its approval to the basic principles of the information society strategy beforehand.

This is a summary of the most important activities in the Digital Agenda for Estonia 2020, which laid down the steps planned in the context of national ICT policy for implementing the vision of information society for 2020, along with its activity areas. The objectives and activity areas are planned as two broader **sub-fields**: **developing information society** (including promoting communications and state information system, e-governance and services, ICT skills and the reputation of e-Estonia) and **developing cyber security.**

GENERAL OBJECTIVE

<div style="border:1px solid">

A well-functioning and secure environment has been created in Estonia

for the broad-based use and development of smart ICT solutions.

</div>

The general objective of the Digital Agenda 2020 for Estonia was set based on a vision of information society which holds that the uptake of ICT must allow Estonia to achieve the strategic objectives set forth in the "Estonia 2020" competitiveness strategy and the sustainable development strategy "Sustainable Estonia 21".

The achievement of the general objective is evaluated on the basis of the following indicators[10]:

1. **Proportion of use of 100 Mbit/s or faster internet[11]**
   Starting level: 3.6% (2012) → Interim level: 13% (2017)→Target level: 60% (2020)

2. **Percentage of inhabitants not-using internet [12] in Estonia aged 16-74**
   Starting level: 16% (2013) → Interim level: 11% (2018)→Target level: 5% (2020)

3. **Satisfaction with quality of public services:**
   a. **among inhabitants aged 16-74**
      Starting level: 67% (2012) → 64,6% (2016)→ Target level: 85% (2020)
   b. **among entrepreneurs**
      Starting level: 76% (2012) → 85.31% (2016)→ Target level: 90% (2020)

4. Percentage of ICT specialists in the employed population
Starting level: 4.9% (2014) → Interim level: 6,8% (2017) → Target level: 8% (2020)

5. Estonia experiences no cyber incidents crippling to the functioning of information society
Starting level: 0 (2017) → Target level: 0 (2020)

---

[8]http://infoyhiskond.eesti.ee/eesti-infouhiskonna-arengukava-2020
[9] The EU's information society priorities are set forth in the Digital Agenda for Europe: http://ec.europa.eu/digital-agenda/"
[10] The indicators are also included under the following measures – some of the measures have been "elevated", becoming criteria for the general objective of the entire strategy. The indicators can be found on the website: infoyhiskonnamoodikud.mkm.ee
[11]Share of subscriber agreements for cable internet at a speed of 100 Mbit/s and greater.
[12]Non-users are considered to be people aged 16-74 who have not used the internet during the past 12 months or ever.

7. According to surveys, Estonian inhabitants feel secure and trust the digital governance

    a. Percentage of those who forgo electronic interactions with public sector or service providers on considerations of avoiding security risk[13]
        Starting level: 3.1% (2015)➔Target level: ≤ 3.1%[14] (2020)

    b. Percentage of those using secure electronic identity[15] among inhabitants with an electronic identity[16]
        Starting level: 57.6% (2017) → Target level ≥ 65% (2020)

SUB-FIELD 1: DEVELOPING INFORMATION SOCIETY

The following describes five sub-objectives. Implementing the activities contained in the sub-objectives will have the following results:

A) Estonian inhabitants and companies will have access to fast Internet connections based on modern technology.

B) Basic infrastructure of an information system enabling secure transmission of data and provision and consumption of services is guaranteed.

C) The inhabitants and companies of both Estonia and other countries use convenient and effective electronic services

D) Inhabitants with better skills and educational level use information and communication technology for improving their quality of life and engage in higher value-added work.

E) Digital development that harnesses smart technology, infrastructure and digital development will open doors for Estonian companies to seek new business opportunities and export.

SUB-OBJECTIVE 1: DEVELOPMENT OF THE ELECTRONIC COMMUNICATIONS MARKET AND CONNECTIONS

Electronic communications infrastructure is the foundation of the development of information society, because the use and development of ICT solutions require internet connectivity. The development of communications infrastructure in turn depends on the effectiveness of the functioning of the communications market. The development of infrastructure has to take place with foresight – taking into account technology trends and the needs of companies and inhabitants so as to enable the growth of well-being and productivity. The **development of the basic broadband connection network** will be completed.

<div style="border:1px solid black">

<p align="center" style="color:red">**Target: everyone in Estonia can use high-speed internet**</p>

Indicators

1. Availability of 30 Mbit/s internet[17] for all inhabitants of Estonia
    a) Availability of cable internet for all households
        Starting level: 61% (2012) → Interim level: 80% (2017)→ Target level: 100% (2020)
            [*Source: Competition Authority*]
    b) Availability of mobile internet across the entire territory of Estonia
        Starting level: 34% (2013) → Interim level: 96 (2017)→ Target level: 80% (2020)
            [*Source*: *Technical Surveillance Authority*]

</div>

---

[13] Those aged 16-74 who have refrained from using the internet in the last 12 months due to security risks: interaction with public sector institutions or service providers. https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database
[14] The target level of both criteria will be updated in the course of a review in 2020
[15] Secure electronic identity in the case of 2017 data was considered to include state-issued identities:
[16] Number of people who have used the eID service at least once in the past year.
[17]Availability means coverage with internet connections – the possibility of connecting to fast internet (at least 30 Mbit/s).

> **2. Proportion of use of 100 Mbit/s or faster internet[18]**
> Starting level: 3.6% (2012) → Interim level: 13% (2017) →Target level: 60% (2020)
> [*Source*: *Competition Authority*]

1. Support is provided for the **expansion of the broadband connection consumer network** in areas with market disruptions. For this purpose:
    a. the **administrative burden** resulting from building a communication network will be **reduced** by simplifying the relevant legal framework;
    b. if necessary, **establishment of last-mile connections** is supported in areas with market disruption, including above all in rural areas.
2. If necessary, the sufficiency of **international internet connections** will be analysed and support activities planned.
3. An **Estonian 5G activity plan** will be developed and implemented to stimulate the establishment and introduction of next-generation wireless communication networks in Estonia. Activities aimed at doing so include:
    a. the availability of the necessary radio frequency resources will be ensured (public procurements will be held in the 700MHz and 3.5GHz frequency bands);
    b. the potential areas of use of 5G and connectivity needs will be analysed; if necessary, activities and support projects for increasing awareness will be conducted;
    c. participation in international cooperation projects – above all with the Nordics, Baltics and Poland.
4. **Transition to IPv6** will be promoted. Among other things, the changeover to IPv6 will be continued in the public sector, and private sector service providers will also be encouraged to do so.
5. If necessary, the **domestic regulations in the field of electronic communications** will be updated, in order to ensure conformity to changing European Union and international legal acts, the development needs of the market and connections. Estonia will also participate in European Union and international legislative drafting.
6. The **principle of net neutrality** will continue to be supported, meaning that electronic communication undertakings may not limit, in their communication network, end users' access to legal content services, internet sites or platforms used.
7. Estonia will be an advocate at the **international level for rights and opportunities to use a free and open internet (including social media channels)** and contribute its proposals to the corresponding international cooperation.

SUB-OBJECTIVE 2: DEVELOPMENT OF THE STATE INFORMATION SYSTEM

The state information system is the set of state databases and information systems and services provided by them. For this interlinked system to function and support Estonia's development, it will be necessary to develop the state information system as a whole, alongside individual systems – for example, its central services' infrastructure components (platforms) on which various systems and services are based; and architecture and relevant agreements. The state information system can support the development of the entire society and economy. For this purpose, Estonia is developing a single service space supported by the state information system. To do so, the underlying platforms must be developed, re-use promoted, and access to information and data promoted, among other things. The service space must be increasingly open and uniform internationally, as companies and individuals are active across borders – particularly in the area of the European Union single market.

---

[18]Share of users with subscription agreements for cable internet at a speed of 100 Mbit/s and up.

Target: the state information system supports the activities of Estonia's inhabitants and undertakings
at home and across borders

Indicators

1. **Use of secure electronic identity:**
   a. **Percentage of those using secure electronic identity** (ID card, mobile-ID, digital ID, among inhabitants with an electronic identity [19]
      Starting level: 37% (2013) → Interim level: 57.6% (2017)→ Target level: 65% (2020)
         [*Source*: *SK ID Solutions AS*]
   b. **Number of new companies founded by e-residents**
      Starting level: 0 (2013) → Interim level: 2765 (2017)→Target level: 20000 (2020)
         [*Source*: *e-Residency programme*]

2. **Number of countries with which Estonia has opened cross-border public services based on the basic services infrastructure (e.g. based on X-road or electronic identity)[20]**
   Starting level: 0 (2013) → Interim level: 2 (2017)→ Target level: 7 (2020)
      [Source: *State Information System Authority*]

3. **Number of companies that have joined X-road**
   Starting level: 179 (2013) → Interim level:236(2017)→Target level: 240 (2020)
      [*Source*: *State Information System Authority*]

Activity areas

1. The central components of the state information system and solutions for interoperability will be developed so that they conform to the development of technology and function in a secure manner. For this purpose:

   a) **the central technological solutions for electronic identity (eID) and digital trust services** (digital signature, digital stamp etc.) will continue to be developed. Among other things, the development and administration of eID basic services (authentication and digital signing) will be centralized and they will be provided as a platform service.
   b) a white paper for identity management and identity documents has been developed and is updated periodically. It lays out broad-based future scenarios pertaining to eID and the eID carrier and impacts of various strategic choices;
   c) the uptake of digital ID among foreign nationals will be promoted – i.e., the **implementation of the e-Residency programme will be continued** with the aim of attracting, based on the advanced digital infrastructure and e-services, entrepreneurs to operate across borders in Estonia;
   d) **the development of X-road** as a freeware means of secure data exchange will be continued, including for facilitating the use of X-road for different parties (including the private sector) and making it compatible with other national or international data exchange platforms;
   e) **the state information system administration platform (RIHA) will be updated** in order to ensure an overview that is more up-to-date and enables executive decision-making, interoperability with the state information system and data quality;
   f) solutions for **information portals** that provide simple and secure **access for data and information** (the state portal eesti.ee, the open data portal etc.) and their uptake will be promoted;
   g) **service design approach and service-based management** will be implemented in the development of all base infrastructure components and information systems, and alternative solutions will be created for all components and risks related to their use will be managed;

---

[19]Number of people who have used eID service at least once in the past year.
[20]A basic infrastructure component for our purposes is joint developments with foreign countries of components in use in Estonia. It does not include recognition of eID means by other countries in the context of eIDAS.

h) **the activities of the Nordic Institute for Interoperability Solutions will be developed further** and other joint projects will be carried out for common development of central components of foreign countries' systems;

i) the **availability of spatial data** maintained by the state will be developed constantly and address data, classifiers and other assurance systems will be modernized, facilitating and simplifying their use by the private and third sectors;

j) **awareness and skills** of companies will be raised for use of central components of the state information system.

2. The interoperable functioning of the state information system will be strengthened. For this purpose:

a) the **existence of unified principles for developing information systems in the state and adherence to the principles** will be ensured. To do so, the basic documents pertaining to the state's interoperability will be updated, standards will be developed and awareness will be raised). The capability for data administration of information systems will be developed using data catalogues;

b) if necessary, Estonia will participate in **ICT standardization activities,** focusing above all on fields important for supporting domestic innovation or protecting existing investments.

3. In order to stimulate innovation (including in the private sector), ensure the operational reliability of the state information system and increase the cost-effectiveness of the state ICT services, the joint use and re-usability of data and technologies will be promoted. For this purpose:

a) **management of the development of the state's IT architecture will be strengthened,** including the corresponding organization of work and means of cooperation;

b) when it comes to new software and hardware developments, **transition to architecture that consolidates common domains and functions** will be preferred;

c) the state information system will be transformed to reflect the principles of **microservice-based architecture**, including for increased opening and joint use of systems and data through API interfaces;

d) **the adoption of cloud services** will be advanced in the public sector. Among other things, manuals on secure use of cloud infrastructure will be kept current, **a central government cloud service** will be developed, and, on that basis, a digital marketplace for more flexible procurement and sharing of solutions;

e) the **availability of public sector data in the form of machine-readable open data** will be promoted, including the corresponding development projects and awareness, and the open data activity plan will be carried out. The principle of access to (open) data will be created immediately upon developing new information systems or updating existing information systems;

f) the **joint use and re-use of data** (including personal data) between public and private sector (link) as well as between the private sector and other parties will be advanced, relying on the relevant initiatives, development projects (including platforms) and development of (legal and other) frameworks;

g) support for the use of **open standards and open specifications** will be continued;

h) **sharing via repositories** of reusable software, practice and the corresponding data (e.g. code, manuals and training materials etc.);

i) possibilities of development of **platform services – i.e., jointly usable applications and components** will be analysed constantly, and the common analysis and development of (software) solutions will be advanced**;**

j) **new means of involving the private sector (including start-ups)** in the development and supply of state information system and software solutions will be tested and promoted;

k) **pilot projects for new technologies** for the development of new solutions for the state information system and central components will be carried out, such as artificial intelligence, blockchain, the Internet of Things, and technologies that advance privacy.

4. Preconditions and possibilities will be developed for cross-border provision and use of services. For this purpose:

a) **Estonian information systems will be integrated** with pan-European services infrastructure solutions, and, if necessary, **bilaterally with those of other countries, using and distributing the X-road platform to the maximum extent**;

b) **cross-border functioning of electronic authentication and trust services** with European Union countries and if possible with third countries or international organizations will be promoted;

c) **information regarding the benefits of digital signing and electronic authentication will be disseminated,** above all in regard to cross-border business;

d) the carrying out of development projects and policy initiatives in regard to **cross-border data exchanges and e-services that are the most important for the Estonian population and undertakings** will be initiated or supported bilaterally as well as regionally and at the European Union level. Among other things, a priority aim is to support the development of the **real-time economy** and the reduction of bureaucracy related to the (cross-border) movement of goods and services;

e) Estonia will participate actively in the planning of the **legal and technological framework that supports the development of the European Union**'s **digital internal market** and in carrying out corresponding initiatives.

5. The developments in information society domain in Estonia and the rest of the world will be followed in order to identify changing needs and opportunities for the development of the state information system. For this purpose:

a) international **trends** in the field of ICT, digital government and information society will be followed, analysed and introduced;

b) studies on the development of **Estonia's** information society will be commissioned and published;

c) **statistics in specific fields will be developed;** among other things, systematization of statistics already being gathered. If necessary, new criteria and methodologies will be developed and Estonia will participate in international statistics development projects.

SUB-OBJECTIVE 3: SMART PUBLIC GOVERNANCE

Economic competitiveness and societal development is underpinned by good public governance. Countries will have to function better and better with less money in order to respond to the population's increasing expectations of receiving more convenient services.

Smart use of ICT holds noteworthy potential for shaping better public administration. To accomplish this, conditions must be created and a course must be set for uptake of ICT in policy fields and public-sector institutions, both for provision of public services and for improving the functioning of institutions.

Target: public services[21] are convenient for users and effective for the state.

Indicators

1. **Percentage of the population who are aware of public e-services:**
   a. **among inhabitants aged 16-74**
      Starting level: 29%(2012)→ will be determined at the end of 2018 → Target level: 90% (2020)
   b. **among entrepreneurs**
      Starting level: 34% (2012) → will be determined at the end of 2018 →Target level: 90% (2020)
         [*Source*: *Ministry of Economic Affairs and Communications*]

2. **Satisfaction with quality of public e-services;**
   c. **among inhabitants aged 16-74**
      Starting level: 67% (2012) → Interim level: 64,6% (2016)→ Target level: 85% (2020)
   d. **among entrepreneurs**
      Starting level: 76% (2012) → Interim level: 85,3% (2016) → Target level: 90% (2020)
         [*Source*: *www.riigiteenused.ee catalogue[22]*]

3. **Percentage of e-services encompassed by uniform quality measurement**

Starting level: will be determined at end of 2018 → target level: 95% (2020)
[*Source*: *www.riigiteenused.ee catalogue]*

4. **Average time spent by clients on use of e-service**
Starting level: will be determined at the end of 2018 →target level: will decrease by 20% (2020)[23]
[*Source*: *www.riigiteenused.ee catalogue[24]]*

5. **Number of functioning event services**
Starting level: 0 (2017) →Target level: 7 (2020)
[Source: *Ministry of Economic Affairs and Communications]*

6. **Number of artificial intelligence applications adopted in the Estonian public sector**
Starting level: 5 (2018) → Target level: 50 (2020)
[*Source*: *Ministry of Economic Affairs and Communications*]

Activity areas

1. **The quality of public (e-)services will be made more consistent and increased; to do so, cooperation between institutions that provide public services will be made more effective.** For this purpose:
   a. principles for developing cross-sector integral solutions will be developed and the implementation, monitoring and consultation for the regulation on the fundamental principles for organizing services and administering information[25] will be organized;
   b. constant analysis will be devoted to and proposals will be made for amending **legal acts and work processes** related to provision of services, **in order to take into account the possibilities of ICT** (e.g. so citizens and undertakings would not have to submit as many applications and services would function imperceptibly for users);
   c. **possibilities of providing feedback** regarding services immediately after use of service will be developed and the feedback received will be used to improve services so as to **raise satisfaction with services**;
   d. the **catalogue of public services** will be kept up to date to know how many services government institutions provide and at what quality. The interoperability of the catalogue with the state's other catalogues and portals (such as RIHA, the eesti.ee state portal, State Gazette) will be ensured in order to synchronize them with each other;
   e. **activities to support development and cooperative creation of services will be carried out** (e.g. PR and training events, studies, hackathons etc.) and initiatives for raising awareness among target groups of the services and the provision of services;
   f. organization of the work of the **public services council** will continue and exchange of experiences of the owners of services in different fields will be promoted.
2. **Public services will be made simpler and more efficient for users – the aim is to provide services such that the users' needs are met integrally and rapidly, as proactively and "invisibly" as possible (i.e. with the minimal need for intervention by the user).** For this purpose:
   a. a course will be set toward designing and **developing inter-sectoral and inter-institutional event-based services**. The principle is that the user must be able to get things done in one interaction, automatically and proactively if at all possible, i.e. when prompted to do so by the government.
   b. the processes of provision of public services and ICT support services will be developed integrally in order to **do away with the need to submit data repeatedly or turn repeatedly to institutions**. various agencies must re-use and cross-use data submitted by persons within the constraints of the purpose for which they were submitted, as long as the persons do not prohibit such uses.

---

[23] The objective is to measure the total time expended in consumption of e-services and the decrease in the time, among other things via proactiveness.
[24] Methodology: Guidelines for submission of quality indicators of material direct public services:
https://www.mkm.ee/sites/default/files/content-editors/20180213_teenuste_kvaliteedi_juhis_atn_kinn.pdf
[25] Regulation on organizing services and administering information: https://www.riigiteataja.ee/akt/131052017007

c. the availability of services, including event services **through different channels** will be promoted – to do so, the relevant development and pilot projects (e.g. for testing digital TV etc. as a channel for providing public services). In addition, the interoperability of service channels will be promoted so that users would be able to cross-use them, receive service from any public or private sector channel: the so-called no-wrong-door principle. Interfaces such as online banks, sales and tourism portals will be developed.

d. possibilities will be developed for users of services to receive **information on the course of provision of service**

e. **consultation on use of** (e-) services will be made more effective, including through the use of various channels (such as call centres, social media etc.) and technologies;

f. people will have simple **ways of keeping track of whether their personal data have been used in the state information system**, and if so, by whom and for what reason: Among other things, the central data tracking application will be developed further;

g. **user interfaces** for service channels and public-sector ICT solutions will be developed to make them equally accessible by everyone;

h. **Estonian-language technology applications** will be adopted for use of services. At the same time, the availability of Estonian public services will be improved by developing multilingual ICT solution, if the users' target group includes people who speak a language other than Estonian;

i. to service clients pre-emptively and to reduce the burden on companies related to communicating with the state, technological solutions that rely on exchange of data in real time, speed up processes and enable more precise predictive decisions to be made will be adopted.

3. **The functioning and management of public sector institutions will be made more effective through ICT solutions.** For this purpose:

   a. **Integral data administration will be implemented** in the public sector, providing an overview of the information developed and collected by institutions in order to make productive use of the information generated in different channels (e.g. service point, social media, post, information system, information gateway, document management system);

   b. **the system for long-term retention of information** will be organized and **promoted** information will be kept at institutions only as long as it is needed for active work or substantiation and after the need has lapsed, the information will be destroyed or handed over to an archive;

   c. the **implementation of paperless administration** will be continued, including the changeover to **e-invoices and e-receipts;**

   d. The **uptake of artificial intelligence applications** in the public sector will begin. An activity plan will be developed for this purpose (including pilot projects);

   e. the **capability of the public sector for using data analytics and research** will be raised, including the corresponding awareness and skills. Statistics Estonia will begin to be transformed into a centre of excellence for public sector data administration and research, which would support the making of data-based decisions nationwide, integrating data administration and analytics – taking into consideration the systems that secure the state information system;

4. **The process of development of public services will be promoted and IT administration at institutions will be made more effective** on order to increase the performance of development projects**.** For this purpose:

   a. **ICT-related knowledge and skills among mid-level and top-level managers in the public sector will be promoted,** including in the field of service design and use of data**;**

   b. **Sectoral ICT strategies** will be developed and updated annually in all areas of public governance. The strategies will be the basis for planning of developments and decisions to allocate (additional) state IT funding:

   c. **Knowledge and cooperation among IT managers** in the public sector will be advanced through networks and events;

   d. the planning and **management** of **ICT development projects** will be made more effective; for instance, through establishing requirements, consultation by the Ministry of Economic Affairs and Communications and supervision of priority projects;

e. **the state's role as a smart customer** will be reinforced and cooperation formats with the private sector will be developed (including new procurement formats), e.g. using best practices guidelines, sample documents and trainings.

f. possibilities will be analysed for a **major overhaul** of the **state's IT administration** system to ensure the constant renewal and sustainability of the e-state.

5. The **development and implementation of sectoral and cross-sectoral ICT development projects** related to the previous activities will be supported, in particular:

a. **joint projects** between sectors and government levels, e.g. for integral provision or delegation of services, for creation of central ICT solutions that support the development capacity of local governments ;

b. new **software development or engineering projects** that will help to improve the quality of public services and reduce the expenses on provision of services in the longer term (e.g. reducing the need for counter service and software administration costs);

c. development projects that support the **inception of invisible services, automation of processes and reduction of bureaucracy;**

d. **government institutions' data analytics projects** and projects that raise **the capability of research**;

e. **pilot projects for testing and implementing novel solution models** (above all, artificial intelligence, blockchain and language technology solutions). The principle here is that even unsuccessful projects can be learned from;

f. **Digitization** of Estonia's **cultural heritage,** and **preservation** of the heritage as digital and **making it available** in digital form;

g. **developing environments that enable participation and inclusion and applications for internet voting.**

Sub-objective 4: Development of ICT skills

The technological solutions created and to be created and expansion of infrastructure will be beneficial only if people have skills for using and perpetuating ICT solutions.

The aim is to consistently develop digital literacy to keep a (digital) gap from arising or deepening in society – so that through ICT, all people in Estonia would have enough awareness and skills to ensure their quality of life and well-being, use public services etc. The sine qua non for use of e-solutions is that people are aware of the possibilities and risks of information society, including having the skills to protect themselves from the dangers.

On the other side, developing higher ICT skills in the entire population is of increasing importance. This opens a possibility for a growth in higher value-added, more internationally competitive business activity to arise and corresponding job creation. The need will not be limited to ICT specialists. As the digital revolution is reaching all walks of life and sectors of the economy, ICT skills will be needed for new business opportunities as well for maintaining existing jobs throughout the economy.

A number of activity areas will be implemented in the framework of lifelong learning strategy, where aspects related to ICT skills make up a part of the broader whole of lifelong learning. The more precise distribution of activities and resources between strategies and decision-makers will be agreed upon on a running basis in the implementation stage (e.g. in preparing programmes, support measure regulations etc.).

Target: people know how to use and are able to use the internet to improve their quality of life, and have the ICT skills needed for doing higher value-added work

Indicators

---

1. **percentage of internet non-users[26] among Estonian inhabitants aged 16-74**
   Starting level: 18% (2013) → Interim level: 11% (2018) →Target level: 5% (2020)
      [*Source: Statistics Estonia*]

2. **Percentage of those aged 16-74 among Estonian inhabitants who have used e-commerce:**
   Starting level: 49% (2014; EU average 45%) → Interim level: 61,3% (2018; EU average 62%)
   2017→ Target level: EU average 2020 (2020)
      [*Source: Statistics Estonia and Eurostat*]

3. **Percentage of ICT specialists in the employed population [27]**
   Starting level: 4.9% (2013) → Interim level: 6,8% (2017) →Target level: 8% (2020)
      [Starting level *source: Praxis 2013; interim and target level: Statistics Estonia*]

4. **Percentage of top-level specialists in the employed population**
   Starting level: 9.3% (2014) → Interim level: 10.8% (2017) →Target level: 12% (2020)
      [*Source: Statistics Estonia[28]*]

Activity areas

1. **Acquisition of basic ICT skills in general educational schools will be promoted, in basic schools in particular.** For this purpose:
   a. **the ICT competency** of teachers and students will be measured (e.g. testing, participation in international comparative studies, thematic external evaluations), on the basis of which development activities and **in-service training for teachers will be planned**;
   b. measures will be developed for **reducing the shortage of** computing and information science **teachers**;
   c. activities will be planned for **integrating in-depth study of information technology** into the mandatory learning outcomes in the state curriculum and possibilities for in-depth study of technology will be offered to intermediate level and talented students;
   d. the provision of **technology education** (including hobby education) will be expanded to the pre-primary education level;
   e. through renovation and establishment of spot networks of general educational schools, preconditions will be created for use of ICT-based study resource solutions.

2. Support will be provided for **acquisition of basic ICT skills among adults who are internet non-users.** For this purpose:
   a. support will be provided to **regional community initiatives for learning ICT skills**;
   b. ICT basic skills training and corresponding training for trainers will be offered;
   c. novel **ICT based study resources** will be developed and distributed, including for independent study.

3. The **awareness of the population as regards the possibilities and dangers of information society** will be raised. For this purpose:
   a. support will be provided for acquisition of knowledge and skills for increasing personal **competitiveness and well-being**. For example, people's awareness of smart consumption (including the benefits of online commerce), possibilities for learning over the internet, flexible work formats, ICT sector career opportunities etc. will be raised;
   b. the population's (including entrepreneurs') knowledge about **secure use of computers and the internet** will be raised in order to create trust in participating in information society, with e.g. emphasis placed on skills for protecting personal data and secure use of mobile devices.

---

[26]Non-users are considered to be people aged 16-74 who have not used the internet during the past 12 months or ever
[27] The share of ICT specialists among the employed population is based on the annual Workforce Study from Statistics Estonia. The total number of ICT specialists in 2017 was about 44,800.
[28] EMTAK classification of areas of economic activity 1-82; 90-99

4. Possibilities for growing **the percentage of ICT specialists in the employed population** will be expanded. For this purpose:
    a. The IT-Academy 2016+ programme will be carried out. Among other things, attention will be devoted to the development of ICT higher education when developing curricula, and the organization of internships in ICT fields will be made more effective.
    b. The IT Academy strategy for vocational education will be prepared and its pilot programme will be carried out.
5. The **acquisition of higher ICT skills will be developed in the context of other vocational and higher education fields and other economic sectors.** For this purpose:
    a. **possibilities for self-evaluation** for defining the level of ICT skills will be developed;
    b. support will be provided for **training programmes** that enable acquisition of higher ICT skills (e.g. in the fields of data analysis and research, law etc.);
    c. **pilot programmes for re-training and in-service training for population with low or obsolete qualifications** will be initiated
    d. the knowledge and skills of leaders and managers/executives in public and private sector alike will be raised through information outreach and training activities in order to uptake of secure ICT and raising the competitiveness of companies.
6. Support will be provided for the **development of research areas in the ICT field and increase in the volume of corresponding research** (including in fields outside ICT). For this purpose:
    a. studies on the **development of Estonia information society** will be commissioned and published;
    b. in cooperation with research institutes and entrepreneurs, the compiling of above all **interdisciplinary research papers** that deal with the development of information society will be promoted.

SUB-OBJECTIVE 5: GREATER INTERNATIONAL AWARENESS OF "E-ESTONIA"

Estonia's image as "e-Estonia" is key for opening doors to both the ICT sector for new business opportunities as well as supporting the competitiveness of all undertakings in exporting any solutions and attracting investments. It also supports the achievement of Estonia's foreign policy aims. Maintaining the reputation depends in large part on the general development of Estonian information society and the achievement of the objectives of this strategy. To ensure a good reputation and awareness, it will be a wise to make additional direct efforts. Among other things, this will make it more likely that Estonia can attract and retain top ICT minds.

Target: Estonia has an international reputation as a leading "e-state" and information society

Criterion

1. **Coverage of e-Estonia in the world's media:[29]**
    a) **Amount of coverage in social media and traditional media**
       Starting level: 8,000 stories (2017) → Target level: 10 000 (2020)[30]
    b) **Number of stories in quality international professional/specialized publications**
       Starting level: 1 (2017) number of stories in international thematic publications → Target level 5 (2020)
          [*Source: Enterprise Estonia media monitoring*]

Activity areas

1. **Estonian e-state, ICT sector and information society-related knowledge will be created and distributed, implementing and updating the e-Estonia image action plan.** For this purpose:
    a. **international events** will be organized in Estonia;

---

[29]The monitoring includes Estonian e-state topics that were covered in social media and traditional media, including ones in which the e-state or information society received a secondary mention. The monitoring includes coverage in recognized international thematic publications. Such segments had a strong Estonian orientation – they dealt primarily with the Estonian e-state.
[30]The 8000 stories were distributed as follows in 2017: social media 3400, traditional media (web publications) 2600.

b. Estonia participates in **international information society-related conferences,** fairs and other events as well as at competitions in foreign countries.

c. the e-Estonia experience, solutions, players and future plans are proactively promoted in the **international media**, including on **social media.**

d. **analyses regarding the development of information society in Estonia and around the world** will be conducted and disseminated;

e. materials introducing e-Estonia will be developed and disseminated (including printed matter, web content, interactive demo materials etc.)

f. active participation in international information society and e-state related **policy planning, exchange of experience and cooperation.**

2. **Development of private and public-sector cooperation for more effectively disseminating e-state experience and generating export possibilities.** For this purpose:

a. **e-Estonia Showroom activities will be developed,** including the physical environment, hosting of delegations visiting Estonia and the system for involving companies and information exchange;

b. a **system for involving government institutions' experts** in companies' export projects will be developed and implemented;

c. support will be provided **in the form of interaction at the state level for Estonian companies' sales, consultation and development projects abroad**, entering into cooperation agreements with other countries in the case of interest from companies and need, hosting foreign delegations and organizing visits to other countries.

SUB-FIELD II ENSURING CYBER SECURITY

Cyber security is now universally accepted as an inseparable part of the functioning of the state and economy and internal and external security. Accelerating, diversifying and largely unpredictable digitalization mean major challenges in evaluating potential risks and threats.

SUB-OBJECTIVE 1: SUSTAINABLE DIGITAL SOCIETY

The primary task is to ensure the resilience of vital functions (strategic infrastructure and services) to cyber threats. The sub-objective focuses on one hand on resolving current problem area that have the greatest impact, and on the other hand on ensuring flexible readiness for coping with future trends. The basis and key to both is to possess a state-wide strategic big picture, interoperability, functioning community and inclusive planning.

Target: Estonia is a sustainable digital society with a strong technological resilience and readiness for coping with crisis.

Criterion[31]

1. Total number of open services[32] in the government network.
Starting level: */will be determined by end of 2018 /*→ Target level (2022): 0
[Source: State Information System Authority]

2. Total number of open services in Estonian cyber space.
Starting level: */will be determined by end of 2018 /*→ Target level (2022): Has decreased by one-third
[Source: State Information System Authority]

Activity areas

1. Technological resilience will be made more effective. For this purpose:

a. the principles of **data security and protection** will be observed in the architecture of state information systems,

b. **baseline security requirements** will be applied **comprehensively**;

c. the security of **critical databases** and **secure data exchange** between state institutions will be ensured;

---

[31] The indicators are based on the RAPID7 National Exposure Index https://www.rapid7.com/

[32] An open service is one that is offered in Estonian cyberspace and is accessible to all internet users but which should not be accessible to all internet users (e.g. admin interfaces that should not be available).

d.   risks related to new-generation technologies will be **evaluated and administered systemically**.
2. **Prevention of, readiness for and management** of incidents and crises are ensured. For this purpose:
   a.   the **capability for early detection and prevention of cyber threats** will be strengthened**;**
   b.   **cyber security will be integrated into national crisis and defence planning** and regular drills will be conducted**.**
3. **Comprehensive management** of the field will be ensured and a **cohesive community** will be developed. For this purpose:
   a.   the cyber security field will be managed comprehensively and **capabilities will be consolidated;**
   b.   a united **cyber security community** will be developed and an inclusive planning process will be ensured consistently.

SUB-OBJECTIVE 2: DEVELOPMENT OF THE CYBER SECURITY ENTERPRISE AND RESEARCH AND DEVELOPMENT

In universities, private companies and the public sector alike, Estonia will have outstanding competence in various cyber security schools of thought, above all when it comes to sectors like digital identity, cryptography, cyber security skills, education and exercises and data integrity. At the same time, commercialization of research is a problem for Estonia and throughout Europe: research publications are published but they do not evolve into actual prototypes, products and patents.

For internationally successful research and development and enterprise in the sector to take shape, Estonia will have to focus clearly on its unique strengths in the world, which above all are its electronic identity and secure data exchange (X-road) architecture ecosystem along with trust services. For Estonia, strong sectorial competence in the private sector and research institutes will mean potential for economic growth through the sector's success and readiness for coping in crisis, as hiring the entire necessary competence in the public sector is not a feasible option.

Target: Estonia possesses strong, innovative, research-based and globally competitive cyber security enterprise and research and development activity, covering the competences that are key for the state.

Indicators

1. Export volume of companies in the sector[33]
   Starting level (2017): */to be determined during 2018 /* → Target level (2022): has doubled
   [Source: Study of workforce needs in the cyber sector (Praxis, 2019)]

2. Number of new start-ups in the field of cyber security
   Starting level (2018): */to be determined during 2018 /* → Target level (2022): */to be determined during 2018 /*
   [Source: Start-up Estonia]

2. Number of doctorates defended in the field of cyber security:
   Starting level: 1.7 doctorates per year (2014-2017) →Target level: 2.5 doctorates per year (2019-2022)
   [Source: University of Tartu, TalTech]

Activity areas

1. R&D and research-based enterprise in the field of cyber security will be supported and promoted. For this purpose:
   a.   preconditions will be created for **cooperation between private sector, state and academia** that emphasizes strengths and promotes innovation;
   b.   a **cyber security R&D strategy** will be developed to define the research cooperation and R&D focus areas that are key for the state;

---

[33] It is a challenge to define cyber security as a sector as there is no classification code and a large share of companies are engaged in cyber security only as a part of their primary activity. Thus, support from professional organizations and regular research must be relied on to define the sector.

c. **the founding and development of start-ups in the cyber field** will be supported.

The strength of Estonia's cyber trademark will require a deliberate and integral approach to international topics. Estonia's external relations on cyber topics must be proactive to remain above the ever-closer global competition. In this effort, Estonia's existing strengths can be replied on, and also fields in which Estonia could be in the leading role and globally visible could also be developed.

As good examples, the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn allows Estonia to be prominently on the map when it comes to NATO cyber security issues. Alike, the competence created by the State Information System Authority allows Estonia to do the same in issues related to the EU and the civilian sector. Considering Estonia's successful experience in developing cyber expertise to this point, activities related to development cooperation in the field of cyber security could be made more effective. There should be an active inclusion of cyber deterrence, attack attribution and collective countermeasures in cooperation with other likeminded countries. It is also important to engage in cooperation with law enforcement bodies at international levels, which is a precondition for successful proceedings on cybercrimes for offering more effective protection against such crimes.

Target: Estonia is a strong partner to be reckoned with on the international arena.
Criterion

1. The expert analysis from the Ministry of Foreign Affairs and other responsible institutions[34] as to the substantive quality and focus of Estonia's international relations:

> Starting level (2018): Cooperation with international organizations and other countries takes place through individual initiatives built inconsistently across various sectors and institutions. There is a lack of an integral and systemic big picture of cooperative mechanisms to use resources pursuant to Estonia's foreign policy priorities.
> →Target level (2022):
> * Under the leadership of Ministry of Foreign Affairs and with the involvement of other responsible institutions, cooperation with different international organizations and other countries is coordinated in a coordinated and systematic manner.
> *Estonia's foreign policy priorities will serve as the basis for taking a systemic approach.
> * In cooperation with strategic foreign partners, there is a strong practical dimension in the form of joint exercises and exchange of information that will ensure successful incident resolution.
> * Estonia has raised its visibility by increasing development cooperation.
> * The Ministry of Foreign Affairs is the central institution for exchange of information in international organization when it comes to rotation of cyber diplomacy experts.
> *[Source: Ministry of Foreign Affairs, Economic Affairs and Communications]*

Activity areas

1. **Cooperation with strategic external partners** will be made more effective. For this purpose:
   a. Estonia will be ensured **sufficient representation** and **competence** on cyber topics at Estonian foreign representations and at the European Union, NATO and the UN;
   b. effort will be devoted to the processes of **developing international law** by **lobbying on Estonia's positions**;
   c. **bilateral cooperation formats** with key partners **will be developed,** joint exercises will be held regularly;

---

[34] Ministry of Foreign Affairs, Ministry of Economic Affairs and Communications, State Information System Authority, Ministry of Defence

d.   Estonia participates in international **defence cooperation** and contributes to increasing cyber security.

2. **Sustainable international cyber defence** will be promoted**.** For this purpose:

   a.   a **leading contribution** will be made to ensuring competitive and sustainable **cyber capability** in partner countries;

   b.   Estonia will participate in **creating a European Union cyber assistance network**.

SUB-OBJECTIVE 4: A CYBER LITERATE SOCIETY

For members of society to be able to operate securely in cyber space, it is a top priority to ensure a future supply of young specialists for organizations responsible for cyber security, and thus attention must be devoted to talent programmes, formal education and in-service training. The need for specialists can be sensed in three groups – institutions responsible for public sector cyber security, vital service providers and enterprise in the cyber sphere. It is necessary to continue to introduce the prevalent risks to the broader public, share advice for hedging risks, and emphasize that development of knowledge and skills in the field of cyber security is the joint responsibility of everyone operating in cyber space.

**Target: As a society, Estonia is cyber literate and
there is an ample supply of future specialists in the sector**

Indicators

1. Percentage of those aged 16-74 who have experienced a security risk while using the internet in the last 12 months (proportion of all internet users, %)[35]
>   Starting level: 44.8% (2010) → 27.7% (2015)→ Target level: ≤ 20% (2022)
>   *[Source: Statistics Estonia]*

2. Use of an officially confirmed ICT security policy in companies (% of companies with 10+ employees)
>   Starting level: 16.9% (2015) → Target level: ≥ 25% (2022)
>   *[Source: Statistics Estonia]*

3. Level of knowledge and skills of employees of government institutions and local governments, measured on the basis of a test of practical skills.
>   Starting level: N/A (2018)[36]→ Target level: ≥ 75% level satisfactory (2022)
>   *[Source: State Information System Authority]*

4. Estimated workforce shortage[37]
Starting level: *will be determined by end of 2018 /(Target level: has not grown (2022)*
>   *[Source: Study of workforce needs and education in the cyber security field (Praxis, 2018)]*

Activity areas

1. **The cyber awareness of citizens, state and private sector will be raised**. For this purpose:

   a.   **awareness building activities** will be carried out for the **broader public**;

---

[35]Experience with at least one of the following security risks: virus or other malware infection that resulted in lost time and/or data; misuse of personal information entered online or other breach of privacy, financial damage through following instructions in malicious email or in spoofed website, card payment fraud, children accessing adult content on the web.

[36] Starting level to be determined according to results of target group who have taken the test as of end of 2018.

[37] A cyber workforce study was commissioned by Ministry of Economic Affairs and Communications for the first time in 2018 to map the professional profiles of cyber security specialists and on that basis, evaluate the need for workforce today and in five years' time. The assessment of the availability of workforce was given by the companies in the sample as a subjective opinion and this established the situation in 2018. Provided that the various measures are successfully implemented, the workforce shortage / estimate of the shortage will not have grown by the end of the period.

b. **cyber security related knowledge and skills among students and teachers will be measured systematically and provision of cyber security trainings for teachers in general education and vocational schools will be ensured**;

c. a **systemic nationwide platform for raising cyber awareness** will be developed for state institutions and local governments;

d. the cyber security related **knowledge and skills of the country's mid-level and top-level leaders/managers** will be strengthened.

2. Talent will be developed corresponding to demand in the state and private sector. For this purpose:

a. **cyber defence education** in general education schools and the potential of talented youth will be developed;

b. a systematic overview of cyber defence specialists' workforce needs will be ensured;

c. the **quality of formal education and in-service training** for specialists in the fields of cyber defence and internal security will be ensured;

d. Estonia's **international cyber justice competence** will be developed.

IMPLEMENTATION OF THE STRATEGY

The general responsibility for implementation of all activity areas will lie with the Ministry of Economic Affairs and Communications. Other ministries and institutions, including agencies in the jurisdiction of the Ministry of Economic Affairs and Communications, will be responsible for specific activities contained in the activity areas in a number of cases. The more detailed roles and division of labour will be set forth in the implementation plan and, starting in 2020, in programmes.

6.1. Implementation plan and programmes

The strategy will be carried out through the implementation plan and programmes, where the activities will be planned for the four-year period of the national budgetary strategy and in greater detail for a two-year perspective. The implementation plan and the programmes will set forth in more detail the activities to be carried out in specific years in the context of the measures for fulfilling the objectives of the strategy, along with the persons responsible and the funding sources.

BUDGET FORECAST

Sub-fields[38]	2019	2 020	Total for 2014-2020
Sub-field 1: DEVELOPING INFORMATION SOCIETY	32,900,000	26,400,000	218,840,000
Sub-field II: ENSURING CYBER SECURITY	2,100,000	2,100,000	4,200,000
Total budget for the strategy, 2014-2020	**35,000,000**	**28,500,000**	**223,040,000**

---

[38]The budget for the cyber security sub-field is set forth on the basis of the workforce expenses in the cyber security field of the Ministry of Economic Affairs and Communications State Information Systems Department and the State Information System Authority's cyber security division budget and includes workforce expenses, management expenses and investments for 2019-2020. The strategy's total budget for 2014-2020 does not include expenses on ensuring cyber security prior to 2018.