CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Anna-Maria Osula

# National Cyber Security Organisation: Estonia

Tallinn 2015

*www.ccdcoe.org*
*publications@ccdcoe.org*

**Other reports in this series**

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in France

National Cyber Security Organisation in Italy

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the USA

**Upcoming in 2015**

National Cyber Security Organisation in Germany

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Latvia

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Spain

Series editor: Kadri Kaska (Researcher, NATO CCD COE)

Information in this study was checked for accuracy as of March 2015.

# About this study

This report is a part of a NATO CCD COE project that assembles a comprehensive overview of existing national organisational models for ensuring cyber security in NATO Nations that are Sponsoring Nations to the NATO CCD COE.

The study outlines the division of cyber security tasks and responsibilities between different agencies, describes their mandate, tasks and competences, and the coordination among them. In particular, it describes the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and crisis management. It also offers a summary of the national information society setting and e-government initiatives as well as the national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

The result is a series of country chapters, outlining national cyber security management structures by nation.

The project contributes to awareness among NATO Allies about cyber security management in the varied national settings, thus supporting nations enhancing their own organisational structure, encouraging the spread of best practices, and contributing to the development of cooperation between different national institutions in NATO nations.

# About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, the United Kingdom and the USA as Sponsoring Nations and Austria as a Contributing Participant. The Centre is neither part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

# ESTONIA

By Anna-Maria Osula
Researcher, NATO CCD COE

## Table of Contents

# 1. Introduction: information society indicators

Due to limited human resources and budget constraints, the tiny country of Estonia has had to adopt technological solutions and innovative efficient approaches to its public sector services. As a trailblazer of advanced e-governance, Estonia boasts substantial public e-services, offering its citizens online voting, digital signatures and e-tax refunds.[1] The risk of shattering this comfortable and effective online lifestyle is the very reason why cyber security can be seen as more of a priority for Estonia than for most other countries.[2] However, despite being well-known for its *e*-stonia reputation, latest statistics reveal that Estonia still has to make wise choices in order to compete with the information society indicators of more advanced EU countries.

## 1.1. Internet infrastructure availability and take-up

83% of Estonian households have access to the internet at home and 82% of the population are regular internet users, ranking Estonia 9th in the EU.[3] 94% of enterprises had a fixed broadband connection in 2013, which was the 13th result in the EU. Nor is Estonia in the forefront with standard fixed broadband coverage and availability or fixed broadband take-up or speed of provided fixed broadband subscriptions. However, Estonia has had 100% advanced 3G mobile broadband coverage and 97% mobile broadband take-up which is one of the highest in the EU. Internet speeds vary in Estonia with 81% of subscribers attaining at least 2Mbps and among those with a mobile broadband subscription 57%, 23%, and 4%, may access speeds of at least 10Mbps, 30Mbps, and 100Mbps respectively.

## 1.2. E-government and private sector e-services

Availability of Estonian e-government services (via the X-road system)[4] for citizens and enterprises has been 90-100% since 2010. Over 90% of residents use the Estonian ID card,[5] which enables electronic authentication when using online services, and Estonia has carried out online voting for local and parliamentary elections in Estonia eight times since 2005.[6] Hundreds of e-services are provided and promoted by the state through the e-Service Portal 'eesti.ee'[7], but only an average of 51% of individuals were reported as having used e-government services in 2014.[8] However, the use of certain public services such as the e-Tax Board is very popular among residents, resulting in over 94% of income tax returns in 2012 being submitted online.[9] Also, certain private services such as e-Banking are heavily used, and 98% of banking transactions are conducted via the internet.[10] Among businesses, the use of e-government services is much higher, reaching 95%.

Ordering goods or services online is not that common in Estonia, and other e-business indicators also show an average position in the EU rankings.

---

[1] See e.g. 'How Did Estonia Become a Leader in Technology?', *The Economist*, 30 July 2013 <http://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21>.
[2] Estonian Internal Security Service, *Annual Review*, 2013, 19 <https://www.kapo.ee/cms-data/_text/138/124/files/kapo-annual-review-2013-eng.pdf>.
[3] Unless explicitly stated otherwise, the statistics in this section are taken from the EU Digital Agenda Scoreboard: EU Digital Agenda, 'Country Ranking Table, on a Thematic Group of Indicators — Digital Agenda Scoreboard', 2014 <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators>.
[4] E-Estonia, 'X-Road' <https://e-estonia.com/component/x-road/>.
[5] 'Estonian ID-Card' <http://id.ee/?lang=en&id=>.
[6] Estonian National Electoral Committee, 'Statistics - Internet Voting - Voting Methods in Estonia - Estonian National Electoral Committee' <http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics>.
[7] 'Eesti.ee - Gateway to E-Estonia' <https://www.eesti.ee/eng/>.
[8] Country Ranking Table, on a Thematic Group of Indicators (n 3).
[9] 'E-Estonia - Estonia.eu' <http://estonia.eu/about-estonia/economy-a-it/e-estonia.html>.
[10] ibid.

# 2. Strategic National Cyber Security Objectives

## 2.1. National cyber security foundation

Estonia was one of the first countries in the world to adopt a national cyber security strategy in 2008.[11] The strategy was drafted by the Ministry of Defence for the period 2008-2013 and was accompanied by Implementation Plans. The 2008 strategy offered a comprehensive view of cyber security and outlined the following core areas: application of a graduated system of security measures in Estonia; development of Estonia's expertise in and awareness of information security; development of an appropriate regulatory and legal framework to support the secure and seamless operability of information systems; and promoting international cooperation aimed at strengthening global cyber security.[12] In September 2014, the renewed *Cyber Security Strategy for 2014-2017*[13] was adopted, the renewal process being led by the Ministry of Economic Affairs and Communication, with more than 30 public and private sector parties as well as academia involved in the development process.[14]

An additional strategy – *Digital Agenda 2020* – has been published with the aim of creating an environment that facilitates the use of ICT and the development of smart solutions in Estonia. Among other proposals, the *Digital Agenda 2020* envisions creating data centres in safe third party countries to act as data embassies, offshore protection to secure public data in the event of a national emergency, as well as proposed the idea of e-residency[15] – a state-issued secure digital identity for non-residents that allows digital authentication and the digital signing of documents.[16] Matters related to cyber crime are also being touched upon in the *Goals for Criminal Policy until 2018*.[17]

## 2.2. National cyber security strategy objectives

The renewed Cyber Security Strategy for 2014-2017 continues to implement many of the goals found in the former Cyber Security Strategy for 2008-2013. The strategy begins with an analysis of the current cyber security situation in Estonia by outlining the sectoral progress, trends and challenges. The document then turns to the principles of ensuring cybersecurity, its objectives and sub-goals.[18]

The overall goal of the strategy is to 'increase cybersecurity capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace.'[19] The sub-goals for the strategy include:

- ensuring the protection of information systems underlying vital services by defining methods for uninterrupted operation and resilience of vital services, and the protection of critical information infrastructures against cyber threats;
- strengthening the fight against cybercrime by ameliorating detection of cyber crime and international cooperation, as well as promoting education and awareness raising;

[11] Estonian Ministry of Defence, *Cyber Security Strategy*, 2008 <http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf>.
[12] ibid.
[13] Estonian Ministry of Economic Affairs and Communications, *Cyber Security Strategy 2014-2017*, <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>.
[14] Vabariigi Valitsuse 17.09.2014 korraldus nr 390 '"Küberjulgeoleku strateegia 2014–2017" ja selle rakendusplaani aastateks 2014–2017 heakskiitmine' (RT III, 19.09.2014, 3) (Endorsement of the Cyber Security Strategy 2014-2017 and its Implementation Plan, Order of the Government of the Republic, in Estonian).
[15] Estonian e-residency <https://e-estonia.com/e-residents/about/>
[16] Estonian Ministry of Economic Affairs and Communications, *Digital Agenda 2020 for Estonia*, 2013. <https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf>.
[17] Riigikogu, *Kriminaalpoliitika arengusuunad aastani 2018*, 2010 <https://www.riigiteataja.ee/akt/13329831>.
[18] Cyber Security Strategy 2014-2017 (n 13).
[19] ibid, 8.

- further developing national cyber defence capabilities by addressing different levels of civil and military competencies, and international cooperation;
- managing evolving cyber security threats by adopting independent cyber security solutions, backed by cyber security training and training opportunities, research and development and entrepreneurship; and
- focusing on cross-sectoral activities such as adjusting the legal framework and developing cyber foreign policy.[20]

The strategy is accompanied by an implementation plan for the period 2014-2017, which is not publicly available.

# 3. National Organisational Structure for Cyber Security and Cyber Defence

## 3.1. Cyber security policy coordination

The responsibility for overall cyber security policy coordination lies with the **Ministry of Economic Affairs and Communications**, whom it was handed over from the Ministry of Defence that held the task until 2011.[21]

As an inter-agency body, the **Cyber Security Council of the Security Committee of the Government** has, since 2009, been supporting strategic level inter-agency cooperation and overseeing the implementation of Cyber Security strategy objectives.[22] Additionally, the Council is tasked to monitor the success of the strategy by submitting annual progress reports to the Government outlining the ongoing realisation of the objectives set out in the Implementation Plans.[23] In retrospect, it has been echoed that during the period 2009-2013 the work of the Cyber Security Council was impeded by organisational deficiencies and that the Council did not, in practice, fulfil the supervisory role very well.[24] It has been suggested that sufficient interest and support from political leaders to ensure that cyber policy received as much attention (and funding) as it needed was also lacking.[25]

Estonia recognises the importance of being an active cyber security advocate in the international arena. It has been one of the leading countries in promoting initiatives related to cyber security in NATO, the EU, the United Nations, the Council of Europe, OSCE, ITU, and other international organisations.[26]

## 3.2. Cyber incident management and coordination

The **Estonian Information Systems Authority** (*Riigi Infosüsteemi Amet*, RIA) was established in 2011 as Estonia's central cyber security competence and coordination centre within the governance area of the Estonian Ministry of Economic Affairs and Communications. RIA is responsible for the development and administration of state information systems, as well as drafting related policies and strategies, coordinating the implementation of

[20] ibid, 8-12.
[21] Estonian Information System Authority, *Summary of the Estonian Information System's Authority on Ensuring Cyber Security in 2012*, 2012 <https://www.ria.ee/public/publikatsioonid/EISA_on_Cyber_Security_2012.pdf>
[22] Cyber Security Strategy 2014-2017 (n 18).
[23] ibid.
[24] Piret Pernik and Emmet Tuohy, *Cyber Space in Estonia: Greater Security, Greater Challenges* (ICDS) <http://www.icds.ee/fileadmin/media/icds.ee/failid/Piret%20Pernik%20-%20Cyber%20Space%20in%20Estonia.pdf>.
[25] ibid.
[26] ibid.

security standards, organising activities related to cyber security, and handling security incidents either reported or occurring on Estonian networks.[27]

One of RIA's principal areas of responsibility lies within exercising supervision[28] over the continuous application of security measures used by those information systems that support vital services to the Estonia state and their related information assets.[29] RIA also undertakes activities related to the protection of critical information infrastructure such as conducting risk analyses and preparing respective security measures. In case of a violation of the security requirements in the provision of vital services, RIA can also conduct extra-judicial proceedings such as imposing fines.[30]

Another core area of responsibility derives from the Public Information Act that identifies RIA together with the Data Protection Authority as supervisors for compliance with the Act.[31] According to the Act, in exercising state supervision over the databases and related activities[32] and if under the circumstances prescribed in the Law Enforcement Act,[33] RIA may apply special state supervision measures stated in the Law Enforcement Act such as questioning individuals, requiring the production of documents,[34] entry into and examination of premises,[35] and administering a movable property.[36] Such legal provisions have been adopted recently and their practical applicability remains to be seen. Additionally, RIA is coordinating the development and administration of the administration system for the state's information system as well as the implementation of other systems that ensure their functioning.[37]

Within RIA, the **Estonian Computer Emergency Response Team** (CERT-EE) is responsible for handling security incidents within Estonian computer networks, providing warnings for preventing security incidents, raising the security awareness of users, managing the X-Road and state portal 'eesti.ee,' and preparing reports about the spread of malware and incidents that have taken place in Estonian computer networks.[38] The support provided by CERT-EE depends on the type and severity of a security incident, on the number of users potentially affected, and on the resources available to the organisation.[39] CERT-EE also administers the Virtual Situation Room – a tool for crisis prevention that enables efficient cooperation between service providers, government agencies and also between the service providers themselves.[40] Since 2013, state entities are obliged by law to

[27] Majandus- ja kommunikatsiooniministri 25.04.2011 määrus nr 28 'Riigi Infosüsteemi Ameti põhimäärus' (RT I, 27.01.2015, 9) (Statutes of Estonian Information System Authority, Regulation of the Minister of Economic Affairs and Communications, in Estonian).

[28] Hädaolukorra seadus (RT I, 16.12.2014, 14) (Emergency Act, in Estonian; English translation available at <https://www.riigiteataja.ee/en/eli/517122014005/consolide>). § 47 (2) p 2).

[29] ibid, § 40. Ensuring electronic security of provision of vital service, '(1) A provider of a vital service shall be obligated to ensure the constant application of security measures in regards to the information systems used for the provision of the vital service and the related information assets.'

[30] ibid, § 52, 56 (5).

[31] Avaliku teabe seadus (RT I, 12.07.2014, 33) (Public Information Act, in Estonian; English translation available at <https://www.riigiteataja.ee/en/eli/522122014002/consolide>) § 44.

[32] Defined in Public Information Act, ibid, § $53^1$ (1).

[33] These circumstances vary but may include for example, if the measure is necessary for ascertaining or countering a serious threat; if a person's life, health or physical inviolability is in danger due to his or her need of assistance; if it is necessary for preventing, ascertaining or countering a threat or for eliminating disorder upon ensuring the compliance with the requirements established by or on the basis of law, and the verification of the compliance with such requirements lies within the competence of the law enforcement agency entering the premises. The example derives from § 50 (1) of the Law Enforcement Act. Korrakaitseseadus (RT I, 31.12.2014, 28) (Law Enforcement Act, in Estonian; English translation available at <https://www.riigiteataja.ee/en/eli/528012015003/consolide>).

[34] ibid § 30.

[35] ibid § 50–51.

[36] ibid § 52.

[37] Estonian Information System Authority, 'Activities of RIA' <https://www.ria.ee/activities-of-ria/>.

[38] ibid.

[39] Estonian Information System Authority, 'CERT Estonia' <https://www.ria.ee/cert-estonia>.

[40] Estonian Information System Authority, 'Virtual Situation Room' <https://www.ria.ee/vsr/>.

report immediately to CERT-EE all significant cyber security incidents against their systems as well as submit quarterly cyber security reports.[41]

RIA is also involved in developing national cyber security strategies and policies, coordinating training for users and developers of those information systems that belong to the state's network of information systems, and for organising studies inspecting the use of the state's information system.[42]

## 3.3. Military cyber defence

The National Security Concept (2010) identifies cyber threats as having the potential to cause significant damage to the society.[43] Similarly, the *Main Guidelines of Estonia's Security Policy until 2015* views the development of cyber security-related capacities as one of the key measures for preventing and combating of foreign intelligence gathering and subversive activities targeted against the state.[44]

### 3.3.1. Ministry of Defence

The **Ministry of Defence** (MOD) is the coordinating authority for cyber defence in the area of national defence.[45] MOD's overall function is to make proposals for planning national defence policy, implementing the planned activities, and organising national defence. The Ministry's main area of responsibility includes outfitting and managing the Defence Forces, the Defence Resources Agency, the Information Board, the educational institutions of the Defence Forces, and other entities.[46] A separate department that was launched in February 2014 focuses specifically on cyber policy. The department, consisting of cyber security technical and policy experts, is coordinating the development of information systems and information technology in MOD's jurisdiction, engaging in policy planning in MOD's jurisdiction, and steering the implementation of the policy.[47] In addition, MOD and its subordinate entities are involved in organising cyber-related exercises such as the NATO Cyber Coalition.[48] Moreover, in 2014 MOD proposed to NATO that the Defence Forces' cyber range could be used as the Alliance's main cyber defence training field.[49] NATO has welcomed the offer and details for the use of the range are being discussed while MOD has committed to continue investing in the cyber range in order to upgrade and supplement its equipment and capability based on experiences gained in international exercises.[50]

Although the size of the budget dedicated to cyber defence is not publicly available, MOD has confirmed that it will continue to prioritise cyber defence both internationally and domestically, using for this purpose, among other things, the synergy created by the ongoing cooperation between the Defence League's Cyber Defence Unit and the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE).[51]

---

[41] Vabariigi Valitsuse 15.03.2012 määrus nr 26 'Infoturbe juhtimise süsteem' (RT I, 19.03.2012, 4) ) (Regulation No. 26 of 15 March 2012 of the Government of the Republic, 'Information Security Management System', in Estonian), § 4 (6).
[42] CERT Estonia (n 39).
[43] Riigikogu, *National Security Concept of Estonia*, 2010 <http://www.kmin.ee/files/kmin/img/files/National_Security_Concept_of_Estonia.pdf>.
[44] Riigikogu resolution, *Approval of the Main Guidelines of Estonia's Security Policy until 2015* <https://www.siseministeerium.ee/29744/>.
[45] Estonian Ministry of Defence, *Estonian National Defence Strategy*, 2011 <http://www.kmin.ee/files/kmin/img/files/KM_riigikaitse_strateegia_eng(2).pdf>.
[46] 'Estonian Ministry of Defence' <http://www.kaitseministeerium.ee/en/ministry-of-defence>.
[47] Estonian Ministry of Defence, 'Ministry of Defence to Establish Cyber Policy Department', 2013 <http://www.kmin.ee/en/ministry-of-defence-to-establish-cyber-policy-department>.
[48] Estonian Ministry of Defence, 'Estonia Hopes to Host NATO Cyber Defence Exercises in Future as Well', 2013 <http://www.kaitseministeerium.ee/en/estonia-hopes-to-host-nato-cyber-defence-exercises-in-future-as-well.>.
[49] Estonian Ministry of Defence, 'NATO Secretary General Thanks Estonia for Offer of Cyber Range', 2014 <http://www.kaitseministeerium.ee/en/nato-secretary-general-thanks-estonia-for-offer-of-cyber-range>.
[50] ibid.
[51] Estonian Ministry of Defence, *National Defence Development Plan 2013-2022*, 2013 <http://www.kaitseministeerium.ee/files/kmin/nodes/13373_NATIONAL_DEFENCE_DEVELOPMENT_PLAN_2013.pdf>.

### 3.3.2. Estonian Defence Forces

As a structural unit of the **Estonian Defence Forces**, one of Staff and Signal Battalion's tasks is to ensure the availability and functionality of the Defence Forces' static and deployed strategic communication and information technology. This is largely coordinated by the **Strategic Communication Centre** (*Strateegiline sidekeskus,* S2K), which is responsible for, *inter alia*, administering, maintaining, and controlling measures related to information technology and networks, furnishing entities under MOD governance with ICT-related services, carrying out defence-oriented electronic warfare research and development projects, and planning cyber defence in general, as well as, since 2012, organising the activities of the Cyber Lab.[52] Estonia has offered the latter facility to NATO for cyber defence training and exercises to the benefit of both the Alliance as well as individual member-states.[53] So far, the Cyber Lab has successfully hosted NATO's annual cyber defence exercise, Cyber Coalition,[54] and the NATO CCD COE exercise Locked Shields.[55]

Since 2008, the Defence Forces have also hosted the **NATO Cooperative Cyber Defence Centre of Excellence** (NATO CCD COE)[56] – an international military organisation focusing on enhancing NATO's and its Sponsoring Nations' cyber defence capabilities. Estonia has repeatedly stated the importance of continuous support to the organisation.[57]

### 3.3.3. Estonian Defence League

In addition to the MOD, national cyber defence is supported by the Estonian Defence League's Cyber Defence Unit that includes cyber security professionals from both public and private entities.[58] The **Estonian Defence League** (*Kaitseliit*) is a voluntary, militarily organised, armed, national defence organisation that acts within the area of government of the Ministry of Defence and has a sub-unit dedicated to cyber defence – the Cyber Defence Unit.[59] The recently adopted Estonian Defence League Act[60] explicitly integrates the Cyber Defence Unit into the national defence system, providing it with a legally established mandate and a framework for its structure, management, membership, and functioning.

## 3.4. Crisis prevention and crisis management

Estonia has enacted two principal legal acts that serve as the main regulatory framework for crisis management: the Emergency Act (2009)[61] and the State of Emergency Act (1996),[62] both entailing a comprehensive approach and not specifically focusing on cyber crises. The implementation of both acts is closely followed by the **National Crisis Management Committee**, led by the **Minister of Interior**.[63]

---

[52] Kaitseministri 18.06.2013 määrus nr 38 'Staabi- ja sidepataljoni põhimäärus' (RT I, 21.06.2013, 13) (Statutes of the Staff and Signal Battalion, Regulation of the Minister of Defence, in Estonian).
[53] Eesti Kaitsevägi, 'Terras: NATO kavandab eestisse küberharjutusvälja loomist', 2014 <http://www.mil.ee/et/uudised/8255>.
[54] Estonian Ministry of Defence (n 48).
[55] Eesti Kaitsevägi (n 53).
[56] 'NATO CCDCOE' <http://ccdcoe.org/>.
[57] Kaitseministeerium, *Sõjalise kaitse arengukava 2009-2018*, p. 17 <http://www.kaitseministeerium.ee/files/kmin/img/files/SKAK_2010_est(3).pdf>
[58] Kaitseliit, 'Estonian Defence League's Cyber Unit' <http://www.kaitseliit.ee/en/cyber-unit>.
[59] Kadri Kaska, Anna-Maria Osula, LTC Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League* (NATO CCD COE, 2013).
[60] Kaitseliidu seadus (RT I, 21.06.2014, 52) (The Estonian Defence League Act, in Estonian; English translation available at <https://www.riigiteataja.ee/en/eli/512092014008/consolide>).
[61] Emergency Act (n 28).
[62] Erakorralise seisukorra seadus (RT I, 16.12.2014, 12) (State of Emergency Act, in Estonian; English translation available at <https://www.riigiteataja.ee/en/eli/517122014004/consolide>).
[63] Vabariigi Valitsuse 02.10.2001 määrus nr 312 'Vabariigi Valitsuse kriisikomisjoni põhimäärus ja koosseis' (RT I, 29.03.2013, 10) (Statutes and Composition of the Government's Crisis Management Committee, Regulation of the Government of the Republic, in Estonian).

The Emergency Act provides the legal basis for crisis management, including emergency preparation and response, as well as ensuring the continuous operation of vital services. The provisions therein do not reflect state planning in the event of a military threat.[64] The Act addresses a wide spectrum of national emergency situations, establishing both an organisational emergency handling structure and procedural frameworks for responding to emergencies.

Emergency management and government coordination during a crisis, as well as ensuring the continuous well-functioning operation of these services, belong to the area of competence of different stakeholders. For example, the **Ministry of Economic Affairs and Communications** is appointed to oversee the continuous functioning of communications networks that form the backbone of critical information infrastructure,[65] with the **Ministry of the Interior** acting as the central coordinating body.[66] A 'large-scale cyber attack' is recognised as one possible emergency where the responsibility for the management of conducting risk assessments falls to RIA and the responsibility for management of conducting the contingency plans to Ministry of Economics and Communication.[67] In 2013 the risk of a large scale cyber incident has been assessed as 'high', whereas in 2011 it was assessed as 'very high'.[68]

The Emergency Act also regulates protection of critical infrastructure. The primary responsibilities of providers of vital services are to prepare an up-to-date 'continuous operation risk assessment'[69] and a 'continuous operation plan'[70] for vital services under their ownership or control; immediately notify the national entity in whose area of competence this vital service belongs if an event is either significantly disturbing the continuous operation of a vital service or poses an impending risk to do so; providing information to requesting bodies upon request; and fulfil all other responsibilities assigned to them by the legal authorities to ensure the continuous operation of vital services.[71]

A State of Emergency is declared in the event that a threat emerges which undermines the constitutional order of Estonia such as terrorist activity, extensive conflict, forceful isolation, or mass disorder, with the caveat that it is not possible to eliminate such a threat without recourse to the measures provided for in the State of Emergency Act.[72] The Act provides the basis, conditions, and procedure for the declaration of a state of emergency, outlining the competence of the nominated authorities of emergency management, the measures to be implemented, and the rights, duties, and liabilities during a state of emergency.[73] The Prime Minister is the chief authority during a state of emergency,[74] and unlike the Emergency Act, the State of Emergency Act requires that a state of emergency be declared on the proposal of the President of the Republic or the

[64] Emergency Act (n 35) § 1 (1).
[65] ibid § 34.
[66] ibid § 36. For an analysis of the role of the Ministry of the Interior as a coordinating body, see Sorainen, *Kriisireguleerimise valdkonna juriidiline analüüs*, 2013 <https://www.siseministeerium.ee/public/Kriisireguleerimise_valdkonna_juriidiline_analuus.pdf>.
[67] Vabariigi Valitsuse 25. aprilli 2013. a korralduse nr 208 'Nende hädaolukordade nimekiri, mille kohta koostatakse riskianalüüs ja lahendamise plaan, ning hädaolukorra riskianalüüsi ja hädaolukorra lahendamise plaani koostamiseks pädevate täidesaatva riigivõimu asutuste määramine' lisa (RT III, 30.04.2013, 16).
[68] Estonian Ministry of the Interior, *2013. Aasta hädaolukordade riskianalüüside kokkuvõte.* <https://www.siseministeerium.ee/public/Riskianalyys_kokkuvote_2013.pdf>.
[69] See § 38 of the Emergency Act; siseministri 08.06.2010 määrus nr 16 'Toimepidevuse riskianalüüsi koostamise juhend' (RT I 2010, 33, 179) (Guidelines for Preparing Continuous Operation Risk Assessments, Regulation of the Minister of the Interior, in Estonian).
[70] See § 39 of the Emergency Act; siseministri 21.06.2010 määrus nr 17 'Toimepidevuse plaani koostamise juhend' (RT I 2010, 33, 180) (Guidelines for Preparing Continuous Operation Plans, Regulation of the Minister of the Interior, in Estonian).
[71] Emergency Act (n 35) § 37.
[72] State of Emergency Act (n 62) § 2 (1), (2), 3.
[73] ibid § 1.
[74] ibid § 18.

Government of the Republic,[75] after which it will become possible to restrict rights and freedoms in the interest of national security and public order.[76]

## 3.5. Intelligence

The **Estonian Internal Security Service** (*Kaitsepolitseiamet,* KAPO) is the principal actor in detecting and preventing cyber threats deriving from cyber intelligence, extremism, terrorism, and attempted sabotage. It mostly works through intelligence and criminal investigations, together with national and international partners.[77] The annual review 2013 describes the current threat picture and highlights the importance of cyber intelligence.[78]

[75] ibid § 14.
[76] ibid § 4.
[77] Estonian Internal Security Service (n 2) 18.
[78] ibid 12.

# References


Avaliku teabe seadus (RT I, 12.07.2014, 33) (Public Information Act, in Estonian; English translation available at <https://www.riigiteataja.ee/en/eli/522122014002/consolide>).

Eesti Kaitsevägi, 'Terras: NATO kavandab eestisse küberharjutusvälja loomist', 2014 <http://www.mil.ee/et/uudised/8255>.

'Eesti.ee - Gateway to E-Estonia' <https://www.eesti.ee/eng/>.

'E-Estonia - Estonia.eu' <http://estonia.eu/about-estonia/economy-a-it/e-estonia.html>.

E-Estonia, 'X-Road' <https://e-estonia.com/component/x-road/>.

Erakorralise seisukorra seadus (RT I, 16.12.2014, 12) (State of Emergency Act, in Estonian; English translation available at <https://www.riigiteataja.ee/en/eli/517122014004/consolide>).

'Estonian e-residency' <https://e-estonia.com/e-residents/about/>.

'Estonian Ministry of Defence' <http://www.kaitseministeerium.ee/en/ministry-of-defence>.

'Estonian ID-Card' <http://id.ee/?lang=en&id=>.

Estonian Information System Authority, 'Activities of RIA' <https://www.ria.ee/activities-of-ria/>.

Estonian Information System Authority, 'CERT Estonia' <https://www.ria.ee/cert-estonia>.

Estonian Information System Authority, 'Virtual Situation Room' <https://www.ria.ee/vsr/>.

Estonian Information System Authority, *Summary of the Estonian Information System's Authority on Ensuring Cyber Security in 2012*, 2012 <https://www.ria.ee/public/publikatsioonid/EISA_on_Cyber_Security_2012.pdf>

Estonian Internal Security Service, *Annual Review*, 2013, 19 <https://www.kapo.ee/cms-data/_text/138/124/files/kapo-annual-review-2013-eng.pdf>.

Estonian Ministry of Defence, 'Estonia Hopes to Host NATO Cyber Defence Exercises in Future as Well', 2013 <http://www.kaitseministeerium.ee/en/estonia-hopes-to-host-nato-cyber-defence-exercises-in-future-as-well.>.

Estonian Ministry of Defence, 'Estonia Hopes to Host NATO Cyber Defence Exercises in Future as Well'.

Estonian Ministry of Defence, 'Ministry of Defence to Establish Cyber Policy Department', 2013 <http://www.kmin.ee/en/ministry-of-defence-to-establish-cyber-policy-department>.

Estonian Ministry of Defence, 'NATO Secretary General Thanks Estonia for Offer of Cyber Range', 2014 <http://www.kaitseministeerium.ee/en/nato-secretary-general-thanks-estonia-for-offer-of-cyber-range>.

Estonian Ministry of Defence, *Cyber Security Strategy*, 2008 <http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf>.

Estonian Ministry of Defence, *Estonian National Defence Strategy*, 2011 <http://www.kmin.ee/files/kmin/img/files/KM_riigikaitse_strateegia_eng(2).pdf>.

Estonian Ministry of Defence, *National Defence Development Plan 2013-2022*, 2013 <http://www.kaitseministeerium.ee/files/kmin/nodes/13373_NATIONAL_DEFENCE_DEVELOPMENT_PLAN_2013.pdf>.

Estonian Ministry of Economic Affairs and Communications, *Cyber Security Strategy 2014-2017*, <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>.

Estonian Ministry of Economic Affairs and Communications, *Digital Agenda 2020 for Estonia*, 2013. <https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf>.

Estonian Ministry of the Interior, 2013. *Aasta hädaolukordade riskianalüüside kokkuvõte*. <https://www.siseministeerium.ee/public/Riskianalyys_kokkuvote_2013.pdf>.

Estonian National Electoral Committee, 'Statistics - Internet Voting - Voting Methods in Estonia - Estonian National Electoral Committee' <http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics>.

EU Digital Agenda Scoreboard: EU Digital Agenda, 'Country Ranking Table, on a Thematic Group of Indicators — Digital Agenda Scoreboard', 2014 <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators>.

'How Did Estonia Become a Leader in Technology?', The Economist, 30 July 2013 <http://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21>.

Hädaolukorra seadus (RT I, 16.12.2014, 14) (Emergency Act, in Estonian; English translation available at <https://www.riigiteataja.ee/en/eli/517122014005/consolide>).

Kadri Kaska, Anna-Maria Osula, LTC Jan Stinissen, The Cyber Defence Unit of the Estonian Defence League. NATO CCD COE, 2013.

Kaitseliidu seadus (RT I, 21.06.2014, 52) (The Estonian Defence League Act, in Estonian; English translation available at <https://www.riigiteataja.ee/en/eli/512092014008/consolide>).

Kaitseliit, 'Estonian Defence League's Cyber Unit' <http://www.kaitseliit.ee/en/cyber-unit>.

Kaitseministeerium, Sõjalise kaitse arengukava 2009-2018, p. 17 <http://www.kaitseministeerium.ee/files/kmin/img/files/SKAK_2010_est(3).pdf>

Kaitseministri 18.06.2013 määrus nr 38 'Staabi- ja sidepataljoni põhimäärus' (RT I, 21.06.2013, 13) (Statutes of the Staff and Signal Battalion, Regulation of the Minister of Defence, in Estonian).

Korrakaitseseadus (RT I, 31.12.2014, 28) (Law Enforcement Act, in Estonian; English translation available at <https://www.riigiteataja.ee/en/eli/528012015003/consolide>).

Majandus- ja kommunikatsiooniministri 25.04.2011 määrus nr 28 'Riigi Infosüsteemi Ameti põhimäärus' (RT I, 27.01.2015, 9) (Statutes of Estonian Information System Authority, Regulation of the Minister of Economic Affairs and Communications, in Estonian).

'NATO CCDCOE' <http://ccdcoe.org/>.

Piret Pernik and Emmet Tuohy, *Cyber Space in Estonia: Greater Security, Greater Challenges* (ICDS) <http://www.icds.ee/fileadmin/media/icds.ee/failid/Piret%20Pernik%20-%20Cyber%20Space%20in%20Estonia.pdf>.

Riigikogu resolution, *Approval of the Main Guidelines of Estonia's Security Policy until 20*15. <https://www.siseministeerium.ee/29744/>.

Riigikogu, *Kriminaalpoliitika arengusuunad aastani 2018*, 2010 <https://www.riigiteataja.ee/akt/13329831>.

Riigikogu, *National Security Concept of Estonia*, 2010 <http://www.kmin.ee/files/kmin/img/files/National_Security_Concept_of_Estonia.pdf>.

Siseministri 08.06.2010 määrus nr 16 'Toimepidevuse riskianalüüsi koostamise juhend' (RT I 2010, 33, 179) (Guidelines for Preparing Continuous Operation Risk Assessments, Regulation of the Minister of the Interior, in Estonian).

Siseministri 21.06.2010 määrus nr 17 'Toimepidevuse plaani koostamise juhend' (RT I 2010, 33, 180) (Guidelines for Preparing Continuous Operation Plans, Regulation of the Minister of the Interior, in Estonian).

Sorainen, *Kriisireguleerimise valdkonna juriidiline analüüs*, 2013 <https://www.siseministeerium.ee/public/Kriisireguleerimise_valdkonna_juriidiline_analuus.pdf>.

Vabariigi Valitsuse 02.10.2001 määrus nr 312 'Vabariigi Valitsuse kriisikomisjoni põhimäärus ja koosseis' (RT I, 29.03.2013, 10) (Statutes and Composition of the Government's Crisis Management Committee, Regulation of the Government of the Republic, in Estonian).

Vabariigi Valitsuse 15.03.2012 määrus nr 26 'Infoturbe juhtimise süsteem' (RT I, 19.03.2012, 4) ) (Regulation No. 26 of 15 March 2012 of the Government of the Republic, 'Information Security Management System', in Estonian).

Vabariigi Valitsuse 17.09.2014 korraldus nr 390 '"Küberjulgeoleku strateegia 2014–2017" ja selle rakendusplaani aastateks 2014–2017 heakskiitmine' (RT III, 19.09.2014, 3) (Endorsement of the Cyber Security Strategy 2014-2017 and its Implementation Plan, Order of the Government of the Republic, in Estonian).

Vabariigi Valitsuse 25. aprilli 2013. a korralduse nr 208 'Nende hädaolukordade nimekiri, mille kohta koostatakse riskianalüüs ja lahendamise plaan, ning hädaolukorra riskianalüüsi ja hädaolukorra lahendamise plaani koostamiseks pädevate täidesaatva riigivõimu asutuste määramine' lisa (RT III, 30.04.2013, 16).