CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

The Cyber Defence Unit of the Estonian Defence League

Legal, Policy and Organisational Analysis

Kadri Kaska, Anna-Maria Osula, LTC Jan Stinissen

Tallinn 2013

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre) and it represents the views and interpretations of the Centre. This publication does not represent the opinions or policies of NATO and is designed to provide an independent position.

Third-party sources are quoted as appropriate and the Centre is not responsible for the content of the external sources referenced in this publication. The Centre assumes no responsibility for any loss or harm arising from the use of information contained in this publication. Copies of this publication may be distributed for non-profit and non-commercial purpose only.

Contact

NATO Cooperative Cyber Defence Centre of Excellence
Filtri tee 12, Tallinn 10132, Estonia
publications@ccdcoe.org
www.ccdcoe.org

Contents

Introduction

The Cyber Defence Unit of the Estonian Defence League, or the 'Estonian Cyber Defence League' as it is widely referred to, has caught worldwide attention as an innovative model for the involvement of volunteers in national cyber defence. Originating in the long-time collaboration of both public and private sector cyber security experts of Estonia, and emerging in the aftermath of the 2007 cyber attacks against Estonian information infrastructures, the unit is focused on strengthening the professional cyber defence skills of its volunteer members in order to prepare and enhance support capabilities that can be provided in crisis. The effect of the Cyber Defence Unit, in that it promotes public-private sector cooperation in cyber security, strengthens cyber security awareness in the population, and supports prevention and response to cyber threats, is wider still.

The Estonian Defence League's role in national cyber security is recognised by several policy and legislative documents, including the National Security Strategy[1] and the National Defence Development Plan 2013–2022[2]. The recently adopted Estonian Defence League Act[3] explicitly integrates the Cyber Defence Unit into the national defence system, providing it with a legally established objective and a framework for structure, management, membership, and functioning.

The Estonian Ministry of Defence has requested the NATO CCD COE to conduct a study of the Cyber Defence Unit model with an overall aim to promote and support similar initiatives in other countries. Specifically, the study is to outline the legal context of using volunteers in national cyber defence, identify the main issues and concerns about the Cyber Defence Unit, and address them in a legal context. However, given the close connection of the legal issues to policy and organisational matters, and especially the fact that the concept and organisation of the Cyber Defence Unit is in a continuous process of development, it became necessary to extend the scope of the study somewhat and also address policy and organisational issues closely related to the legal aspects.

The paper is divided into six chapters. The first chapter will outline the background of the emergence of the Cyber Defence Unit by explaining the history of national cyber security collaboration in Estonia and the proposal to form a cyber defence volunteer corps which, while addressing a new security area, builds on an existing national model. It will also summarise the inclusion of the proposed entity into the existing Estonian Defence League Organisation and give a brief overview of the role of the latter in national defence history.

In the second chapter, the status, mission and objective of the Cyber Defence Unit as part of the Estonian Defence League organisation are explained, together with clarifying the position of the entity within the national defence organisation.

Chapter three explains the organisational setup of the Cyber Defence League, and chapter four examines the acquisition of (and exclusion from) membership as well as members' rights, duties, and liability.

The fifth chapter identifies the tasks of the Cyber Defence Unit as defined in various legal acts, examines, from a legal perspective, the potential to engage the Cyber Defence Unit to support both governmental and private sector entities, and looks at the legal framework for engaging the Cyber Defence Unit in activities relevant for national security.

---

[1] Valitsuse 31.12.2010 korraldus nr 515 ''Riigikaitse strateegia' heakskiitmine' (National Defence Strategy.) RT III, 05.01.2011, 7. English translations of policy documents and legal acts are, where available, referred under the *Bibliography* section of this paper.

[2] Vabariigi Valitsuse 24.01.2013 korraldus nr 35 'Riigikaitse arengukava 2013-2022' (National Defence Development Plan 2013–2022) RT III, 29.01.2013, 8.

[3] Kaitseliidu seadus (RT I, 20.03.2013, 1). Hereafter abbreviated as KaLS.

Finally, chapter six discusses the main concerns raised by the use of volunteers in national cyber defence, based on the Cyber Defence Unit example. These include supervision of the activities of the Cyber Defence Unit, concerns revolving around the Cyber Defence Unit's potential access to confidential information, the availability of the Cyber Defence Unit as a resource in crisis, and the status of members during international armed conflict. Again, while primarily addressed or 'addressable' by legal or regulatory means, many of these concerns are organisational or policy-related in nature, calling for attention from these perspectives as well.

The analysis is mainly based on Estonian national law, primarily the 2013 Estonian Defence League Act, together with other relevant national legal acts relating to the national defence organisation, national crisis management, and cyber security, as applicable in September 2013. In issues addressed by international law, such as the status of members of the Cyber Defence Unit during international armed conflict, relevant international law instruments are considered. With a few exceptions, the paper builds on publicly available sources.

The authors hope that the paper will provide useful insight into the model and functioning of the Cyber Defence Unit in order to support the emergence and strengthening of similar initiatives in other nations, and that it will offer input to the concept improvement and the further development of the Cyber Defence Unit.

We are grateful to the following persons for their support:

- General (Ret.) Johannes Kert of the Estonian Ministry of Defence, Mr Jaan Priisalu of the Estonian Information System's Authority, Mr Erik Amann of the Estonian Defence League, Cpt Uko Valtenberg of the Estonian Defence Forces and Dr Rain Ottis of the Tallinn University of Technology, for sharing their thoughts and vision as well as engaging at the Cyber Defence Unit workshop conducted in Tallinn in June 2013;
- Participants at the Cyber Defence Unit workshop who provided feedback, asked questions, and helped to refine our understanding of the characteristics and engagement expected from a cyber defence voluntary expert corps, the main concerns relating to such a body, and other valuable insight;
- CPT Pascal Brangetto for his perceptive comments and helpful feedback in the review of the draft paper.

1. History and Background

National Cyber Security Collaboration in Estonia

Estonia has enjoyed a long-standing national ICT security cooperation among commercial, governmental, and academic bodies. Since the late 1990s, prominent examples in this field have included cooperation among commercial banks to offer secure Internet banking services since 1996; the creation of a national electronic identification infrastructure to enable the launch of digital authentication and digital signatures in 1999[4]; and developing the physical and service infrastructure for the launch of electronic voting in public elections in 2005.

In 2006, the Estonian national Computer Emergency Response Team (CERT) was established to manage and coordinate the handling of security incidents in computer networks belonging to the .ee domain.[5] A few months later in 2006, the largest telecommunications service providers and commercial banks, as well as the Ministry of Economic Affairs and Communications, signed a Memorandum of Understanding to launch 'Computer Security 2009', a collaboration project intended to enhance the security of public and private e-services and to promote public awareness about protecting information systems.[6] This format was later joined by a number of other key e-service providers in Estonia.[7]

Against this background, the cyber attacks against Estonian information infrastructures that accompanied the 2007 spring 'Bronze Nights' protests met a collaboration network already in place; and indeed the horizontal collaboration between private and public sector information security experts was generally viewed as a major factor for successfully handling the attacks.[8] The importance of public-private partnership was therefore also reflected in the Estonian Cyber Security Strategy, adopted a year after the incident in May 2008. This document recognised the centrality of cooperation of all stakeholders – of public and private sectors as well as of civil society – as a key principle and guideline for attaining the objectives of the strategy and achieving a strong level of cyber security.[9]

Consequently, when the idea was proposed in September 2007 to 'form a 'Cyber Defence League' similar to the existing Estonian Defence League organisation'[10], it was eagerly welcomed by the

---

[4] Seletuskiri digitaalallkirja seaduseelnõu juurde. Digitaalallkirja seadus (151 SE) Tallinn, 1999. http://www.riigikogu.ee/?op=emsplain2&content_type=text/html&page=mgetdoc&itemid=991820001.

[5] Riigi Infosüsteemide Arenduskeskuse põhimäärus (RTL 2004, 158, 2375) as of 1 January 2006 (Statute of the Estonian Informatics Centre); *see also* About CERT Estonia. Estonian Information System's Authority, https://www.ria.ee/cert-estonia/.

[6] 'Arvutikaitse 2009' koostööleping (Memorandum of Understanding for 'Computer Security 2009'. Tallinn, 23 May 2006. http://www.arvutikaitse.ee/wp-content/uploads/2006/12/arvutikaitse2009_lepingu_tekst.pdf.

[7] Such as the largest energy supplier, additional commercial banks, the major educational e-service provider, as well as the largest governmental e-service providers. Kõik suurimad e-teenuste pakkujad on Arvutikaitse 2009 partnerid. 3 Dec 2007 http://www.vaatamaailma.ee/?cat=6&paged=2.

[8] Cyber Security Strategy Committee. Cyber Security Strategy. Ministry of Defence. Tallinn 2008. P. 14. http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (text adopted by decree No. 201 of the Government of the Republic of 8 May 2008; RTL 2008, 40, 563); *see also* Eneken Tikk, Kadri Kaska, Liis Vihul. International Cyber Incidents: Legal Considerations. CCD COE, 2010. P. 24.

[9] Cyber Security Strategy, *id*. P. 7.

[10] The proposal was made by Mr. Ülo Jaaksoo, a member of Estonian Academy of Sciences (informatics) and CEO of Cybernetica AS (a leading Estonian company in the research, development and manufacturing of software solutions, and theoretical and practical security). See the proposal being presented (in Estonian): http://www.youtube.com/watch?v=NHxuowkQxCI.

cyber security community as well as the Minister of Defence.[11] The project was envisioned by the community as an instrument to offer a meaningful contribution to cyber security, and it met well with the expectation of the Cyber Security Strategy to identify and develop forms of collaboration and communication among the various stakeholders involved. Also, there was a realisation that such an entity could meet the strategy objective of raising public awareness on cyber threats and cyber security.[12] The creation of an informal cooperation network was initiated within the Estonian Defence League shortly after the proposal; a working group called by the Ministry of Defence further developed the concept, and in early 2011, a Cyber Defence Unit was appended to the existing Estonian Defence League as a structural unit.[13]

The emerging concept of the Cyber Defence Unit was reflected more clearly in the 2010 National Defence Strategy, in that an expectation was expressed that the Estonian Defence League should 'develop a cyber-defence capability'. The strategy also prioritised the ability of the Estonian Defence League in 'responding to any threats arising from the development of information technology'.[14]

The first cyber defence units were *de facto* formed within the Defence League's territorial units of Tallinn and Tartu in 2009.[15] In January 2011, the Cyber Defence Unit was formally established within the Estonian Defence League.[16]

Estonian Defence League

The Estonian Defence League organisation has a long tradition in the history of Estonian independence and statehood. The league was founded in November 1918, a few months after the Estonian declaration of independence from Soviet Russia, as an armed voluntary defence organisation, with functions mainly related to ensuring public order.[17] The organisation then became a foundation for the development of the Estonian armed forces, border guard, and prison service; from 1924 to 1940, it bore a major role in public national defence education and military training.[18]

By 1940, the membership of the Defence League had grown to 42,000,[19] from a total population of 1.13 million people[20] (in comparison, the regular Estonian Defence Forces at the time consisted of 1,500 officers, 2,400 non-commissioned officers and 12,000 conscripts[21]).

---

[11] Holger Roonemaa. Aaviksood vaimustas mõte küberkaitseliidu loomisest. Eesti Päevaleht, 2 Oct 2007. http://www.epl.ee/news/eesti/aaviksood-vaimustas-mote-kuberkaitseliidu-loomisest.d?id=51103195.

[12] Cyber Security Strategy, *supra* note 8. Reflected, e.g., in pp. 7, 34.

[13] Seletuskiri Vabariigi Valitsuse määruse "Vabariigi Valitsuse määruste muutmine" eelnõu juurde (Explanatory Memorandum to the draft regulation on amending certain government regulations), 22.11.2010. http://eelnoud.valitsus.ee/main#TnXRXqdL; Valitsus asutas Kaitseliidu küberkaitseüksuse. Kaitseministeerium, 20.01.2011, http://www.kmin.ee/et/valitsus-asutas-kaitseliidu-kuberkaitseuksuse.

[14] *Supra* note 1, p. 9.

[15] Urmas Jaagant. Küberkaitseliit pakub harjutuskeskkonda vabatahtlikele IT-spetsialistidele. Eesti Päevaleht, 14 Apr 2010. http://www.epl.ee/news/eesti/kuberkaitseliit-pakub-harjutuskeskkonda-vabatahtlikele-it-spetsialistidele.d?id=51274411.

[16] Vabariigi Valitsuse määrus nr 16 'Vabariigi Valitsuse määruste muutmine seoses Kaitseliidu küberkaitse üksuse loomisega'. RT I, 25.01.2011, 3. (Government Regulation on the amending of secondary legal acts with regard to establishing the Cyber Defence Unit within the Estonian Defence League).

[17] Tanel Laan. Ühine tahe. Kaitseliit 1925-1940. Kaitseliit, 2012. http://www.kaitseliit.ee/files/kaitseliit/img/files/yhine_tahe_web.pdf. Pp. 6-11.

[18] Ajalugu. Kaitseliit – rahva algatatud omariikluse pant. Kaitseliit, http://www.kaitseliit.ee/et/ajalugu1.

[19] Laan, *supra* note 17, p. 94.

[20] Ene-Margit Tiit. Pilguheit äsjasele rahvaloendusele. Riigikogu Toimetised 26, 2012. http://www.riigikogu.ee/rito/index.php?id=16265.

[21] Ajalugu. Kaitsevägi. http://www.mil.ee/et/kaitsevagi/organisatsioon/kv-ajalugu.

The Estonian Defence League was dismissed in June 1940 in the course of the occupation of the Estonian Republic by Soviet Russia.[22] It was restored as the legal successor of the pre-WWII organisation in February 1990.[23]

Since April 1992, the Defence League was included in the Estonian Defence Forces as a voluntary component and subjected to the command of the Chief of Staff of the Estonian Defence Forces.[24] The 1999 Estonian Defence League Act defined the Estonian Defence League as a voluntary, militarily-organised national defence organisation, part of the Estonian defence forces and operating in the area of government of the Ministry of Defence.[25]

The current Estonian Defence League Act[26] applicable from April 2013, makes a clear organisational distinction between the Estonian Defence League and the Estonian Defence Forces, although it also functionally links the Defence League to the Defence Forces.[27] The Act defines the organisation's place in the setup of national defence, its purpose, functions, structure, legal basis for activity and management, and membership. The Act identifies the Cyber Defence Unit as a component in the structure of the Estonian Defence League organisation, which functions under the general framework for the Defence League with some specifics applicable.

[22] 1940. aasta kuum suvi. Kaitseliit. http://www.kaitseliit.ee/et/1940.-aasta-kuum-suvi.
[23] *Supra* note 18; Kaitseliidu seadus (RT I, 08.07.2011, 48) (Estonian Defence League Act), § 3. (Hereafter abbreviated as KaLS 1999).
[24] Vabariigi Valitsuse 28. aprilli 1992. a määrus nr 128 'Kaitseliidu kohast riigi kaitsesüsteemis' (RT 1992, 18, 261; RT I 2000, 4, 31) (The Place of the Defence League in the Estonian National Defence System); Kolmas algus. Kaitseliit 1990-1993. Tallinn, 2010. Pp. 51, 54. (Available online at http://www.kaitseliit.ee/files/kaitseliit/img/files/kolmas_algus.pdf).
[25] KaLS 1999, § 1.
[26] See *supra* note 3.
[27] See chapter three of this paper for further elaboration.

2. Status, Mission and Objective

Legal Status of the Estonian Defence League and its Place in the National Defence Organisation

Due to the Cyber Defence Unit being established as a structural unit of the Estonian Defence League[28], its status and terms of reference derive from the legal acts defining the status of the latter.

The basis for the organisation of Estonian national defence is defined in the Constitution of the Republic of Estonia[29] together with the Peacetime National Defence Act[30] and the Wartime National Defence Act[31]. Both these acts make generic references to the Estonian Defence League, with the Peacetime National Defence Act referring to the legal status of the Defence League to be provided by a separate Act.[32] In wartime, the Estonian Defence League would be subjected to the Commander of the Defence Forces.[33]

The Estonian Defence League Act identifies the Defence League as a voluntary national defence organisation operating in the area of government of the Ministry of Defence. It is militarily organised, possesses arms, engages in military exercises, and fulfils functions laid upon it by law; and is explicitly defined as outlying any political faction and activity. [34]

Image 1. Estonian national defence organisation.

By nature, the Estonian Defence League is a legal person in public law whose legal status is defined by law and secondary legal acts.[35] As a legal person, the Defence League has the right to enter into

---

[28] KaLS § 9 (1).

[29] Article 126 (in Chapter X) stipulates that the organisation of national defence will be provided in the Peacetime National Defence Act and the Wartime National Defence Act. A general assumption is taken in both the Constitution and the two above-mentioned acts that the Estonian Defence League is a national defence organisation within the meaning of the Constitution. *See* Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. Tartu Ülikool, 2012. Available online at http://www.pohiseadus.ee/. Paragrahv 126, http://www.pohiseadus.ee/ptk-10/pg-126/.

[30] Rahuaja riigikaitse seadus (RT I, 20.03.2013, 23). Hereafter abbreviated as RRKS.

[31] Sõjaaja riigikaitse seadus (RT I, 10.07.2012, 33). Hereafter abbreviated as SRKS.

[32] RRKS § 13 (2).

[33] SRKS § 4 (1), § 12 (2) 1).

[34] KaLS §§ 2 and 6.

[35] KaLS § 3 (2). Based on the distinction made in the General Part of the Civil Code Act (RT I, 06.12.2010, 12). According to § 24, a legal person is a subject of law founded pursuant to law either as a legal person in private law (legal person founded in private interests) or a legal person in public law, which includes the state, local governments and other legal persons *founded in the public interest and pursuant to an Act concerning such legal person*, which is explicitly the case for the Estonian Defence league. *See* § 25 (2) of the General Part of the Civil Code Act).

agreements and engage in various forms of economic, educational and organisational activities within limits defined by the law.[36] Its rights can only be expanded or limited by law,[37] meaning that the competence to extend or narrow the mandate or the privileges of the Estonian Defence League rests with the *Riigikogu* (Parliament) only. As a structural unit of the Estonian Defence League, the Cyber Defence Unit has no independent legal capacity.

Mission and Objective of the Cyber Defence Unit

The purpose of the Estonian Defence League is to enhance the preparedness of the population to defend the independence of Estonia and its constitutional order by relying on free will and self-initiative.[38] This principal purpose applies for both the organisation in general as well as the Cyber Defence Unit in particular.

In accordance with its general purpose, the mission of the Cyber Defence Unit is defined as an endeavour 'to protect Estonia's high-tech way of life by protecting information infrastructure and supporting the broader objectives of national defence'.[39] The identified objectives of the Cyber Defence Unit centre around three main themes:[40]

a) *developing a network of cooperation, including for crisis response*. This is sought by strengthening cooperation among qualified volunteer IT specialists as well as by the creation of a network to combine the expertise of public and private sectors to act in crisis;
b) *improving the security of critical information infrastructure* by raising the level of security of critical information infrastructure, both through regularly sharing threat awareness and disseminating best practices as well as enhancing preparedness for operating during a crisis situation;
c) *promoting awareness, education and training* both by providing continuous information security education and training to members as well as actively participating in cyber security training networks, including international ones.

[36] KaLS § 79 (1) and (2).
[37] KaLS § 3 (3).
[38] KaLS § 2 (3).
[39] Estonian Defence League's Cyber Unit. The Defence League, http://www.kaitseliit.ee/en/cyber-unit.
[40] *Id.*; Küberkaitse üksus. Kaitseliit, http://www.kaitseliit.ee/et/kuberkaitse-uksus.

3. Organisation

Legal Basis

The principles of structure and management of the Estonian Defence League are defined in Chapter 2 of the Estonian Defence League Act. The chapter addresses the division of the Estonian Defence League into structural units, relationships of command and subordination, the setup and competence of collegial bodies, and other organisational issues.

The structure, leadership and internal arrangement of the organisation, as well as the establishment of managing bodies and the tasks and composition of such bodies, are further elaborated in the Statutes[41] of the Estonian Defence League, established by a regulation of the Government of the Republic.[42]

Management and Command

Until the entry into force of the new Defence League Act on 1 April 2013, the Commander of the Defence Forces was commanding both organisations, the Estonian Defence Forces and the Estonian Defence League.[43] The new Act aims to refine the tasks entrusted to the Estonian Defence League as well as to clarify the relationship between the two bodies. It states that the Estonian Defence League is led by the Commander of the Defence League placed under the direct command of the Commander of the Estonian Defence Forces.[44] This should be read together with the following provisions that define the tasks and areas of competence of both the Commander of the Estonian Defence League and the Estonian Defence Forces, as clarified below.

The role of the Commander of the Estonian Defence Forces in relation to the Estonian Defence League is specified in § 12 of the Estonian Defence League Act. The Commander of the Estonian Defence Forces approves the requirements for military capability and preparedness of the Estonian Defence League, approves action plans[45] for war-time mobilisation and formation together with the composition and equipment of wartime and reserve units[46], supplies the Defence League with the military equipment necessary for carrying out certain tasks outlined by the Estonian Defence League Act, proposes the peacetime positions within the Estonian Defence League, and gives his opinion on the Development Plan of the Estonian Defence League.[47]

The Commander of the Estonian Defence League is nominated to and released from office by the Government of the Republic, under a joint recommendation of the Minister of Defence and the Commander of the Estonian Defence Forces.[48]

---

[41] 'Statutes' is the translation of 'põhimäärus' and should in this context be equalled with 'Kodukord' as stipulated in KaLS § 5.

[42] The current Statutes were adopted upon the 1999 Act and are to be replaced, based on the 2013 Defence League Act (a relevant delegation is contained in KaLS § 5 (1)). At the time of drafting this paper (September 2013), a final draft of the Statutes was not yet available.

[43] KaLS 1999, § 10 (1).

[44] KaLS § 11 (1).

[45] In the extent concerning the Estonian Defence League, this authority may be delegated to the Commander of the Defence League.

[46] These comprise all Estonian Defence Forces units in reserve, without consideration for their membership in Estonian Defence League.

[47] KaLS § 12 1)-5).

[48] KaLS § 11. The position of the Commander of Estonian Defence League may only be manned by regular members of the Defence Forces. This also applies to certain other positions, including those of the Chief of Staff of the Estonian Defence League and the commanders of Defence League units (including that of the

The tasks of the Commander of the Estonian Defence League are listed in § 13 of the Estonian Defence League Act and include, for example, managing and representing the Estonian Defence League, administering the responsibilities and cooperation related to the Estonian Defence League, and establishing the Statutes of the structural units, including the Statutes of the Cyber Defence Unit. The Commander also administers the Defence League's Development Plan and approves the League's training and activity plans. The heads of Estonian Defence League's structural units report directly to the Commander of the Estonian Defence League.[49]

As an organisation that unites in itself elements of both a voluntary and military organisation, the Defence League entail rather specific organisational characters. The division of roles indicated in the Defence League Act reflects that, for the purposes of military training and in the context of direct chain of command, the Commander of the Estonian Defence League is subject to the Commander of the Estonian Defence Forces. However, as underlined by the explanatory memorandum[50] accompanying the Act, the domain of military training is the only area within the activities of the Estonian Defence League subject to the direct authority of the Commander of the Estonian Defence Forces.[51] Furthermore, it is added that even though the Commander of the Estonian Defence League serves directly under the Commander of the Defence Forces, the latter does not have the right to use chain of command for the management of the Estonian Defence League during peace time.[52] On the other hand, according to the Wartime National Defence Act, in war time the Commander of the Estonian Defence Forces is in charge of both organisations.[53]

The Estonian Defence League's own command structure takes into account the specific features of a voluntary military organisation. This means that military activities are led by the Commander of the Estonian Defence League, whereas voluntary and purely organisational matters belong to the competence of the Defence League's collegial bodies.[54] In addition to other organisational tasks outlined in the Defence League Act, the collegial bodies have an advisory capacity in questions of military training and the preparation of national military defence capabilities.[55]

The Cyber Defence Unit in the Estonian Defence League Structure

The Estonian Defence League's structural units are the Headquarters of the Defence League, district units (located roughly according to the Estonian administrative-territorial division in 15 counties), the Cyber Defence Unit, the Defence League School, Women's Home Defence and two youth organisations. The district units, as well as the Cyber Defence Unit, are led by a unit commander. Conditions for the formation of a structural unit's governing body, its tasks, and issues related to membership are to be outlined in the Statutes of the Estonian Defence League.

The Cyber Defence Unit is one of the structural units of the Estonian Defence League and operates under the same legal framework. Its activities and responsibilities are outlined in the Estonian

---

Cyber Defence Unit). KaLS § 11 (5); Explanatory Memorandum to the Estonian Defence League Act (*infra* note 50), p. 16.

[49] KaLS 9 (2).

[50] Seletuskiri kaitseliidu seaduse eelnõu juurde. 05.03.2012. (Explanatory Memorandum to the Estonian Defence League Act) http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=93442de2-07bc-49f9-9a09-b4d81d8c251b&.

[51] *Id.*, p. 4.

[52] *Id.,* p. 17.

[53] SRKS § 4 (1) and § 12 (2) 1).

[54] Collegial bodies are the central bodies ('keskorganid') of the Defence League (i.e. the central assembly ('keskkogu'), central management board ('keskjuhatus'), central audit committee ('keskrevisjonikomisjon') and the Council of Elders ('vanematekoda')), as well as the management bodies of the structural unit (such as the Cyber Defence Unit) and any subunits of the latter. KaLS § 17 (2), (3).

[55] KaLS § 17 (2).

Defence League Act, the Estonian Defence League's statutes, and further defined in the Statutes of the Cyber Defence Unit adopted by the Commander of the Defence League by means of a directive. The commander of the Cyber Defence Unit reports directly to the Commander of Estonian Defence League.

The Commander of the Cyber Defence Unit is subordinated to the Commander of Estonian Defence League, his tasks being outlined in the Statutes of the Estonian Defence League. In addition to the tasks defined in the Statutes, the Cyber Defence Unit Commander's areas of responsibility include aspects related to operational readiness, issues related to the equipment, supplies and other technical means and the education and training of the members of the unit.[56]

The unit has an own staff, led by the Chief of Staff and reporting to the commander of Cyber Defence Unit. The Staff is mostly used for assisting the Cyber Defence Unit commander in planning, analysing, preparing different activities and drawing conclusions. The Staff is manned by both volunteers and paid personnel, and consists of several sections of volunteers dealing with different aspects of Cyber Defence Unit work such as logistics, analyses, training, etc. [57]

The Cyber Defence Unit consists of sub-units or cells, entailing the Cyber Defence Unit's principal operational capabilities. The cells are expected to be able to fulfil tasks related to passive and active cyber defence,[58] as well as organisation and maintenance tasks.[59] Local Cyber Defence Unit cells operate in Tallinn and Tartu; in addition, there is a team of architects whose main task is to do research on necessary technological means, propose new tools and develop the interoperability of various systems.[60]

The Statutes of the Cyber Defence Unit foresee a periodic review and updating of the structure of the Cyber Defence Unit and the description of its functions. The update should take place at least once a year, giving the Commander of the Estonian Defence League the opportunity to specify Cyber Defence Unit's tasking.[61]

The current structure and tasking of the Cyber Defence Unit have not been updated since 2011 and may thus need revision. The procedures, tasking and subordination of different cells and sub-units could be expressed in a more clear fashion; however, certain flexibility in structure and tasking might be beneficial for operational purposes.

[56] Kaitseliidu ülema 18.10.2011 käskkiri nr K-O.2-4/16806u 'Kaitseliidu küberkaitse üksuse funktsioonikirjelduse kinnitamine' (Cyber Defence Unit Directive).
[57] *Id*.
[58] For a more detailed discussion on the substantive tasks of the Cyber Defence Unit, see chapter five of this paper.
[59] *Id*.
[60] *Id*.
[61] *Id*.

4. Membership

General Principles

The principles of membership in the Cyber Defence Unit follow the framework outlined in the Estonian Defence League Act, specifically Chapter 3 ('Members, Their Rights and Duties'), Chapter 6 ('Liability of Members') and Chapter 7 ('Guarantees'). The Act makes very few distinctions with regard to membership in particular structural units; most requirements apply commonly to all members of the Estonian Defence League organisation, including those of the Cyber Defence Unit.

Membership of the organisation normally takes place in the form of *active membership*; in addition, member categories of *youth members*, *supporting members*, and *honorary members* exist.[62] The categories have different qualification requirements and limits to participation in the organisation; however, since this division bears little substantial importance for the functioning of the Cyber Defence Unit, this paper deals with active members only, unless specifically indicated otherwise.

The Estonian Defence League organisation in total (combined with its sub-entities of the women's defence organisation and youth organisations) currently has over 22500 members,[63] with nearly 14000 holding membership of the core organisation. Members of the Cyber Defence Unit form a part of the core organisation; however, their number is not published separately.

Admission and Exclusion

Qualifying Requirements for Membership

The applicable 2013 Estonian Defence League Act defines a minimal and objectively assessable set of criteria for membership: a potential member has to be at least 18 years of age and be an Estonian citizen.[64] More detailed requirements are defined by the 2000 Statutes (currently in force, but to be replaced by new Statutes based on the 2013 Estonian Defence League Act)[65]: in order to apply for active membership in the Estonian Defence League and thereby join the Cyber Defence Unit, the applicant must have an impeccable record, be loyal to the Estonian Republic and recognise the independence and constitutional order of Estonia.[66] By nature, these are morally rather than legally binding criteria that the joining member will pledge adherence to, even though there is possibility to attach certain legal relevance to them.[67]

Specific additional expectations apply for membership in the Estonian Defence League's Cyber Defence Unit. Generally, persons with knowledge and experience in information security can apply

---

[62] KaLS § 25; § 22 (3). A person of 7-18 years of age may become a youth member upon compliance with criteria set forth by law and upon parental consent; however, a youth member can only participate in the activities of the Estonian Defence League youth organisations and cannot belong to the Estonian Defence League's main units, including the Cyber Defence Unit, before the age of 16. A supporting member may be a person that recognises and actively supports the Estonian Defence League's objectives, and an honorary member one whose achievements are of special merit to the Estonian Defence League. Honorary and supporting members do not need to hold Estonian citizenship. *See* KaLS § 25; § 22 (3); § 26-27.

[63] This number reflects total number of individuals holding a membership in the organisation. A person cannot belong to more than one structural unit at a time.

[64] KaLS § 24 (1).

[65] The new Statutes were in the process of drafting by the Ministry of Defence at the time of this analysis, but not yet published for comment. For this reason, this review is based on the 2000 Statutes (*infra*, note 66) which will, according to KaLS § 100, remain in force until replaced.

[66] Vabariigi Valitsuse 13.01.2000 määrus nr 15 'Kaitseliidu põhikirja kinnitamine' (RT I, 19.07.2011, 9) (Statutes of the Estonian Defence League). Section 3.1.

[67] Exclusion from membership is possible on the grounds of the member having submitted false data upon application for membership. See section *Becoming a member; quitting membership* in this Chapter.

for membership. This requirement does not mean exclusively technical knowledge and skills, but can include other areas relevant to cyber security, such as legal or policy experts, educators etc.[68]

Each candidate must have two member referees to recommend his or her candidacy: these persons are also morally responsible for the candidate's suitability.[69] Combined, such measures support the expectation of the Cyber Defence Unit that, rather than being a mass organisation, the unit should constitute a core group of highly professional and trained specialists who will promote cyber security objectives in the wider population.[70]

Factors that disqualify a member candidate (and require the exclusion of a person from membership[71]) include an insufficient health condition, record of disciplinary misconduct or criminal offence, and having knowingly submitted false information upon applying for membership. An applicant may also be refused membership on the grounds of his/her history of inappropriate behaviour or perceived threat to safety.[72]

The current regulation on health requirements was adopted under the previous Estonian Defence League Act[73] and will be applicable until replaced. The regulation makes no distinction with regard to the physical condition of the members of the Cyber Defence Unit; it could be argued that some of the conditions included in the regulation are not reasonable with regard to cyber security experts and may act as an unnecessary barrier to joining the organisation, although they allow for easier administration of membership.[74]

Acquiring Membership

The procedure for acquiring membership is to be defined in the Statutes of the Estonian Defence League, approved by the Government of the Republic.[75] Pending their adoption, the 2000 text is applicable[76]; the following overview is therefore based on the latter, assuming that the principles of acquiring membership are not likely to be substantially altered.

The basis of applying for membership in the Estonian Defence League is a written request, which is to be submitted to the head of the particular Estonian Defence League unit where membership is sought, i.e. directly to the commander of the Cyber Defence Unit.[77] The application is to be supplemented by recommendations of the candidate by one or more existing members[78], and

---

[68] Frequently asked questions, http://www.kaitseliit.ee/en/frequently-asked-questions; The main tasks of the EDL CU, http://www.kaitseliit.ee/en/the-main-tasks-of-the-edl-cu.
[69] *Supra* note 66. Section 3.10; Frequently asked questions, *supra* note 68.
[70] *Id*.
[71] KaLS § 30 (8).
[72] KaLS § 24.
[73] Vabariigi Valitsuse 21.12.1999 määrus nr 406 'Kaitseliidu tegevliikmeks võtmist ja tegevliikmeks olekut takistavate füüsiliste puuete ja psüühikahäirete loetelu ning Kaitseliidu tegevliikmeks võtmise ja tegevliikmeks oleku võimalikkuse asjaolude kindlakstegemise korra kinnitamine'. (Physical and mental disorders that preclude membership in the Estonian Defence League; procedure for ascertaining the physical and mental health condition of member candidates.) RT I 1999, 99, 880.
[74] As member status currently allows for presumption of a certain health condition that makes it possible to participate in all activities of the Estonian Defence League.
[75] KaLS § 5 (1) 3).
[76] KaLS § 100.
[77] *Supra* note 66. Section 3.10.
[78] In case the candidate has no referees, the person may be subjected (in case of his/her consent) to a 'candidacy period' for up to one year of duration. This entitles the candidate to participate in the activities of Estonian Defence League, without, however, having a member's rights or obligations. *See supra* note 66. Section 3.13.

applicants to the Cyber Defence Unit also subject themselves to a background check.[79] A candidate's acceptance to the organisation is decided on the basis of subsidiarity (by the head of the unit where membership is sought) within three months of application.[80] Upon acceptance, an oath of loyalty is taken.[81]

Each member of the Estonian Defence League can belong to only one of the structural units; double roles are not accepted.[82] Hence, a member serving in the Cyber Defence Unit cannot serve simultaneously in the territorial units or the General Staff. This facilitates a clearer focus for both the activities and member profiles: the Cyber Defence Unit therefore brings together key specialists from positions important for national defence, patriotically minded IT-capable individuals, and experts from other fields necessary for cyber security.[83]

Suspension and Termination of Membership

The procedures for suspension, amendment and termination of membership are defined in the Estonian Defence League Act. Membership can be ended either on a voluntary basis by submitting a relevant application, by exclusion due to the member's death or declaration as missing, or by expelling a member. The latter may occur because of the presence or appearance of the disqualifying factors described above, due to neglect of duty, or due to the member committing a disciplinary offence.[84] In the case of leaving or expulsion from the organisation, the former member is required to return any assets that were allocated to him by the Defence League.[85]

Membership in the organisation can also be suspended, either on the member's own initiative or by a decision of an authorised person or body (head of the Cyber Defence Unit) in cases defined by law. Suspension of membership implies a member's removal from all activities in the Cyber Defence Unit; such member is likewise required to return the organisation's assets in his care.[86]

Members' Rights and Duties

Rights and Guarantees

Members' rights include the right to participate in the activities of the Estonian Defence League (and in those of the particular unit that they hold membership in), to enter into an employment or service contract with the Estonian Defence League, wear the Estonian Defence League uniform[87], emblems and insignia, and be informed about the activities of the Estonian Defence League.[88]

The right to participate does not only refer to the status of a member within the Estonian Defence League organisation: in accordance with the law, members may use up to ten days of unpaid leave in order to participate in the activities of the Estonian Defence League, with the possibility to request (partial) compensation which is paid by the Defence League.[89] Likewise, for costs incurred in relation to fulfilling the tasks foreseen for members by law, a compensation mechanism is established.[90]

---

[79] Korduma kippuvad küsimused. Kaitseliit, http://www.kaitseliit.ee/et/korduma-kippuvad-kusimused.
[80] *Supra* note 66. Section 3.12.
[81] *Supra* note 66. Section 3.14-3.15.
[82] KaLS § 22 (2).
[83] Küberkaitse üksus, *supra* note 40.
[84] KaLS § 30 (5)-(8), (11).
[85] KaLS § 30 (12).
[86] KaLS § 29.
[87] The Estonian Defence League has an own uniform, which conforms to the requirements set out in KaLS § 8.
[88] KaLS § 31.
[89] KaLS § 57 (1) and (4).
[90] KaLS § 67.

Members, with the exception of members who are in the active service of the Estonian Defence Forces, also have the right to be elected into the collegial bodies of the Estonian Defence League.[91] Additional criteria may apply as defined by the Estonian Defence League Act and the Statutes.

Members have the right to possess, carry and store at their residence both their personal weapons and those granted by the Defence League, as well as self-defence and special equipment (such as handcuffs). [92] Additional prerequisites apply for handling and use of weapons, including prior training and licencing requirements.[93]

Guarantees apply for members who are injured or die while fulfilling tasks of the Estonian Defence League.[94]

Duties and Responsibilities

Members' duties are defined in a rather generic manner: they include an obligation to defend the independence and constitutional order of Estonia, follow the legal acts outlining the activities and responsibilities of the Estonian Defence League, and look after the property of the Defence League handed into their care.[95]

Members are not *per se* automatically obliged to participate in a particular activity of the Defence League. The voluntary nature of the organisation implies a member's freedom to decide on his or her participation, and the actual involvement of members is enforced by moral rather than regulatory means. On the one hand, the law permits a member of the Defence League to refuse to commence service duty, if he cites compelling reasons, and forbids any disciplinary penalty to be imposed on him for that reason.[96] On the other hand, the member's oath of loyalty, given as membership was acquired, morally binds him to give his best to support the organisation and its objectives.

There appears to be a strong appreciation among the leadership and paid staff of the organisation for the members' commitment to participate in the organisation. In the Cyber Defence Unit especially, members are typically recruited from among valued professionals with strong manifested cyber security skills[97], who often hold demanding jobs with their employer and participate in the activities of the Unit in addition to their working duties and without receiving remuneration. To ensure active participation in the activities of the Cyber Defence Unit, appropriate motivation mechanisms are vital. This includes the quality of the activities, such as training, and meaningfulness of tasking, which regulatory measures cannot effectively replace.

However, once a member has taken up a duty of service, he is, from the moment of commencing the duty until it is considered completed by the person or entity giving the task[98], required to follow a legitimate order of his superior in accordance with the Estonian Defence League Act.[99] The recipient has a right – and in certain cases, an obligation – to refuse unlawful orders as well as those that exceed the authority of the giver or are unrelated to duty, those that require illegal activity or

[91] KaLS § 18 (3), § 19 (3), § 20 (3), § 21 (1); § 31 (2).
[92] KaLS § 42 (1); KaLS § 40 (1).
[93] KaLS § 42 and 43.
[94] KaLS § 58-66.
[95] KaLS § 32.
[96] KaLS § 33 (6).
[97] *Supra* note 68.
[98] KaLS § 33 (3)–(5).
[99] KaLS § 32 (1) 4). Note that the regulation of orders under the Defence League Act is somewhat different from that applicable in the Estonian Defence Forces. The latter will not apply to members of the Estonian Defence League unless they participate in reserve trainings of the Estonian Defence Forces as reservists. KaLS § 34.

activity exceeding the authority of the recipient, and those that demean human dignity or put the life, health or property of persons into unreasonable danger.[100]

While carrying out duties of service, the member is obliged to wear the uniform and insignia of the Estonian Defence League, or wear insignia of the Defence League on his civilian attire.[101]

The non-political nature of the Estonian Defence League and the prohibition of political activities by political parties and other political associations as well as their representatives[102] is also relevant in the context of members' role and activities in the Cyber Defence Unit.

Liability and Disciplinary Action

The general terms of responsibility for conduct apply as set out in national legislation. Members of the Cyber Defence Unit are personally and financially responsible for the means granted to them by the Estonian Defence League, including any firearms and ammunition.[103] Liability may also be incurred under the Law of Obligations Act in case of damage to the rights and interests of the Estonian Defence League.[104]

For disciplinary offences committed, members of the Cyber Defence Unit are liable to disciplinary action under the framework applicable to all members of the Estonian Defence League as defined in Chapter 6 of the Defence League Act. Disciplinary authority lies with the commander of the relevant unit, i.e. the commander of the Cyber Defence Unit.[105] Disciplinary offenses include damage to the image of the Defence League, non-compliance with the legal requirements for members' duties, as well as non-compliance with an order.[106]

While disciplinary liability can only occur if the member is guilty of the commission of a wrongful act (by either intention or (grave) negligence, i.e. (grave) disregard for member duties)[107], complying with an illegal order does not constitute grounds for discharge from responsibility.[108]

[100] KaLS § 38 (1).
[101] KaLS § 32 (1) p 6.
[102] KaLS § 6.
[103] KaLS § 53 (1), 5.
[104] KaLS § 53 (1); võlaõigusseadus, RT I, 11.06.2013, 9 (Law of Obligations Act), § 1043 (with Chapter 53).
[105] KaLS § 53 (3).
[106] KaLS § 53 (2).
[107] KaLS § 53 (11)–(15).
[108] KaLS § 38 (5).

5. Tasks and Deployment

Core and Supplementary Tasks

This chapter will focus on the tasks relevant for the Cyber Defence Unit. However, being a part of the Estonian Defence League organisation, the tasking of the Cyber Defence Unit is largely consistent with the general principles, preconditions, and procedural framework applicable for the overall organisation[109], which merits a brief overview of the overall tasks of the Estonian Defence League in order to provide a context for the more specific activities of the Cyber Defence Unit.

The **core tasks** of the Defence League derive from the purpose of the Estonian Defence League to enhance the nation's readiness to defend the independence of Estonia and its constitutional order, and are defined in § 4 of the Estonian Defence League Act. They include general duties to strengthen the will and capacity to defend the nation, to enhance military defence capabilities and to be involved in improving and ensuring the security of residents. As such, the focus of the activities of the Cyber Defence Unit is not substantially different from the more traditional units of the organisation. § 4 also identifies more specific tasks, some of which – such as the provision of military and related training and education – are well applicable to the Cyber Defence Unit, while others are not directly relevant, such as promoting physical culture and sports among the population or providing guarding support to national defence property and to Estonian foreign representations.[110] In addition, the Defence League may be given other tasks under separate legal acts.[111]

In addition to these core tasks outlined in the Estonian Defence League Act, there are a number of activities where the Estonian Defence League may be engaged, upon need, by other entities. Two such **supplementary tasks** are outlined in the Estonian Defence League Act – namely the involvement in ensuring cyber security under the direction of a competent authority, and participation in the Estonian Defence Forces reserve training sessions; for others, reference is made to other legal acts (briefly identified below in the next paragraph). The task of assistance to ensure cyber security directly concerns the capability of the Cyber Defence Unit; some of the other supplementary tasks (again identified below) are also relevant for the Cyber Defence Unit, while others do not bear a direct significance.

As recognised in the Estonian Defence League Act, the Defence League may be requested to support *police activitie*s in accordance with the Police and Border Guard Act.[112] While the latter Act makes no direct reference to the involvement of the Estonian Defence League, the organisation could be engaged under the general framework for assistance (as stipulated in § 7^{14} of the Police and Border Guard Act) to assist the police in activities related to countering threats and eliminating disturbances. In principle, that could also mean engaging the Cyber Defence Unit for countering cyber threats, provided that the conditions for assistance as outlined in this provision are met.

The Defence League and its members may be requested to assist in resolving major *rescue events*[113] in accordance with the Rescue Act[114], and be engaged in *resolving emergencies*[115], supporting rescue

---

[109] KaLS itself only makes two references to the issue of cyber with regard to tasking.
[110] KaLS § 4 (1).
[111] KaLS § 4 (1) 8). An example is the authorisation to a suitably trained Defence League member to regulate traffic under the Traffic Act (RT I, 02.07.2013, 12), § 8 (3) in certain events.
[112] KaLS § 4 (2) 6). Politsei ja piirivalve seadus, RT I, 02.07.2013, 18. (Police and Border Guard Act; hereafter abbreviated as PPVS).
[113] Incidents that directly endanger the life, health or property of persons or the environment through physical or chemical processes. Päästeseadus, RT I 2010, 24, 115; 29.12.2011, 206 (Rescue Act, hereafter abbreviated as PäS), § 3 (1).
[114] *Id*. Again, the Rescue Act makes no mention Estonian Defence League or its members in particular; the involvement of the Estonian Defence League organisation or individuals in resolving rescue events occurs in

operations and ensuring safety in accordance with the Emergency Act.[116] The potential assignments under these two Acts vary: the Defence League may be tasked to immediate and urgent activities related to countering and eliminating threats and alleviating the effects of rescue events[117]; they may be involved in ensuring safety in an emergency situation area, or used in prevention of damage to objects with high risk of attack, and other similar duties. Under the Emergency Act, the Estonian Defence League may, furthermore, be engaged in the prevention or countering of certain criminal offences, such as the prevention of acts of terrorism (Penal Code[118], § 237)[119], which also includes a cyber component.

Finally, the Estonian Defence League may be engaged in the event of a *state of national emergency* in case of the presence of a threat against the constitutional order of Estonia.[120] An extraordinary condition in itself, the state of national emergency does not automatically emerge in case of the manifestation of the abovementioned circumstances, but has to be declared by the Parliament upon the proposal of the President or the Government of the Republic.[121] Only then can the Estonian Defence League be engaged to fulfil certain tasks. The potential role of the Estonian Defence League in the event of a state of national emergency includes four tasks, of which one is potentially relevant for the Cyber Defence Unit: the prevention and restraining of attacks against objects of vital importance to the state (including attacks against the objects of constitutional bodies).[122] The list is conclusive; however, the Estonian Defence League may simultaneously be engaged to fulfil tasks listed in the Emergency Act as described in the previous section, i.e. the potential task list of the Estonian Defence League during a national emergency is wider than it appears from the State of Emergency Act.

In general, the tasking and involvement options identified above fully apply only to active members (see Chapter 4, *General Principles*).[123] The principle of members' voluntary engagement will apply; any members of the Estonian Defence League ensuring security and safety may also need to have

---

accordance with the general arrangement for volunteer participation in the activities of the national rescue authority (Rescue Board). Engagement is based on the principle of voluntarity, so the Estonian Defence League, likewise, can be involved in rescue activities in case there are volunteers among its members for the particular purpose.

[115] Events similar to rescue events in nature, but characterised by an elevated degree of severity, including severe and extensive disruptions in the continuous operation of vital services. Hädaolukorra seadus, RT I, 30.10.2012, 3 (Emergency Act; hereafter abbreviated as HOS). § 2 (1).

[116] KaLS § 4 (2) 1). For Emergency Act, see *id*.

[117] HOS § 31 (1); PäS § 5 (1) 1).

[118] Karistusseadustik, RT I, 05.07.2013, 10. (Penal Code, hereafter abbreviated as KarS).

[119] HOS § 31 (1) 2)-5).

[120] KaLS § 4 (2) 3); erakorralise seisukorra seadus (State of Emergency Act). RT I, 29.12.2011, 208. (Hereafter abbreviated as ErSS), § 15 (1). Such threats may arise out of a violent attempt to overthrow the constitutional order of Estonia, acts of terrorism, extensive violent pressure activities or inter-group conflicts, or other similar events outlined in the State of Emergency Act.

[121] ErSS § 13. This option has never been used however, not even during the 2007 spring street riots and cyber attacks.

[122] ErSS § 15 (1). The other tasks include restraining of different illegal or violent activities.

[123] KaLS §25 (5), § 27. Youth members cannot be involved in military training or the military aspects of national defence preparation; nor can they be tasked where the Estonian Defence League is engaged in accordance with other laws foreseeing the possibility of reliance on the Defence League – including engagement in ensuring cyber security. The latter is similarly restricted to supporting members, but they can be involved in rescue and emergency tasks. For honorary members, their involvement depends on their status prior to their election to the honorary status. Honorary members elected from active membership are authorised to participate on equal terms with active members; those elected as supporting members or with no prior status in the Estonian Defence League, as well as supporting members, mainly only participate in the core activities of the Estonian Defence League.

undergone relevant training for such activities.[124] This means that the actual extent of assistance available from the Estonian Defence League is dependent on the capability and availability of members – as discussed in the previous chapter, members have a right to refrain from participation in certain circumstances.

Neither the Estonian Defence League Act nor the Wartime National Defence Act specifically addresses the tasks of the Cyber Defence for wartime. The Defence League would be brought directly under the command of the Commander of the Estonian Defence Forces without distinction between the tasks of the two organisations.[125]

Tasks and Activities Relevant for the Cyber Defence Unit

Core Tasks: Education and Training

As described by the Cyber Defence Unit itself, their twofold focus of activities is, on the one hand, to assist civilian structures in peacetime and, on the other hand, to create support capabilities that can be provided in times of crisis.[126] The Cyber Defence Unit's mission is no different from the overall mission given to the Estonian Defence League organisation in this matter – education and training form a core of the Unit's routine activities. This concerns both improving the knowledge, skills, experience and attitude of members[127] to meet the organisation's objectives, as well as increasing cyber security awareness and cyber security among the population.

For members, the Cyber Defence Unit offers training and exercise opportunities on a regular basis. The Unit has organised a number of seminars, information sharing and training events as well as field studies since 2010. The Unit has also participated in and supported several exercises – both cyber defence exercises (such as the annual NATO CCD COE Locked Shields exercise) as well as overall defence and crisis management exercises (such as the Estonian Defence Forces annual Spring Storm exercise) to practice and refine cyber defence skills and information exchange procedures.[128] External training and awareness raising events have also been conducted: in 2011-2012, the Cyber Defence Unit held eight cyber defence seminars for governmental institutions, with another four carried out in or planned for 2013.[129]

Members who belong to the Cyber Defence Unit also participate in military training carried out by the Estonian Defence League and conducted for the entire Defence League organisation. The content and other requirements for military training are outlined by the Commander of the Estonian Defence Forces.[130]

Core Tasks: Strengthening and Ensuring the Security of the Population

The Defence League Act is ambiguous about the involvement of the Cyber Defence Unit and its members in providing consultation, security solution testing and similar expert skills to other parties with the purpose of strengthening and improving their cyber security posture. Indeed, the Cyber Defence Unit has supported various public and private sector entities, such as supplying malware

[124] That is the case for engagement in resolving emergencies, HOS § 33.
[125] SRKS § 4 (1).
[126] Jaagant, *supra* note 15.
[127] KVTS § 6 (1).
[128] Uko Valtenberg. Estonian Defence League - Cyber Defence Unit. *Presentation at CyCon workshop*, 4 June 2013.
[129] *Id.*
[130] KVTS § 6 (2)-(3).

screening solutions for public school computers and assisting with the installation and security testing of the national electronic voting system.[131]

Whether such activities are viewed as part of the core duties of the Estonian Defence League, or as a supplementary task where the Cyber Defence Unit is engaged by a competent public authority, determines the availability of the expert knowledge and skills of the Cyber Defence Unit. In the first case, such involvement is a matter of the organisation's own scope of authority, while in the latter case, their involvement is only possible if certain prerequisites are met, and following a determined procedure.

Regardless of the fact that a specific 'cyber provision' also exists in the task list of the Estonian Defence League, there are arguments in support of the view that not all external cyber security activities should fall under that framework. Non-emergency activities of the Unit which conform to the criteria recognised in the first section of § 4 of the Defence League Act[132] – strengthening and ensuring the security of the residents of Estonia – can be considered to be forming part of the core tasks of the Estonian Defence League. The Defence League is authorised under the Defence League Act to enter into agreements with the purpose of fulfilling its tasks and, if needed, engage other parties for that end.[133] Considering the widespread availability and high take-up margin of online public services, as well as the reliance of residents, economy, and public administration on functioning information systems, it is safe to assume that the security of information systems forms a part of the wide perception of security[134] and therefore meets the criteria set out by the above cited subsection of § 4. Therefore, such activities that involve the offering of professional expertise of the members of the Cyber Defence Unit for preventive purposes can be approached as a matter of the discretion of the Estonian Defence League.[135]

Supplementary Tasks: Cyber Security Assistance

As recognised above, the Estonian Defence League Act foresees the possibility of engaging the Estonian Defence League in ensuring cyber security under the leadership of a competent authority.[136] The arrangement of such involvement is to be defined by government regulation, i.e. in secondary legislation based on the Estonian Defence League Act. A draft of the regulation has been proposed by the Minister of Defence but not adopted at the time of this analysis, so the following discussion is based on the public version of the draft regulation as of April 2013.[137]

---

[131] SNORT for Schools introduced in cooperation with the Estonian CERT: *see* 'Küberkaitseliit aitab Tartu koolide arvutitest tõrjuda kurivara'. Kaitseliit, 09.02.2011. http://www.kaitseliit.ee/et/kuberkaitseliit-aitab-tartu-koolide-arvutitest-torjuda-kurivara; Ainesektsioonide töö kokkuvõte 2011 I pool. http://www.opetajatemaja.ee/index.php?noframe=1&mod=docs&doc=581&h=59f3; Vabariigi Valimiskomisjoni 5.6.2013 kiri nr 22-7/13-7/2 (Letter of the Estonian National Electoral Committee in reply to Eesti Keskerakond memorandum with regard to electronic voting) http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=6a20e142-506a-410a-a151-dcb65b5df950&; Kaitseministeeriumi majandusaasta aruanne 2010, lk 9, p. 6. http://www.kmin.ee/files/kmin/img/files/Majandusaasta_aruanne_2010 (1).pdf; Valtenberg, *supra* note 128.

[132] KaLS § 4 (1) 3).

[133] KaLS § 79 (2) 1), 8).

[134] As defined by the internal security policy adopted by the Parliament. Riigikogu 10.06.2008 otsus 'Eesti turvalisuspoliitika põhisuundade aastani 2015 heakskiitmine' (Internal Security Policy) (RT I 2008, 25, 165).

[135] A public authority viewpoint is also relevant here (there are limits to the tasks that a public administration authority can outsource to an external body). A deeper discussion would however remain beyond the scope of this study.

[136] KaLS § 4 (2).

[137] Vabariigi Valitsuse määrus 'Kaitseliidu kaasamise tingimused ja kord küberturvalisuse tagamisel'. Eelnõu kavand, 22.03.2013. (Draft regulation on the engagement of the Cyber Defence Unit in ensuring cyber security). http://eelnoud.valitsus.ee/main#tALQG5K7.

According to the draft regulation, the engagement of the Estonian Defence League to ensure cyber security under the guidance of a competent governmental body means the involvement, upon prior agreement, of members of the Estonian Defence League identified by the Commander of the Defence League.[138] This would primarily mean qualified members within the Estonian Defence League's Cyber Defence Unit; however, the draft does not explicitly limit such authorisation to the Unit, so in practice the circle could be both wider (suitably skilled members in other, e.g. territorial units) or narrower (one or more members of the Cyber Defence Unit with narrowly specialised skills).

The objective of the Cyber Defence Unit in such engagement is defined in the draft regulation as 'activities intended to ensure the continuous functioning of ICT services or deterring threats against the continuous functioning of such services.' The draft accommodates a wide range of measures, both passive – e. g. data monitoring and malware analysis – as well as active measures, i.e. those of a more preventive nature, including security testing ICT solutions and threat mitigation, but also the prevention of cybercrime.[139]

The draft makes no mention of who the owner of such supported ICT assets and services might be, so it does not preclude assistance to the private sector in protecting their ICT assets as long as such assistance complies with the procedure (discussed below) and the limits outlined in the regulation.

Supplementary Tasks: Cyber Security in Emergency and Crisis

As recognised in the beginning of this chapter, the general framework relating to engaging the Defence League in emergency situations could have specific application to the Cyber Defence Unit. In accordance with the Emergency Act, the Estonian Defence League may be used in prevention of damage to objects with high risk of attack.[140] Such high-risk objects include the territory, buildings and equipment used for the provision of a vital service, the physical damage or destruction of which would significantly impair continuous operation of the entire vital service and which are therefore highly likely to be attacked.[141] The Act does not specifically identify the potential role, once engaged, of the Defence League in general or the Cyber Defence Unit in particular; authorisation is given to the Government of the Republic to decide this on a case-by-case basis.[142] Similarly, the Emergency Act foresees the possibility to engage the Defence League in the prevention or countering of certain criminal offences, including the prevention of acts of terrorism as defined in the Penal Code, which explicitly contains a cyber element: the definition of terrorist crime includes '*interference with computer data or hindrance of operation of computer systems as well as threatening with such acts, if committed with the purpose* to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population'.[143]

Preconditions and Procedure for Engaging the Cyber Defence Unit in Supplementary Tasks

Principles and Preconditions

The role of the Estonian Defence League, in those instances where the law foresees the possibility to engage them, is always in a supplementary capacity, whether this principle is explicitly stated in the particular legal act or constitutes a *de facto* precondition. The Emergency Act permits recourse to

[138] *Id*., § 1 (1).
[139] *Id.*, § 1 (2) and (3).
[140] HOS § 31 (1) 4).
[141] HOS § 41 (1).
[142] HOS § 31 (4).
[143] HOS § 31 (1) 3); KarS § 237 (1) (emphasis added).

the Estonian Defence League if a public authority[144] is unable to complete the task or do so in a timely manner, and if there are no other means for completing the task.[145] The same criteria apply for the engagement of the Cyber Defence Unit under the Estonian Defence League Act.[146] The Emergency Situation Act does not foresee such a precondition explicitly, but applies it *de facto* as the engagement of the Estonian Defence League is outlined as an optional course.[147]

The primary body to determine the necessity of engaging the Cyber Defence Unit would be the State Information System's Authority, whose competence includes the management of state information system security and supervision over the security of nationally critical information systems, as well as coordinating the handling of security incidents in Estonian computer networks.[148] Other bodies to potentially engage the Cyber Defence Unit include the Ministry of Interior (a lead body in both emergency situations and during national emergency[149]); authorities in the area of government of the latter, such as the Police and Border Guard Board, the Rescue Board[150], and the Internal Security Service[151]; as well as other offices bearing internal security tasks.[152]

Private bodies who would like to request the engagement of the Cyber Defence Unit can do so indirectly by approaching the State Information System's Authority or other authorised bodies, who will first have to assess their own capability to address the issue.

Procedure of Decision

According to the *draft regulation*, the (normally written) request to engage the Cyber Defence Unit is made by either the entity responsible for cyber security or that responsible for internal security. The request is to be addressed to the Commander of the Defence League and is to include the purpose of engaging the Cyber Defence Unit, together with an outline of the projected tasking and the presumable timeframe of their engagement. [153]

The engagement of the Cyber Defence Unit is decided by the Commander of the Estonian Defence League, whose discretion has to involve the urgency of the potential threat to critical infrastructure and the possible danger to the health and lives of people as well as to property and environment. The availability of suitably skilled members, the effect of the Unit's engagement on the other tasks of the Defence League, and the foreseeable costs involved are also to be taken into account.[154]

Under both the *Emergency Act* and the *Emergency Situation Act*, the proposal to engage the Estonian Defence League is made by the minister of the interior upon prior coordination with the

---

[144] 'Public authorities' are exclusively identified by law (Public Service Act § 6, Government of the Republic Act § 39 (3)). Generalised, these include all public bodies fulfilling the legislative, executive and judicial functions, including ministries with their subordinated bodies, the Defence Forces, the Offices of the Parliament, President and Government, etc. Avaliku teenistuse seadus, RT I, 26.03.2013, 5 (Public Service Act), Vabariigi Valitsuse seadus RT I, 11.07.2013, 7 (Government of the Republic Act, hereafter abbreviated as VVS).

[145] HOS § 31 (7); PPVS § 7^{14}.

[146] Draft regulation, *supra* note 137, § 1 (4).

[147] ErSS §15 (1).

[148] Majandus- ja kommunikatsiooniministri 25.4.2011 määrus nr 28 "Riigi Infosüsteemi Ameti põhimäärus". RT I, 24.05.2013, 19. § 8.

[149] HOS § 31 (4), § 3 (3); ErSS §15 (2) and § 20 (1).

[150] Based on the draft regulation. The draft mentions the authority responsible for cyber security and the authority responsible for internal security. *Supra* note 137, § 2 (1).

[151] I.e. *Kaitsepolitseiamet*.

[152] VVS § 66; Seletuskiri Vabariigi Valitsuse määruse „Kaitseliidu kaasamise tingimused ja kord küberturvalisuse tagamisel" eelnõu juurde. 02.04.2013, http://eelnoud.valitsus.ee/main#tALQG5K7. (Explanatory Memorandum to the Draft Regulation on Estonian Defence league engagement in cyber security).

[153] Draft regulation, *supra* note 137, § 2 (1)-(3).

[154] *Id*., § 3 (1)–(2).

minister of defence.[155] The engagement of the Estonian Defence League is decided by the Government of the Republic (approval of the President is required for activities under the Emergency Act).[156]

The Emergency Act and the Emergency Situation Act have equal requirements for the decision: the order of the Government to engage the Defence League is to define:

- the task that the Defence League is to be used for;
- the number of members involved;
- the duration of the engagement;
- the territory of their engagement;
- subordination of members while engaged.[157]

The decision is to be forwarded to the Commander of the Defence League and the Parliament notified without delay.[158]

Requirements During Engagement

Members of the Cyber Defence Unit engaged by a competent authority to ensure cyber security will be subjected to a superior appointed by the Commander of the Estonian Defence League or by the commander of the Cyber Defence Unit. The latter in turn will be subjected to the authority of a superior appointed by the authority requesting the engagement of the Cyber Defence Unit.[159]

The chain of command would be similar in the engagement of the Cyber Defence Unit in crime prevention and in protecting high-risk objects under the Emergency Act, as well as in the situation of national emergency: the Commander of the Defence League would subject the Cyber Defence Unit, via the unit commander, to the official appointed by the Government of the Republic.[160]

In addition, the activities of the Cyber Defence Unit in ensuring cyber security would always be carried out under the direction of a competent body specified by law.[161]

Under the Emergency Act, there is a limitation on the length of the period of engagement of the Estonian Defence League – a non-renewable period of 30 days.[162] In situations of national emergency, the Defence League may be used for the entire duration of the national emergency.[163] No time limitations are foreseen under the draft regulation on the engagement of the Cyber Defence Unit.

As for requirements in deployment, members have the right to refuse certain orders (such as those unreasonably endangering the health of persons or the property of the Estonian Defence League, or those requiring skills or abilities that the particular member does not possess); such refusals have to be justified and are subject to an assessment by a superior.[164] While the Estonian Defence League members do not receive salary for their participation, both members as well as the Estonian Defence League organisation may in certain cases require reimbursement for direct and reasonable costs

[155] HOS § 31 (4); ErSS § 15 (2).
[156] HOS § 31 (3); ErSS § 15 (5).
[157] HOS § 32; ErSS § 15 (5).
[158] HOS § 33 (1)–(2); ErSS § 15 (6)–(7).
[159] Draft regulation, *supra* note 137, § 4 (1)–(2).
[160] HOS § 33 (1); ErSS § 15 (6).
[161] KaLS § 4 (2) 4), HOS § 33 (1), ErSS § 18 (4).
[162] HOS § 31 (6).
[163] ErSS § 15 (3).
[164] KaLS § 33 (6)–(8).

incurred due to their engagement.[165] The engaging body is required to ensure the safety of Estonian Defence League members involved.[166]

Means and Resources for Task Fulfilment

By law, various means are foreseen to enable and support carrying out the tasks assigned to the Estonian Defence League. Some of such means have relevance for the Cyber Defence Unit, but the Defence League Act in general does not specifically address supplying the Cyber Defence Unit for carrying out its tasks. As referred to in chapter four, the League has a permanent peacetime military staff that is headed by the Commander of the Defence League and supports the latter in carrying out his tasks.[167] Secondly, for tasks allocated to the Estonian Defence League, the Estonian Defence Forces in collaboration with the Ministry of Defence supply the Estonian Defence League with the necessary equipment. The range of different equipment is defined in law in a rather detailed manner, but does not include ICT assets.[168] Likewise, the Estonian Defence League is entitled to use, free of charge and upon prior coordination, the facilities and equipment of the Estonian Defence Forces,[169] but again, the list of such facilities and equipment makes no reference to ICT infrastructure or supplies. Therefore, the use of external equipment and supplies can occur mainly on a contractual basis by utilising the right to enter into agreements, as defined in § 79 of the Estonian Defence League Act, with the purpose of fulfilling its tasks.

The tasks and activities of the Defence League are funded by revenue from four main sources: membership fees, allocations from the State budget, donations and sponsorship, and contractual revenue from services provided or appropriation of assets.[170]

Some Concluding Remarks

From the various legal acts foreseeing the engagement of the Estonian Defence League, it is apparent that the expectations and procedures are mainly focused on the traditional functions of the Defence League and are yet to adapt to the existence and capabilities of the Cyber Defence Unit within the organisation. With the only exception of the Government Regulation on cyber security assistance yet to be adopted, the potential tasks of the Cyber Defence Unit, or cyber security related tasks of the Estonian Defence League, are not explicitly addressed in the legal acts. This is not necessarily a problem, as long as the legal acts foreseeing the engagement of the Estonian Defence League would enable a definite assessment of whether such engagement includes cyber security assistance or not. While a sufficient level of abstraction allows for flexibility in response and, as such, is beneficial considering the rapidly evolving nature of the cyber environment, the Estonian Defence League is a military-nature organisation, which does not deal well with ambiguity. Uncertainty about the central question of the permissibility of certain activities, as well as the procedural differences contained in the various legal acts, do not facilitate a rapid response to cyber threats.

However, it is also important to understand that the benefit of the Cyber Defence Unit goes beyond their formal activities. Often cited by professionals involved in cyber security services, the cyber security community operates on trust. By participating in the various activities foreseen by law – both training and exercises as well as providing assistance to governmental bodies and critical infrastructure providers – the members of Cyber Defence Unit not only refine their knowledge and skills but create the informal communication channels and relationships of trust that are central to

---

[165] KaLS § 67 (2), Draft regulation, *supra* note 137, § 5.
[166] KaLS § 59 (2).
[167] KaLS § 9 (3).
[168] KaLS § 12 3) identifies arms and ammunition, uniform, and other military equipment.
[169] KLS § 79 (4).
[170] KaLS § 82.

effective cooperation in case of a major cyber incident. Thereby, they not only improve the capability and capacity of the Cyber Defence Unit, but indirectly also contribute to stronger cyber resilience and threat response capability for their employers and the wider society.

6. Legal and Organisational Considerations

The novel concept of using volunteers in national cyber defence raises several legal as well as organisational and policy questions. Among these are questions about supervision over the activities of the Cyber Defence Unit and its individual members, concerns regarding members' access to confidential information, the measures supporting the availability of the Cyber Defence Unit during crises, and the status of members in terms of international law. The items discussed below do not represent a comprehensive list of concerns, but derive from practical observations and the most typically raised questions. Also, the items are in no particular order.

Upon a closer look however, the issues mentioned below constitute challenges rather than inherent shortcomings, and thus should not be viewed as deficiencies of the model but issues requiring awareness, analysis and informed political, strategic, or tactical decision-making.

It can be expected that as the model of the Cyber Defence Unit gains recognition beyond national borders and as its experience base expands, additional questions will arise: whether other countries could ask for assistance from the Cyber Defence Unit; whether and how persons residing outside of the country could participate in the activities of the Unit; and what should be the (reasonable) legal remedies for potential damages to third parties that may occur as a result of activities of the Cyber Defence Unit. While the present paper will not provide an analysis into these issues, they are worth retaining for future consideration in the further development of the concept of the Cyber Defence Unit.

Supervision over the Activities of the Cyber Defence Unit

Given the substantial role of the Cyber Defence Unit in the national cyber defence structure, special attention needs to be paid to ensuring that the procedures related to the Cyber Defence Unit's activities would entail sufficient supervision. Therefore, a frequently recurring question is tied to concerns with ensuring that the Cyber Defence Unit and its members are not engaged in unlawful activities, or in other words, how to make sure that Cyber Defence Unit's activities are legal by nature, proportionate, and within the limits of their competence.

In principle, the current system has such security mechanisms already built into the model of the Cyber Defence Unit, whereas some aspects related to the organisational and individual member level are worth being pointed out separately.

Supervision on the Organisational Level

As explained in the previous chapter, the tasking of the Estonian Defence League, including, in particular, the Cyber Defence Unit, is defined by law, with further detailing in secondary legislation. This means that the Cyber Defence Unit's mandate to act, but also the substantive as well as procedural boundaries for their activities, are given by the Parliament and further specified by the Government and the Minister of Defence in accordance with their competence, which facilitates both transparency as well as controllability.

The Cyber Defence Unit's structure and its hierarchical relation to the Commander of the Defence League as well as the direct chain of command relationship with the Commander of the Defence Forces, its position in the overall national defence system and being ultimately subjected to the President who is constitutionally the supreme commander of national defence[171] form a well-established system of checks and balances. Also, as part of the national defence system, the Defence League fulfils executive power functions of the Estonian Republic and thus falls within the general

[171] Põhiseadus, RT I, 27.04.2011, 2 (The Constitution of the Republic of Estonia; hereafter abbreviated as PS), § 127.

supervision mechanism for executing public authority with accompanying requirements deriving from the Constitution[172], Administrative Procedure Act[173], and other legal acts. According to § 3 of the Estonian Constitution, governmental authority is to be exercised solely pursuant to the Constitution (including Chapter II of the Constitution which defines fundamental rights, freedoms and duties) and laws which are in conformity therewith. The rights and privileges of the Defence League can be extended or restricted only by law[174] and the Defence League is prohibited to carry out any political activities related to political parties and other political organisations.[175] Acts and procedures of the Estonian Defence League can be disputed in court in accordance with § 15 of the Estonian Constitution.[176] In addition, the Estonian Defence League Act foresees the option of extrajudicial challenge proceedings in accordance with the Administrative Procedure Act, in case a person considers their rights to have been violated or freedoms restricted by an administrative act issued by the Estonian Defence League or in the course of administrative proceedings carried out.[177]

By law, the Ministry of Defence exercises state supervision over the Estonian Defence League.[178] Additional sectoral supervisory competence may be held by other state bodies and officials authorised by law – such as the State Audit Office in matters of Estonian Defence League economic activities or the Estonian Defence Forces that supervise the fulfilment of the requirements set by the Commander of the Estonian Defence Forces.[179] In all these occasions, the supervisory body has the right to:

1) request information and documents from the Estonian Defence League,
2) suspend or annul an administrative act or activity of the Defence League, including the Cyber Defence Unit, or
3) require the Defence League to amend an illegal or faulty act or activity.[180]

Suvervision on the Individual Member Level

With regard to supervision over the activities of individual members of the Cyber Defence Unit, there are both legal and social/organisational trust ensuring mechanisms. These include:

a) requirements for joining the organisation, such as a background check and referees *(*see Chapter 4: *Becoming a member, quitting membership*);

b) requirements for the conduct and activities of members, both those stipulated in the Estonian Defence League Act as well as those that members voluntarily subject themselves to upon joining – such as the commitment to consistently participate in the activities of the Defence League (see Chapter 4: *Members' Rights and Duties*);

c) disciplinary liability foreseen in law, including the possibility to expel a member upon breach of law or Estonian Defence League rules of conduct (see Chapter 4: *Liability and Disciplinary Action*).

---

[172] Such as the requirement to exercise governmental authority solely in conformity with the law. PS § 3 (1).
[173] Haldusmenetluse seadus, RT I, 23.02.2011, 8. (Administrative Procedure Act, hereafter abbreviated as HMS).
[174] KaLS § (3).
[175] KaLS § 6.
[176] PS § 15: 'Everyone whose rights and freedoms have been violated has the right of recourse to the courts. Everyone is entitled to petition the court that hears his or her case to declare unconstitutional any law, other legislative instrument or measure which is relevant in the case.'
[177] KaLS § 1 (2); HMS Chapter 5.
[178] KaLS § 85 (2).
[179] KaLS § 85 (1) and (3).
[180] KaLS § 85 (4).

The Cyber Defence Unit has internal monitoring mechanisms to ensure that members do not engage in offensive cyber activities. Externally, when the Cyber Defence Unit is engaged by a competent body as explained in chapter five to support ensuring cyber security, they are accountable to the head of that entity, who also performs supervision of their activities.

Finally, adherence to the requirement and limits stipulated for the activities of the Cyber Defence Unit is ensured by awareness raising among members – the Unit's prime peacetime focus and main area of engagement is training and enhancing preparedness to defend information systems by strengthening the expertise of the unit in information security.

Access to Information

When engaged to support cyber security objectives in accordance with the procedure described in the previous chapter, the Cyber Defence Unit will occasionally have access to the infrastructure of both governmental and private sector entities, and may therefore potentially access data that the requesting party deems confidential, such as commercial or state secrets. More importantly, the possibility of the Cyber Defence Unit effectively offering consultation and support remains limited if the infrastructure owner cannot, for legal reasons or in the fear of damage to his business interests, disclose information about the infrastructure such as its setup, capacity, or vulnerabilities.

Confidential Business Information

Commercial infrastructure owners typically consider details about their infrastructure a commercial secret.[181] The risk of such information becoming available to competitors or becoming public could discourage the affected organisation from turning to the Cyber Defence Unit for assistance in case of a severe incident, which on the one hand, would produce duplication of cyber security efforts and/or deprive the organisation of access to the best available expertise, but on the other hand, may also facilitate spill over of an incident to other, (inter)connected systems.

Normally, giving third parties access to such infrastructure would involve the prior conclusion of a Non-Disclosure Agreement; however, in the event of an actual incident, there may not be time to negotiate such an agreement in a way that would mitigate disclosure risks for the infrastructure owner. Also, major incidents are likely to have unique characteristics in each case, which also affects the content of information that needs protection.

Neither the Estonian Defence League Act nor the draft regulation on Cyber Defence Unit engagement place any obligations on members of the Estonian Defence League with regard to keeping confidential business information, unlike, for example, the Electronic Communications Act that obliges the relevant supervisory authorities to keep confidential information about communications infrastructure that has become known during the fulfilment of official tasks and that the infrastructure owner considers confidential.[182] General obligations arising out of other legal acts, such as the Competition Act which defines the notion of commercial secrets and establishes obligations with regard to keeping commercial secrets, do not cover these relationships. The Penal Code only addresses the unjustified disclosure and use of business secrets of which the person

[181] Konkurentsiseadus, RT I, 05.07.2013, 8 (Competition Act), § 63. The Competition Act gives undertakings significant leeway in defining what they consider a commercial secret. Such a decision would have to be reasoned, and exceptions apply to classifying certain data, but in general, the decision is based on the subjective assessment of the undertaking that the disclosure of certain information may damage its interests. Based on the practice of, e.g. relevant supervisory bodies for electronic communications network operators and service providers (i.e. the Technical Surveillance Authority or the Estonian Competition Authority), information about infrastructure is routinely considered a commercial secret.

[182] ESS § 148 (5) and § 144 (2), § 61.

became aware in connection with his or her professional or official duties, if such act was committed for commercial purposes or with the aim to cause damage.[183]

In the absence of appropriate legal remedies to ensure confidentiality of sensitive data, the affected infrastructure owner's decision to engage the Cyber Defence Unit to assist during a cyber incident will remain a matter of case-by-case risk weighing and prioritisation. Considering the relevance of this problem for many private sector players, defining an obligation of confidentiality in relation to Cyber Defence Unit and infrastructure providers might be both reasonable and beneficial.

State Secrets and Classified Information

Similarly to the private sector, the public sector is also keen to protect information regarding their infrastructure. The State Secrets and Classified Foreign Information Act details a number of items of information concerning security, alarm, communication and information systems, which are to be classified up to the *Confidential* level.[184] Access to them requires a prior security clearance, the obtaining of which is a lengthy procedure consuming up to three or more months[185] and therefore unproductive to be initiated once a crisis situation has already emerged. A solution would be that at least a critical amount of members of the Cyber Defence Unit, based on voluntarity, go through the security screening procedure and obtain a security clearance. This would place a certain administrative burden upon the Estonian Defence League to analyse and implement clearance mechanisms in accordance with the State Secrets and Classified Foreign Information Act, but the maintenance of such system would not necessarily demand significant additional resources from the Estonian Defence League. Actual access of Cyber Defence Unit members to classified information would anyway be determined by the infrastructure owner on a 'need to know' basis, judging each case separately, so issuing security clearance to Cyber Defence Unit members would not generate a security risk *per se*.

Resource Availability

Cyber Defence Unit as a Voluntary and Supplementing Capacity

As discussed in Chapter 5, the Cyber Defence Unit offers specialised cyber defence expertise in three main ways: training and exercises, cyber security assistance in peacetime, and cyber security assistance in emergencies and crises (including the special case of a state of national emergency under the State of Emergency Act). In this paragraph, the availability of resources for these tasks is discussed. Possible issues centre round the type of resource that is the most valuable and unique in the Cyber Defence Unit: its members, the cyber defence experts.

Regarding the availability of personnel, it is important to emphasise that the Cyber Defence Unit is a *voluntary* unit where members both join and are deployed on a voluntary basis. As noted in the previous chapter (see Chapter 5, *Preconditions and Procedure for Engaging the Cyber Defence Unit in Supplementary Tasks*), the role of the unit is primarily a *supplementary* one. Based on the Estonian Defence League Act, the League, and the Cyber Defence Unit, will be engaged 'when needed'.[186] The draft regulation on involving Estonian Defence League in ensuring cyber security proposes additional cumulative criteria, i.e. both have to be manifested at the same time: the Estonian Defence League

[183] KarS § 377.
[184] Riigisaladuse ja salastatud välisteabe seadus, RT I, 22.12.2011, 24. (State Secrets and Classified Foreign Information Act, hereafter abbreviated as RSVS), § 10.
[185] RSVS § 33 (3)–(4).
[186] KaLS § 4 (2).

(in practice, the Cyber Defence Unit) may be engaged when the 'responsible governmental entity is unable to timely fulfil its task', and when there are 'no other means for completing the task'.[187]

The Cyber Defence Unit therefore cannot be regarded as being the sole or even main entity to provide the nation's cyber security. Even in emergencies and crisis situations, the engagement of the unit will be as an additional, supplementary capacity, and only when needed.

Availability of the Cyber Defence Unit members

With regard to the Cyber Defence Unit's task to provide or support training and exercises, the rule to only engage on a voluntary basis does not seem to raise an issue. The same goes for the task of providing cyber security assistance in peacetime. Training and exercises and other 'peacetime' activities to support civilian (and military) entities can be planned ahead and – if necessary – can be coordinated with the members' employers.

The Cyber Defence Unit can also be engaged in case of an emergency or crisis. Based on the current model, one cannot fully rely on the availability of the unit members to provide assistance in those cases. In crisis situations, deployment is still voluntary. Moreover, in the event of a major cyber incident or crisis, the members of the Cyber Defence Unit are likely to have urgent tasks and responsibilities at the organisation where they hold their 'day job', be it a governmental post or a private sector company, e.g. a provider of critical (information) infrastructure.

The role of the Cyber Defence Unit is seen as supplementary to the role of the responsible governmental entity, in peacetime as well as in emergency situations and crises. However, as stated above, also in emergencies and crises the Cyber Defence Unit is only to be engaged 'when needed', and, anticipating the proposed regulation on involving the Cyber Defence Unit, it may be engaged when the responsible government entity is 'not able to fulfil its task (in a timely fashion)' and has 'no other means for completing the task' available. Rather than merely supplying additional capacity, the unit is therefore likely to be engaged to provide specialised expertise that the affected or requesting entities do not otherwise possess. This means that, despite the fact that its role is intended to be supplementary, the Cyber Defence Unit's contribution would be unique, and non-availability of personnel could affect the ability to conduct successful cyber defence. Hence, the current purely volunteer model may not fully correspond with the possible needs in times of emergency and crisis.

A way to remedy this shortcoming could be to conclude agreements with the employers of key members in order to assure their availability in crisis situations. Yet, a contractual solution is likely to remain limited, as such employers cannot reasonably be expected to not include in the agreement a *force majeure* clause to excuse non-performance in case of unforeseeable crisis situations – i.e. exactly those circumstances when the government entities would most likely wish to rely on the Cyber Defence Unit's assistance. Therefore, it may be sensible to consider additional legislative guarantees for members (and their employers) participating in cyber defence activities during crises, as distinguished from those applicable for participation in the regular activities of the Estonian Defence League, such as training.[188] The Estonian Defence League Act currently does not distinguish between the 'normal' and crisis regimes, yet the guarantees in the current Act are weaker than those recognised in the 1999 Act. Furthermore, neither the Emergency Act nor the Emergency Situations Act address the issue of employers' duties with regard to their employees who are members in the Defence League, or provide any support to employers who would be willing to 'lend' their experts during crisis situations.

[187] Draft regulation, *supra* note 137, § 1 (4).
[188] For existing guarantees, *see* Chapter 4, *Members' Rights and Duties.*

On the other hand, these limits to the availability of members are not to be viewed as an inherent fault or shortcoming of the model *per se*. Non-availability should be taken into account in the cyber defence preparation and planning. It shifts the focus of activities from 'recruiting as many people as possible to carry a central role in cyber crisis', to ensuring the quality of the more routine daily activities of the Cyber Defence Unit, such as training, and also building the network of experts who are likely to communicate effectively in a cyber crisis situation. It is worth recalling that effective cooperation was viewed as a key factor to the success of responding to the cyber attacks that hit Estonia in 2007, and has since time and again been emphasised as a crucial element for mitigating attacks, e.g. by major botnets.[189]

Status During International Armed Conflict

International Armed Conflict

As discussed in the previous chapters, the Cyber Defence Unit members are entitled to wear a uniform, have the right to possess and carry arms, and are subject to disciplinary authority. However, the Cyber Defence Unit is not a military unit and its members are not soldiers. The question then arises what the legal status of members of the Cyber Defence Unit would be during an international armed conflict. Would they be combatants, and if so, how would that be relevant?

'An international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations, occurring between two or more states.'[190] The law of armed conflict is the body of law that regulates the conduct during armed conflicts, including, potentially, the use of cyber methods and means of warfare, and consists of international treaties, such as the Geneva Conventions and Hague Conventions, as well as case law and customary international law. It defines the conduct and responsibility of States and individuals engaged in hostilities, and provides protective status to certain categories of persons and objects.

Combatant Status

The law of armed conflict does not prohibit any category of persons from participating in an international armed conflict, including cyber operations, but does tie participation to different legal consequences, depending on the category to which an individual belongs. For combatants, it means certain forms of protection, but they are also considered as legitimate targets of attack. Combatants are entitled to combatant immunity, that is, they may not be prosecuted for having engaged in belligerent acts that are lawful under the law of armed conflict. For instance, a combatant who conducts cyber operations that violate domestic criminal law may not be prosecuted for such actions as long as they are carried out in compliance with the law of armed conflict. (Those individual members who commit war crimes retain their combatant status, but may be tried for these crimes.) Combatants are also entitled to treatment as prisoners of war upon capture.[191]

The law of armed conflict defines conditions for combatant status.[192] There are basically two categories:

---

[189] See, e.g. Conficker Working Group: Lessons Learned. June 2010 (Published January 2011). http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf, p. 17; Tikk, Kaska, Vihul, *supra* note 8.

[190] Tallinn Manual on the International Law Applicable to Cyber Warfare, Michael N. Schmitt, gen. ed., Cambridge University Press, 2013. Rule 22, p. 79.

[191] Geneva Convention III, especially Parts II and III.

[192] Geneva Convention III, Art. 4A (1) and (2). Strictly speaking, these criteria only define who is entitled to prisoner of war treatment. They are however generally accepted as criteria for combatant status.

- members of the *armed forces* of a Party to the conflict as well as *members of militias or volunteer corps forming part of such armed forces* are combatants;
- members of *other militias* and members of *other volunteer corps*, including those of organised resistance movements, belonging to a Party to the conflict, must, to be recognised as combatants, fulfil four conditions:
    - being commanded by a person responsible for his subordinates;
    - wearing a distinctive emblem or attire that is recognisable at a distance;
    - carrying arms openly; and
    - conducting operations in accordance with the law of armed conflict.

Although in Geneva Convention (III), Article 4A, the four conditions are set for the second category, there is a widespread view that they also apply to the first category, i.e. that members of the armed forces, and members of militias or volunteer corps forming part of such armed forces also have to meet the four conditions to qualify for combatant status.[193]

Members of the armed forces and members of the organised armed groups as referred to, that do not fulfil the four conditions, and civilians that directly participate in hostilities, will be considered 'unprivileged belligerents' that will not have combatant status and will therefore not be entitled to combatant immunity or to be treated as a prisoner of war. They can lawfully be targeted however.

The qualification of a civilian 'directly participating' in hostilities entails three cumulative criteria: the act carried out by the individual must have the intended or actual effect of negatively affecting the adversary's military operations or capabilities, or alternatively, inflicting death, physical harm, or material destruction on persons or objects protected against direct attack; there must be a direct causal link between the act in question and the harm intended or inflicted; and the acts must be directly related to the hostilities.[194]

Cyber Defence Unit and Combatant Status

The members of the Cyber Defence Unit would have to fulfil the conditions described above in order to have combatant status in a situation where Estonia is a Party to an international armed conflict.

Do members of the Cyber Defence League belong to the first category? In peacetime, the Estonian Defence League and its Cyber Defence Unit are not part of the Estonian Defence Forces.[195] In wartime, in accordance with the Wartime National Defence Act, the Commander of the Estonian Defence Forces assumes command of both organisations.[196] For this to occur, a 'state of war' has to be declared by the Parliament or the President of the Republic.[197] Being under the command of the Commander of the Defence Forces is not exactly the same as 'forming part of such armed forces'. However, that probably doesn't preclude the Estonian Defence League, after a declaration of the 'state of war', to be considered as part of the armed forces. In that case the Cyber Defence Unit members would belong to the first category of combatants; the unit would be a 'volunteer corps forming part of the armed forces'.

---

[193] There is a dissenting view that says that they are combatants by default regardless of whether they fulfil the four conditions or not. See also: *supra* note 203, p. 97.
[194] *Id*., p. 119.
[195] The relationship between the Estonian Defence League and the Estonian Defence Forces is described in the first three chapters of this paper. *See*: Chapter 1, *Estonian Defence League,* Chapter 2 *Legal Status of the Estonian Defence League and its Place in the National Defence Organisation*, and Chapter 3).
[196] SRKS § 4 (1) and § 12 (2) 1).
[197] SRKS § 2 and 3.

Apart from that it is of course possible that individual Cyber Defence Unit members are mobilised in the Estonian Defence Forces.

In case the 'state of war' has not been declared, and therefore the Estonian Defence League, and its Cyber Defence Unit, has not been brought under the command of the Commander of the Estonian Defence Forces, or the Cyber Defence Unit members otherwise are not recognised as 'combatants of the first category', would they still belong to the second category of combatants? They would have to meet the conditions as specified.

As to the requirement of 'belonging to a Party' – this means at least a *de facto* relationship between the organised group and a Party to the conflict, be it via agreement with the State or by factual behaviour that makes clear for which party the group is fighting. The Estonian Defence League and its Cyber Defence Unit are installed by the State and perform functions in support of or on behalf of the State. One can safely conclude that the Cyber Defence Unit, in conducting its legally based tasks, is 'belonging to a Party'. Regarding the four other conditions, the following can be concluded:

a) They are *'commanded by a person responsible for his subordinates'*. This requirement is built into the very model of the Estonian Defence League, including the Cyber Defence Unit, as addressed in chapters four and five of this paper.

b) They *'wear a distinctive emblem or attire that is recognisable at a distance*'. This typically means that the individuals wear a uniform. This requirement serves to have a clear distinction between combatants as legitimate targets and civilians, who are not legitimate targets. One could adopt the view that there is no reason why this requirement would not apply to individuals engaged in cyber operations.[198] The fact that the operations are conducted far behind the frontline and without using firearms doesn't mean that the military-civilian distinction is not important. (A parallel can be drawn to a military logistic unit working far behind the front, where wearing of the uniform is not an issue of debate.) The Estonian Defence League members have a uniform[199]; the requirements for wearing it are to be defined by the Commander of the Defence League[200], and it would be prudent to consider the aspect of military-civilian distinction in the requirements.

c) They '*carry arms openly*'. This requirement also serves the purpose to distinguish combatants and civilians. However, it does not seem to be relevant with regard to cyber operations.[201]

d) Their '*conduct of operations is in accordance with the law of armed conflict*', which, based on the above, would prove the decisive criterion for determining the status of members of the Cyber Defence Unit as combatants. Members of the Cyber Defence Unit who do not meet these criteria would be considered 'unprivileged belligerents'.

An issue may arise out of those members of the Cyber Defence Unit who are neither mobilised nor *de facto* performing under the command of the Commander of the Estonian Defence Forces, but continue their assignment in cyber security services, e.g. at the critical infrastructure provider ensuring the supply of vital services to the population. Their situation is not that clear. As long as they keep their membership in the Cyber Defence Unit, and they fulfil the four conditions (commanded by a person responsible for his subordinates, distinctive emblem or attire, carry arms openly, and conduct in accordance with the law of armed conflict), there are sufficient reasons to regard them as combatants.

---

[198] This was what the International Group of Experts that prepared the 'Tallinn Manual' concluded. *Supra* note 190, p. 99.
[199] KaLS § 8.
[200] Id., section 2.
[201] *Supra* note 190, p. 100.

Summary

The Cyber Defence Unit of the Estonian Defence League is a national collaboration model for cyber security professionals, structurally integrated into the Estonian voluntary paramilitary national defence organisation, the Estonian Defence League. In line with the purpose of the Estonian Defence League to enhance the national defence capability and readiness, the Cyber Defence Unit works to ensure the secure functioning of national information infrastructure, enhancing national cyber security cooperation and strengthening cyber defence support capabilities that can be provided in crisis.

The Cyber Defence Unit builds on two national phenomena. One is the well-established national private-public ICT security cooperation, which spans over nearly two decades since the early days of publicly available online services and proved itself strong in the 2007 cyber attacks against Estonia. Another is the long-existing volunteer national defence tradition, manifested in the Estonian Defence League organisation which has a clearly defined organisational structure, principles and pattern of operation, and a sizeable membership. In such an environment, the emergence of a bottom-up initiative to support national defence and security objectives with regard to the emerging security threats from the ICT environment can be regarded as a rather organic development. The choice to include a volunteer cyber defence expert corps in the existing volunteer national defence organisation has allowed the organisation to benefit from the support of an established structure both organisationally, regarding funding, and in terms of a legal framework for their management and activities.

The Estonian Defence League, of which the Cyber Defence Unit is a part, is a legal person under Estonian law with a distinct place in the organisation of national defence as defined by the Constitution and the Peacetime and Wartime National Defence Acts. Its functioning and activities are governed by a specific law – the Estonian Defence League Act – that defines the organisation as a voluntary national defence organisation, which operates in the area of government of the Ministry of Defence, is militarily organised, possesses arms, engages in military exercises and fulfils functions laid upon it by law.

The overall purpose of the Estonian Defence League in general – likewise applicable to the Cyber Defence Unit – is to enhance the preparedness of the population to defend the independence of Estonia and its constitutional order by relying on free will and self-initiative. In line with this general purpose, the Cyber Defence Unit seeks 'to protect Estonia's high-tech way of life by protecting information infrastructure and supporting the broader objectives of national defence'[202] with a threefold objective: developing a cooperation network of cyber experts, strengthening the security of critical information infrastructure, and promoting cyber security awareness.

The Cyber Defence Unit is integrated into the Estonian Defence League, constituting one of the structural units of the latter. It has its own staff, manned by both volunteers and paid personnel, and consists of sections dealing with both administrative aspects of the Unit's operation and tasks related to cyber defence. The Unit is led by a commander subordinated to the Commander of Estonian Defence League. The latter is appointed by the national government and is, for the purposes of military command, subjected to the authority of the Commander of the Estonian Defence Forces. However (referring to the peacetime situation), the role of the Commander of the Defence Forces towards the Defence League is limited, by law, to aspects of military capability, and not used for the administration of the Estonian Defence League, which remains a unique combination of a non-governmental organisation and military command.

Membership of the Estonian Defence League, and likewise of the Cyber Defence Unit, is based on the principle of voluntarity – this applies to joining and leaving the organisation, but also to

[202] Estonian Defence League's Cyber Unit. The Defence League, http://www.kaitseliit.ee/en/cyber-unit.

members' participation in the activities of the Unit. A person wishing to join the Cyber Defence Unit must meet the age and citizenship requirements defined by law; he must have a sufficient health condition, a clean record and a good moral standing. The Cyber Defence Unit expects their potential members to possess knowledge and experience in information technology or in other relevant disciplines; however, rather than looking to build a mass organisation, the focus is on a high professional qualification and the creation of an efficient and reliable cooperation network. Membership can be sought by application, backed by references of existing members, the head of the Unit being authorised to decide on acceptance. Membership can be suspended or terminated either upon a member's own initiative, or upon the initiative of the Estonian Defence League due to the failure of the member to comply with membership requirements and for disciplinary offences.

Members give an oath of loyalty to undertake to defend the independence and constitutional order of Estonia, follow the legal acts outlining the activities and responsibilities of the Defence League, and look after the property of the Defence League handed into their care; yet, they are not automatically obliged to participate in a particular activity of the Estonian Defence League. Participation is ensured by moral rather than regulatory means; refusal to participate may not entail a disciplinary penalty to the member. Once a member has taken up a duty of service, however, he is, from the moment of commencing the duty until it is considered completed by the person or entity giving the task, required to follow a legitimate order of his superior, while having the right (and in certain cases, an obligation) to refuse unlawful orders.

The tasks of the Estonian Defence League occur in two main categories: *core tasks,* detailed in the Estonian Defence League Act, with the focus on enhancing the nation's defence readiness and capability and ensuring the security of the residents, and *supplementary tasks*, where the Estonian Defence League is engaged to assist another governmental body in specific situations – primarily to provide support in emergency and crisis. Both the core tasks and the supplementary tasks have specific relevance for the Cyber Defence Unit. Similarly to the Estonian Defence League in general, the Cyber Defence Unit participates in military and related training and education, with specific attention on improving the knowledge, skills, experience and attitude of members to meet the organisation's objectives, as well as increasing cyber security awareness and cyber security among the population. In the framework of the core task of strengthening and ensuring the security of the residents, the Cyber Defence League is also entitled to provide cyber defence expert skills to other national entities with the purpose of strengthening and improving their cyber security posture.

In addition, the Estonian Defence League may be engaged to help ensure cyber security under the leadership of a competent authority. Such engagement entails activities to safeguard the continuous functioning of ICT services and deter threats against them, by means of both passive (such as data monitoring and malware analysis) and active measures (such as security testing ICT solutions and threat mitigation). In more severe cases of crisis or national emergency, other legal acts also foresee the possibility of engaging the Estonian Defence League, and these provisions can also be largely applied to the Cyber Defence Unit's assistance. Recipients of such assistance could be both public and private sector entities; however, the circle of requesting entities is delimited by legislation, and certain preconditions and procedural requirements apply for engaging the Defence League in general and the Cyber Defence Unit in particular.

Members' participation in both the core and the supplementary tasks of the Estonian Defence League will remain subject to the principle of voluntarity; at the same time, their participation is supported by legislative guarantees, including the right to non-paid leave and compensation for costs incurred. Members do not receive salary for their engagement in the activities of the Defence League. For these reasons, the participation of the Estonian Defence League is viewed as a supplementary capacity – the Defence League is engaged on the twofold condition that the particular State authority is unable to complete the tasks (in a timely fashion) and that there are no other means for completing the task at hand.

In war time, the Estonian Defence League would be brought directly under the command of the Commander of the Estonian Defence Forces, without distinction between the tasks of the Defence League and the Estonian Defence Forces.

Certain legal, organisational and policy considerations that have arisen with regard to the Cyber Defence Unit and its operation are discussed in the final chapter of the paper. These recurring questions have centred on the supervision over the activities of the Cyber Defence Unit and its individual members, concerns regarding members' access to confidential information, measures supporting the availability of the Cyber Defence Unit during crisis, and the status of members during an international armed conflict. Each of these topics is addressed in the chapter within the context of applicable law, highlighting main issues of concern and providing proposals for a potential course of remedy with the purpose of promoting awareness, analysis and informed decision-making. The last chapter also identifies some questions that are likely to arise as the model of the Cyber Defence Unit gains recognition beyond national borders and as its experience base expands, and retains them for future consideration.

To conclude, it is observable that the Cyber Defence Unit in its current form is an emerging and evolving capability that is in the process of being fully established within the formal legal system, but the model is not yet a final product; in fact, the founders and leaders of the organisation refer to the current setup as an 'experimental structure'.[203] Furthermore, the discussion of the place and role of the Cyber Defence Unit in the national defence capability requires continuing engagement from interested parties. Considering the bottom-up emergence of the model, the voluntary nature of the Estonian Defence League organisation into which the Cyber Defence Unit is integrated, and its role as an enhancer of existing collaborations and refiner of earlier collaborative models, an incentive-based approach will remain to have a strong role in the further development of the organisation.

[203] E.g. General (Ret.) Johannes Kert in the NATO CCD COE Workshop 'Voluntary Participation in National Cyber Defence', 4 June 2013.

Glossary of Abbreviations

CERT	Computer Emergency Response Team
ErSS	State of Emergency Act
HMS	Administrative Procedure Act
HOS	Emergency Act
KaLS 1999	Estonian Defence League Act
KaLS	Estonian Defence League Act
KarS	Penal Code
PäästeS	Rescue Act
PPVS	Police and Border Guard Act
PS	The Constitution of the Republic of Estonia
RRKS	Peacetime National Defence Act
RSVS	State Secrets and Classified Foreign Information Act
SRKS	Wartime National Defence Act
VVS	Government of the Republic Act

Bibliography

Legal Acts

International Law Instruments

Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949.

Acts Adopted by the Parliament

Avaliku teenistuse seadus (ATS) (*Civil Service Act*). Adopted 13 Jun 2012, entry into force 01 Apr 2013; RT I, 06.07.2012, 1.
Unofficial English translation (consolidated text as of 1 April 2013)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=2013X11&keel=en&pg=1&ptyyp=RT&tyyp=X&query=avaliku+teenistuse

Eesti Vabariigi põhiseadus (PS) (*The Constitution of the Republic of Estonia*). Adopted 28 June 1992, entry into force 03 Jul 1992, RT I, 27.04.2011, 2.
Unofficial English translation (text with July 2011 relevance)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X0000K2&keel=en&pg=1&ptyyp=RT&tyyp=X&query=p%F5hiseadus

Elektroonilise side seadus (ESS) (*Electronic Communications Act*). Adopted 08 Dec 2004, entry into force 01 Jan 2005. RT I, 05.07.2013, 3
Unofficial English translation (consolidated text as of 15 July 2013)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X90001K8&keel=en&pg=1&ptyyp=RT&tyyp=X&query=elektroonilise+side

Erakorralise seisukorra seadus (ErSS) (*State of Emergency Act*). Adopted 10 Jan 1996, entry into force 16 Feb 1996, RT I, 29.12.2011, 208.
Unofficial English translation (text with August 2002 relevance)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XX10024&keel=en&pg=1&ptyyp=RT&tyyp=X&query=Erakorralise+seisukorra+seadus

Hädaolukorra seadus (HOS) (*Emergency Act*). Adopted 15 Jun 2009, entry into force 24 Jul 2009, RT I, 30.10.2012, 3.
Unofficial English translation (consolidated text as of 1 April 2013)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXX26K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=h%E4daolukorra

Haldusmenetluse seadus (HMS) (*Administrative Procedure Act*). Adopted06 Jun 2001, entry into force 01 Jan 2002; RT I, 23.02.2011, 8
Unofficial English translation (consolidated text as of 1 January 2012)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40071K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=haldusmenetluse

Kaitseliidu seadus (KaLS 1999) (*Estonian Defence League Act*). Adopted on 8 Feb 1999, entry into force 05 Mar 1999. RT I, 08.07.2011, 48
No English translation available.

Kaitseliidu seadus (KaLS) (*Estonian Defence League Act*). Adopted 28 Feb 2013, entry into force 01 Apr 2013, RT I, 20.03.2013, 1.
No English translation available.

Kaitseväeteenistuse seadus (KVTS) (*Military Service Act*). Adopted 13 June 2012, entry into force 01 Apr 2013, RT I, 02.07.2013, 7.
No English translation available.

Karistusseadustik (KarS) (*Penal Code*). Adopted 06 June 2001, entry into force 01 Sep 2002, RT I, 05.07.2013, 10.
Unofficial English translation (consolidated text as of 1 June 2013)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K11&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusseadustik

Konkurentsiseadus (KonkS) (*Competition Act*). Adopted 05 June 2001, entry into force 01 Oct 2001, RT I, 05.07.2013, 8.
Unofficial English translation (consolidated text as of 15 July 2013)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X50066K9&keel=en&pg=1&ptyyp=RT&tyyp=X&query=konkurentsiseadus

Liiklusseadus (LS) (*Traffic Act*). Adopted 17 Jun 2010, entry into force 01 Jul 2011; RT I, 02.07.2013, 12.
Unofficial English translation (consolidated text as of 1 July 2013)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXXXX10K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=liiklusseadus

Politsei ja piirivalve seadus (PPVS) (*Police and Border Guard Act*). Adopted 6 May 2009, entry into force 01 Jan 2010 (partially 1 Jan 2012); RT I, 02.07.2013, 18.
Unofficial English translation (consolidated text as of 1 September 2013)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=2012X03K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=politsei

Päästeseadus (PäästeS) (*Rescue Act*). Adopted 05 May 2010, entry into force 01 Sep 2010. RT I, 29.12.2011, 206.
Unofficial English translation (consolidated text as of 1 January 2012)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=2012X23&keel=en&pg=1&ptyyp=RT&tyyp=X&query=p%E4%E4steseadus

Rahuaja riigikaitse seadus (RRKS) (*Peacetime National Defence Act*). Adopted12 June 2002, entry into force 15 Aug 2002. RT I, 20.03.2013, 23
Unofficial English translation (consolidated text as of 1 April 2013)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X90030K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=riigikaitse+seadus

Riigisaladuse ja salastatud välisteabe seadus (RSVS) (*State Secrets and Classified Foreign Information Act*). Adopted 25 Jan 2007, entry into force 01 Jan 2008; RT I, 22.12.2011.
Unofficial English translation (consolidated text as of 1 January 2012)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXX0007K3&keel=en&pg=1&ptyyp=RT&tyyp=X&query=riigisaladuse

Sõjaaja riigikaitse seadus (SRKS) (*Wartime National Defence Act*). Adopted28 Sep 1994, entry into force 31 Oct 1994, RT I, 10.07.2012, 33
No English translation available.

Tsiviilseadustiku üldosa seadus (TSÜS) (*General Part of the Civil Code Act*). Adopted 27 Mar 2002, entry into force 01 July 2002, RT I, 06.12.2010, 12.
Unofficial English translation (consolidated text as of 5 April 2011)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30082K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=tsiviilseadustiku

Vabariigi Valitsuse seadus (VVS) (*Government of the Republic Act*). Adopted 13 Dec 1995, entry into force 01 Jan 1996, RT I, 11.07.2013, 7.
No English translation available.

Võlaõigusseadus (VÕS) (*Law of Obligations Act*). Adopted 26 Sep 2001, entry into force 01 Jul 2002, RT I, 11.06.2013, 9.
Unofficial English translation (consolidated text as of 1 May 2013)
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30085K6&pg=1&tyyp=X&query=v%F5la%F5igusseadus&ptyyp=RT&keel=en

Secondary National Legislation

Government of the Republic

Vabariigi Valitsuse 28.04 1992. a määrus nr 128 'Kaitseliidu kohast riigi kaitsesüsteemis' (The Place of the Estonian Defence League in the National Defence System). RT 1992, 18, 261; RT I 2000, 4, 31

Vabariigi Valitsuse 21.12.1999 määrus nr 406 'Kaitseliidu tegevliikmeks võtmist ja tegevliikmeks olekut takistavate füüsiliste puuete ja psüühikahäirete loetelu ning Kaitseliidu tegevliikmeks võtmise ja tegevliikmeks oleku võimalikkuse asjaolude kindlakstegemise korra kinnitamine' (Physical and mental disorders that preclude membership in the Estonian Defence League; procedure for ascertaining the physical and mental health condition of member candidates.) RT I 1999, 99, 880

Vabariigi Valitsuse 13.01.2000 määrus nr 15 'Kaitseliidu põhikirja kinnitamine' (Statutes of the Estonian Defence League). RT I, 19.07.2011, 9.

Vabariigi Valitsuse 20.01.2011. a määrus nr 16 'Vabariigi Valitsuse määruste muutmine seoses Kaitseliidu küberkaitse üksuse loomisega' (Amending Government Regulations in relation to the Establishing of the Cyber Defence Unit). RT I, 25.01.2011, 3.

Minister of Economics and Communications

Majandus- ja kommunikatsiooniministri 11.09.2003 määrus nr 224 'Riigi Infosüsteemide Arenduskeskuse põhimäärus' (Statute of the Estonian Informatics Centre) (RTL 2004, 158, 2375)

Majandus- ja kommunikatsiooniministri 25.4.2011 määrus nr 28 'Riigi Infosüsteemi Ameti põhimäärus' (Statute of the Estonian Information System's Authority) RT I, 24.05.2013, 19.

National Policy Instruments

Eesti turvalisuspoliitika põhisuundade aastani 2015 heakskiitmine (Estonian National Security Policy). Adopted 10 June 2008. RT I 2008, 25, 165.

Vabariigi Valitsuse 08.05.2008 korraldus nr 201 'Küberjulgeolekustrateegia' (Cyber Security Strategy). RTL 2008, 40, 563. *Unofficial English translation*
http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

Vabariigi Valitsuse 31.12.2010 korraldus nr 515 '"Riigikaitse strateegia" heakskiitmine'. (National Defence Strategy) RT III, 05.01.2011, 7. *Unofficial English translation*
http://www.kaitseministeerium.ee/files/kmin/img/files/KM_riigikaitse_strateegia_eng(2).pdf

Vabariigi Valitsuse 24.01.2013 korraldus nr 35 'Riigikaitse arengukava 2013-2022'. (National Defence Development Plan 2013–2022) RT III, 29.01.2013, 8. *Unofficial English translation of the summary*
http://www.kaitseministeerium.ee/files/kmin/nodes/13373_NATIONAL_DEFENCE_DEVELOPMENT_PLAN_2013.pdf

Other Sources

'Arvutikaitse 2009' koostööleping (Memorandum of Understanding for 'Computer Security 2009'. Tallinn, 23 May 2006. http://www.arvutikaitse.ee/wp-content/uploads/2006/12/arvutikaitse2009_lepingu_tekst.pdf

1940. aasta kuum suvi. Kaitseliit. http://www.kaitseliit.ee/et/1940.-aasta-kuum-suvi

Ainesektsioonide töö kokkuvõte 2011 I pool. Informaatika ainesektsioon. http://www.opetajatemaja.ee/index.php?noframe=1&mod=docs&doc=581&h=59f3

Ajalugu. Kaitseliit – rahva algatatud omariikluse pant. Kaitseliit, http://www.kaitseliit.ee/et/ajalugu1

Ajalugu. Kaitsevägi. http://www.mil.ee/et/kaitsevagi/organisatsioon/kv-ajalugu

Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. Tartu Ülikool, 2012. Available online at http://www.pohiseadus.ee/. Paragrahv 126, http://www.pohiseadus.ee/ptk-10/pg-126/

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

Frequently asked questions, http://www.kaitseliit.ee/en/frequently-asked-questions

Jaagant, Urmas. Küberkaitseliit pakub harjutuskeskkonda vabatahtlikele IT-spetsialistidele. Eesti Päevaleht, 14 Apr 2010. http://www.epl.ee/news/eesti/kuberkaitseliit-pakub-harjutuskeskkonda-vabatahtlikele-it-spetsialistidele.d?id=51274411

Kaitseliidu ülema 18.10.2011 käskkiri nr K-O.2-4/16806u 'Kaitseliidu küberkaitse üksuse funktsioonikirjelduse kinnitamine' (Cyber Defence Unit Directive)

Kaitseministeeriumi majandusaasta aruanne 2010. http://www.kmin.ee/files/kmin/img/files/Majandusaasta_aruanne_2010 (1).pdf

Kõik suurimad e-teenuste pakkujad on Arvutikaitse 2009 partnerid. 3 Dec 2007 http://www.vaatamaailma.ee/?cat=6&paged=2

Korduma kippuvad küsimused. Kaitseliit, http://www.kaitseliit.ee/et/korduma-kippuvad-kusimused

Küberkaitse üksus. Kaitseliit, http://www.kaitseliit.ee/et/kuberkaitse-uksus

Küberkaitseliit aitab Tartu koolide arvutitest tõrjuda kurivara. 09.02.2011. http://www.kaitseliit.ee/et/kuberkaitseliit-aitab-tartu-koolide-arvutitest-torjuda-kurivara

Laan, Tanel. Ühine tahe. Kaitseliit 1925-1940. Kaitseliit, 2012. http://www.kaitseliit.ee/files/kaitseliit/img/files/yhine_tahe_web.pdf

Ottis, Rain. Cyber Security Organisation, NATO Cooperative Cyber Defence Centre of Excellence, October 2012.

Roonemaa, Holger. Aaviksood vaimustas mõte küberkaitseliidu loomisest. Eesti Päevaleht, 2 Oct 2007. http://www.epl.ee/news/eesti/aaviksood-vaimustas-mote-kuberkaitseliidu-loomisest.d?id=51103195

Seletuskiri digitaalallkirja seaduseelnõu juurde. Digitaalallkirja seadus (151 SE) Tallinn, 1999. http://www.riigikogu.ee/?op=emsplain2&content_type=text/html&page=mgetdoc&itemid=991820001

Seletuskiri kaitseliidu seaduse eelnõu juurde. 05.03.2012. (Explanatory Memorandum to the Estonian Defence League Act) http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=93442de2-07bc-49f9-9a09-b4d81d8c251b&

Seletuskiri Vabariigi Valitsuse määruse „Kaitseliidu kaasamise tingimused ja kord küberturvalisuse tagamisel" eelnõu juurde. 02.04.2013, http://eelnoud.valitsus.ee/main#tALQG5K7. (Explanatory Memorandum to the Draft Regulation on Estonian Defence league engagement in cyber security)

Seletuskiri Vabariigi Valitsuse määruse "Vabariigi Valitsuse määruste muutmine" eelnõu juurde (Explanatory Memorandum to draft regulation on amending certain government regulations), 22.11.2010. http://eelnoud.valitsus.ee/main#TnXRXqdL

Tallinn Manual on the International Law Applicable to Cyber Warfare, Michael N. Schmitt, gen. ed., Cambridge University Press, 2013.

The main tasks of the EDL CU. Estonian Defence League. http://www.kaitseliit.ee/en/the-main-tasks-of-the-edl-cu

Tiit, Ene-Margit. Pilguheit äsjasele rahvaloendusele. Riigikogu Toimetised 26, 2012. http://www.riigikogu.ee/rito/index.php?id=16265.

Tikk, Eneken; Kaska, Kadri; Vihul, Liis. International Cyber Incidents: Legal Considerations. CCD COE, 2010.

Vabariigi Valimiskomisjoni 5.6.2013 kiri nr 22-7/13-7/2 (Letter of the Estonian National Electoral Committee in reply to Eesti Keskerakond memorandum with regard to electronic voting) http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=6a20e142-506a-410a-a151-dcb65b5df950&

Vabariigi Valitsuse määrus 'Kaitseliidu kaasamise tingimused ja kord küberturvalisuse tagamisel'. Eelnõu kavand, 22.03.2013. (Draft regulation on the engagement of the Cyber Defence Unit in ensuring cyber security. http://eelnoud.valitsus.ee/main#tALQG5K7

Valitsus asutas Kaitseliidu küberkaitseüksuse. Kaitseministeerium, 20.01.2011, http://www.kmin.ee/et/valitsus-asutas-kaitseliidu-kuberkaitseuksuse

Valtenberg, Uko. Estonian Defence League - Cyber Defence Unit. *Presentation at CyCon workshop*, 4 June 2013