7th round of Mutual Evaluations

The practical implementation and operation of European policies on prevention and combating Cybercrime

ANSWERS TO THE QUESTIONNAIRE
LATVIA

RIGA

11 February 2016

1. GENERAL MATTERS

1.1.
Please indicate whether your MS has a national cyber security strategy.
If so, please explain whether and how it addresses cybercrime.
Provide a copy or web link to its full text, and if possible, translation in English or in French.

The Cyber Security Strategy of Latvia 2014-2018 was adopted by the Cabinet of Ministers (government) in January 2014.

Rule of law in cyberspace and reduction of cybercrime is one of the key areas of action (subsection 4.2).

It is stated that reduction of cybercrime requires action in two basic directions:

– preventive work for the reduction of criminal offences;
– effective combating of crime.

In Latvia, like in a number of other EU Member States, there is no common definition of "cybercrime"; there are cyber-dependent crime and cyber-enabled crime (or crime with an online element) (please, see answers to Q 2.A. 1. and Q 2.A.5. in this regard).[1]

1.2.
Briefly outline your national priorities with regards cybercrime, particularly in the area of prevention, legislation, capacity building, training, public awareness and international cooperation.
Are the national priorities linked to the strategic goals and operational action plans elaborated for the EU "Cybercrime" Priority?

A. National priorities

The national priorities with regard to cybercrime are set out in different (including sectoral) policy planning documents.

[1] Please, see also report on the United Kingdom (10952/2/15; page 17).

1. Policy planning documents on cybersecurity, including cybercrime

1.1. Cyber Security Strategy of Latvia 2014-2018 (CSS) and amendments[2] (with an Action plan)

According to the CSS, in light of combatting cybercrime, e-evidence related capacity should be enhanced. Cybercrime investigation, collection and assessment of e-evidence requires special knowledge; sufficient competence level of law enforcement officials, prosecutors and judges is crucial to ensure the rule of law in cyber space.

Taking this into account, the CSS foresees the following required actions:

I Legislative actions –

- to assess the present situation and further necessary legislative amendments that would provide punishment for causing damage to the security or operation of information systems directed towards automatic data processing systems;
- to facilitate discussions and exchange of opinions on new information and communication technologies (ICT) crimes and improvement of the legal basis in line with the international trends;
- to develop a unified mechanism for listing criminal offences in cyber space (statistics) (covering law enforcement agencies, prosecution and courts).

II Actions on capacity building and training –

- to assess and to develop the existing capacity of acquiring and analysing e-evidence in the process of investigation of cybercrimes (by developing the State Police competence and improving cooperation with the Information Technology (IT) Security Incidents Response Institution (CERT.LV) (for more information, please, see answer to Q 3.C.1.);
- to develop methodical materials on the ICT sector aimed at increasing knowledge of police officers, officials directing criminal proceedings and judges; in addition, to implement an in-depth training programme on combating cybercrime.

III Actions on prevention and fight against cybercrime –

- to establish a special unit dealing with cybercrime under the State Police;

[2] Instruction No. 347 adopted by the Cabinet of Ministers (government) on 9 July 2014; available in Latvian.

- to combat and to investigate cybercrime by assessing and improving the existing resources, procedures, cooperation mechanisms and their efficiency.

IV Actions on public awareness raising (also prevention measures) –

- to increase competence of educational institutions/teaching staff and their contribution to educating children and youth on ICT security (by integrating these issues into education process and by organising the relevant learning activities that would boost understanding on information security, privacy protection and usage of e-services); additionally, opportunities must be ensured for children and youth to report violations on internet and to receive support from a psychologist; also continuous training for the teaching staff on cyber security must be organized;
- to develop educational and informative materials on cyber security (for educational institutions and interest groups) that would be easily accessible and adjusted to various age groups;
- to create an ICT security laboratory and to organise scientific conferences on topical issues concerning cyber security and cybercrime (in cooperation with universities and scientific institutes);
- to implement educational and informative campaigns and other measures for the overall enhancement of awareness and understanding in the society on cyber security, cybercrime and existing threats.

V Actions regarding international cooperation –

- to cooperate with different international organizations working on cybercrime reduction and prevention.

1.2. Action Plan by the Cabinet of the Ministers (government) 2016, addendum, Action 156

Establishment of a special unit dealing with cybercrime under the State Police is mentioned.

2. Sectoral policy (home affairs) planning documents with regard to cybercrime

2.1.State Police Strategy 2014-2016 and State Police Working Plan 2016

The State Police Strategy 2014-2016 states that combating offences by using high technologies must be improved.

According to the Working Plan of the State Police in 2016, fight against all type of cybercrime is one of the four top priorities. As regards the cybercrime specifically, point 2.1. states that the State Police should carry out activities aimed at enhancing implementation of the Criminal Procedure Law provisions (in order to simplify and make more effective the investigations); also a clear reference to implementation of the CSS is made (point 2.8.).

2.2.Action Plan on fight against organised crime 2014-2016

The Action Plan foresees that work of the law enforcement agencies and the relevant security agencies should be strengthened; in addition, awareness and knowledge on the new trends, dynamics and the level of threats of organized crime (including cybercrime) should be raised.

2.3.State Police Crime Prevention Strategy 2014-2017

The Strategy entails the main principles, objectives, strategic directions, priorities and approaches (situation prevention, social prevention) regarding crime prevention.

According to the Strategy, internet safety is one of the five priority areas in crime prevention.

3. Other sectoral policy planning documents with regard to cybercrime

3.1. Intellectual Rights Protection and Enforcement Guidelines for 2015-2020[3]

The Guidelines emphasize the necessity to establish a special unit dealing with the cybercrime (including copyright offences) under the State Police.

3.2. Guidelines for the prevention of juvenile delinquency and protection of children against crimes 2013-2019[4]

The Guidelines set out preventive measures that will help children to avoid crime and to report on suspicious content in internet (i.e., information campaigns on safe use of internet, availability of hotlines).

[3] Adopted on 1 April 2015; available in Latvian.
[4] Adopted on 21 August 2013; available in Latvian.

3.3. Guidelines for the Prevention of Trafficking in Human Beings 2014-2020[5]

The Guidelines foresee a notification of cases on recruiting persons (i.e., victims/potential victims) through internet social networks as well as information providing on the potential cases or attempts of trafficking in human beings.

B. Linkage to the EU Policy cycle for organised and serious international crime

As regards the **EU Policy cycle** for organised and serious international crime, in the context of Latvia, the following EU priorities have been pointed out in the **Action Plan on fight against organised crime 2014 – 2016** (thus indicating that these priorities have a national importance): (1) trafficking in human beings; (2) excise fraud and MTIC fraud; (3) synthetic drugs; (4) heroin; (5) cybercrime; (6) organized property crime.

Taking into account that Latvia has put a particular focus on cybercrime, in 2015 and 2016[6], the State Police has either led activities of the operational action plans or has participated (will participate) in the OAP activities under the following strategic priorities (as defined in the multi-annual strategic plans (MASPs)):

Cybercrime (card fraud)		
Year	***2015***	***2016***
Goal 2 – ensuring that law enforcement and judicial authorities have access to the right tools, platforms, training and technical information to combat non-cash payment fraud including new developments in industry such as payment tools or emerging threats and countermeasures	Participation in two activities	Participation in one activity
Goal 3 – raising awareness of non-cash payment fraud as a crime with a serious economic impact and as a facilitator of other serious forms of crime among law enforcement and judicial authorities, the public and private sector and citizens	Leading one activity; participation in one activity	Participation in one activity

[5] Adopted on 21 January 2014, available in Latvian.
[6] According to the State Police Working Plan 2016, participation in the OAP activities has been clearly stated as one of the actions to be implemented by the State Police (under point 3.3. "International cooperation").

Goal 5 – improving the exchange of intelligence, information and evidence among law enforcement and judicial authorities across EU and non-EU countries to target OCGs involved in non-cash payment fraud, including by fostering closer cooperation	Participation in two activities	Participation in one activity
Goal 6 – increasing cross-border investigations and prosecutions against OCGs involved in non-cash payment fraud in the EU and beyond, including financial investigations and asset recovery to make non-cash payment fraud less attractive to criminals	Participation in two activities	Participation in three activities
Goal 8 – promote harmonisation of legislation in the EU to address legal loopholes in non-cash payment fraud cases, including jurisdictional issues, criminalisation of specific stages of criminal activities and levels of sanctions	Participation in one activity	-
Cybercrime (online child sexual exploitation)		
Year	***2015***	***2016***
Goal 2 – to increase and improve the capacity and capability to combat online child sexual exploitation within the EU, with a focus on victim identification, expertise in investigation and forensic techniques	Participation in one activity	-
Goal 4 – to facilitate and encourage cooperation and the exchange of online child sexual exploitation information by industry, civil society and EU law enforcement, with a view to using EC3 as a focal point	-	Participation in two activities
Goal 5 – to increase and improve international operational cooperation amongst judicial authorities and law enforcement against online and related offline child sexual exploitation	Participation in one activity	Participation in one activity
Goal 6 – to raise awareness and share best practise on combating online child sexual exploitation by pooling tools, research and techniques amongst industry, academia, law enforcement, prosecutors and judges	Participation in two activities	Participation in one activity

Goal 7 – to facilitate and to promote efforts of industry to reduce the availability of child sexual exploitation material on the internet	-	Participation in one activity
Cybercrime (cyber-attacks)		
Year	***2015***	***2016***
Goal 1 – to build a comprehensive intelligence picture in order to jointly prioritise common threats and key targets	Participation in six activities	Participation in three activities
Goal 2 – to tackle the prioritised threats and targets through joint operational activities, including disruptive actions, joint investigations and coordinated prosecutions	Participation in three activities	Participation in one activity
Goal 3 – to improve operational and judicial cooperation and coordination with third countries on the prioritised threats and targets	-	Participation in one activity
Goal 4 – to maximise collaboration with non-law enforcement actors including CERTs and private sector, stepping up coordination of efforts, exchange of information and building prevention and detection capacities	Participation in one activity	-
Goal 6 – to build and strengthen cyber capabilities i.e. by developing adequate resources and tools and improving expertise, knowledge and skills available to law enforcement, judiciary and key partners such as academia	Participation in one activity	Participation in two activities
Goal 7 – to strengthen cyber security awareness, responsibility, resilience and agility of private users and professionals, in particular operators of critical infrastructure and information systems, in order to minimise threats to victims and damages of cybercrime	Participation in one activity	-

As regards to the question whether national priorities are linked to the MASP strategic goals and OAPs, it should firstly be underlined that Latvia has followed the initial call to integrate the EMPACT[7] concept in the national planning process as such. Hence, as noted above, there is a clear linkage between EU and national crime priorities established.

[7] European multidisciplinary platform against criminal threats

It should also be noted that Latvia (similarly to other EU Member States) participates:

- in those EU priorities which pose the greatest threat on the ground at national level;
- in the EU priorities in case if Latvia is directly involved in a specific phenomenon (for instance, trafficking in human beings);
- in implementation of those strategic goals and specific OAP activities which do correspond/are linked to the national priorities and measures/activities (which are, for instance, envisaged in the following documents: State Police Strategy 2014-2016, State Police Working Plan 2016, Action Plan on fight against organised crime 2014 – 2016, State Police Crime Prevention Strategy 2014-2017 (please, see also above)).

1.3.
Please indicate which governmental institutions are responsible for the prevention of and fight against cybercrime.
Briefly outline their roles as well as their way of collaboration, cooperation and coordination with other institutions/bodies?

According to the CSS, the Ministry of Defence (MoD) coordinates development and implementation of the IT security and protection policy, as well as deals with international cooperation. Hence, in the context of **cyber security** as such, the MoD has the main coordinating role.

Fight against cybercrime however is within the exclusive competence of the Ministry of the Interior (mainly the State Police and in specific cases also the Security Police, please, see below).

1. Prevention

According to the CSS, several ministries are involved in cybercrime prevention actions:

- **Ministry of Interior** (the State Police, the Security Police) focusses on public awareness raising and campaigns (covering issues such as new trends of cybercrime, risks and how to avoid them);
- **Ministry of Education and Science** within the competence promotes knowledge and understanding of cyber space and its secure use;
- **Ministry of Welfare** implements social policy and policy on protection of children's rights.

2. Fight against cybercrime

Latvia has fully implemented the Convention on Cybercrime and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Thus, according to the national legislation, the **State Police** is responsible for fight against:

- offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of device);
- computer-related offences (computer related forgery, computer related fraud);
- content related offences (offences related to child pornography);
- offences related to infringements of copyright and the elated rights.

More on the State Police, please, see answer to Q 3.B.1.

The **Security Police**[8] is responsible for the fight against dissemination of racist and xenophobic material through the computer systems.

3. Way of coordination with other institutions/bodies, collaboration and cooperation

Coordination is based on the mutual cooperation principle where each institution/entity in performing its functions cooperates with the other involved parties **directly** or **through the National IT Security Council** (Council).

The Council is established by the Law on the Security of IT; it is also the central platform for information exchange and cooperation between the public and private sector.

Council's operation is ensured by the **National Cyber Security Policy Coordination Section** of the MoD.

Currently the following institutions/entities participate in the Council:

1) MoD;
2) Ministry of Foreign Affairs;[9]

[8] The Security Police is one of the three security and intelligence services in Latvia besides Constitution Protection Bureau and the Defence Intelligence and Security Service. The Security Police is counterintelligence and security service, which gathers tnformation from different sources, carries out its analysis, informs senior officials about the threats identified to the national security as well as takes measures to neutralise them.

[9] Coordinates international cooperation and Latvia's participation in various international initiatives related to the cyber security.

3) Financial and Capital Market Commission;[10]
4) Bank of Latvia;[11]
5) Ministry of Economics;[12]
6) Ministry of the Interior, the State Police and the Security Police (please, see also above);[13]
7) CERT.LV (please, see also answer sto Q 1.2. and Q 3.C.1.);[14]
8) Ministry of Education and Science (please, see above);
9) Ministry of Welfare (please, see above);
10) *Net-Safe Latvia* Safer Internet Centre (please, see answer to Q 5.A.5.);[15]
11) National Armed Forces and Cyber Defence Unit of the National Guard (please, see answer to Q 4.4.);[16]
12) IT sector NGOs (please, see answer to 10.C.1.);[17]
13) Ministry of Transport;[18]
14) Constitution Protection Bureau;[19]
15) Ministry of Justice and Data State Inspectorate (please, see answer to Q 1.7.);[20]
16) State Joint Stock Company "Latvian State Radio and Television Centre";[21]
17) Ministry of Environmental Protection and Regional Development.[22]

In addition, in the context of coordination, the National Cyber Security Policy Coordination Section of the MoD regularly informs the **Cabinet of Ministers** (government) (by submitting progress reports) and the Latvian **Parliament** *(Saeima)* (the Security and Defense Committee) on the state of play on implementation of the CSS (the Parliament thus is fulfilling its supervisory function in this regard). In addition, as for the parliamentary dimension, it should also be noted that *Saeima* takes a rather active

[10] Regulates and supervises activities in cyber space of members of the financial and capital market cyber space.
[11] Promotes secure and smooth operation of payment systems; credit institutions are responsible for secure availability of electronic services in their sector.
[12] Develops economic policy and promotes the development of competitiveness and innovation.
[13] Overall – responsible for implementing policies for combating crime, public order, security protection and the protection of rights and legal interests of individuals; coordinates also the settlement of crisis situations.
[14] Monitors and analyses developments in cyber space, reacts to incidents and coordinates their prevention, carries out research, organises educational events and training, as well as supervises the implementation of obligations specified in the Law on the Security of IT. CERT.LV provides support for Latvian and foreign state and municipal institutions, entrepreneurs, and individuals.
[15] Ensured by the Latvian Internet Association, educates society about possible risks and threats online; promotes the use of secure internet content.
[16] Responsible for providing support in crisis situations.
[17] Support, consultation and cooperation with the Council in developing and implementing the cyber security policy.
[18] Organises the implementation of communication policy.
[19] Oversees the critical infrastructure.
[20] Responsible for developing, organising and coordinating the policy on rights in the field of personal data protection, freedom of information and supervision of electronic documents. The Ministry of Justice is also responsible criminal law policy.
[21] The only provider of trust certification services, which ensures the infrastructure of electronic identity cards and electronic signatures.
[22] Organises the governance of state ICT and coordinates the electrisation of public services; State Regional Development Agency ensures the operation and development of solutions for shared use of state ICT.

role and puts forward a number of topical issues, also those related to collaboration and cooperation between the different state actors (for instance, lately there has been a call to strengthen cooperation between the Cyber Defence Unit of the National Guard (which is a part of National Armed Forces) and the relevant State Police structure; for more information about these entities, please, see answers to Q 3.B.1. and Q 4.4.).

Please, see also answer to Q 3.C.2.

1.4.
Please specify the main trends in your MS with regard to cybercrime in the recent years.
If possible, provide in % the share of cybercrime in the total criminality picture in your MS.

The main **trends** in 2015/2016 (so far) with regard to cybercrime:

- extortion related to DDoS and Ransomware attacks against private sector (merchants);
- usage of Latvian hosting possibilities – due to the fact, that in Latvia there is a very high internet speed and a very good connection quality, there is a tendency that the Latvian internet connections are increasingly used for committing criminal offences from abroad (this in particular refers to CSE and malicious software). In addition, also anonymity issue has to be highlighted (reselling IP ranges to private internet service providers (ISP) who are not registered as electronic communications merchants);
- spreading of child pornography and materials containing paedophilia on internet; this trend has developed over a longer time period;
- phishing attacks and malicious software (malware);
- malware attacks on banking systems and e-bank users;
- "card sharing" – protected cable television decoding card/information sharing on code.

As regards the **percentage** (share of cybercrime in the total criminality picture in Latvia), in 2015, 47 406 criminal proceedings in total were initiated in Latvia, 453 of which are related to cybercrime that constitute 0.96% of all criminal proceedings. From all these criminal proceedings, the State Police initiated 44 900, 427 of which are related to cybercrime that constitutes 0.95% of the total criminality picture.

Cybercrime in a broader context (i.e., not only those Articles of the Criminal Law mentioned in the statistics table in answer to Q 1.6.) constitutes 1.54% of all criminal proceedings in Latvia.

1.5.

Please describe how your statistics on cybercrime are compiled in terms of: participating institutions/bodies; are they integrated; input from the private sector; are judicial statistics kept separately from the LEA statistics?

If possible, specify the share of input both of LEA and private sector into your national statistics.

1. Law enforcement statistics

All law enforcement agencies have access to the **Integrated Interior Information System** (IIIS) (Information Centre of the Ministry of the Interior is the manager and holder of this register). The IIIS consists of different sub-information systems, including the Punishment Register which *inter alia* entails data on:

- initiated criminal proceedings and criminal offences;
- accused persons;
- specific information on criminal proceedings (from KRASS; please, see below).

Information is provided by the authorities which, according to the Criminal Procedure Law, are authorised to perform criminal proceedings. Authorised users have a direct access to the IIIS.

Information Centre of the Ministry of the Interior also is a manager and holder of the **Criminal Procedure Information System** (KRASS) which encompasses information on the initiated criminal proceedings, detected criminal offences, officials directing the proceedings, individuals having the right for the assistance of a defence counsel and victims. Information in the KRASS is entered in on-line regime no later than on the next working day following the performance of the procedural actions, the registration of the act or the coming into effect of the judgement of a court.

2. Judicial statistics

Judicial statistics is kept separately from the law enforcement statistics.

The **Court Information System** (TIS) is managed by the Ministry of Justice; its aim is to facilitate record registering, to store and to process judicial information, to exchange it as well as to gather statistics.

As for now, the law enforcement authorities can access judicial statistics. The entire data set (starting from the initiated criminal proceeding till data on conviction) cannot be obtained under one information system; however, some of the systems are interlinked (for instance, TIS is linked to KRASS (ensures data exchange, except for the statistics), whilst KRASS is linked to the Punishment Register which is part of the IIIS).

3. Role of the private sector

The private sector does not provide input into national statistics on cybercrime; however, CERT.LV, gathers statistics which *inter alia* is based also on data submitted by the private sector.

1.6.

Please provide any available statistics on the number of registered cases, investigations, prosecutions, final convictions, as well as the number of persons investigated, prosecuted for and convicted of cybercrime acts in the last 2 years.

Please note that initiated criminal proceedings (criminal cases submitted by the State Police to the Public Prosecutor's Office for criminal prosecution) may not be finalized within 1-2 years; hence, for instance, the final conviction delivered in 2015 may refer to criminal offence registered earlier than in 2014.

Available statistic data:

Criminal Law	Initiated criminal proceedings (in total)[23]		Initiated criminal proceedings by the State		Registered criminal offences		Criminal cases submitted by the State Police to the Public Prosecutor's office for criminal prosecution		Final conviction	
	2015	2014	2015	2014	2015	2014	2015	2014	2015	2014
Article 78 (2)[24]	8	10	0	0	8	7	0	0	6	7
Article 144[25]	9	12	7	6	8	21	1	4	1	0
Article 148[26]	41	37	35	35	34	34	26	23	4	9
Article 166[27]	84	48	82	47	226	82	29	27	17	10
Article 177[1] [28]	60	52	59	52	67	60	14	14	3	10
Article 193[1] [29]	248	220	240	212	385	484	146	115	23	40
Article 241[30]	1	2	2	1	1	1	0	1	0	0
Article 243[31]	1	1	1	1	1	1	0	0	1	0
Article 244[32]	1	2	1	2	1	2	0	0	0	0
Article 244[1][33]	0	0	0	0	0	0	0	0	0	0
Article 78 (2)[34]	0	0	0	0	0	0	0	0	0	0

[23] Total number of criminal proceedings initiated by the State Police, Security Police and Public Prosecutor's Office of the Republic of Latvia
[24] Triggering of national, ethnic and racial hatred
[25] Violating the confidentiality of correspondence and information to be transmitted over telecommunications networks
[26] Infringement of copyright and neighbouring rights
[27] Violation of provisions regarding the demonstration of a pornographic performance, restriction of entertainment of intimate nature and handling of a material of pornographic nature
[28] Fraud in an automated data processing system
[29] Obtaining, manufacture, distribution, utilisation and storage of data, software and equipment for illegal acts with financial instruments and means of payment
[30] Arbitrary accessing automated data processing systems
[31] Interference in the operation of automated data processing systems and illegal actions with the information included in such systems
[32] Illegal operations with automated data processing system resource influencing devices
[33] Acquisition, development, alterations, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment
[34] Triggering of national, ethnic and racial hatred

1.7.

How does your MS protect Fundamental rights/freedoms and Internet? (privacy, protection of personal data, freedom of expression) when tackling cybercrime?

1. Legal requirements

The fundamental rights and freedoms are protected by the **Constitution** of the Republic of Latvia; Article 89 declares that State shall recognize and protect fundamental human rights in accordance with this Constitution, laws and international agreements binding upon Latvia. Article 96 states that "everyone has the right to inviolability of his or her private life, home and correspondence"; according to Article 99 "everyone has the right to freedom of thought, conscience and religion". Article 100 provides that "everyone has the right to freedom of expression, which includes the right to freely receive, keep and distribute information and to express his or her views" and that "censorship is prohibited".

As regards safeguards envisaged in the **Criminal Procedure Law**, please, see answer to Q 2.B.1.

In addition, the **Operational Activities Law** (Article 5) states that "if a person believes that a body performing operational activities has through its actions infringed the lawful rights and freedoms of the person, such person is entitled to submit a complaint to a prosecutor who, after conducting an examination, shall provide an opinion with respect to the conformity to law of the actions of the officials of the body performing the operational activities, or the person may bring an action in court".

2. Data State Inspectorate

Data State Inspectorate (DSI) is a state administration institution responsible for supervising the compliance of persona data protection according to Personal Data Protection Law. It operates independently and autonomously but is also subject to the supervision of the Ministry of Justice.

DSI has the following tasks:

- to carry out accreditation of trusted certification service providers and to supervise them (Electronic Documents Law);
- to supervise compliance with the legal provisions on unsolicited commercial messages (Law on Information Society Services).

1.8.

Are there dedicated budget allocations for the prevention of and fight against cybercrime? Do you benefit from EU funding to tackle cybercrime?

Since there are several State Police entities involved in prevention and fight against cybercrime (please, see answer to Q 3.B.1.), there are no budgetary allocations specifically dedicated only to cybercrime. Issues related to human resources, technical resources and other matters are financed within the relevant budgetary lines of the State Police's general budget.

As regards the EU funding, a project "Capacity building to prevent and fight against cybercrime" is one of the national priorities within the Internal Security Fund. The assigned amount of funding for this activity is expected to be 865 775 euros. It is planned to use this funding to acquire new cyber forensic equipment, to build high-speed optical network with a powerful client-server at its core and to train experts on cyber forensics.

1.9.

Are you party to the CoE Convention on Cybercrime?

If not yet, please explain the reasons and indicate when you are planning to complete the ratification process.

Yes.

The CoE Convention on Cybercrime and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems is applicable in Latvia from 1 June 2007.

2. LEGAL ASPECTS

2.A.

Criminalisation

In respect of legislation and other rules, please provide copies in the original language and, if possible in English or in French, of relevant laws and explanatory memoranda, as well as any guidelines or instructions (ministerial or from the judiciary) to prevent/tackle cybercrime, as addressed as a subject to this evaluation.

In cases where the questions of this chapter relate to the implementation of the Directive 2013/40/EU on attacks against information systems and the implementation-process is not yet complete in your MS (transposition date 4 September 2015), please indicate (i) what you have already in place following the implementation of the Council Framework Decision 2005/222/JHA and (ii) how you plan to implement Directive 2013/40/EU.

Criminal Law in Latvian is available here (with the latest amendments of 12 November 2015); please find translation in English attached (however, amendments of 29 October 2015 and 12 November 2015 are not reflected).

On the Procedures for the Coming into Force and Application of the Criminal Law in Latvian is available here (with the latest amendments of 29 October 2015); please find translation in English attached (amendments which have been adopted after 25 April 2013 are not reflected).

Criminal Procedure Law in Latvian is available here (with the latest amendments of 12 November 2015); please find translation in English attached (however, amendments which have been adopted after 23 May 2013 are not reflected).

Operational activities Law in Latvian is available here (with the latest amendments of 1 March 2012); please find translation in English attached.

Latvian Administrative Violations Code in Latvian is available here (with the latest amendments of 4 June 2015); please find translation in English attached (amendments which have been adopted after 20 May 2010 are not reflected).

Electronic Communication Law in Latvian is available here (with the latest amendments of 17 December 2015); please find translation in English attached (amendments which have been adopted after 13 March 2014 are not reflected).

Law On Information Society Services in Latvian is available here (with the latest amendments 19 May 2011); please find translation in English attached.

Law on the Security of IT in Latvian is available here (with the latest amendments of 5 February 2015); please find translation in English attached (amendments which have been adopted after 6 November 2013 are not reflected).

Personal Data Protection Law in Latvian is available here (with the latest amendments of 6 February 2014); please find translation in English attached.

Law on Pornography Restrictions in Latvian is available here (with the latest amendments of 12 December 2013); please find translation in English attached (amendments are not reflected).

Protection of the Rights of the Child Law in Latvian is available here (with the latest amendments 26 November 2015); please find translation in English attached (amendments which have been adopted after 6 March 2014 are not reflected).

Law on Judicial Power in Latvian is available here (with the latest amendments of 18 June 2015); please find translation in English attached (amendments which have been adopted after 26 September 2013 are not reflected).

Office of the Prosecutor Law in Latvian is available here (with the latest amendments of 5 March 2015); please find translation in English attached (amendments which have been adopted after 8 June 2000 are not reflected).

2.A.1.

Which cybercrime acts (among those listed in Table 2) are criminalised?

Please indicate for each one of them:

- ***the title and relevant provisions in your legislation***
- ***the definition used;***

- ***intent/recklessness;***
- ***aggravating/mitigating factors;***
- ***minimum and maximum penalties.;***
- ***multiple crimes/recidivism***
- ***incitement, aiding and abetting, and attempt***

1. Specific provisions on cybercrime

1.1. Acts unique to information systems, in particular those related to cyber attacks[35]

According to provisions of the Criminal Law, the following acts are criminalized:

1) violating the confidentiality of correspondence and information to be transmitted over telecommunications networks (namely, illegal interception; Article 144):

- for a person who commits *intentional violation of the confidentiality of personal correspondence*, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 1);
- for a person who commits *unlawful interception of publicly unavailable data transmissions or signals in telecommunications networks, as well as unlawful acquisition of publicly unavailable electromagnetic data from a telecommunications network in which such data is present*, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 2);
- for committing the acts provided for in paragraph one or two, if such are committed *for purposes of acquiring property*, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 144 paragraph 3);

2) obtaining, manufacture, distribution, utilisation and storage of data, software and equipment for illegal acts with financial instruments and means of payment (Article 193[1]):

- for a person who commits *obtaining or distribution of such data as enable illegal*

[35] Illegal access to information system; illegal system interference; illegal data interference; illegal interception of computer data; misuse of devices - production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools.

utilisation of financial instruments or means of payment, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 193[1] paragraph 1);

- for a person who commits *utilisation of such data as enable illegal utilisation of financial instruments or means of payment, or who commits manufacture or adaptation of software or equipment for the commission of the crimes provided for by Article 193*[36] *of the Criminal Law, or commits obtaining, storage or distribution of such software or equipment for the same purpose*, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 193[1] paragraph 2);
- for a person who commits the acts provided for by *paragraph one or two, if commission thereof is in an organised group*, the applicable punishment is deprivation of liberty for a term of two years and up to ten years, with or without confiscation of property and with police supervision for a term up to three years (Article 193[1] paragraph 3);

3) <u>arbitrary accessing automated data processing systems</u> (Article 241):

- for a person who commits *arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused*, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 241 paragraph 1);
- for the criminal offence provided for in paragraph one, if it has been committed *for purposes of acquiring property*, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 2);
- for the acts provided for in paragraph one, *if serious consequences have been caused thereby, or if they are directed against automated data processing systems that process information related to State political, economic, military, social or other security*, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 241 paragraph 3);

[36] The article refers to illegal activities with financial and means of payment.

4) interference in the operation of automated data processing systems and illegal actions with the information included in such systems (Article 243):

- for a person who commits *unauthorised modifying, damaging, destroying, impairing or hiding of information stored in an automated data processing system, or knowingly entering false information into an automated data processing system, if substantial harm has been caused* thereby, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 1);
- for a person who commits *knowingly interference in the operation of an automated data processing system by entering, transferring, damaging, extinguishing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused*, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 243 paragraph 2);
- for the criminal offence provided for in paragraph one or two, if it has been committed *for purposes of acquiring property*, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine and with or without police supervision for a term up to three years (Article 243 paragraph 3);
- for the acts provided for in paragraph one or two, if they have been *committed by an organised group or if they have caused serious consequences, or if they are directed against an automated data processing system that processes information related to State political, economic, military, social or other security*, the applicable punishment is deprivation of liberty for a term up to seven years, with or without confiscation of property and with or without probationary supervision for a term up to three years (Article 243 paragraph 5);

5) illegal operations with automated data processing system resource influencing devices (Article 244):

- for a person who commits *the illegal manufacture, adaptation for utilisation, sale, distribution or storage of such tool (device, software, computer password, access code or similar data), which is intended for the influencing of resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for purposes of committing a criminal offence*, the applicable

punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 1);

– for a person who commits the same acts, *if serious consequences has been caused* thereby, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 244 paragraph 2);

6) acquisition, development, alterations, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment (Article 244[1]):

– for a person who commits *electronic communications network terminal equipment identification in an electronic communications network for necessary data alterations or the acquisition, storage or distribution of data intended for such purposes, as well as the acquisition, development, storage or distribution of programs or equipment intended for such purposes without the consent of the manufacturer or the authorised person thereof,* if such activities have been committed for purposes of acquiring property or if it has been committed by a group of persons pursuant to prior agreement, or if it has caused *significant harm,* the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine.

1.2. Content-related acts, in particular those related to child sexual abuse online and child pornography[37]

The following acts are criminalized:

1) encouraging to involve in sexual acts (Article 162[1]):

– for a person who *encourages a person who has not attained the age of sixteen years to involve in sexual acts or encourages such person to meet with the aim to commit sexual acts or enter into a sexual relationship using information or communication technologies or other means of communication, if such act has been committed by a person who has attained the age of majority*, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine and with probationary supervision for a term up to five years (Article 162[1] paragraph 1);

[37] Computer-related production, distribution or possession of child pornography; computer-related solicitation or "grooming" of children.

- for the acts provided for in paragraph one, if it has been *committed against an under aged person,* the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine and with probationary supervision for a term up to five years (Article 162^1 paragraph 2);

2) violation of provisions regarding the demonstration of a pornographic performance, restriction of entertainment of intimate nature and handling of a material of pornographic nature (Article 166):

- for a person who commits *violation of provisions regarding the demonstration of a pornographic performance or other provisions regarding the restriction of entertainment of intimate nature, or provisions regarding the handling of a material of pornographic nature, if substantial harm has been caused by commission* thereof, the applicable punishment is deprivation of liberty for a term up to one year or temporary deprivation of liberty, or community service, or a fine (Article 166 paragraph 1);
- for a person who commits the *visiting or demonstration of such pornographic performance or the handling of such materials of pornographic nature which contain child pornography, sexual activities of people with animals, necrophilia or sexual gratification in a violent way*, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property and with probationary supervision for a term up to three years (Article 166 paragraph 2);
- for a person who commits *encouraging, involvement, forced participation or utilisation of minors in a pornographic performance or the production of a material of pornographic nature,* the applicable punishment is deprivation of liberty for a term up to six years, with or without confiscation of property and with probationary supervision for a term up to three years (Article 166 paragraph 3);
- for a person who commits *encouraging, involvement, forced participation or utilisation of persons who have not attained the age of sixteen years in a pornographic performance or the production of a material of pornographic nature,* the applicable punishment is deprivation of liberty for a term of three years and up to twelve years, with or without confiscation of property and with probationary supervision for a term up to three years (Article 166 paragraph 4);
- for a person who commits the acts provided for in paragraph three or four, if they have been committed by *an organised group or if they have been committed by means of*

violence, the applicable punishment is deprivation of liberty for a term of five years and up to fifteen years, with or without confiscation of property and with probationary supervision for a term up to three years (Article 166 paragraph 5);

1.3. Acts where computer/IT systems were involved as tool or target, in particular online card fraud harm[38]

The following acts have been criminalized:

1) illegal activities involving personal data of natural persons (Article 145):

– for *illegal activities involving personal data of a natural person, if it has caused substantial harm*, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (Article 145 paragraph 1);
– for *illegal activities involving personal data of a natural person, if they have been performed by a personal data processing administrator or operator for the purpose of vengeance, acquisition of property or blackmail*, the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine (Article 145 paragraph 2);
– for *influencing a personal data processing administrator or operator or the data subject, using violence or threats or using trust in bad faith, or using deceit in order to perform illegal activities involving personal data of a natural person*, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine (Article 145 paragraph 3);

2) fraud in an automated data processing system (Article 177^1):

– for a person who commits the *knowingly entering of false data into an automated data processing system for the acquisition of the property of another person or the rights to such property, or the acquisition of other material benefits, in order to influence the operation of the resources thereof (computer fraud)*, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Article 177^1 paragraph 1);
– for a person who commits *computer fraud, if it has been committed by a group of persons*

[38] Computer-related fraud or forgery; computer-related identity offences; sending or controlling sending of spam.

pursuant to prior agreement, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine, with or without confiscation of property (Article 177^1 paragraph 2);

- for a person who commits *computer fraud, if it has been committed on a large scale or if it has been committed in an organised group*, the applicable punishment is deprivation of liberty for a term of two years and up to ten years, or a fine, with or without confiscation of property and with or without police supervision for a term up to three years (Article 177^1 paragraph 3).

As regards spam, it shall be noted that according to Article 204^{16} of the **Latvian Administrative Violations Code** *in the case of violation of the prohibition on sending commercial information as specified in the law*, a warning shall be issued or a fine shall be imposed on natural persons in an amount from 140 to 500 euros, for legal persons – from 700 to 7100 euros. The competent supervisory authority is the DSI (please, see also answer to Q 1.7.).

2. General provisions on intent and recklessness (2.1.), aggravating and mitigating factors (2.2.), multiple crimes and recidivism (2.3.), incitement, aiding and abetting (2.4.), and attempt (2.5.)

2.1.Intent/recklessness

Article 8 of the Criminal Law (on forms of guilt) states that "only a person who has committed a criminal offence *deliberately (intentionally)* or through *negligence* may be found guilty of it", by further explaining that "in determining the form of guilt of a person who has committed a criminal offence, the mental state of the person in relation to the objective elements of the criminal offence must be established".

According to Article 9 "a criminal offence shall be considered to have been committed *deliberately (intentionally)* if the person has committed it with a *direct or indirect intent*". It further explains that a criminal offence shall be considered to have been committed with:

- a *direct intent* if the person has been aware of the harm caused by his or her act or failure to act and has knowingly committed it or also been aware of the harm caused by his or her act or failure to act, foreseen the harmful consequences of the offence and has desired them;

- an *indirect intent* if the person has been aware of the harm caused by his or her act or failure to act, foreseen the harmful consequences of the offence and, although has not desired such consequences, has knowingly allowed them to result.

According to Article 10 "a criminal offence shall be considered to be committed through *negligence* if the person has committed it through *criminal self-reliance or criminal neglect*". It is further explained that a criminal offence shall be considered to have been committed through:

- *criminal self-reliance* if the person has foreseen the possibility that the harmful consequences of his or her act or failure to act would result and nevertheless carelessly relied on these being prevented;
- *criminal neglect* if the person did not foresee the possibility that the consequences of his or her act or failure to act would result, although according to the actual circumstances of the offence he or she should have and could have foreseen the referred to harmful consequences.

2.2.Aggravating/mitigating factors

According to Article 46 of the Criminal Law on general principles for determination of punishment, in determining the amount of punishment, the circumstances *mitigating or aggravating* the liability shall be taken into account.

Article 47 sets out the following circumstances which *shall be* considered as circumstances *mitigating* the liability, namely, if:

- perpetrator of the criminal offence has admitted his or her guilt, has freely confessed and has regretted the criminal offence committed;
- offender has:
    - actively furthered the disclosure and investigation of the criminal offence;
    - voluntarily compensated the harm caused by the criminal offence to the victim or has eliminated the harm caused;
    - facilitated the disclosure of a crime of another person;
- criminal offence was committed:
    - as a result of unlawful or immoral behaviour of the victim;

- exceeding the conditions regarding the necessary self-defence, extreme necessity, detention of the person committing the criminal offence, justifiable professional risk, the legality of the execution of a command and order;
- by a person in a state of diminished mental capacity.

However, also other circumstances which are related to the criminal offence committed, *may be* considered as circumstances mitigating the liability.

According to Article 48, the following *may be* considered to be *aggravating* circumstances, namely, if:

- the criminal offence was committed:
  - while in a group of persons;
  - taking advantage in bad faith of an official position or the trust of another person;
  - against a woman, knowing her to be pregnant;
  - against a person who has not attained sixteen years of age or against a person taking advantage of his or her helpless condition or of infirmity due to old-age;
  - against a person taking advantage of his or her official, financial or other dependence on the offender;
  - with particular cruelty or with humiliation of the victim;
  - taking advantage of the circumstances of a public disaster;
  - employing weapons or explosives, or in some other generally dangerous way;
  - out of a desire to acquire property;
  - under the influence of alcohol, narcotic, psychotropic, toxic or other intoxicating substances;
  - due to racist, national, ethnic or religious motives;
- the criminal offence:
  - has caused serious consequences;
  - constitutes *recidivism* of criminal offences;
  - was related to violence or threats of violence, or the criminal offence against morality and sexual inviolability was committed against a person to whom the perpetrator is related in the first or the second degree of kinship, against the spouse or former spouse, or against a person with whom the perpetrator is or has been in unregistered marital relationship, or against a person with whom the perpetrator has a joint (single) household;

- the person committing the criminal offence, for purposes of having his or her punishment reduced, has knowingly provided false information regarding a criminal offence committed by another person.

2.3.Multiple crimes/recidivism

According to Article 24, multiplicity of criminal offences is "the commission (or allowing) by one person of two or more separate offences (act or failure to act) which correspond to the constituent elements of several criminal offences, or the commission (or allowing) by a person of one offence (act or failure to act) which corresponds to the constituent elements of at least two different criminal offences". It is further explained that "multiplicity of criminal offences is constituted by aggregation and *recidivism* of criminal offences".

Article 27 explains that "*recidivism* of a criminal offence is constituted by a new intentional criminal offence committed by a person after the conviction of such person for an intentional criminal offence committed earlier, if the criminal record for such has not been set aside or extinguished in accordance with the procedures laid down in law".

2.4.Incitement, aiding and abetting

Article 19 on participation states that "criminal acts committed knowingly by which two or more persons (that is, a group) jointly, knowing such, have directly committed an intentional criminal offence shall be considered to be participation (*joint commission*)" and that "each of such persons is a participant (joint perpetrator) in the criminal offence".

According to Article 20 on joint participation "an act or failure to act committed knowingly, by which a person (joint participant) has jointly with another person (perpetrator), participated in the commission of an intentional criminal offence, but he himself or she herself has not been the direct perpetrator of it, shall be considered to be joint participation" and that "*organisers*[39], *instigators*[40] *and abettors*[41]are joint participants in a criminal offence".

[39]A person who has organised or directed the commission of a criminal offence.
[40]A person who has encouraged another person to commit a criminal offence.
[41]A person who knowingly has promoted the commission of a criminal offence, providing advice, direction, or means, or removing impediments for the commission of such, as well as a person who has previously promised to conceal the perpetrator or joint participant, the instrumentalities or means for committing the criminal offence, trail of the criminal offence or the objects acquired by criminal means or has previously promised to acquire or to sell these objects.

2.5.Attempt

According to Article 15 on completed and uncompleted criminal offences "a conscious act (failure to act), which is directly dedicated to intentional commission of a crime, shall be considered to be an *attempted* crime if the crime has not been completed for reasons independent of the will of the guilty party".

2.A.2.
Does your legislation provide for liability of legal persons for cybercrime?
Specify the nature (criminal/non-criminal) and scope of the liability (the offences), and the sanctions provided.

1. Criminal law

1.1. Liability

According to Article 70[1] of the Criminal Law, a court or a public prosecutor *may apply* a coercive measure to a legal person governed by private law, including State or local government capital company, as well as partnership, if a natural person has committed the offence in the interests of the legal person, for the benefit of the person or as a result of insufficient supervision or control, acting individually or as a member of the collegial authority of the relevant legal person:

- on the basis of the right to represent the legal person or act on the behalf thereof;
- on the basis of the right to take a decision on behalf of the legal person;
- in implementing control within the scope of the legal person.

1.2. Scope of liability (the offences)

All criminal offences provided for in the Special Part of the Criminal Law (Article 71 – 356).

1.3. Coercive measures

Article 70[2] sets out the following types of coercive measures applicable to a legal person:

– liquidation;[42]
– restriction of rights;[43]
– confiscation of property;[44]
– monetary levy.[45]

One or several of the above-mentioned coercive measures may be applied (however, this does not refer if liquidation is applied).

In determining the *type* of coercive measure, the nature of the criminal offence and the harm caused shall be taken into account, and in determining the extent of a coercive measure the following conditions shall be observed:

– the actual action of a legal person;
– the nature and consequences of the acts of a legal person;
– measures, which a legal person has performed in order to prevent the committing of a criminal offence;
– the size, type of activities and financial circumstances of a legal person;
– measures, which a legal person has performed in order to compensate for the losses caused or prevent the damage caused;
– whether a legal person has reached a settlement with the victim.

However, for a criminal violation and a less serious crime a public prosecutor, in drawing up an injunction regarding coercive measure, may determine monetary levy or restriction of rights as a coercive measure to a legal person.

2. Latvian Administrative Violations Code

Article 14^1 of the Latvian Administrative Violations Code on corporate liability states that "in special cases provided for in (..) [the] Code and binding regulations issued by local government

[42]According to the Criminal law "a legal person shall be liquidated (compulsory termination of the activities of a legal person) only in such cases, if the legal person has been especially established for the committing of a criminal offence or if a serious or especially serious crime has been committed".
[43] "Restriction of rights is the deprivation of specific rights or permits or the determination of such prohibition, which prevents a legal person from exercising certain rights, receive State support or assistance, participate in a State or local government procurement procedure, to perform a specific type of activity for a term of one year and up to ten years".
[44] "Confiscation of property is the compulsory alienation to State ownership without compensation of the property owned by a legal person; property owned by a legal person, which has been transferred to another person, may also be confiscated".
[45] "A monetary levy, in conformity with the seriousness of the criminal offence and the financial circumstances of a legal person, shall be determined in the amount of ten and up to hundred thousand minimum monthly wages specified in the Republic of Latvia at the time of the rendering of the adjudication, indicating in the adjudication the amount of the monetary levy in the monetary units of the Republic of Latvia".

councils (..) *legal persons* shall be subject to liability for administrative violations" and that also "*persons performing commercial activity*, but which are not legal persons, shall be subject to liability for administrative violations as legal persons".

2.A.3.

Does your legislation provide for specific criteria e.g. high economical, political or social impact or number of affected systems, level of damages, which would classify the cyber-attack as a "serious" or "large scale" cyber-attack?

General overview (please note that the overview refers to criminal offences mentioned in the first and third category; please, see answer to Q 2.A.1):

Article of the Criminal Law	**Reference to "large scale"**	**Reference to "substantial harm"**	**Reference to "serious consequences"**	**Reference to acts which are "directed against automated data processing systems that process information related to State political, economic, military, social or other security"**
Article 145[46]	-	paragraph 1	-	-
Article 166[47]	-	paragraph 1	-	-
Article 177[1] [48]	paragraph 3	-	-	-
Article 241[49]	-	paragraph 1	paragraph 2	
Article 243[50]	-	paragraph 1 and 2	paragraph 5	
Article 244[51]	-	-	paragraph 2	-
244[1] [52]	-	article as such	-	-

[46] Illegal activities involving personal data of natural persons.
[47] Violation of provisions regarding the demonstration of a pornographic performance, restriction of entertainment of intimate nature and handling of a material of pornographic nature.
[48] Fraud in an automated data processing system.
[49] Arbitrary accessing automated data processing systems.
[50] Interference in the operation of automated data processing systems and illegal actions with the information included in such systems.
[51] Illegal operations with automated data processing system resource influencing devices.
[52] Acquisition, development, alterations, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment.

According to Article 20 of *On the Procedures for the Coming into Force and Application of the Criminal Law* "liability for an offence, provided for in the Criminal Law, which has been committed on a **large scale**, shall apply if the total value of the property which was the subject of the offence was not less than fifty times the minimum monthly wage[53] as specified in the Republic of Latvia at that time" by further explaining that "the value of the property shall be determined according to the market prices or prices equivalent thereto at the time when the offence was committed".

As regards the notion of **substantial harm**, Article 23 clarifies that "liability for the criminal offence provided for in the Criminal Law, by which substantial harm has been caused, shall apply, if as the result of the criminal offence not only significant financial loss[54] has been caused, but also other interests protected by law were threatened, or if such threat was significant".

Article 24 specifies that "liability for a criminal offence provided for in the Criminal Law that has caused **serious consequences** shall apply if the criminal offence has resulted in death of a person, or serious bodily injuries or psychological trauma to at least one person, moderate bodily harm to a number of persons or financial loss on a large scale have been inflicted, or other serious harm has been caused to the interests protected by law".[55]

[53] Currently – 370 euros.
[54] Financial loss, which at the time of committing the crime exceeds five times the minimum monthly wage as determined at the time in the Republic of Latvia, shall be deemed to be significant financial loss.
[55] The criteria for the specification of the level of seriousness of bodily injury are provided for in annexes to this Law.

2.A.4.

How are minor cases treated?

Concept of a "minor case" is non-existent in the Criminal Law.

According to the Criminal Law *criminal offences* in Latvia are divided into *criminal violations*[56] and *crimes* (according to the nature and harm of the threat to the interests of a person or the society); *crimes* are further divided as follows: *less serious crimes*[57], *serious crimes*[58] and *especially serious crimes*.[59] These offences are treated in accordance with the relevant legal acts, primarily the Criminal Law and the Criminal Procedure Law.

Currently experts are working on further simplification of the criminal procedure (concrete amendments to the Criminal Procedure Law are being discussed)[60]; this would refer to criminal violations and less serious crimes.

Additional information:

According to Article 371 (paragraph 2^1) of the Criminal Procedure Law on refusal to initiate proceedings "an investigator with a consent of a public prosecutor *may refuse* the initiation of criminal proceedings, if a criminal offence has been committed that has the features of a criminal offence, but which *has not caused such harm* that would warrant the application of a criminal punishment".

Also Article 379 on termination of criminal proceedings and releasing a person from criminal liability (paragraph 1) states that "an investigator with a consent of a supervising public prosecutor, public prosecutor or a court *may terminate* criminal proceedings, if a criminal offence has been committed that has the features of a criminal offence, but which *has not*

[56] A criminal violation is an offence for which the Criminal Law provides for deprivation of liberty for a term exceeding fifteen days, but not exceeding three months (temporary deprivation of liberty), or a type of lesser punishment

[57] A less serious crime is an intentional offence for which the Criminal Law provides for deprivation of liberty for a term exceeding three months but not exceeding three years, as well as an offence, which has been committed through negligence and for which the Criminal Law provides for deprivation of liberty for a term up to eight years.

[58] A serious crime is an intentional offence for which the Criminal Law provides for deprivation of liberty for a term exceeding three years but not exceeding eight years, as well as an offence, which has been committed through negligence and for which the Criminal Law provides for deprivation of liberty for a term exceeding eight years.

[59] An especially serious crime is an intentional offence for which the Criminal Law provides for deprivation of liberty for a term exceeding eight years or life imprisonment.

[60] In 2015, a project on simplifying investigation of less serious crime was finalized (EU co-financed); the aim was to find a better balance between (a) the resources used at the investigation and (b) the actual harm less serious crime have caused to the society.

caused harm that would warrant the application of a criminal punishment".

2.A.5.
Are there other types of cybercrime covered by your national legislation which are not mentioned in Table 2 above?

Yes.

In addition to criminal offences listed in answer to Q 2.A.1., the following relevant acts (namely, cyber-dependent and cyber-enabled criminal acts) might be mentioned:

- Article 78 (triggering of national, ethnic and racial hatred) paragraph 2 of the Criminal Law: for a person who commits the same acts [*acts directed towards triggering national, ethnic, racial or religious hatred or enmity*], if they are committed by a group of persons or a public official, or a responsible employee of an undertaking (company) or organisation, or *if it is committed utilising an automated data processing system*, the applicable punishment is deprivation of liberty for a term up to five years or temporary deprivation of liberty, or community service, or a fine;
- Article 88 (terrorism) paragraph 2 refers to cyber-terrorism: for a person who commits destruction or damage to physical objects, *automated data processing systems, electronic networks*, as well as other objects located in the territory or the continental shelf of the State, if such activities are committed for the purpose provided for in paragraph one of this Article[61], the applicable punishment is life imprisonment or deprivation of liberty for a term of eight and up to twenty years, with or without confiscation of property and with probationary supervision for a term up to three years;
- Article 148 (infringement of copyright and neighbouring rights):
  - for a person who commits *infringement of copyright or neighbouring right*, if such infringement has caused *substantial harm to rights and interests protected by law of a person*, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine (paragraph 1);
  - for a person who commits the criminal offence provided for in paragraph one of this Article, if it has been committed *by a group of persons pursuant to prior agreement*,

[61] Namely, "(..) for the purpose of intimidating inhabitants or with the purpose of inciting the State, its institutions or international organisations to take any action or refrain therefrom, or for purposes of harming the State or the inhabitants thereof or the interests of international organisations (terrorism) (..)".

the applicable punishment is deprivation of liberty for a term up to four years or temporary deprivation of liberty, or community service, or a fine (paragraph 2);

- for a person who commits infringement of copyright or neighbouring right if it is committed *in large scale or by an organised group, or by compelling, by means of violence, threats or blackmail, the renouncing of authorship, or commits compelling of joint authorship, if it is committed by means of violence, threats or blackmail*, the applicable punishment is deprivation of liberty for a term up to six years, with deprivation of the right to engage in specific employment for a term up to five years and with or without police supervision for a term up to three years (paragraph 3);

– Article 182 (arbitrary consumption of electricity, thermal and gas, arbitrary utilisation of electronic communications services):
  - for a person who commits arbitrary consumption of electricity, thermal energy or gas services or *arbitrary utilisation of electronic communications services*, if *substantial material damage* has been caused thereby, the applicable punishment is temporary deprivation of liberty or community service, or a fine;
  - for a person who commits arbitrary consumption of electricity, thermal energy or gas services or arbitrary utilisation of electronic communications services, if it is committed on a *large scale* or *if it has been committed by a group of persons pursuant to prior agreement*, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine;
– Article 245 (violation of safety provisions regarding information systems): for a person who commits violation of provisions regarding *information storage and processing, which have been formulated in accordance with an information system or the protection thereof, or violation of other safety provisions regarding computerised information systems, where committed by a person responsible for compliance with these provisions*, if such has been a cause of stealing, destruction or damage of the information, or other *substantial harm* has been caused thereby, the applicable punishment is temporary deprivation of liberty or community service, or a fine.

2.A.6.
Do you plan to amend your existing legislation or introduce new legislation on cybercrime?
If so, for what reason?
If relevant, indicate any provisional planning in this regard?

Are there any difficulties already foreseen in this respect? If so, how you plan to overcome them?

No.

2.A.7.
Please indicate any other binding or non-binding rules/ministerial or judiciary instructions relevant for the application of the cybercrime specific legislation.

There are internal rules/instructions which *inter alia* refer to the application of the cybercrime specific legislation. For instance, order (internal legal act) of the State Police on centralized request and obtaining of the electronic evidence (please, see answer to Q 2.B.4).

In the context of the State Police, there are also several cooperation agreements concluded which contribute to the effectiveness of cybercrime investigation. For instance, in 2012 a cooperation agreement between the State Police and CERT.LV was concluded which *inter alia* states that CERT.LV will inform the State Police about the registered incidents with a view to Articles 117^1, 241, 243, 244, 244^1, 245 and other relevant articles of the Criminal Law; it also entails a specific provision on CERT.LV's assistance on specific IT security issues (by, for instance, delivering specialist opinions).

2.B. Procedural issues

2.B.1.
According to your legislation can fundamental rights and freedoms, in particular privacy, personal data, freedom of expression be limited for the purposes of cybercrime investigation/prosecution?
If so, please briefly describe.

Yes, the general rules of the Criminal Procedure Law apply also to cybercrime investigation/prosecution.

1. Guaranteeing fundamental rights and freedoms

According to Article 12 of the Criminal Procedure Law "criminal proceedings shall be performed in conformity with internationally recognised civil rights and without allowing for the imposition of unjustified criminal procedural duties or excessive intervention in the life of a person" by further explaining that "civil rights *may be restricted* only in cases where such restriction is required for public safety reasons, and only in accordance with the procedures laid down in (..) [Criminal Procedure] Law according to the character and danger of the criminal offence".

The article also states that "application of safety measures related to the deprivation of liberty, the infringement of the immunity of publicly inaccessible places, and the confidentiality of correspondence and means of communication shall be permitted only with the *consent of the investigating judge or court*".

Furthermore, "an official, who performs the criminal proceedings, has a *duty to protect the confidentiality of the private life of a person* and the commercial confidentiality of a person" and that "information regarding such confidentiality shall be obtained and used only in the case where such information is necessary in order to clarify conditions that are to be proven".

Finally, the article also states that "*a natural person has the right to request* that a criminal case does not include information regarding the private life, commercial activities, and financial situation of such person or the betrothed, spouse, parents, grandparents, children grandchildren, brothers or sisters of such person, as well as of the person with whom the relevant natural person is living together and with whom he or she has a common (joint) household, *if such information is not necessary for the fair regulation of criminal legal relations*".

2. Investigative judge

It shall be also noted that in Latvia there is a concept of an "investigative judge" who, according to Article 40 of the Criminal Procedure Law, is a "judge whom the chairperson of the district (city) court has assigned, for (..) *the control of the observance of human rights in criminal proceedings*".

Article 41 further clarifies the following *duties* of an investigative judge:

During an investigation and criminal prosecution:	From a court of first instance to the commencement of the adjudication of a case:
– to decide on the application of compulsory measures in the cases provided for by law; – to decide on the applications of a suspect or an accused regarding the amending or revoking of the security measures that have been applied with a decision of the investigating judge; – to examine complaints regarding a security measure applied by a person directing the proceedings; – to decide on the performance of procedural actions; – *to decide on complaints in relation to an unjustified violation during criminal proceedings of confidentiality that is protected by law;* – to decide on the request of a person who has the right to assistance of a defence counsel to give a discharge of payment regarding the use of the assistance of an advocate.	– the application of an accused in relation to the amending or revocation of security measures; – the proposal of a public prosecutor in relation to the selection or amendment of a security measure; – the acquaintance of a person involved in criminal proceedings, who has the right to get acquainted with the materials of a criminal case, with special investigative actions that are not attached to a criminal case (primary documents).

It should be underlined that investigating judge is not permitted to replace a person directing the proceedings and a supervising public prosecutor in pre-trial criminal proceedings by giving instructions regarding the direction of an investigation and the performance of investigative actions.

2.B.2.

Please specify which of the following investigative techniques are permissible under your national law, including the relevant legal provisions and any specific conditions, such as derogations from the general regime:

- ***search and seizure of information system/computer data;***
- ***real-time interception/collection of traffic/content data;***
- ***preservation of computer data;***
- ***order for stored traffic/content data;***
- ***order for user information.***

Search and seizure *(in general)*

Article 179 of the Criminal Procedure Law states that "*search* shall be conducted for the purpose of finding objects, documents, corpses, or persons being sought that are significant in criminal proceedings"; Articles 180-185 further specify the procedure to be followed and other relevant issues.

Article 186 states that "*seizure* is an investigative action whose content is the removal of objects or documents significant to a case, if the performer of the investigative action knows where or by whom the concrete object or document is located and a search for such object or document is not necessary, or such object or document is located in a publicly accessible place"; additional seizure related matters are regulated in Articles 187-188.

Submission of objects and documents requested by a person directing the proceedings

According to Article 190 of the Criminal Procedure Law, a person directing the proceedings, without conducting the seizure provided for in Article 186 (please, see above), is entitled "to *request* from natural or legal persons, in writing, objects, documents and information regarding the facts that are significant to criminal proceedings, including in the form of electronic information and document that is processed, stored or transmitted using electronic information systems".

It is further stated that "if natural or legal persons do not submit the objects and documents requested by a person directing the proceedings during the term specified by such person

directing the proceedings, the person directing the proceedings shall conduct a seizure or search in accordance with the procedures laid down in (..) [the Criminal Procedure] Law".

It is also stated that "the heads of legal persons have a duty to perform a documentary audit, inventory, or departmental or service examination within the framework of the competence thereof and on the basis of a request of a person directing the proceedings, and to submit documents, within a specific term, together with the relevant additions regarding the fulfilled request".

Storage of data

Article 191 of the Criminal Procedure Law on storage of data located in an electronic information system states that "a person directing the proceedings *may assign* (..) *the owner, possessor or keeper of an electronic information system* (a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) *to immediately ensure the storage, in an unchanged state, of the totality of the specific data necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system*".

It further explains that "the duty to store data may be specified for a term of up to *thirty days*, but such term *may be extended*, if necessary, by an investigating judge by a term of up to thirty days".

Disclosure and issue of data stored

According to Article 192 of the Criminal Procedure Law, disclosure and issue of data stored in an electronic information system are regulated as follows:

– *during the pre-trial criminal proceedings* – "an investigator with the consent of a public prosecutor or a data subject and a public prosecutor with the consent of a higher-ranking prosecutor or a data subject *may request, that the merchant of an electronic information system disclose and issue the data to be stored in the information system* in accordance with the procedures laid down in the Electronic Communications Law[62]" (please, see also answer to Q 9.1.);

[62] According to Article 71[1] of the Electronic Communication Law "data to be retained *shall be retained and transferred* to pre-trial investigation institutions, persons performing investigative field work, State security institutions, the Office of the Public Prosecutor

- *during the pre-trial criminal proceedings* – "the person directing the proceedings *may request* in writing, based on a decision of an investigating judge or with the consent of a data subject, that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Article 191 of this Law" (please, see above on storage of data);
- *in adjudicating a criminal case* – "a judge or the court panel may request that a merchant of electronic communications discloses and issues the data to be stored in accordance with the procedures laid down in the Electronic Communications Law or that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Article 191 of this Law" (please, see above).

Control of means of communication *(a special investigative action[63])*

Article 218 of the Criminal Procedure Law states that "the control of telephones and other means of communications without the knowledge of the members of a conversation or the sender and recipient of information shall be performed, based on a decision of an investigating judge, if there are grounds to believe that the conversation or transferred information may contain information regarding facts included in circumstances to be proven, and if the acquisition of necessary information is not possible without such operation".

It further explains that "the control of telephones and other means of communication with the written consent of a member of a conversation, or the sender or recipient of information, shall be performed if there are grounds to believe that a criminal offence may be directed against such persons or the relative thereof, or also if such person is involved or may be enlisted in the committing of a criminal offence".

and the courts in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings"; "an electronic communications merchant *shall ensure the transfer* of data to be retained to (..) [these] institutions (..) on the basis of a *request* therefrom". The Article also states that "an electronic communications merchant shall *ensure the retention of retained data in such volume as they are acquired or processed in providing electronic communications services*, as well as ensuring the protection thereof against accidental or unlawful destruction, loss or modification, or processing or disclosure not provided for in this Law (..)". According to this law, an electronic communications merchant is a "merchant or a branch of a foreign merchant who has the right to perform commercial activity, to ensure a public electronic communications network or provide electronic communications services in accordance with the procedures laid down in the Electronic Communication Law".

[63] Is performed if, in order to ascertain conditions to be proven in criminal proceedings, the acquisition of information regarding facts is necessary without informing the person involved in the criminal proceedings and the persons who could provide such information.

Control of data located in automated data processing system *(a special investigative action)*

Article 219 of the Criminal Procedure Law states that "search of an automated data processing system (a part thereof), the data accumulated therein, the data environment, and the access thereto, as well as the removal thereof without the information of the owner, possessor, or maintainer of such system or data shall be performed, based on a decision of an investigating judge, if there are grounds to believe that the information located in the concrete system may contain information regarding facts included in circumstances to be proven".

It further explains that "a person directing the proceedings *may request*, for the commencement of an investigative action, that the person who oversees the functioning of a system or performs duties related to data processing, storage or transmission *provide the necessary information, ensure the completeness of the information and technical resources present in the system and make the data to be controlled unavailable to other users*" and that "a person directing the proceedings may prohibit such person to perform other actions with data subject to control, as well as shall notify such person regarding the non-disclosure of an investigative secret".

It is also clarified that "in a decision on control of data present in an automated data processing system an investigating judge may allow a person directing the proceedings to remove or store otherwise the resources of an automated data processing system, as well as to make copies of these resources".

Control of the content of transmitted data *(a special investigative action)*

Article 220 of the Criminal Procedure Law states that "the interception, collection and recording of data transmitted with the assistance of an automated data processing system using communication devices located in the territory of Latvia without the information of the owner, possessor, or maintainer of such system shall be performed, based on a decision of an investigating judge, if there are grounds to believe that the information obtained from data transmission may contain information regarding facts included in circumstances to be proven".

2.B.3.

Are the following defined in your legislation or practice: computer data, content data, traffic data, order for search/seizure of information system, networks managed or controlled by suspects of cybercrime?

Terms such as automated data processing system,[64] publicly unavailable data, ICT and electronic communications network terminal equipment are used in the Criminal Law; definitions however are not provided.

The Electronic Communications Law, for instance, contains the following definitions:

- **electronic communications merchant** – a merchant or a branch of a foreign merchant who has the right to perform commercial activity, to ensure a public electronic communications network or provide electronic communications services in accordance with the procedures laid down in the Electronic Communications Law;
- **electronic communications service** – a service that is usually ensured for remuneration and which wholly or mainly consists of the transmission of signals in electronic communications networks;
- **electronic communications service provider** – an electronic communications merchant who provides publicly accessible electronic communications services, utilising the public electronic communications network;
- **electronic communications network** – transmission systems, switching and routing equipment (including network elements which are not being used) and other resources, which irrespective of the type of transmitted information permits the transmission of signals utilising wires, radio waves, optical or other electromagnetic means in networks, including:
  a) satellite networks, fixed networks (channel and packet switching networks, including Internet) and mobile terrestrial electronic communications networks,
  b) networks, which are utilised for radio and television signal distribution,
  c) cable television and cable radio networks, electricity cables systems to the extent that they are utilised in order to transmit signals;
- **access** – a service provided to another electronic communications merchant with specific conditions for access to equipment and services necessary for the ensuring of electronic

[64] Automated data processing systems can be further divided as follows: (1) state information systems; (2) IT critical infrastructure; (3) systems procession personal data; (4) systems of financial and capital market members; (5) public electronic communication network systems; (6) national/municipal government systems; (7) other systems of both legal and natural persons.

communications services, including the use thereof for the distribution of information society services or broadcast content services. Access includes access to electronic communications network elements and the associated facilities thereof with wire or non-wire connections, especially access to the subscriber line, as well as equipment and services, which are necessary in order to ensure services in the subscriber line, access to physical infrastructure (including buildings, cable lines, cable ducts and antenna masts and towers utilised to ensure electronic communications networks), access to the relevant software systems (including operational support systems), access to information systems and databases in order to perform orders, deliveries, maintenance and damage prevention requests and preparation of bills, access to number translation or systems, which offer similar possibilities, access to electronic communications networks (especially for roaming), access to conditional access systems for digital television services and access to virtual network services;

- **terminal equipment** – equipment (for example, telephone sets, facsimile machines, modems, data transmission equipment, private automatic telephone exchanges, private networks, and public pay telephones) that is intended for direct or indirect connection to public electronic communications network termination points;
- **identifiable terminal equipment** – a terminal equipment, for which the manufacturer has granted an identifier for the recognition in an electronic communications network;
- **end-user** – an electronic communications services user who does not utilise such services to ensure electronic communications services to other persons;
- **access to data flow** – provision of digital subscriber line services by the operator to another merchant of electronic communications so that it could offer broadband access to the Internet for the end-user;
- **traffic data** – any information or data, which is processed in order to transmit information by an electronic communications network or to prepare accounts and register payments, except the content of transmitted information;
- **location data** – data, which is processed in an electronic communications network or processed using electronic communications services and indicates the location of the terminal equipment of an electronic communications service user; for public mobile electronic communications networks, satellite networks and non-wire networks, which are utilised for the distribution of radio or television signals, it shall be the geographic location (address) of the terminal equipment of an electronic communications service user, but for public fixed networks, cable television and cable radio networks, and

electricity cable systems to the extent that they are utilised in order to transmit electronic communications signals – the termination point address;

- **location information database** – a database, which contains information regarding location data;
- **data to be retained** – the traffic data referred to in Annexes 1[65] and 2[66] to the Electronic Communications Law, location data and the associated data thereof, which is necessary in order to identify the subscriber or user;

In addition, please, see answer to Q 2.B.2. on the Criminal Procedure Law where notions of "search" and "seizure" (in general terms) are explained. The Criminal Procedure Law also refers to "decision on a search" (Article 180[67]) and "decision on seizure" (Article 187[68]).

2.B.4.

Please explain how e-evidence, as defined under your legislation or practice (specify what is considered as e-evidence according to your law or working definition) is collected, stored and transferred to the prosecutor or the court to be used in a trial.

According to Article 136 of the Criminal Procedure Law "*electronic evidence* in criminal proceedings may be information regarding facts in the form of electronic information that has been processed, stored, or broadcast with automated data processing devices or systems".

[65] Refers to public fixed telephone network operators and public mobile telephone network operators.

[66] A public electronic communications network operator shall retain the following data:

- the user ID(s) allocated;
- the user ID and telephone number allocated to any connection entering the public telephone network;
- the given name, surname or designation and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the connection;
- voice telephony call [utilising Internet Protocol (IP)] recipient ID or telephone number;
- the given name, surname or designation and address of the subscriber or registered user and user ID of the intended recipient of the call;
- the date and time (based on a certain time zone) of the log-in and log-off of the public Internet access service, together with the IP address, whether dynamic or static, allocated by the Internet access service provider, and the user ID;
- the date and time (based on a certain time zone) of the log-in and log-off of the sending of e-mail or voice telephony call [utilising Internet Protocol (IP)];
- the type of public Internet access service;
- the calling telephone number for dial-up access; and
- the digital subscriber line (DSL) or other access line ID of the originator of the connection.

[67] A search shall be conducted with a decision of an investigating judge or a court decision; it shall indicate who will search and remove, where, with whom, in what case, and the objects and documents that will be sought and seized. It is also stated that in emergency cases where, due to a delay, sought objects or documents may be destroyed, hidden, or damaged, or a person being sought may escape, a search shall be performed with a decision of the person directing the proceedings (in this case, a search shall be performed with the consent of a public prosecutor).

[68] A seizure shall be conducted with the decision of a person directing the proceedings; it shall indicate who will seize an object or document, where, with whom, in what case, and the objects and documents that will be seized.

In addition, it should also be noted that, according to Article 135 paragraph 2 which refers to the term "*document*", it has been explained that "computerised information media and recordings made with sound- and image-recording technical means (..) shall also be considered documents, within the meaning of evidence (..)".

As regards collection, storage and transfer of electronic evidence, please, refer to the answers to:

- Q 2.B.2. (the relevant articles of the Criminal Procedure Law and the Electronic Communication Law);
- Q 9.1. (Electronic Communication Law and Cabinet Regulation No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled").

Additional information:

With respect to practical arrangements and good practice regarding electronic evidence, there is a *single contact point* designated at the State Police which is in charge of both requesting and receiving the necessary data from electronic communications merchants (hence there is a centralized cooperation between the State Police and electronic communications merchants established). For this purpose, a specific data base has been designed. The single contact point is available 24/7 and receives requests from all State Police structures (in each region (regional State Police entity) a contact person is designated).

2.B.5.
What are the admissibility rules for e-evidence, if any?
Do they differ if the e-evidence is obtained outside your Member State?

Article 130 of the Criminal Procedure Law on *admissibility of evidence* (also refers to electronic evidence) states that "it shall be admissible to use information regarding facts

acquired during criminal proceedings, if such information was obtained and procedurally fixed in accordance with the procedures laid down in the Criminal Procedure Law".

It further elaborates that "information regarding facts that has been acquired in the following manner shall be recognised as *inadmissible and unusable* (..): (1) using violence, threats, blackmail, fraud, or duress; (2) in a procedural action that was performed by a person who, in accordance with (..) [the Criminal Procedure] Law, did not have the right to perform such operation; (3) allowing the violations specially indicated in (..) [the Criminal Procedure] Law that prohibit the use of a concrete piece of evidence; (4) violating the fundamental principles of criminal proceedings".

The Article at the same time states that "information regarding facts that has been obtained by allowing other procedural violations shall be considered *restrictedly admissible*, and may be used in proving only in the case where the allowed procedural violations are not essential or may be prevented, or such violations have not influenced the veracity of the acquired information, or if the reliability of such information is approved by the other information acquired in the proceedings".

These admissibility rules refer also to electronic evidence obtained outside Latvia (namely, which are obtained according to Chapter 83 "Request to a Foreign State Regarding the Performance of Procedural Actions" of the Criminal Procedure Law).

2.B.6.
Do you perform electronic or remote forensic examination?
If so, please provide details.

1. State Police

Forensic examination is carried out by the Forensic IT Unit of the Forensics Department of the State Police; forensics refer to both cybercrime and other criminal offences where there are electronic evidence. Forensics is carried out in a laboratory by analysing the seized objects (thus remote examination is not carried out).

In 2014, the Forensic IT Unit carried out 290 forensic examinations; in 2015 (10 months) – 200.

As regards the forensic examinations, *mainly the following tasks are carried out*: settings of network (their identification, search); recovery of deleted documents; information search and recovery of deleted information; recovery of deleted graphical files; search, export and recovery of graphic and video files (with regard to pornography, children sexual abuse and other); search of banknote images in data devices; search and recovery of deleted e-signatures; search of information regarding e-mailing services (their usage, visiting); exporting of history (regarding internet visits) and recovery of deleted history; confirmation regarding downloading/uploading of files; search and recovery of credit card data; analysis of various operating systems (mainly, *Windows, Linux, Unix, Mac OS*); analysis of *Microsoft Windows* operating system register; file carving/recovery; log file analysis; file and file container password cracking/removing; tasks related to data hiding software and encryption software; spyware detection and log analysis; tasks related to remote management software and analysis of log files; tasks related to viruses; search of data of the (also conversion); analysis of magnetic card reading equipment (skimmers) (also self-made equipment (skimmers)); export and recovery of SIM card information; analysis of mobile phone/smartphone memory and information recovery; analysis of tablets; analysis of GPS equipment; data retrieval and analysis of digital photo/video equipment; data retrieval and analysis of consoles; password extraction from hard disks.

In future the Forensic Department intends to focus more in-depth on issues such as recovery of information from damaged data devices as well as information retrieval from damaged mobile phones/smart phones and tablets.

As regards the IT inspection (or – so called pre-analysis before the forensic examination is done), the following activities are carried out: export of the existing documents; search/selection (through keywords) of the relevant documents (doc, xls, pdf, others); export of the existing graphic files; export of e-mails; export and recovery of chat correspondence.

It shall also be noted that Economic Crimes Enforcement Department (Unit 4 – Cybercrime Enforcement Unit) of the State Police carries out internet intelligence (or so called live/network analysis) (please, in addition, see answer to Q 3.B).

2. *State Forensic Science Bureau (SFSB)*

SFSB is an institution, supervised by the Ministry of Justice, providing forensic investigation services to the law enforcement agencies (if so requested) as well as to other legal and natural entities.

IT/computer forensics is among the areas in which the SFSB provides its services (for instance, information search, recovery of deleted documents, analysis of documents in hard drive, flash, CD and other electronical data devices).

Remote forensic examination is not carried out.

2.B.7.

With regard to encryption, please describe the following:

- ***possible problems you have encountered with encryption;***
- ***in which areas and how were those problems addressed;***
- ***how do the authorities involved cooperate with each other;***
- ***are there specialist centres;***
- ***is decryption carried out in cooperation with private companies;***
- ***in which areas has it not yet been possible to deal with the problem of encryption effectively;***
- ***what is done to address any security concerns that may arise in that context?***

The major problem is accessibility of those encrypted data which are protected by technologically advanced passwords.

Overall the Forensic IT Unit of the Forensic Department of the State Police has the necessary equipment which allows to determine the form of encryption and to access the encrypted information; however, there is limited computation capacity which prevents to achieve better results (hence, if the password is technically advanced and tit cannot be retrieved in a reasonable period of time, the encryption process is ceased). In this regard, Latvia sees as clear added value of EC3's encryption/decryption platform. In light of the encryption issue, Latvia also highly values the availability of the Europol Platform for Experts.

The Forensic IT Unit does not cooperate with the private companies; however, experts may inform the person directing the proceedings[69] that there is need to involve private sector in order to gain the necessary additional information.

2.B.8.
Please describe the special investigative techniques used for the purpose of cybercrime investigation in your MS.
Which ones are most commonly used?

Please, see answer to Q 2.B.2. (special investigative actions).

2.B.9.
Please describe a good practice/lesson learned in respect to the use of a cybercrime investigation technique, if any.

With respect to good practices:

- the State Police has a *close and regular cooperation with the security units of banks and CERT.LV* on malware related issues; this cooperation considerably contributes to the investigation as such;
- Latvia has an *advanced legal framework on pornography* and hence there are *no major qualification issues*; for instance, apart from other countries, in Latvia it was possible to commence a criminal proceeding on so called *Shreck* pornography case which contains a sound recording/talk/animation of a pornographic nature. [70] According to the Law on Pornography Restrictions, "material of a pornographic nature" is a "composition, printed matter, image, computer programme, film, video or sound recording, television programme, or radio programme, other material in any form or type (..)";
- Latvia has a *good cooperation experience with Europol and Interpol in certain targeted cases*; for instance, there was an operative meeting at Europol on a criminal group, formed in Latvia, which was setting up ATM skimmers in the Baltics, UK, Poland and Russia; as

[69] According to the Criminal Procedure Law, a person directing the proceedings shall be: 1) an investigator or in exceptional cases a public prosecutor – in an investigation; 2) a public prosecutor – in a criminal prosecution; 3) a judge who leads the adjudication – in preparing a case for trial, as well as from the moment when a adjudication is announced with which legal proceedings are completed in the court of the relevant instance, until the transferral of the case to the next court instance or until the execution of the adjudication; 4) the composition of a court – during a trial; 5) a judge – after entering into effect of a court adjudication.
[70] As a consequence, this file, for instance, in English language still is available on internet.

a result, several persons participating in this criminal group, were detained in Sweden and Russia.

As a general remark, it should also be mentioned that in Latvia there is a *quick legislative response* to the problems/challenges identified in practice.

2.C. Jurisdiction

2.C.1.
Does your national law provide for jurisdiction with regard to cybercrime acts committed partially/entirely outside the territory of your MS?
If so, please describe the criteria used (e.g. active/passive personality principle).

According to Article 4 of the Criminal Law (on applicability of the Criminal Law outside the territory of Latvia) "*Latvian citizens, non-citizens and foreigners who have a permanent residence permit for the Republic of Latvia*, shall be held liable, in accordance with (..) [the Criminal] Law, in the territory of Latvia for an offence committed in the territory of another state or outside the territory of any state irrespective of whether it has been recognised as criminal and punishable in the territory of commitment".

For an offence committed by a *natural person* "*acting in the interests of a legal person registered in the Republic of Latvia*, for the benefit of the person or as a result of insufficient supervision or control thereof in the territory of another state or outside the territory of any state irrespective of whether it has been recognised as criminal and punishable in the territory of commitment the legal person may be applied the coercive measures provided for in (..) [the Criminal] Law" (please, see answer to Q 2.A.2.).

It further explains that "*foreigners who do not have permanent residence permits for the Republic of Latvia* and who have committed serious or especially serious crimes in the territory of another state which have been directed against the Republic of Latvia or against the interests of its inhabitants, shall be held criminally liable in accordance with (..) [the Criminal] Law irrespective of the laws of the state in which the crime has been committed, if they have not been held criminally liable or committed to stand trial in accordance with the laws of the state where the crime was committed".

Foreigners who do not have a permanent residence permit for the Republic of Latvia and "who have committed a criminal offence in the territory of another state or outside the territory of any state, in the cases provided for in international agreements binding upon the Republic of Latvia, irrespective of the laws of the state in which the offence has been committed, shall be held liable in accordance with (..) [the Criminal] Law if they have not been held criminally liable for such offence or committed to stand trial in the territory of another state".

2.C.2.
How do you resolve conflicts of jurisdiction when two or more MS can investigate and prosecute the same perpetrator for cybercrime acts committed outside their respective territories?
Please provide details of any experience you have had in this area.

In general, conflicts on jurisdiction are resolved via consultation process (in accordance with the Council of Europe legal instruments) as well as by using the *Eurojust* coordination meetings. However, the General Prosecutor's Office has not had such an experience regarding cybercrime.

In addition it should be noted that according to Article 25 of the Criminal Procedure Law "a person may not be tried or punished in Latvia if such person has been convicted or acquitted for the same offence in a foreign state with which Latvia has an agreement regarding mutual recognition of criminal judgments or an agreement regarding the observance of the principles of *ne bis in idem*" and "if a person has been convicted in a foreign state, the part of the punishment that has already been served is to be included in the punishment in the case of repeat adjudication".

2.C.3.
Indicate specific problems and solutions found as regards the establishment of jurisdiction for cybercrime acts committed in the "cloud" or collecting related e-evidence that is stored in the "cloud"?

There are no specific problems and solutions found with regard to the "cloud" issue in Latvia. In Latvia's view, this is a rather global challenge which should/could be addressed at the EU level.

As a general remark, similarly to other countries, if the provider of a "cloud" service is registered in Latvia, investigative actions are carried out in accordance with the relevant national legislation; if the service is registered outside the criminal jurisdiction of the Republic of Latvia – request for criminal legal assistance is used.

Please, see also answer to Q 2.C.1. (on applicability of the Criminal Law outside the territory of Latvia).

Additionally, in a wider context, it should be noted that the State Police has a good cooperation experience with *Microsoft* (a number of requests, submitted by the State Police, have been positively responded).

2.C.4.
Have you used provisions related to the Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings in relation to cybercrime case?
Have you referred cases to Eurojust in order to solve conflict of jurisdiction?
Please provide details about your specific experience.

No.

2.C.5.
Do you consider the existing legal framework sufficient for investigation and prosecution of cybercrime committed outside your national territory?
If not, describe the main shortcomings and provide ideas how in your opinion those could be overcome.

With regard to cybercrime and electronic evidence (data storage requests in particular), *timing* plays a crucial role; in most of the cases requests for criminal legal assistance unfortunately

are not/cannot be fulfilled in a timely enough manner (for instance, in one cybercrime case request, sent by the State Police, was fulfilled after two years).

Taking this into account, the general observation is that "request for criminal-legal assistance" instrument does not correspond to the actual investigation/prosecution needs in the digital age; in light of cybercrime, the implementation procedure of "request for criminal legal assistance" instrument should be reviewed.

3. NATIONAL STRUCTURES

3.A. Judiciary (prosecution and court)

3.A.1.   ***Are cybercrime acts dealt in your country by a general or specialised prosecution/court? Please indicate respectively their number, place within the internal judiciary structure, special powers related to cybercrimes.***

1. Prosecution

According to Article 1 of the Office of the Prosecutor Law ,the Office of the Prosecutor is an *institution of judicial power*, which independently carries out supervision of the observance of law within the scope of the competence determined by the law.

The Office of the Prosecutor is composed of:

- the Office of the Prosecutor General;
- Offices of Prosecutors of judicial regions;
- Offices of Prosecutors of districts (cities);
- specialised Offices of the Prosecutor;
- Service of the Administrative Director.

Powers related to cybercrime (i.e. cyber-dependent and cyber-enabled crime):

Cybercrime	**Entity supervising pre-trial investigation, conducting criminal prosecution and maintaining charges of the State**
Cybercrime within the territory of Riga judicial region (including Articles 241, 243, 244, 244[1] and 245 of the Criminal Law)	Prosecutor's Office of Investigation of Finance and Economic Crimes[71]
Cybercrime where computer/IT systems were involved as tool or target (paragraph 3 of Article 177[1] of the Criminal Law)	Prosecutor's Office for Organized Crime and Other Branches[72]

[71]A specialised Office of the Prosecutors; has a status of the Office of Prosecutors of district.
[72] A specialised Office of the Prosecutors; has a status of the Office of Prosecutors of judicial region.

Other cybercrime (covered by the 7th round of mutual evaluations, please, see in addition answer to Q 2.A.1.).	Prosecutor's Office of general jurisdiction[73]

2. Courts

According to Article 82 of the Constitution "in Latvia, court cases shall be heard by *district (city) courts, regional courts and the Supreme Court*, but in the event of war or a state of emergency, also by military courts".

There are *no special (extraordinary) courts* in Latvia (paragraph 5 of Article 1 of the Law On Judicial Power clarifies that "special (extraordinary) courts, which do not observe the procedural norms prescribed by law and replace the courts referred to in paragraph three[74]of this Article, are not allowed and shall not be established").

Hence, in Latvia the cyber-dependent crime cases and cyber-enabled crime cases are heard by ordinary district (city) courts[75] and regional courts[76] as well as the Supreme Court.[77]

3.A.2.
What measures have been taken or are planned to strengthen the capacity to investigate/prosecute cybercrimes in your MS?

The Office of the Prosecutor pays a particular attention to the training of prosecutors; efforts in this regard will be intensified.

In 2014, prosecutors have participated in the following training activities:

- in Latvia:

[73] Territory of (1) Riga judicial region; (2) *Vidzeme* judicial region; (3) *Kurzeme* judicial region; (4) *Zemgale* judicial region; (5) *Latgale* judicial region; may have a status of status of the Office of Prosecutors of district or judicial region.
[74] Judicial power in the Republic of Latvia is vested in district (city) courts, regional courts, the Supreme Court and the Constitutional Court, but in state of emergencies or during war – also military courts.
[75] *District and city courts* are the courts of first instance in civil, criminal and administrative cases.
[76] *Regional courts*, as appellate courts, hear civil, criminal and administrative cases in a panel of three regional court judges (until 1 January 2014 the regional courts also acted as the first instance courts in certain categories of cases).
[77] *The Supreme Court* comprises a Senate, consisting of three divisions (Civil Cases, Criminal Cases and Administrative Cases); it is the court of appeal on points of law (*cassation*), unless the law provides otherwise. Until 31 December 2014 the Supreme Court also had two chambers (on Civil Cases and Criminal Cases) which functioned as the appellate instance in cases which have been reviewed by regional courts as the first instance courts. Taking into account the on-going judiciary reforms, as for 1 January 2015 the Chamber on Criminal Cases ceased to function; the Chamber on Civil Cases will function until 31 December 2016.

- "Cybercrime" (organized by the Office of the Prosecutor in cooperation with the Latvian Judicial Training Centre; 54 participants);
- "Cybercrime and electronic evidence" (organized by the Office of the Prosecutor in cooperation with the Latvian Judicial Training Centre; 57 participants);
- "Cybersecurity crisis management" (organized by CERT.LV; one participant);

– abroad:
- "Judicial and technical aspects of cybercrime" (organized by the Academy of European Law; Trier, Germany; three participants).

In 2015, prosecutors have participated in the following training activities:

– in Latvia:
- "Planning and justifying the search and seizure of electronic evidence: practical implications for legal practitioners in criminal proceedings before presenting evidence in court" (organized by the Academy of European Law in cooperation with the Latvian Judicial Training Centre; five participants);

– abroad:
- "Basic course on judicial and technical aspects of cybercrime" (organized by the Academy of European Law; Trier, Germany; two participants);
- "Digital piracy – investigation and prosecution" (Hungary; one participant).

3.A.3.
Please specify the main obstacles to successful prosecution of cybercrimes in your MS. Have you experienced particular difficulties in prosecuting and/or obtaining conviction for any specific offence?
Could you describe the reasons.

The Office of the Prosecutor has identified the following main obstacles and difficulties:

– according to Article 19 of the Electronic Communications Law, electronic communications merchants have a duty to ensure (in accordance with the procedures laid down in Article 71^1 of the Law[78]) the storage of data to be retained for *18 months*,

[78] As already noted (please, see also footnote 62), according to Article 71^1 of the Electronic Communication Law "data to be retained shall be retained and transferred to pre-trial investigation institutions, persons performing investigative field work, State security institutions, the Office of the Public Prosecutor and the courts in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings"; "an electronic communications merchant shall ensure the transfer of data to be retained to (..) [these] institutions (..) on the basis of a request therefrom". The Article also states that "an electronic communications merchant shall ensure the retention of retained data in such volume as they are acquired

as well as the transfer of such data (also to the Office of the Public Prosecutor); in some (complicated and long-lasting) cases **18 months for data storage is too short period of time;**

- **anonymous internet service providing** (pre-paid internet, WiFi, one IP address to several/many objects);
- electronic communications merchant's **inability to submit the requested information** in a **timely manner**;
- **possibility to use one IP address by thousands/a day** (agreements of IP address usage);
- **long time** for receiving **IT forensic examination** results (in Latvia, there is lack of experts and overload of existing experts);
- **very limited possibility to receive IP addresses** (registered outside Latvia) in a **timely manner.**

3.B. Law enforcement authorities

3.B.1.

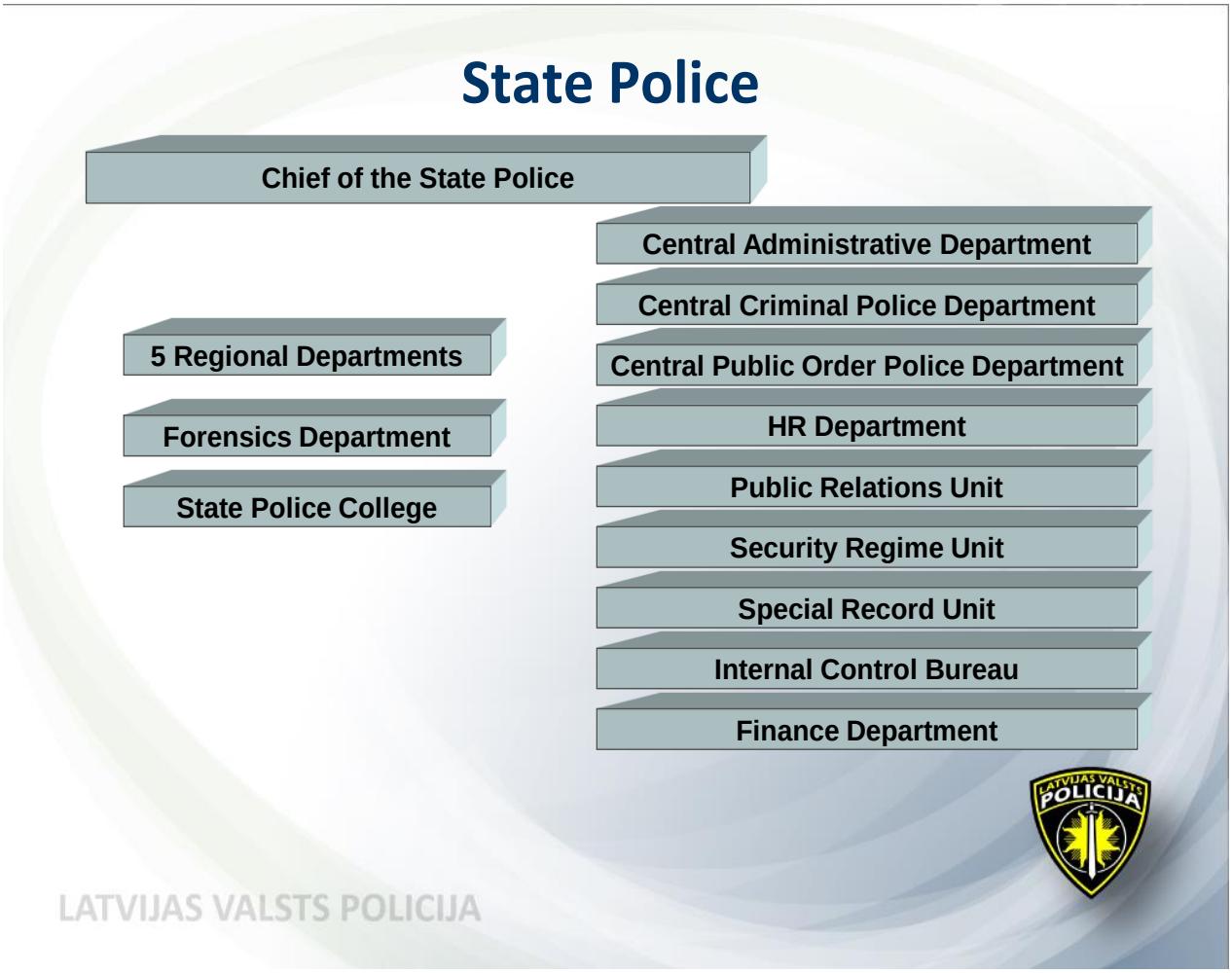
Please describe the law enforcement structure for preventing and combating cybercrime, specifying its composition and powers.

In Latvia the following structures of the State Police are responsible for prevention and fight against cybercrime:

1) the Central Public Order Police Department – prevention of cybercrime;
2) the Central Criminal Police Department – fight against cybercrime.

Please, see the organisational chart of the **State Police** below:

or processed in providing electronic communications services, as well as ensuring the protection thereof against accidental or unlawful destruction, loss or modification, or processing or disclosure not provided for in this Law (..)".



1. Prevention

Crime Prevention Unit (CPU), which is an integral part of the Central Public Order Police Department, is responsible for coordination and implementation of crime prevention activities.

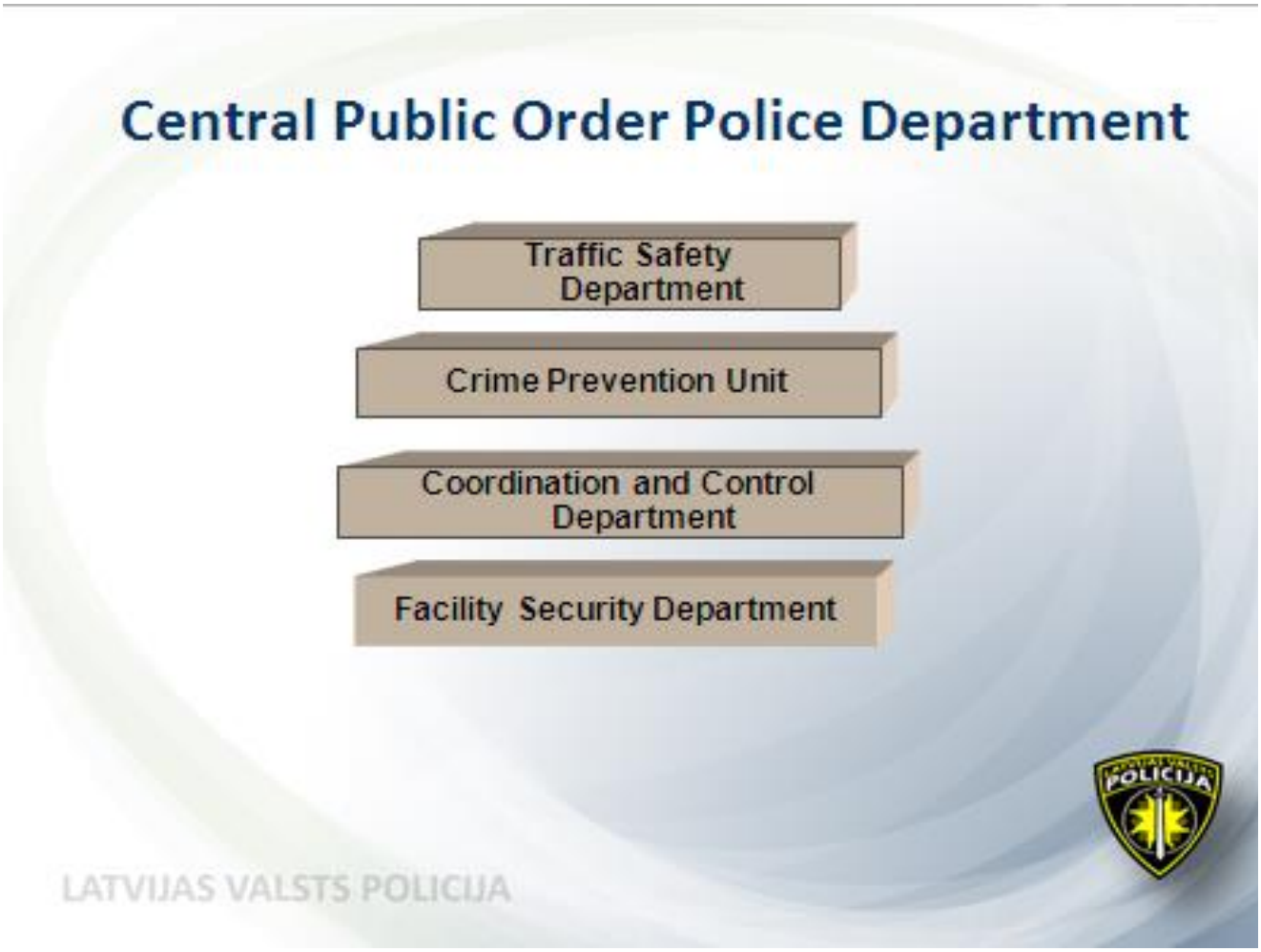
In addition, certain prevention tasks are also implemented at level of the Regional State Departments (5) and districts (with inspectors specialized in various areas).

At the CPU there are four police officers specifically designated for implementing prevention measures in the following fields: (1) drugs; (2) violence (at school; domestic violence); (3) property crimes; (4) cybercrimes. Each officer, in his/her respective field, is in charge of enhancing cooperation with the relevant state/municipal institution, NGOs and other stakeholders as well as of obtaining additional funding.

It should also be mentioned that the CPU has established valuable cooperation with the relevant structures of the Central Criminal Police Department; for instance, the Economic Crimes Enforcement Department (please, see below) consults the CPU officers on novelties and other relevant issues relating cybercrime.

As regards involvement of civil society, in 2016 a volunteer programme will be launched at the State Police; volunteers will raise awareness and spread information to a larger public on a number of topical issues, including on internet safety.

Please, see the organisational chart of the **Central Public Order Police Department** below:



2. Fight against cybercrime

There are five departments at the Central Criminal Police Department; two of them are directly dealing with fight against cybercrime:

– the Economic Crimes Enforcement Department;

– the International Cooperation Bureau.

The Economic Crimes Enforcement Department has four units:

– Unit 1 – Information and Financial Analysis group;
– Unit 2 – Unit for the fight against criminal offences in the field of banks, credit institutions;
– Unit 3 – Unit combatting frauds, malfeasance, money counterfeiting, unlicensed business;
– Unit 4 – Cybercrime Enforcement Unit (CEU).

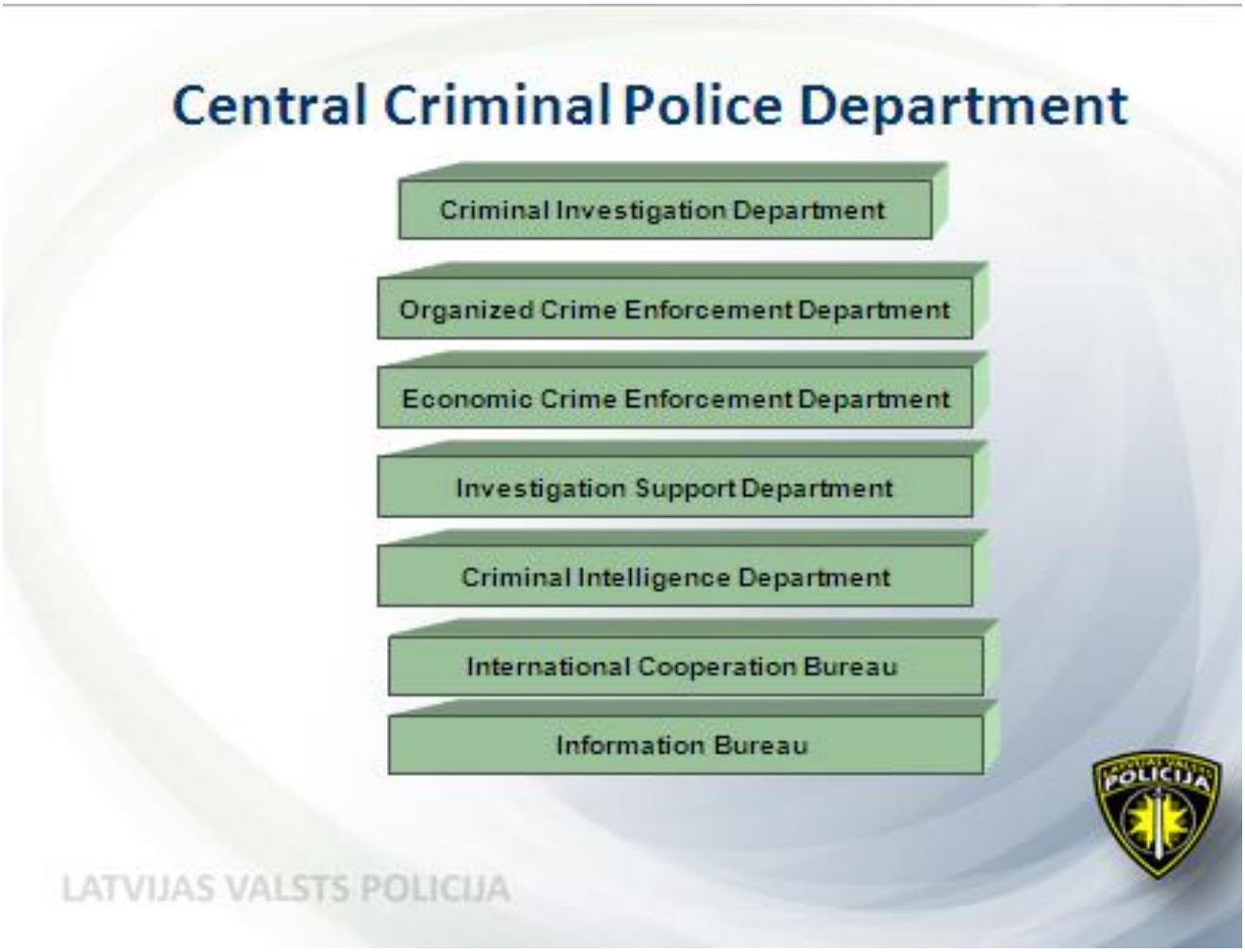
The CEU has 13 officers in total (including the Head of Unit); the task division is as follows:

– Crimes against automated data processing systems group (three officers);
– Operational analysis group (one officer);
– Technical support, internet intelligence[79], crimes against online child sexual abuse group (two officers);
– Intellectual property protection group (two officers);
– Investigative capacity (three officers).

It should also be mentioned that on 7 April 2015 amendments were made to the Cabinet Regulation No 568 on salaries and premiums of those officials who work in authorities subordinated to the Ministry of the Interior (the State Police, included). According to these amendments, those officials who work in the field of fight against cybercrime can be awarded with a premium (up to 400 euros); results of individual performance is the main criteria when deciding upon premium. It should also be noted that this premium can be added to any other premium envisaged by the Cabinet Regulation No 568 (for instance, to the premium on work in the field of organised crime (up to 400 euros) and serious crime (up to 285 euros)).

Please, see the organisational chart of the **Central Criminal Police Department** below:

[79] *Inter alia* monitoring of social media.



3.B.2.

Do you have a specialised body to investigate cybercrime?

If so, please provide details.

If not, please explain which general entities/bodies are responsible for the investigation of cybercrime and whether they have specialised officers.

Are there special posts for IT forensic examiners?

As regards investigation of cybercrime, please, see answer to Q 3.B.1.

With regard to IT forensics examiners – please, see answer to Q 2.B.6. on the Forensic IT Unit of the Forensics Department of the State Police.

As regards the human resources, currently there are four certified experts at the Forensic IT Unit who provide support to investigators; the certified experts have higher education in the IT field.

In fall 2015, establishment of an IT specialist group was commenced; the aim of this group is to deliver a high quality support to the investigators before an expert-examination is determined. Currently there are two specialists who are undergoing training (training is delivered by the experts of the Forensic IT Unit). In the first half of 2016 it is planned to expand the group with two more specialists.

3.B.3.

Please specify the main obstacles to successful investigation of cybercrimes in your MS.

The State Police has identified the following main challenges (ordered according to their priority):

- capacity of the CEU;
- training;
- technical capabilities and equipment (for instance, regarding evidence fixing on the spot);
- fast developing technological novelties (for instance, regarding encryption);
- IT forensics:
    - content-wise – challenges relate to malware and cyber-attacks in particular; CERT.LV as a *specialist*[80] provides valuable contributions which however cannot be regarded as evidence in criminal proceeding (according to the Criminal Procedure Law, evidence in criminal proceedings "may be the conclusion of an *expert*[81] (..) regarding facts and circumstances that has been provided by an expert (..) involved in concrete criminal proceedings";
    - timing-wise – forensic examination is usually carried within 1-2 months.

All these issues are currently being addressed; for instance, it is planned to focus on training and technical capabilities/equipment by implementing a project "Capacity building to prevent and fight against cybercrime" (Internal Security Fund) (please, see answer to Q 1.8.).

3.B.4.

Do you have operational 24/7 contact point for urgent requests?

[80]According to the Criminal Procedure Law "a specialist is a person who provides assistance to an official performing criminal proceedings, on the basis of the invitation of such official, using his or her special knowledge or work skills in a specific field".
[81] Expert of an expert-examination institution (Article 33) or invited expert (Article 34).

Please describe their organisational structure and competences.
Please indicate the procedural steps which are followed in handling the requests (see Preamble, paragraph 22 and Article 13 of Directive 2013/40/EU and Article 35 of the Budapest Convention).

Yes.

The operational 24/7 contact point (CP) is the Operational Coordination and Information Provision Unit (OCIPU) of the International Cooperation Bureau of the Central Criminal Police Department of the State Police.

The Unit acts as an international criminal judicial cooperation "front office", providing a single point of contact (SPOC) by coordinating all international exchange of information in the 24/7 regime (Interpol, Europol, SIRENE, cooperation in criminal matters, cybercrime contact point). Thus, Latvia has implemented a "one stop shop" concept by including all the international police cooperation services in a common data acquisition and processing flow.

Organisational structure

There are 16 employees at the OCIPU: ten duty officers, four police officers (who carry out administrative tasks during the working hours) and one civilian staff (dealing with international projects).

Only police officers are employed as duty officers in the CP (10 police officers working shifts).

Competence

The CP's competence:

- providing and exchanging information between Latvian and foreign law enforcement agencies 24/7;
- assisting Latvian and foreign law enforcement agencies in combating and prevention of organized crime, cybercrime and illegal immigration;

- dealing with persons identification, check of documents, search of wanted and missing persons, search of stolen vehicles and items;
- coordination of involved authorities in cases of prevention and investigation of cross-border crimes, including police cooperation in the framework of Schengen convention (For instance, Article 40-41);
- general police co-operation (Article 39 of Schengen Convention);
- Swedish initiative (Council Framework Decision 2006/960/JHA);
- Prüm hit follow-up procedure.

Officers' competence

The CP officers have investigative powers and applies any investigative measure task related to activities within criminal case. CP also provides instant support in order to perform investigation or criminal proceedings; in addition, it collects electronic evidence in relation to various types of offences.

Most of the CP's officers have attended basic course ("New technologies at police work") organized by the State Police College.[82] Hence, the CP officers have basic knowledge on cybercrime investigation as well as on providing technical advice for stopping or tracing an attack.

Procedural steps

Please see answers to Q 7.A. In addition, it should be mentioned that information exchange is also performed using Interpol, Europol and "Swedish Initiative".[83]

3.C. Other authorities

3.C.1.
Are there other national authorities besides judiciary and LEA responsible involved in the prevention of and fight against cybercrime?
If so, please provide details on their structure and powers.

[82] An educational institution under the authority of the State Police.
[83] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L 386, 29.12.2006., p.89)

Besides judiciary and law enforcement agencies, role of the following entities in prevention and fight against cybercrime should be underlined:

– National IT Security Council;
– CERT.LV;
– *Net-Safe Latvia* Safer Safer Internet Centre.

1. National IT Security Council

Please, see answer to Q 1.3.

2. CERT.LV

Since 1 February 2011 the CERT.LV mission is to promote IT security in Latvia; it operates under the MoD and its competence is regulated by the Law on the Security of IT (please, see also answer to Q 1.3.).[84]

CERT.LV main tasks are to maintain and update information on IT security threats, to provide support in t case of IT security incident, to advise governmental institutions and to organize informative and educational activities for the government employees, IT security professionals and general public.

CERT.LV also supports the IT and Information Systems Security Experts Group "DEG", the initiative for the safer Internet environment "Responsible ISP"[85] and maintains website esidross.lv ("be safe" in English) which is aimed at a wide audience and entails guidance on how to protect computer and to be safe on internet.

[84] According to the Law on the Security of IT (Article 4) "the activities of the Security Incidents Response Institution [CERT.LV] shall be ensured by the leading State administrative institution in the national defence sector [the MoD]" and that "the operational tasks and rights (..) shall be delegated to the Agency of the University of Latvia "Institute of Mathematics and Computer Science of the University of Latvia", which executes such tasks and exercises its rights under the subordination of the relevant State administrative institution in accordance with the funds allocated from the State budget and the conditions of the delegation contract". The article also states that "the leading State administrative institution in the national defence sector shall implement the subordination in accordance with laws and regulations and the provisions of the delegation contract, including controlling an efficient execution of the delegated tasks, giving instructions regarding execution thereof and requesting the necessary information".

[85] Any ISP may apply for this quality sign; the provider must adhere to the Memorandum of Understanding on safe internet environment and fight against materials of pornographic nature on Internet. ISP, for instance, should also cooperate with CERT.LV and inform end users about an infection of a virus in their computers or them becoming a part of a botnet; cooperate with *Net-Safe Latvia* Safer Internet Centre to ensure a rapid extraction of illegal content in the public exchange network; after request of a client, ensure free of charge setting up an internet content filter according to the law.

3. *Net-Safe Latvia* Safer Internet Centre

Please, see answer to Q 5.A.5.

3.C.2.
Please explain how the coordination between the various national authorities with a role in the prevention of and fight against cybercrime is organised in your MS.

As regards prevention – please, see answer to Q 3.B.1. on the CPU. Besides cooperation with the structures within the State Police itself, the CPU also has set up an informal network on cybercrime; a number of state/municipal authorities, non-governmental organizations and other relevant stakeholders are participating.

With regard to fight against cybercrime, the CEU closely cooperates with CERT.LV and *Net-Safe Latvia* Safer Internet Centre (namely, there is horizontal cooperation model which is triggered upon a necessity).

Please, see also answers to Q 2.A.7. and Q 9.5. on the cooperation agreements between the State Police and CERT.LV as well as the Latvian Internet Association.

4. CYBER ATTACKS

4.1.
Has your MS transposed into national legislation Directive 2013/40/EU on attacks against information systems (transposition date 4 September 2015)?
If so, did you experience any difficulties in implementation?

Yes.

The directive is transposed by amendments to the Criminal Law (adopted on 25 September 2014, entered into force on 29 October 2014); please see Articles 144, 241, 243 and 244 (please, see answer to Q 2.A.1. for more details).

No difficulties have been experienced.

4.2.
Could you indicate the nature and number of recent cyber-attacks your MS has been subject to?
Please provide specific details, as appropriate, or share lessons learned or valuable conclusions that might be of interest to the other MS.

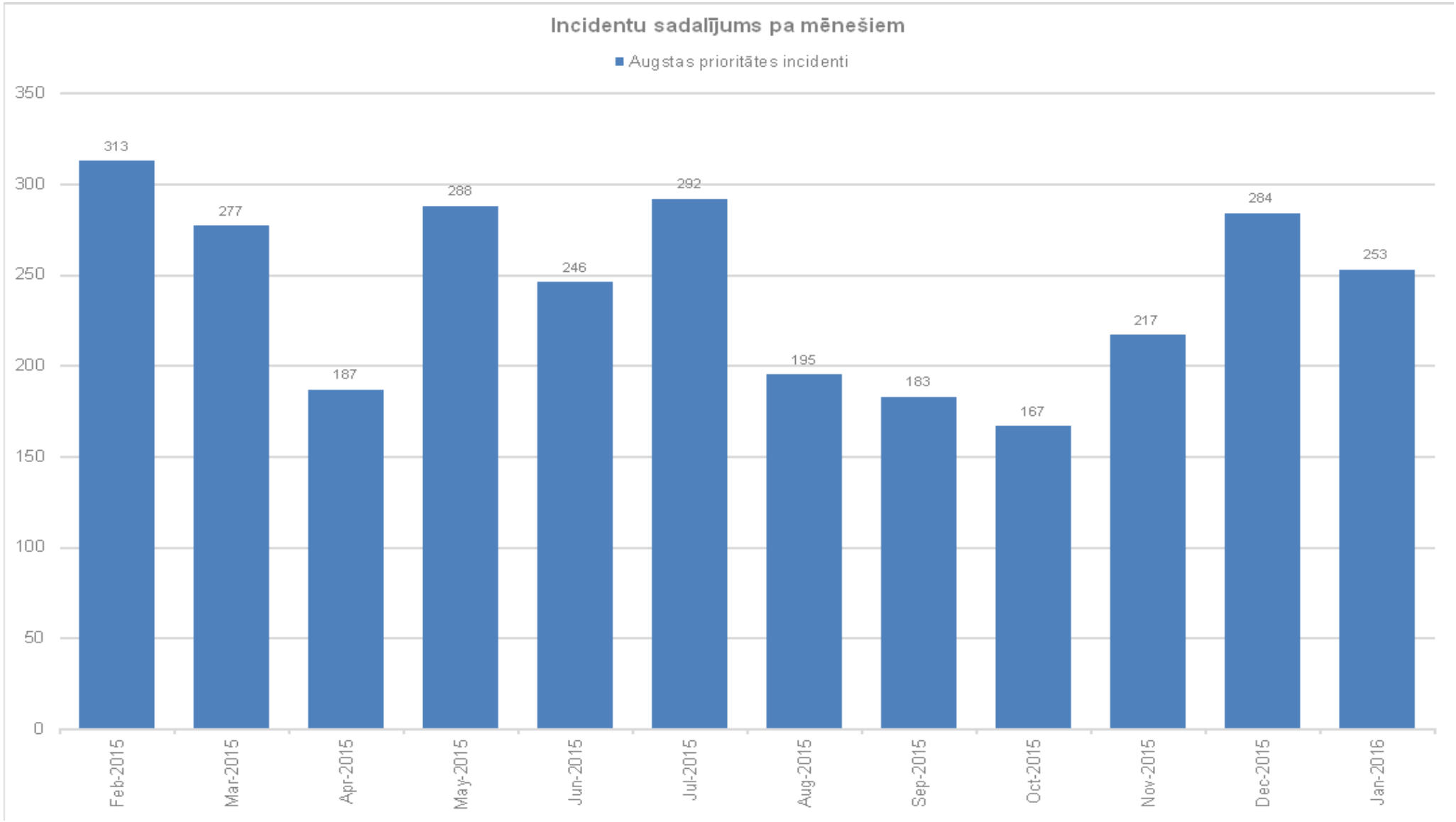
CERT.LV, which is in charge of monitoring cyber-attacks in Latvia, publishes statistics on both high and low priority cyber incidents quarterly (on month-by-month basis); statistics is available here (in Latvian).

1. Number of cyber attacks

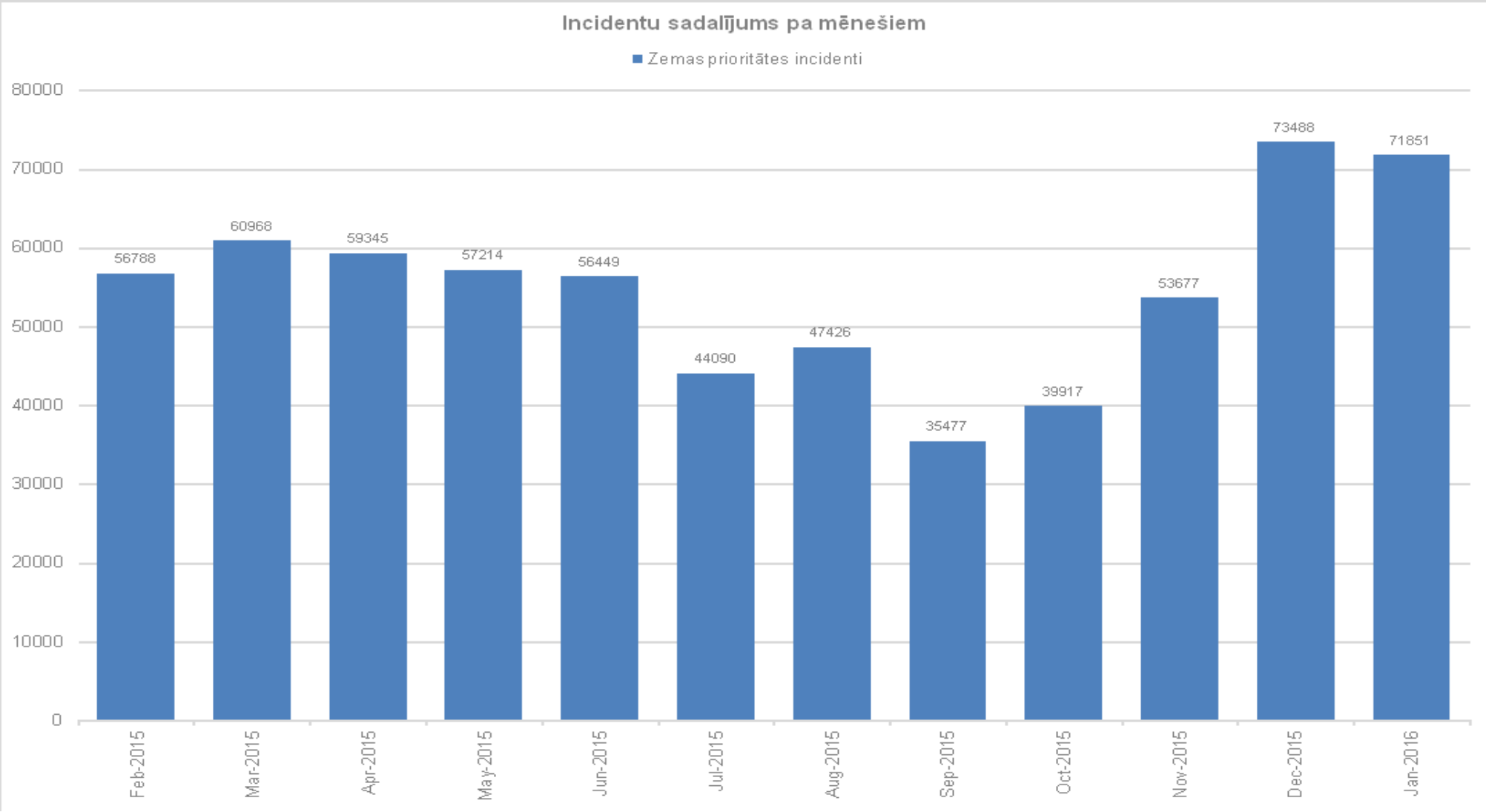
In 2015 there have been 200-300 high priority incidents and on average 50 000 low priority incidents each month. According to CERT.LV incident classification, such elements as information source and affected institutions (for instance, state institutions, critical infrastructure) are evaluated when determining whether the reported incident is of a high priority.

High priority incidents are handled by human action whereas low priority incidents are processed automatically.

Statistics on high priority incidents (February 2015 – January 2016):



Statistics on low priority incidents (February 2015 – January 2016):



2. Nature of cyber attacks

Attacks targeting Latvia's cyberspace are becoming increasingly sophisticated and thoroughly planned; the Latvian financial and public sectors are the usual targets of cyberattacks.

Spectrum of cyber-attacks is very wide: starting from system intrusions to webpage defacement, banking trojans, denial of service attacks and very sophisticated advanced persistent threat (APT) attacks.

Resolution of these incidents and attacks is part of CERT.LV normal operation; it is carried out according to CERT.LV policies and best practices.

3. Lessons learned and conclusions

CERT.LV values the information sharing with other EU Member States within the Computer Security Incident Response Team (CSIRT) cooperation (either bilaterally on case-by-case basis or by using CSIRT cooperation formats such as TF-CSIRT).

At the national level, CERT.LV sets a great importance on the cooperation with the law enforcement and intelligence agencies.

4.3.
Is the private sector under any obligation to report cyber-attacks in your MS?
If so, please provide details on the procedure used, channels and scope of reporting

1. Obligation to report

Law on the Security of IT

According to the Law on the Security of IT, in case of a security incident, a state or local government authority, the owner or lawful possessor of the critical IT infrastructure[86] have an obligation to inform CERT.LV without a delay. Others from private sector may also report incidents to CERT.LV; they receive the required support and assistance.

[86] Infrastructure is approved by the Cabinet of Ministers (government) in accordance with the National Security Law.

Reporting from the private sector is growing; banks and ISPs are the most active reporters.

Criminal Law

It should be noted that certain cyber-dependant crimes and cyber-enabled crimes (and crimes with an online element) are either serious[87] or especially serious[88] crimes.

The Criminal law foresees criminal liability for failing to inform about crimes. Namely, according to Article 315, "for a person who commits failing to inform, where it is known with certainty that preparation for or commission of a *serious or especially serious crime* is taking place, the applicable punishment is deprivation of liberty for a term up to two years or temporary deprivation of liberty, or community service, or a fine".

2. Procedure and channels

Reporting has to be done to CERT.LV by using appropriate channels (e-mail, encrypted e-mail, classified information exchange). CERT.LV also has specific agreements on information sharing with certain private sector companies.

3. Scope

Scope of reporting varies (i.e., depends on the case); however, usually it contains elements such as threat vectors, incident impact and time of incident.

4.4.
Does your MS dispose with a coordinated multidisciplinary mechanism to respond to a serious cyber-attack?
If so, please describe the respective roles of the participating bodies, their responsibilities and procedures.

[87] A serious crime is an intentional offence for which the Criminal Law provides for deprivation of liberty for a term exceeding three years but not exceeding eight years, as well as an offence, which has been committed through negligence and for which this Law provides for deprivation of liberty for a term exceeding eight years.
[88] An especially serious crime is an intentional offence for which the Criminal Law provides for deprivation of liberty for a term exceeding eight years or life imprisonment.

1. General overview on the response mechanism

According to paragraph 5 of Article 4 of the Law on the Security of IT, in case of danger to the State, the Cabinet of Ministers (government) may take a decision on transfer of the tasks, rights and resources of CERT.LV to the National Armed Forces.

In less severe cases, CERT.LV reports to the MoD which further consults the National IT Security Council (please, see answer to Q 1.3.) and reports to the Cabinet of Ministers (government) where the necessary decisions are made.

2. Cyber Defence Unit

Taking into account the existing security threats and concerns as well as limited state resources, a reserve unit – Cyber Defence Unit (CDU) **–** was created in July 2013.

Reserve cyber defence capabilities were formed for both civil and military objectives. The CDU gathers private and public sector IT experts willing to provide support to the state in crisis situation (namely, in case if capabilities of the National Armed Forces and CERT.LV appear to be insufficient).

The CDU is developed on the basis of National Guard[89] which ensures legal basis and procedures to involve highly-qualified IT experts from private sector to fulfil defence tasks in an organised manner.

Currently there are more than 70 volunteers in the CDU (full operational capability stands with 94 volunteers and four professional soldiers). Currently, within the CDU, IT experts improve knowledge, organise and participate in cyber-attack prevention training and, where necessary, provide assistance to both public and private sector.

The main tasks of the CDU:

- to recruit IT experts; to elaborate development and work plan of the CDU;

[89] According to the National Guard of the Republic of Latvia Law, the National Guard is a component of the National Armed Forces, the objective of which is to involve the citizens of Latvia in the defence of the State territory and society and which participates in the planning and execution of the State defence tasks in accordance with the tasks determined in the National Guard of the Republic of Latvia Law.

- to ensure initial military and further professional training of the involved national guards;
- to plan, organise and ensure participation in national and international level trainings (for instance, regular participation in cyber defence training in NATO, EU, bilateral and regional formats, including NATO Cooperative Cyber Defence Centre of Excellence; organisation of regular national level training);
- to form expert examinations in collaboration with military CERT experts of the National Armed Forces and CERT.LV, to participate in new security solution testing and evaluation as well as to provide proposals for the improvement of cyber defence;
- to prepare and to participate in NATO, EU or regional cyber defence units or reserve;
- to promote civil-military collaboration or public and private partnership in the field of cyber defence;
- to promote understanding and knowledge about cyber threats among IT experts and the society; to involve the Young Guard, to promote education of youth and further interest in becoming involved in the field of IT security and defence.

4.5.

What is the role of operators of critical infrastructure and information systems in minimizing cyber-attacks threats and mitigating their effects?

For each critical IT infrastructure, a person responsible for the IT security shall be designated (by the owner or legal manager of the critical infrastructure). The designated person cooperates together with CERT.LV and the Constitution Protection Bureau[90] to ensure protection of the critical IT infrastructure in accordance with the rules set out by the Cabinet of Ministers.

In order to minimize cyber-attack threats and mitigate their effects, the following measures, for instance, are taken: coherent IT security documentation, risk analysis, contingency planning, penetration testing and incident response.

4.6.

What are the obstacles that LEAs face when responding to cyber attacks (e.g. inability to analyze high volume of data, lengthy proceedings, different data retention periods, preserving evidence, limited knowledge/skills/capacity)?

[90] State security service supervised by the Cabinet of Ministers; the main tasks include intelligence, counter-intelligence and protection of state (official) secrets.

Please describe.

Please, see answer to Q 3.B.3.

4.7.
As cyber-attacks often involve criminals from outside EU, do you make use of mutual legal assistance (MLA) instruments to successfully tackle this issue?
If not, provide details on how you tackle this issue/deal with those cases?

Yes, requests for criminal-legal assistance are used (this process, however, is lengthy and rather cumbersome; MLA instruments as such are not designed for digital age needs).

5. OFFENCES RELATED TO CHILD SEXUAL ABUSE ONLINE AND CHILD PORNOGRAPHY

5.1.
Has your Member State transposed into national law Directive2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (transposition deadline 18 December 2013)?
If so, did you experience any difficulties in implementation?

Latvia has fully transposed the Directive; the transposition has been completed by the amendments in Criminal Law (Articles 48, 159-162[1], 164-166).

5.A. Specific questions related to the act/victim

5.A.1.
Are there any software databases specifically designed to identify victims in your MS?

Latvia has no national software database specifically designed to identify victims.

However, to reinforce its capacity in fight against offences related to child sexual abuse online and child pornography, the State Police actively uses international databases/tools, such as:

- **Child Protection System (CPS)** – database on persons regularly violating provisions regarding the handling of a material of child pornography (also within a territory of Latvia);
- **Voyager One** – comprehensive web platform enabling the State Police to detect networks of criminal organisations, as well as child abusers;
- **ICACCOPS** – web based data base which allows to find out which IP addresses shares and uploads illegal materials (it is possible to see Gnutella, Emule, IRC, Gigatribe, TOR, Bittorrent, Freener net IP addresses);
- **Biometric Data Processing System (BDPS)** – data base consisting of biometric data (facial image and ten pressed fingerprints, ten rolled fingerprints and palm prints) from individuals involved in criminal proceedings – suspects, detainees and the convicted. BDPS also includes comparative samples (biological material taken from victims, persons arrested, suspected, accused or convicted, as well as from unidentified bodies, biologically close relatives of missing

persons (children, parents) to ascertain the source of the biological traces) enabling the State Police to identify a missing person or an unidentified body.

From 30 June 2016 the State Police will start using also the International Child Sexual Exploitation (ICSE) Database of Interpol.

5.A.2.
What measures you have in place to avoid re-victimisation if images/videos are not deleted?

According to the Criminal Procedure Law (Article 239 paragraph 4) during the course of an inspection of the location of an event, the performer of the operation may remove objects with traces of a criminal offence (including hardware).

After the final conviction, material evidence (the circulation of which is prohibited by law) shall be transferred to the relevant institutions or destroyed according to a decision of the person directing the proceedings. Hardware containing images/videos related to child sexual abuse online and child pornography are always destroyed (if not fully then partly by erasing material with illegal content).

In order to avoid re-victimization, the State Police is also working on its capacity to prevent further image/video distribution of already downloaded files (i.e. which are downloaded before the removal of hardware).

Additional information:

According to Article 18 of the Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA (Chapter 4. Protection of victims and recognition of victims with specific protection needs) "Member States shall ensure that measures are available to protect victims and their family members from secondary and repeat victimisation, from intimidation and from retaliation, including against the risk of emotional or psychological harm, and to protect the dignity of victims during questioning and when testifying. When necessary, such measures shall also include procedures established under national law for the physical protection of victims and their family members".

In order to fully implement the Directive, amendments to the Criminal Procedure Law have been submitted for the adoption at the Parliament (currently in the last reading).

A new chapter on victim who is in need of special protection will be introduced and new measures implemented (i.e. measures to avoid visual contact between victims and offenders during the giving of evidence (by appropriate means including the use of communication technology); interviews with the victim to be carried out by or through professionals trained for that purpose; all interviews with victims of sexual violence, gender-based violence or violence in close relationships to be conducted by a person of the same sex as the victim, if the victim so wishes (this does not refer to prosecutors and judges); measures to ensure that victim may be heard in the courtroom without being present, in particular through the use of appropriate communication technology).

5.A.3.
What measures you have in place to prevent child sex tourism? (Article 21 of Directive 2011/93/EU requires Member States to establish measures against advertising abuse opportunities and child sex tourism).

According to the Law on Pornography Restriction (Article 8) advertising of material of a pornographic nature is prohibited. Advertising must be presumed as any form or any type of communication or event with an aim to promote the popularity of material of a pornographic nature or demand thereof, associated with economic activities performed with the purpose of acquiring profit.

There is no legal definition provided in the Criminal Law regarding child sex-tourism and its advertising. However, in practice, if a person organizes/advertises such a travel, he/she can be considered as a perpetrator of the relevant criminal offence in the Criminal Law (for instance, Article 162 of the Criminal Law).

In the context of practical measures, it should be mentioned that on 17-18 September 2014 the State Police (six officers), customs authority (four officers) and State Border Guard (eight officers) participated in international operation "HAVEN" (Halting Europeans Abusing Victims in Every Nation), the goal of which was to support the EU Member States in detecting and intercepting child sexual offenders travelling to abuse children. During the operation the State Border Guard at the

Riga International Airport monitored flights from specific countries (i.e., Thailand, Philippines) and reported on suspicious persons to the customs authorities who further performed searches of person's belongings (focussing on hardware with illegal content, child pornography, for instance) and, if necessary, reported to the authorities of Economic Crime Prevention Department of the Central Criminal Police Department of the State Police. Overall nine flights during the operation were inspected and data from 16 hardware collected; strategic analysis of the gathered criminal intelligence was sent to Europol.

5.A.4.
Have you developed specific measures to counteract real time web-based child pornographic performance?

No.

In addition, please, see also answer to Q 5.B.3.

5.A.5.
Have you undertaken specific preventive actions, such as:

- ***making hotlines available and providing specific information on how to make complaints,***
- ***developing information tools for children for safe use of Internet;***
- ***developing information tools on harmful/illegal behaviour online?***

1. Hotlines (helplines) available and providing specific information on how to make complaints

Informing on cybercrime can be done by calling to 112 or 110, or by filling an online registration form. To facilitate the process of reporting on any type of criminal offences, including cybercrime, all the necessary information is displayed in the website of the State Police (available in Latvian, English and Russian).

Complaints related to cybercrime can also be submitted to the *Net-Safe Latvia* Safer Internet Centre via helpline (please, see more information below) or CERT. LV (on cyber-attacks).

2. Information tools for children (and their parents) for safe use of Internet and harmful/illegal behaviour online

2.1.The State Police measures

Overall 61 preventive action in 2014 and 312 actions in 2015 were carried out by the State Police on the safety on internet, such us:

- in order to protect persons, including children from potential abusers on internet, information on **"10 most significant internet communication provisions"** has been made available in the website of the State Police;
- in close cooperation with the *Net-Safe Latvia* Safer Internet Centre **training** on safety on internet for the **inspectors of juvenile cases** was organized;
- **games for children** ("*Sivēns lielpilsētā*", "*Sivēna ziemas diena*") were developed; they are linked to child safety on internet and social networks (profile creation, photo gallery, how to react to unknown messages, negative comments);
- **seminars for children** were organized; the State Police produces a material on cyber safety for children of different ages emphasizing the risks that they may encounter. The main goal is to make children understand what they are risking with by doing seemingly usual things on internet; the material includes information on basic advices to protect themselves from cybercrimes. The State Police has also developed a brochure for children and adults in Braille;
- sexual harassment towards children online becomes an increasingly serious issue and it is not always possible to make children understand risks and to take the necessary measures for their safety; it is crucial to involve parents. Therefore, the State Police has prepared **brochures for parents** on how to better protect their children;
- in 2015, three important **press releases** were prepared in response to sexual offenses committed in cyberspace.[91]

2.2. The *Net-Safe Latvia* Safer Internet Centre measures

[91] In June information was provided on persons detained for storing thousands of child pornography files and publishing this information on their blog that was publicly accessible. In early September information was prepared on an individual who extorted erotic pictures from adolescence and then blackmailed them. In October information was provided on a detained person in whose computer thousands of child pornography and other prohibited pornographic files were found.

The *Net-Safe Latvia* Safer Internet Centre (Centre) is the national contact point for EU *Safer Internet* Programme's Insafe network. The project is c-financed by the European Commission (50%); it lasts 18 months (from 1 January 2015 until 30 June 2016.)

The coordinating institution of the Centre is the Latvian Internet Association in cooperation with the State Inspectorate for Protection of Children's Rights (Inspectorate) and the Municipal Governments Training Centre of Latvia.

The Centre is working in the following three directions:

1) **informing and educating** (target groups: children, adolescents, teachers and parents; content: safety of internet content and the potential threats (incitement to hate, racism, child pornography and pedophilia, emotional harassment on the Internet, identity theft and data abuse); additional information is available here);
2) **reporting about illegal online content and breaches online**[92] (reporting is anonymous; reports are processed and, if necessary, sent for examination to the State Police);
3) **ensuring a helpline 116111 of the Inspectorate** (a possibility for everyone, but especially children and youngsters, to turn for a help on any issue of interest).

As regards the helpline, in 2015, calls from more than 670 children and youngsters were received on internet related issues (*inter alia* cyberbullying, online pornography, sexual exploitation of children); it is two times more as compared to 2014.

Furthermore, with the aim to educate:

- children and youngsters on internet safety, the Inspectorate, in cooperation with the Centre, has created videos reflecting three situations which children/youngsters have experienced/may experience in a real life;[93] also a book on internet safety for the 5-7 years olds' has been created (available in e-version too);
- parents, instructions on safe internet have been created;
- individuals working with children (teachers, social workers), training (free of charge) has been provided.

[92] Centre is also a member of International Association of Internet Hotlines (INHOPE).
[93] For instance, in one video a young girl sends an intimate photo to a young boy abroad via social media (by not knowing him) but in reality the "young boy" is located in the same country and is not "a young boy" at all; he starts blackmailing the girl (requesting money or asking her to send more intimate photos/videos). Please, see the video (in Latvian).

3. Other relevant measures

In order to prevent child pornography and sexual exploitation on internet, the State Police has created a video file ("*police to peer project*") that will automatically appear in cases if person will download image/video files containing child pornography and sexual exploitation.

In the video file the police officer informs the abuser that police has detected his IP address and that the process of identification has just been started; also information on criminal charges is given.

5.A.6.   ***Have you put in place any measures to address the following: sex exploitation/abuse online, sexting, cyber bulling?***

As regards sex exploitation/abuse online and sexting, please, see Article 162[1] of the Criminal Law on encouraging to involve in sexual acts (answer to Q 2.A.1.)

With regard to cyber-bullying, there is no legal definition in place; cyber-bullying as such may range from criminal to non-criminal behavior (depending on consequences)[94] and therefore every case has been treated individually. There are several articles in the Criminal Law that could be referred to in case of cyber-bullying, for instance, Article 150 "Incitement of Religious Hatred", Article 157 "Defamation" and Article 145 "Illegal Activities Involving Personal Data of Natural Persons".

Please, see also answer to Q 5.A.5.

5.B. Filtering/Blocking of access /Removal of content/Take down of web pages containing or disseminating child pornography

5.B.1. ***Does your MS apply any of the following measures: filtering, blocking of access, removal of content, take down of web pages?*** ***If so, please specify in which cases.***	

[94] The cyber-bullying could be limited to posting rumours or gossips about a person on internet or it may reach the level when the victim is severely defamed and humiliated.

According to the Criminal Procedure Law (Article 239 paragraph 4), during the course of an inspection of the location of an event, the performer of the operation may remove objects with traces of a criminal offence (including offences related to child sexual abuse online and child pornography).

In addition, please, see also answer to Q 5.A.2. (on destruction of material evidence) and Q 5.B.3.

5.B.2.
What tools are used to filter websites for child pornographic materials?

There are no technical tools to filter websites for child pornographic materials. However, in this regard, the State Police cooperates with the Centre (please, see answers to Q 5.A.5. and Q 5.B.1.)

5.B.3.
Which authority can authorise or coordinate blocking of access/removal of content/take down of web pages? What is the role and responsibility of private sector?

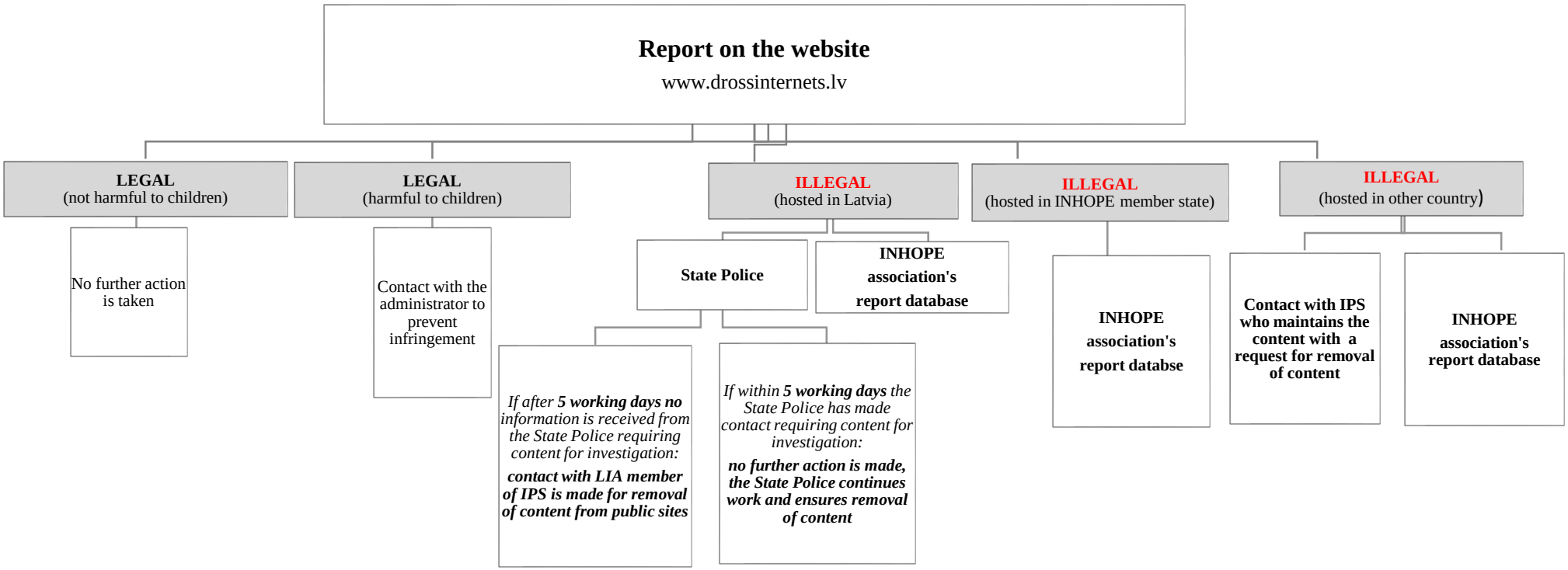
The official, who is authorised to perform criminal proceedings, can also authorise removal of content of web pages (Criminal Procedure Law, Article 239 paragraph 4).

Electronic communications service providers do not have a *legal* obligation to block access, to remove content or to take down web pages; they (for instance, the social media national platform www.draugiem.lv) however cooperate with the law enforcement agencies on a voluntary basis (by reporting on the illegal content they have identified and by blocking/removing it).

Moreover, as already noted in answer to Q 5.A.5., the Centre, as a member of INHOPE, processes the received reports (website www.drossinternets.lv) and, if necessary, sends them to the State Police for further examination.

Please, see below graphic information[95] on the cooperation between the Centre and the State Police:

[95] This graphic information is also an integral part of the cooperation agreement between the Latvian Internet Association and the State Police.


Report on the website
www.drossinternets.lv
LEGAL
(not harmful to children)
LEGAL
(harmful to children)
ILLEGAL
(hosted in Latvia)
ILLEGAL
(hosted in INHOPE member state)
ILLEGAL
(hosted in other country)
No further action is taken
Contact with the administrator to prevent infringement
State Police
INHOPE association's report database
If after 5 working days no information is received from the State Police requiring content for investigation:
contact with LIA member of IPS is made for removal of content from public sites
If within 5 working days the State Police has made contact requiring content for investigation:
no further action is made, the State Police continues work and ensures removal of content
INHOPE association's report databse
Contact with IPS who maintains the content with a request for removal of content
INHOPE association's report database

5.B.4.

Please specify how this is done in practice (e.g. has this power been exercised in agreement with the competent authority).

Is there a separate procedure for urgent cases?

What is your experience in this respect (cases)?

Please, see answers to Q 5.B.1., Q 5.B.3. and Q. 9.1.

Criminal Procedure Law stands for the principle of equality supporting uniform procedural order for all persons involved in criminal proceedings and separate procedure for urgent cases therefore has not been introduced; however, Protection of the Rights of the Child Law states that in lawful relations that affect a child, the rights and best interests of the child shall take a priority.

5.B.5.

How do you deal with cases where the server is located outside your MS?

What EU or other mechanisms do you use in those cases?

Such cases are solved according to the Convention on Cybercrime and by using information channels of Interpol and Europol.

5.C. International cooperation

5.C.1.

Does your MS have any experience in using the International Child Sexual Exploitation Database at Interpol?

According to the Working Plan 2016 of the State Police (action No. 2.15) and the Working Plan 2016 of the Central Criminal Police Department of the State Police (action No. 35) accession to ICSE database will be provided until 30 June 2016 (two connection points are foreseen; training will be provided to six officials).

5.C.2.

Does your MS participate in the European Union Strategic Group of the Heads of National High-Tech Crime Units at Europol and other forms of practical cooperation (including "cyber-patrols")?

Latvia participates in the European Union Strategic Group of the Heads of National High-Tech Crime Units at Europol (Group); however, due to limited human resources, it was not possible for Latvia to attend the Group in 2015.

As regards the practical cooperation, in 2014, the State Police took part in international operation "HAVEN" (Halting Europeans Abusing Victims in Every Nation), the goal of which is to support the EU Member States in detecting and intercepting child sexual offenders travelling to abuse children (please, see also answer to Q 5.A.3).

5.C.3.

Do you have specialized units dealing exclusively with child pornography?

If so, please provide details regarding their composition, size, powers, etc.

There is no specialized unit dealing exclusively with child pornography cases.

Cases on child pornography are investigated by the Central Criminal Police Department of the State Police.

6. ONLINE CARD FRAUD

6.1.

Do citizens and private companies usually report online card fraud offences to LEAs?

If not, please explain the main reasons why not, if known.

Yes, reporting to the State Police on card fraud offences is organized mostly via universal phone number or by sending application to the e-mail: kanc@vp.gov.lv.

However, as regards the commercial banks, in practice they often do not report the offences to the law enforcement agencies (due to the risk to lose their reputation/credibility).

6.2.

Is there sufficient/effective cooperation between industry, banks, private sector and LEAs to prevent and fight online card fraud in general terms and specifically to:

- ***notify police/LEA if they become aware of any abuse of new payment tools developed by industry?***
- ***increase the security of non-cash payment and minimize the vulnerability of magnetic stripes?***
- ***strengthen the authorisation of online transactions and authentication of customers?***

Cooperation can be considered as overall effective.

For instance, the State Police (Cybercrime Enforcement Unit of the Economic Crimes Enforcement Department):

- holds a regular dialogue with the Association of Latvian Commercial Banks (which on voluntary principle unites the banks registered in Latvia and branches of foreign banks);
- actively participates in tripartite cooperation platform where banks (their security units) and CERT.LV are taking a part.

6.3.

Is the LEA equipment (software and hardware), resources, capacity and knowledge at the necessary level to keep up with the pace of criminal development (newer and newer technologies being used by criminals)?

Please provide specific examples, if any.

The technical equipment (i.e., software, technical resources) used by the CEU should be further developed; also knowledge on the newest technologies should be raised (please, see also answer to Q 3.B.3. on general challenges). Currently, the State Police widely uses the training opportunities provided by CEPOL, Europol and other entities. Furthermore, as already noted, one of the State Police's objectives within the Internal Security Fund is to implement a project "Capacity building to prevent and fight against cybercrime" (please, see answer to Q 1.8.). In addition, issues related to strengthening prevention and fight against cybercrime are included in the draft concept (policy planning document) on the State Police development.

As regards the examination on illegal use of payment cards and skimmers, the Forensic IT Unit (Forensic Department of the State Police) has the necessary technical and human resources. In addition, the forensic experts are also participating in training; however, due to the rapid development of IT, such training should be intensified. With regard to forensics in general, please, see also answers to Q 2. B.6., Q 3.B.3. (on existing challenges) and Q 10.B.2. (on training).

6.4.

What concrete measures exist or are being developed in your MS to limit the access of organised criminal groups to:

- ***financial data and credentials,***
- ***skimming devises and software,***
- ***know-how?***

In practice, for instance, commercial banks of Latvia are changing parts of ATM's periodically to reduce the possibility of skimming. Such procedure has been set out also in Automatic Service (gas) stations.

Several commercial banks have set up additional measures to ensure safety with regard to on-line payments. In addition, in order to warn and to protect the potential victims, police and commercial

banks regularly provide information to the public about the risks of cyber criminality and protection of personal data.

6.5.
How does your Member State try to overcome obstacles to cross-border cooperation specifically regarding online card fraud?

In such cases, before the pre-trial investigations, Europol, Interpol and police cooperation information communication channels are used.

During the pre-trial investigations, the relevant MLA instruments and possibilities provided by Europol and *Eurojust*, including the JITs, are being explored (please, see also answer to Q 7.A.3).

7. INTERNATIONAL COOPERATION - TOOLS (MUTUAL LEGAL ASSISTANCE (MLA), SURRENDER/EXTRADITION)

7.A. Mutual legal assistance

7.A.1.
Is there any specific legal basis in your MS for provision of Mutual Legal Assistance (MLA) for cybercrime.

There is no specific legal basis in Latvia for provision of MLA for cybercrime.

The legal basis for provision of MLA, including cybercrime cases is set out in the Criminal Procedure Law (Part C International Co-operation in the Criminal-legal Field) and bilateral agreements in this area.

7.A.2.
Which authorities are responsible for receiving/sending requests for MLA in cybercrime investigations and for taking decisions on such requests?
What communication channels are used to send/receive the request/decision and any additional information?

According to the Criminal Procedure Law (Article 846 on the competent authorities in the examination of a request of a foreign state):

- *in the pre-trial proceedings*: the General Prosecutor's Office examines and decides a request of a foreign state; up to the commencement of criminal prosecution also the State Police;
- *after transfer of a case to a court*: the Ministry of Justice examines and decides a request of a foreign state.

Different communication channels may be used – direct channels, diplomatic channels, Interpol, Europol and *Eurojust.*

7.A.3.

Please provide, if available, statistics on the number of requests sent/received, specifying under which instruments, and as far as possible for which type of cybercrime acts as regards EU MSs and third countries respectively.

I. Statistics on the number of requests received

General Prosecutor's Office:

Year	Cybercrime	Child pornography and sexual exploitation	Illegal Activities with Financial Instruments and Means of Payment
2014	102	4	2
2015	75	1	3

Legal base of cooperation:

- Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (157);
- European Union Convention on Mutual Assistance in Criminal Matters (5, Turkey, Switzerland);
- Agreement on Mutual Legal Assistance between the Government of the Republic of Latvia and United States of America (20);
- Agreement on Mutual Legal Assistance and Legal relationship on Civil matters, Family matters and Criminal matters between the Republic of Latvia and Republic of Belarus (3);
- Agreement on Mutual Legal Assistance and Legal relationship on Civil matters, Family matters and Criminal matters between the Republic of Latvia and Republic of Moldova (1);
- Agreement on Mutual Legal Assistance and Legal relationship on Civil matters, Family matters and Criminal matters between the Republic of Latvia and Russian Federation (1).

State Police:

Year	Cybercrime	Child pornography and sexual exploitation	Illegal Activities with Financial Instruments and Means of Payment
2014	9	2	175
2015	7	1	218

Legal base of cooperation:

- European Convention on Mutual Assistance in Criminal Matters (Albania – 1, Croatia – 1; Georgia – 1, Iceland – 1, Liechtenstein – 4, Norway – 1, Switzerland – 3, Turkey – 3);
- Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union;
- Agreement on Mutual Legal Assistance between the Government of the Republic of Latvia and United States of America (19);
- Agreement on Mutual Legal Assistance and Legal relationship on Civil matters, Family matters and Criminal matters between the Republic of Latvia and Republic of Belarus (3);
- Agreement on Mutual Legal Assistance between the Republic of Latvia, the Republic of Estonia and the Republic of Lithuania (Lithuania – 58, Estonia – 6);
- Agreement on Mutual Legal Assistance and Legal relationship on Civil matters, Family matters, Labour and Criminal matters between the Republic of Latvia and Republic of Poland (97);
- Agreement on Mutual Assistance and Legal relationship on Civil matters, Family matters and Criminal matters between the Republic of Latvia and Russian Federation (10);
- Agreement on Mutual Legal Assistance and Legal relationship on Civil matters, Family matters, Labour and Criminal matters between the Republic of Latvia and Republic of Uzbekistan (1).

II. Statistics on the number of requests sent

General Prosecutor's Office:

Criminal Law					
Year	**Article 243**[96]	**Article 162**[97]	**Article 166**[98]	**Article 177[1]** [99]	**Article 193[1]** [100]
2014	1	0	0	1	0
2015	0	1	2	4	7

[96] Interference in the operation of automated data processing systems and illegal actions with the information included in such systems.
[97] Leading to depravity.
[98] Sending a person for sexual exploitation.
[99] Fraud in an automated data processing system.
[100] Obtaining, manufacture, distribution, utilisation and storage of data, software and equipment for illegal acts with financial instruments and means of payment.

Legal base of cooperation:

- Agreement on Mutual Legal Assistance between the Government of the Republic of Latvia and United States of America (5);
- Agreement on Mutual Assistance and Legal relationship on Civil matters, Family matters and Criminal matters between the Republic of Latvia and Russian Federation (8);
- Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2), mutual recognition principle (1, United Arab Emirates).

State Police:

Criminal Law								
Year	**Article 144**[101]	**Article 166**[102]	**Article 177¹** [103]	**Article 193¹** [104]	**Article 241**[105]	**Article 243**[106]	**Article 244**[107]	**Article 244¹** [108]
2014	5	1	1	13	0	1	0	0
2015	4	2	4	33	1	0	1	3

Legal base of cooperation:

- European Convention on Mutual Assistance in Criminal Matters (United Arab Emirates – 1. Switzerland – 2);
- Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union;
- Agreement on Mutual Legal Assistance between the Government of the Republic of Latvia and United States of America (12);
- Agreement on Mutual Legal Assistance between the Republic of Latvia, the Republic of Estonia and the Republic of Lithuania (Lithuania – 5, Estonia – 1);

[101] Violating the confidentiality of correspondence and information to be transmitted over telecommunications networks.
[102] Violation of provisions regarding the demonstration of a pornographic performance, restriction of entertainment of intimate nature and handling of a material of pornographic nature.
[103] Fraud in an automated data processing system.
[104] Obtaining, manufacture, distribution, utilisation and storage of data, software and equipment for illegal acts with financial instruments and means of payment.
[105] Arbitrary accessing automated data processing systems.
[106] Interference in the operation of automated data processing systems and illegal actions with the information included in such systems.
[107] Illegal operations with automated data processing system resource influencing devices.
[108] Acquisition, development, alterations, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment.

- Agreement on Mutual Assistance and Legal relationship on Civil matters, Family matters and Criminal matters between the Republic of Latvia and Russian Federation (7);
- Agreement on Mutual Legal Assistance and Legal relationship on Civil matters, Family matters, Labour and Criminal matters between the Republic of Latvia and Ukraine (1).

As regards the trial stage, there is no legal assistance requested/received regarding cybercrime.

7.A.4.
Are there any specific procedures or conditions that need to be fulfilled, as regards the various categories of MLA requests related to cybercrime?
Please specify.
How are urgent requests treated?
What is the average response time?

There are no specific procedures or conditions that need to be fulfilled.

The average response time is two months; however, urgent requests are processed as soon as possible (this does not refer to trial stage since no legal assistance has been requested).

7.A.5.
What actions can be requested via MLA in respect to cybercrime?
What are the most common reasons for MLA requests?

Since the MLA in respect to cybercrime is not distinguished from other criminal offences, Latvia ensures co-operation according to the Criminal Procedure Law (Part C, Chapter 64, Article 673); the following actions may be requested:

- extradition of a person for criminal prosecution, trial, or the execution of a judgment, or for the determination of compulsory measures of a medical nature;
- transfer of criminal proceedings;
- execution of procedural actions;
- execution of a security measure not related to deprivation of liberty;
- recognition and execution of a judgment;
- other cases provided for in international treaties.

The most common reasons for MLA requests are information requests from electronic communications merchants and credit institutions with the aim to better prepare for interrogation.

7.A.6.
Do you use informal pre MLA consultation with the respective competent authorities of the other MS in relation to cybercrime?
If so, through which channels?

There have been informal pre MLA consultations with the respective competent authorities of the United States of America (direct channel – meeting in presence).

7.A.7.
Have you encountered specific problems in providing/requesting MLA assistance for offences committed in the "cloud"? If so, how did you address them?

No.

7.A.8.
Have you used a bilateral or multilateral treaty to which your MS is a party in order to execute/send a MLA request related to cybercrime with third state. Please provide details, including legal basis, which State, what type of MLA, results, any difficulties encountered.

Yes, please, see detailed information in answer to Q.7.A.3.

7.B. Mutual recognition

7.B.1.
Have you used any of the following EU mutual recognition instruments in relation to prevention, investigation and prosecution of cybercrimes:

- ***European protection order;***
- ***Mutual recognition of supervision measures;***
- ***Mutual recognition of custodial sentences and measures involving deprivation of liberty;***
- ***Recognition and execution of confiscation orders;***

- ***Mutual recognition of financial penalties;***
- ***Execution of orders freezing property or evidence?***

In the last two years, the General Prosecutor's Office has used execution of orders freezing property or evidence three times.

Other EU mutual recognition instruments have not been used.

7.C. Surrender/Extradition

7.C.1.
According to your legislation which cybercrime acts:
a/ fall in the scope of the EAW list, so as to give rise to surrender
b/ are extraditable.

According to Article 682 of the Criminal Procedure Law (Chapter 65 on extradition of a person to Latvia) the extradition of a person may be requested, if there are grounds to believe that the following is located in a foreign state:

- a person who is a suspect or accused in the committing of a criminal offence that may be punished on the basis of the Criminal Law, and regarding which deprivation of liberty is intended with a maximum limit of not less than one year, if an international agreement does not provide for another term; or
- a person who has been convicted in Latvia with deprivation of liberty for a term of not less than four months.

According to Article 696 of the Criminal Procedure Law (Chapter 66 on extradition of a person to a foreign state) determines the grounds for the extradition of a person:

- a person who is located in the territory of Latvia may be extradited for criminal prosecution, trial, or the execution of a judgment, if a request has been received for temporary arrest or from a foreign state to extradite such person regarding an offence that, in accordance with the law of Latvia and the foreign state, is criminal;
- a person may be extradited for criminal prosecution, or trial, regarding an offence the committing of which provides for a punishment of deprivation of liberty the maximum limit of

which is not less than one year, or a more serious punishment, if the international agreement does not provide otherwise;

- a person may be extradited for the execution of a judgment by the state that rendered the judgment and convicted the person with a punishment that is related to deprivation of liberty for a term of not less than four months, if the international agreement does not provide otherwise;
- if extradition has been requested regarding several criminal offences, but extradition may not be applied for one of such offences because such offence does not comply with the conditions regarding the possible or imposed punishment, the person may also be extradited regarding such criminal offence.

Hence, all cybercrime acts covered by the Criminal Law (please, see answer to Q 2.A.1 and Q 2.A.5.) falls in the scope of the EAW; they give rise to surrender and are extraditable (since they correspond to the requirements of Article 682 and Article 696 of the Criminal Procedure Law).

7.C.2.
Which authorities are responsible for sending/receiving surrender/extradition requests and for deciding on such requests in relation to cybercrime?
What communication channels are used?

According to the Criminal Procedure Law (Chapters 65 and 66) the General Prosecutor's Office is the responsible authority on extradition issues. Direct channels, diplomatic channels, Interpol communication channels and Schengen Information System are used.

The Ministry of Justice is responsible for sending/receiving surrender requests (usually to/from the Ministry of Justice of the other Member State or third country).

7.C.3.
Please provide, if available, statistics on the number of requests sent/received, specifying under which instruments, and as far as possible for which type of cybercrime acts as regards EU MSs or third countries respectively.

I. Statistics on the number of extradition requests received

Year	Computer crime	Child pornography and sexual exploitation	Illegal Activities with Financial Instruments and Means of Payment
2014	1	0	0
2015	7	0	0

Legal base of cooperation:

– Council Framework Decision of 13 June 2002 on the EAW and the surrender procedures between Member States

II. Statistics on the number of extradition requests sent

Year	Criminal Law Article 162[109]	Criminal Law Article 166[110]	Criminal Law Article 193[1] [111]
2014	5	0	1
2015	1	1	2

Legal base of cooperation:

– Council Framework Decision of 13 June 2002 on the EAW and the surrender procedures between Member States

The United States of America, in accordance with Agreement on Mutual Legal Assistance between the Government of the Republic of Latvia and United States of America on 2 December 2012 submitted a request to the General Prosecutor's Office on extradition of Latvian citizen accused of cybercrime. Extradition to the United States of America was made on 9 February 2015.

7.C.4.
Are there any specific procedures or conditions that need to be fulfilled as regards the requests related to cybercrime?
How are urgent requests treated?
Are provisional arrests possible?

[109] Leading to depravity.
[110] Sending a person for sexual exploitation.
[111] Obtaining, manufacture, distribution, utilisation and storage of data, software and equipment for illegal acts with financial instruments and means of payment.

What is the average response time?

No.

If extradition is possible, then also provisional arrests are possible (Criminal Procedure Law, Article 701 and Article 702).

The response time depends on the legal basis of cooperation. If the person is detained and the EAW is applicable, the response time will be up to three months.

7.C.5.
Have you used the surrender procedure provided in the Agreement on the surrender procedure between the EU Member States, Iceland and Norway in relation to cybercrime?

No.

7.C.6.
Have you sent/received requests to/from other third countries in relation to cybercrime?
What legal instruments have you used?

Please, see answer to Q 7.C.3.

8. INTERNATIONAL COOPERATION – PARTNERS (EU AGENCIES, JITS/CYBER PATROLS, THIRD COUNTRIES)

8.A. Cooperation with EU Agencies

8.A.1.
Are there any formal requirements or specific procedures foreseen by your national law in respect of the cooperation between your national authorities and Europol/EC3, Eurojust, ENISA, in relation to cybercrime cases?
If so, please specify.

No.

8.A.2.
Has your MS had any experience of cooperation in a concrete case with Europol/EC3, Eurojust, ENISA?
If so, please describe.

In 2014 and 2015, the General Prosecutor's Office has not requested *Eurojust* assistance in cybercrime cases.

In 2015, the State Police has received and processed 54 requests (sent by the EC3 channel).

8.A.3.
What is your MS's overall assessment of Europol/EC3, Eurojust and ENISA in terms of their contribution in dealing with cybercrime?
How would you assess their added value in international cooperation in relation to cybercrime?

ENISA

ENISA is a valuable venue for information exchange; Latvia also appreciates the analytical documents and research done by ENISA.

EUROPOL, EC3

There is a limited number of cases where Latvia would need an assistance provided by Europol/EC3. However, there are increasingly more cases where Latvia can assist; Latvia stands ready to continue providing the required assistance to other EU Member States and the relevant third countries.

On a more general note regarding the overall assessment, Latvia:

- greatly values the implementation of the EU Policy Cycle on organized and serious international crime and OAPs in the cybercrime priority; Latvia participates in all the sub priorities (please, see also answer to Q 1.2.);
- sees a clear added value of the Focal Points (Terminal, Cyborg, others), the J-CAT and Europol Platform for Experts (which is a valuable source/tool to gain additional knowledge and information on the latest cybercrime tendencies).

In addition, it should also be mentioned that one State Police expert is delegated to participate in the EC3 platform aimed at analysing malware (European Malware Analysis Solution; a solution that supports the forensic examination of malware behaviour in a sandbox environment); Latvia sees this as an important contribution to the State Police's forensic and investigating capacity.

Please, see also answer to Q 2.B.7. on the EC3's encryption/decryption platform.

Eurojust

The State Police has participated in *Eurojust* tactical meeting on territorial jurisdiction of cybercrime and evidence related issues; this experience is regarded as being professionally valuable.

8.A.4.
Would you recommend a better way of making use of Europol/EC3, Eurojust and ENISA in relation to cybercrime?

Contributions of these agencies are adequate.

The General Prosecutor's Office in particular values the assistance provided by *Eurojust* (especially regarding more timely fulfilment of legal assistance requests in complicated cases). Furthermore, also

the added value of coordination meetings has to be mentioned (they significantly contribute to more effective investigation and evidence gathering).

8.B. Participation in JITs and cyber-patrols

8.B.1.
Has your MS participated in JITs in relation to cybercrime?
If so, could you please describe your experience?

No.

8.B.2.
Was EU funding allocated to facilitate this cooperation?
If so, please specify under which financial instrument.

No.

8.B.3.
Do you have experience with participation in cyber patrols?
If so, please provide details as appropriate.

Please, see answer to Q 5.A.3. on international operation "HAVEN" (Halting Europeans Abusing Victims in Every Nation).

8.B.4.
What is your overall assessment of these tools for cooperation?
Have you any suggestions on how they can be improved?

Tools such as JIT and cyber patrols are valuable cooperation instruments; their overall usage should be stepped up.

8.C. Cooperation with third countries

8.C.1.

Describe your policy, if any, with respect to third countries regarding cybercrime prevention and investigation.

The policy is based on Budapest Convention, European Convention on Mutual Assistance in Criminal Matters and bilateral agreements.

8.C.2.

In your experience has the involvement of Europol/EC3/Eurojust brought an added value to cases related to third countries?

If so, explain how.

Yes, with regard to legal assistance requests addressed to Latvia, third countries often use Europol as a channel.

Latvia values the coordinating role Europol has in this regard.

8.C.3.

Can you explain your involvement with Interpol regarding cybercrime issues?

It is less regular as compared to Europol and EC3.

The State Police receives Interpol Cyber Fusion Centre cyber activities reports which undoubtedly contributes to the overall work.

9. CO-OPERATION WITH THE PRIVATE SECTOR

9.1.
Please explain how and on what basis the private sector is involved in the prevention of and fight against cybercrime, e.g. legal or policy obligations.
Please describe how the private sector intervenes, e.g. by providing support in preservation of evidence, identifying of offenders, shutting down of information systems or functions that have been compromised or used for illegal purposes, etc.
Please, describe your experience.

1. Electronic communications merchants

Electronic Communication Law (Article 3) determines the rights and duties of electronic communications merchants; they must ensure, in accordance with the procedures laid down in Article 71^1 of Electronic Communication Law, the storage of data (to be retained for 18 months) and transfer to the institutions specified in law. Please, see more on Article 71^1 in answer to Q 2.B.2.

Based on Article 71^1, the Cabinet **Regulation** No. 820 (of 4 December 2007) was adopted ("Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled").

According to this Regulation, electronic communications merchant shall ensure:

- transfer of the data to be retained in the volume and form indicated in the request;
- registration of the requests, identifying employees who prepare the data to be retained indicated in the request for issuance;
- registration of the issued data to be retained (response to requests), indicating the employee who has issued the relevant data; and
- protection of information on the received requests and issuance of data to be retained in conformity with the regulatory enactments regulating the protection of information.

Electronic communications merchant shall ensure submission of data to be retained within the following time periods after the receipt of a request:

- within *30 days* (if such data is requested which has been retained more than six months ago);
- within *10 days* (if such data is requested which has been retained during the last six months);
- in matters of urgency[112] – within *three hours* (if data requested has been retained within a time period of the last twenty-four hours);
- in matters of urgency – within *an hour* (if specific data referred to Annex 1,[113] Annex 2[114] or paragraphs 1[115] and 2[116] of Annex 3[117] to this Regulation has been requested).

If due to technical limitation reasons, it is not possible to ensure transfer of data to be retained within the time periods specified above, electronic communications merchant should inform the relevant authority, the Office of the Prosecutor or court, and to submit the requested data immediately as soon as possible. Data should be submitted by using specific forms.

Based on above-mentioned Regulation, the Latvian Internet Association has also prepared a short **instruction** (addressed to electronic communications merchants) on seven steps on how to communicate and to submit the necessary information to law enforcement agencies.

2. Electronic communications service providers

Electronic communications service providers (which provide publicly accessible electronic communications services, utilising the public electronic communications network) do not have a legal obligation to block the access to websites and to remove content.

However, in practice, the providers cooperate with the law enforcement agencies on a voluntary basis; they notify the identified illegal content and remove/block it (this, for instance, is also the practice followed by the largest social media www.draugiem.lv in Latvia).

Please, in addition see also answer to Q 2.B.2.

[112] If the transfer of data within 30 days or 10 days may hinder prevention or disclosure of a criminal offence, saving person's life or protection of the State or public safety.
[113] Refers to the request to the electronic communications merchant, which ensures services of the public fixed telephone network.
[114] Request to the merchant of electronic communications merchant, which ensures services of the public mobile telephone network.
[115] The user ID(s) allocated.
[116] The subscriber or registered user to whom an Internet Protocol (IP) address was allocated at the time of the connection - the given name, surname, personal identity number of a natural person or the name, registration number and address, ID and telephone number of a legal person.
[117] Request to the electronic communications merchant, which ensures ensures internet access services.

As regards CERT.LV and *Net-Safe Latvia* Safer Internet Centre, please, see answer to Q 4 (on cyber-attacks) and answer 5.B.3. (offences related to child sexual abuse online and child pornography).

9.2.
Are Internet service providers subject to any specific responsibility/liability under your national law?
If so, please describe.
How are requests for blocking the access/removal of the content or websites handled?

Please, see:

- answer to Q 9.1. (point 2);
- answer to Q 5.B.3.;
- answer to Q 2.A.2. (on liability of legal persons envisaged in the Criminal Law).

9.3.
When the private companies have their main headquarters in a third State have you cooperated directly with the local branches?
If so, has this affected the investigation and the prosecution of the case?
Have private companies been subject to coercive measures, e.g. house searches?

In situations when local branch (of the main headquarter located in a third country) is officially registered in Latvia (Enterprise Register; Commercial Register), information exchange and/-or procedural activities (including coercive measures) are carried out according to the national legislation.

9.4.
Are resources allocated to enhancing/improving the co-operation with the private sector?

Enhancement of co-operation with private sector is carried out within the existing resources.

9.5.

Does your MS use Public Private Partnership (PPP) in the prevention of and fight against cybercrime?

If so, please provide details on their scope, composition, organisation and modalities of operation.

According to Article 1 of the Law On Public–Private Partnership (PPP) the PPP co-operation between the public and private sector *simultaneously* is characterized by the following features:

- the co-operation is between one or several public partners and one or several private partners involved in the PPP procedure;
- the co-operation is carried out in order to meet public needs in performing construction works or providing services;
- it is a long-term co-operation lasting up to 30 years but in the cases laid down in the law – even longer;
- a public and a private partner pool and use the resources available thereto (e.g. property, financial resources, knowledge and experience);
- a public partner and a private partner share the responsibility and risks.

In the sense of this law, Latvia does not use PPP in the prevention and fight against cybercrime.

However, the State Police has signed a cooperation agreement with CERT.LV (please, see also answer to Q 2.A.7.) and a cooperation agreement with the Latvian Internet Association (on illegal content on internet). Agreements provide, for instance, terms regarding information exchange, knowledge exchange/training as well as specific issues such as blocking access of end users and removal of illegal content on internet.

10. PREVENTION OF CYBERCRIME, TRAINING AND AWARENESS RAISING ACTIVITIES

10.A. Prevention

10.A.1.
In what way is the issue of prevention addressed in your national legislation/policy?
Does it include any specific measures or activities in this respect?
If so, please specify.

Please, see answers to Q 1.2. and 1.3.

10.A.2.
Describe any recent or planned prevention activities undertaken by both governmental institutions and non-governmental organisations, including schools and academia.

The State Police currently develops website www.sargi-sevi.lv ("protect/guard yourself" in English; to be launched in June 2016) which will be an information platform on security and prevention issues, including cybercrime. Children and youth will be one of the target groups; for each age group the main security threats/concerns will be listed and explained.

Please, see also answers to Q 5.A.5.

10.B. Training

10.B.1.
Do you provide cybercrime related training to your general and specialised LEAs and the judiciary?
Describe the objectives, subject matters covered, and if possible the frequency and duration of this training.

1. Law enforcement

Training to law enforcement is provided by the State Police College – an educational institution under the authority of the State Police.

The State Police College trains police officers for professional service and provides continuing training to the State Police staff.[118]

As regards the continuing training, in 2015:

- 133 officials/police officers participated in the informal education programme "Usage of the newest IT in police work" (eight academic hours); implementation of this programme continues also in 2016;
- 65 officials/police officers participated in the programme "Usage of electronic communication means in internet; theirs types and control possibilities" (eight academic hours);
- 42 officials/police officers participated in programme "Usage of electronic communication merchant's data in investigating criminal offences" (eight academic hours).

In addition, there is also professional development programme "IT usage in fight against crime" in place; it consists of the following specializations:

- IT specialist (120 academic hours);
- Information processing and analysis specialist (120 academic hours);
- IT specialist in fight against cybercrime (120 academic hours).

Furthermore, with regard to training and knowledge exchange, the State Police (the CEU of the Economic Crimes Enforcement Department) on a daily basis cooperates with various Latvian IT companies and software producers.

2. Judiciary

The Latvian Judicial Training Centre provides continuing training for judges and court employees; a number of different professional qualification-building measures are carried out(seminars, experience exchange trips, etc.) with a special attention to subjects on and improvements to the quality of court judgments as well as to quality work within the legal system of the EU.

[118] Training on cybercrime is also included in the first level professional higher education programme "Police work".

The Latvian Judicial Training Centre also provides training for other legal professionals, including public prosecutors, attorneys, lawyers and employees of governmental bodies and municipal institutions.

In 2015:

- 32 judges and 19 judge assistants undergone training in courses "Cybercrime I" (90 minutes) and "Cybercrime II" (90 minutes);
- two judges participated in two-day seminar "Planning and justifying the search and seizure of electronic evidence: practical implications for legal practitioners in criminal proceedings before presenting evidence in court" (organized by the Academy of European Law in Riga).

It should be also noted that a number training courses are also available online.

Additional information:

Law on Judicial Power foresees a regular evaluation of the professional work of a judge; the objective is to promote continuous professional growth of a judge throughout his/her career thus improving the quality of the work of the judge and the court as such.

The Judicial Qualification Board[119] evaluates the professional work of a judge once every five years (following the approval of the judge for the office with an unlimited term of office). In the evaluation process the Judicial Qualification Board is obliged to analyse also judge's participation in measures aimed at improving his/her qualification.

10.B.2.
Are there any specialised education modules targeted at IT-forensic examiners and cybercrime investigators?

As regards to the continuous training, there are no specialized modules foreseen.

However, the State Police officials (IT-forensic examiners and cybercrime investigators) participate in continuous training provided by the State Police College (please, see answer to Q 10.B.1.) as well as in training courses provided by CEPOL, Europol and other entities.

[119] A self-governing judicial institution which carries out evaluation of the professional work of judges.

10.B.3.

Who is responsible for the provision of cybercrime related training?

To what extent do CEPOL, ECTEG (European Cybercrime Training and Education Group) and Europol/EC3 contribute to the training of your LEAs?

Please, see answer to Q 10.B.1.

CEPOL

The State Police officials frequently participate in CEPOL training.

In 2014, seven State Police officials participated in training courses on cybercrime; nine officials followed the courses online.

In 2015, seven State Police officials participated in training courses on cybercrime; three officials followed the courses online.

It should be also noted that in March 2015, the Latvian Presidency of the Council of the EU in cooperation with CEPOL organized a conference "Cybercrime – Strategic"; the following issues were addressed/discussed: improving methods of cooperation and harmonising investigative methods in cross-border cases related to cybercrime; identifying threats and risks in cybercrime; sharing best practices in cybercrime investigations; establishing a vision for future police cooperation to combat cybercrime; developing ideas on how to improve cooperation between EU and Eastern Partnership countries to fight against cybercrime; identifying current challenges to improve partnerships with the private sector.

ECTEG

Officials from the Forensic IT Unit (Forensics Department of the State Police) participate in the ECTEG training (lately, in training, provided in cooperation with the University College Dublin, which focussed on matters such as malware analysis and investigations as well as forensic scripting using bash).

Europol/EC3

The State Police officials regularly participate in training activities provided by Europol/EC3.

For instance, in 2015, the State Police officials have participated in such training activities/expert meetings as "16th Europol Training Course on Combatting Online Sexual exploitation of Children", "Europol annual expert seminar on child sexual exploitation", "Fighting Internet Paedophilia Project FIIP".

Other training

The State Police officials have also participated in training provided by the Marshall Centre.

In 2014, one official participated in training course "Programme on Cyber Security Studies".

In 2015, one official took a part in a seminar on cyber security "Cyber Alumni Community of Interest (Workshop challenges: Practitioner Action)"; two officials participated in training course "Programme on Cyber Security Studies"

10.B.4.
What are the annual costs for the training/education of your LEA's covered by your authorities (approximate annual budget)?

Training costs are covered by several State Police budgetary lines; this it is not possible to estimate the total annual costs.

10.B.5.
Is training in relation to cybercrime provided to those persons who have a role in the process of international cooperation?
Describe the objectives and length of any such training provision.
Is it proposed that refresher training be provided?
If so, how frequently?

Yes, through regular training modules/programmes provided by the State Police College or other entities (for instance, CEPOL).

10.B.6.

Describe the role of national centres of excellence (if any) in the provision of cybercrime specific training?

N/A

10.B.7.

What is the role of academia?

Are special cybercrime related courses provided in the curricula?

Academia provides a valuable input, for instance:

- a comprehensive manual on investigation cybercrime has been prepared (author: U. Miķelsons);
- significant academic analysis is provided by the Constitutional Court judge U. Ķinis.

At this point, the State Police College has not established cooperation with academia from universities (for instance, University of Latvia, Riga Technical University); this possibility however is currently being explored.

As regards to the second question, there are no special cybercrime related courses provided in the curricula.

10.C. Awareness Raising

10.C.1.

How does your MS generally raise awareness of cybercrime?

What is the role of the private sector (campaigns, EU/national funding).

1. The Latvian Presidency of the Council of the EU *(the first half of 2015)*

The Latvian Presidency focussed on three overarching priorities: *Competitive Europe*, *Digital Europe* and *Engaged Europe.*

Within the priority *Digital Europe* the Latvian Presidency organized a number of events which contributed both to awareness raising and to knowledge exchange, for instance:

- *Digital Assembly 2015 – One Europe, One Digital Single Market* (June 2015): focus on development of the Digital Single Market and issues such as trust, ensuring access and connectivity, building of digital economy for businesses and consumers, promoting of e-society and digital skills;
- *EU28 Cloud Security Conference* (in cooperation with ENISA; June 2015): focus on topics such as legal and compliance issues, technical advancements, privacy and personal data protection, critical information infrastructures, cloud certification;
- *conference on Information and Communication Technologies (ICT) for Information Accessibility in Learning* (May 2015): focus on how the use of ICT in the learning process makes information more accessible, including for people with special needs;
- *seminar on cyber security framework* (May 2015): national strategies of different EU Member States were assessed and best practices shared (for instance, regarding responsible incident detection policy);
- *conference "e-Skills for Jobs 2015"* (March 2015): acquisition of digital skills and creation of new jobs to promote European economic growth were highlighted (also Riga Declaration was adopted).

2. CERT.LV and the State Police

CERT.LV

CERT.LV raises awareness not only about cybercrime but also on (broader) topics such as security and privacy as well as on a number of specific issues (passwords, authentication, others) and particular threats (phishing, malware, e-mail attachments, identity theft).

In 2014, CERT.LV organised/co-organized 95 events with almost 6 000 participants, 2015 – 104 events with 6680 participants. A broad range of participants have taken a part in these events (from school children to IT security professionals and managers).

State Police

The State Police has an active Facebook page (available here) with more than 10 300 followers and a Twitter account (available here) with 43 100 followers.

Information related to cybercrime is regularly disseminated through those social media platforms.

3. The relevant NGOs contributing to awareness raising

"Latvian Information and Communications Technology Association" (LIKTA) (website in LV and EN)

LIKTA was founded in 1998 and it unites leading industry companies and organizations, as well as ICT professionals.

The goal of LIKTA is to foster growth of ICT sector in Latvia by promoting the development of information society and ICT education thus increasing the competitiveness of Latvia on a global scale.

There are also 11 working groups established within LIKTA, for instance, education/professional education development working group, data protection and copyright working group as well as working group on safety and legal issues in digital environment.

In addition, LIKTA annually awards the best e-teacher.[120] In the assessment procedure of candidates, the following elements are evaluated: development of the e-skills and information society enhancement (as such); inclusiveness (regional aspect and the involved society groups); promotion of ICT use and innovation (approach, methods); ICT integration and development of e-skills in the education process. In 2015, there were three finalists; the award was given to a teacher who previously has also been included in Top 500 most innovative IT teachers list (Microsoft programme "Partners in Learning").

Please, see also answer to Q 10.C.2. (on cooperation with the Ministry of Education and Science).

"Latvian Internet Association" (LIA)

Founded in 2000; it focusses on promoting internet accessibility in Latvia, its strengthening, development and popularizing.

[120] Awards are also given in other categories: (1) best e-governance solution; (2) business solution; (3) mobile application; (4) best e-signature integration solution.

Please, see also the initiative *Net-Safe Latvia* Safer Internet Centre (answer to Q 5.A.5).

"Digital Safety Alliance" (DDA)

Launched on 9 February 2016 (during the Safer Internet Day).

DDA aims to raise awareness about safety on internet (in users' friendly language); it will in particular focus on children/youth (social media), safety of e-banking and e-commerce.

4. Events

Cyber security month (each October)

During the cyber security month, a number of activities are carried out.

In 2015, for instance, a conference "Cyber chess. Strategy and tactics in virtual environment" was organized (by CERT.LV in cooperation with a number of partners); it focussed on matters such as secure, stable and resilient identifier systems, cyberterrorism, also different workshops were organized.

At the end of the month, CERT.LV organized an activity *Datorologs* (organized every year since 2012); everyone had a possibility to check their pc, tablet or smartphone free of charge (done by IT specialists), "to cure" them from viruses and receive consultations on internet safety.

E-skills week

Latvia is actively participating in e-skills week; in 2016, the campaign will focus on topics such as (1) digital skills for employment and employability as well as (2) security of ICT and data protection.

In 2016 the e-skills week will take place on 7-11 March; the national coordinators are LIKTA and the Ministry of Environmental Protection and Regional Development. The following main activities are foreseen: activities for school children and youth; training of teachers; digital day for entrepreneurs; regional seminars across Latvia.

E-skills week in Latvia takes place since 2012.

Safer Internet Day

Each year on Safer Internet Day there are a number of awareness campaigns and events organized[121] in Latvia.

For instance, this year (9 February 2016) a special seminar for school teachers was organized (covering issues such as existing challenges with so called "millennium generation" and the relevant teaching methods).

10.C.2.

Given the level of ICT penetration and the early age of ICT tools used, have you considered introducing special courses in the Universities/classes in schools (if so, how early) to make the general public aware/improve their level of awareness of the cybercrime related threats?

The Ministry of Education and Science pays a particular attention to the ICT knowledge integration in education process; for instance, the following elements can be highlighted:

- a pilot project on e-skills (programme "*Datorika*")[122] is implemented in 157 schools; in 2018/2019, a standard on digital competences (based on the pilot project results) will be implemented in the primary schools;
- digital teaching materials and resources are being developed;
- curriculum in line with the latest ICT development tendencies is drafted; the new curriculum will contain requirement on digital and media competence (including e-safety);
- students are being motivated to choose ICT career;
- e-skills of teachers are being enhanced.

The Ministry of Education and Science and institutions subordinated to it have developed a very good cooperation with the private sectors, for instance, with LIKTA (please, see also answer to Q 10.C.1.). In February 2016, the National Centre for Education[123] concluded a memorandum on cooperation

[121] A number of events are organized by kindergartens, schools, youth centers, libraries.
[122] The programme has five levels; they are adjusted to 1-3 graders (7-9 years old students), 4-6 graders (10-12 years old students) and 7-9 graders (13-15 years old students). For instance, competences in programming and algorithmic thinking are being developed.
[123] Its primary function is to develop curriculum for pre-school, basic and general secondary education and vocational education; it develops subject standards and sample teaching- learning programs.

aimed at better integration of ICT knowledge in the education process and its more effective linkage to the labour market.

11. GENERAL OBSERVATIONS AND FINAL REMARKS

11.1.
How do you assess the general capabilities of your MS to prevent and fight cybercrime?

The general capabilities are sufficient; the identified challenges are being addressed.

11.2.
Please provide examples of good practice in combating cybercrime, if any.

1. Regional cooperation

Latvia greatly values the ongoing regional cooperation between the Baltic States (Estonia, Lithuania).

For instance, there is an active experience sharing in the area of prevention between the competent police authorities.

Also, in November 2015, a Memorandum of Understanding has been signed between the CERT Units of all three Baltic States (pledging to step up cooperation on cybersecurity and the protection of IT systems and networks).

2. Cooperation with the United States of America *(extradition of Latvian citizen accused of cybercrime)*

On 23 August 2012, the US District Court Southern District of New York pleaded guilty a Latvian citizen for engaging in a scheme to transmit a computer virus that infected more than a million computers worldwide and caused tens of millions of dollars in losses. On 2 December 2012, the US, in accordance with the Agreement on MLA between the Government of the Republic of Latvia and United States of America, submitted a request to the General Prosecutor's Office on extradition.

On 6 December 2012, the City of Riga Central District Court issued an extradition arrest. On 20 December 2012, the General Prosecutor's Office took a decision that grounds for the extradition are admissible; on 31 January 2013, the Supreme Court of the Republic of Latvia endorsed it.

On 12 April 2013, the Ombudsman of the Republic of Latvia sent a request to the Prime Minister asking to evaluate possible breaches of the European Convention on Human Rights (Convention) as well as to obtain information on human right guaranties in the US in order to avoid any possibilities of violation of human rights.

On 4 July 2013, the US Embassy in Latvia replied that, with regard to the extradition of Latvian citizen to the US, universal human rights will be granted (including, for instance, the right for legal aid/defence attorney).

On 31 May 2013, the Constitutional Court of Republic of Latvia took a decision stating that there are no human right violations in the extradition case.

On 9 February 2015, the Latvian citizen was extradited to the US.

On 5 September 2015, the Latvian citizen pleaded guilty; he was sentenced to imprisonment that was equal to the time already spent in custody.

11.3.
Do you have any suggestions (practical measures or legislative steps) with a view to strengthening prevention and counteracting cybercrime?

N/A

11.4.
Are there any other comments that you would wish to be taken into consideration as part of this process of Mutual Evaluations?

Taking into account the importance given to cybercrime and cybersecurity in the EU Internal Security Strategy 2015-2020, Latvia hopes that the 7th evaluation round will give an additional impetus to our common (EU level) efforts to continue working on the identified issues (e-evidence, "cloud" issue, jurisdictional issues and data retention in particular).

Latvia highly values the initiatives undertaken by the Netherlands Presidency of the Council of the EU (the first half of 2016) and hopes that digital issues will have a prominent role also in other Presidencies' working programmes.