Council of the
European Union

Brussels, 11 April 2017
(OR. en)

5387/1/17
REV 1 DCL 1

GENVAL 4
CYBER 11

DECLASSIFICATION

of document:	5387/1/17 REV 1 RESTREINT UE
dated:	1 March 2017
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Latvia

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

Council of the
European Union

Brussels, 1 March 2017
(OR. en)

5387/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 4
CYBER 11

REPORT

Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Latvia

ANNEX

Table of Contents

1. EXECUTIVE SUMMARY

The visit was perfectly well prepared by the Latvian authorities and included meetings with the relevant bodies involved in preventing and combating cybercrime and in implementing and operating EU policies (e.g. the Ministry of the Interior, the Ministry of Defence, the Security Police, the State Police, the Ministry of Justice and the Prosecutor-General's Office). The preparation and coordination of the visit was exemplary. The Latvian Ministry of the Interior, which coordinated the visit and the various meetings with stakeholders, was exceedingly helpful and ready to arrange further meetings with experts whenever the evaluation team had outstanding questions. Meetings were also held with private organisations, which play an important role in combating and preventing cybercrime and in increasing cybersecurity (CERT.LV, Digital Security Alliance and Net-Safe Latvia and the Latvian Information and Communication Technology Association (LIKTA)), which provided a good overview of how the public-private partnership works.

Latvia has adopted a Cyber Security Strategy of Latvia 2014-2018 (CSS) together with an action plan for its implementation. The Strategy outlines a number of steps, which are being taken with the aim of enhancing Latvia's existing operational capabilities in the fight against cybercrime. The Strategy covers five priority areas, such as: (1) governance and resources of cyber security; (2) rule of law in cyber space and reduction of cybercrime; (3) preparedness and capacity to act in crisis situations; (4) awareness raising, education and research; (5) international cooperation. The second key area is focused on adopting legislative amendments, inter alia to criminalise attacks on automated data processing systems**;** capacity building and training measures; measures to prevent and combat cybercrime; public awareness raising measures; and international cooperation measures.

The Ministry of Defence (MoD) coordinates the development and implementation of the IT security and protection policy, and is also responsible for international cooperation. However, the fight against cybercrime falls within the exclusive competence of the Ministry of the Interior, mainly the State Police and, in specific cases, the Security Police. The State Police is responsible for fighting offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices); computer-related offences (computer-related forgery, computer-related fraud); content-related offences (offences related to child pornography); and offences related to infringements of copyright and related rights. The State Police and the Security Police are responsible for combating the dissemination of racist and xenophobic material through computer systems.

Coordination is based on the mutual cooperation principle, whereby each institution or entity performs its own functions and cooperates with the other parties involved either directly or through the National IT Security Council (the Council). The Council is also the central platform for information exchange and cooperation between the public sector and private sector entities such as financial institutions and NGOs. The wide range of participants seems to contribute to good cooperation and information flow between all relevant stakeholders.

As a general remark, Latvia goes out of its way to make the best possible use of the limited resources available to tackle cybercrime. The idea of simplifying the structure and limiting the spread of functions of the various units in the State Police to achieve the greatest possible return on investment, as put forward in the Cyber Security Strategy, is commendable. One solution could be to concentrate the responsibilities for cybercrime in one State Police unit, with dedicated support from the Forensic IT Unit. Additionally, continued focus should be put on maintaining and increasing resources to strengthen the national capacity to fight cybercrime, especially at the level of the State Police.

There seems to be active cooperation between the State Police and non-governmental organisations such as Net-Safe, as well as between the State Police and CERT.LV. Net-Safe especially often cooperates with the State Police if a serious suspicion of sexual exploitation of minors arises.

The role of Net-Safe is to prevent cybercrime and provide support in cases of child sexual abuse online and pornography. CERT.LV plays an important role in responding to cyber incidents, acting as an intermediary between the private sector, academia and the police. It is a skilled and willing partner to public institutions and society at large (e.g. providing device-cleaning services).

As regards legislation, Latvia has signed and ratified the Convention on Cybercrime and implemented the EU directives related to cybercrime in its national legislation. As in many other countries, no specific definition of cybercrime is provided in Latvian legislation. At the practical level, cybercrime comprises all offences against computer systems and computer data, as well as crimes enabled by the use of a computer system.

Latvia is also working on implementing an improved prevention strategy aimed at raising awareness of the possible dangers of online activities. If targeted to a higher number of relevant vulnerable groups, this would further contribute to improving the overall safety of Latvia's cyber environment. Though many preventive measures have been put in place by various public bodies in Latvia, they are not always coordinated. In the evaluators' view, using a single point to coordinate preventive activities among ministries and other relevant organisations would benefit the whole country, since it would prevent any duplication of preventive work.

EU agencies are known to and used by the Latvian authorities. Since most investigations are run by the State Police, it is the State Police which has participated in Eurojust's coordination meetings in the past, and it is likely to continue to do so in the future. The State Police is therefore also responsible for most inter-state cooperation during investigations of cybercrime cases, using the channels offered by the Europol/EC3 system. However, the Latvian authorities see a need for EU level solutions to improve and accelerate the execution of mutual legal assistance, judicial cooperation and the communication process between Member States and third countries, as well as direct cooperation with foreign ISPs.

The Latvian Judicial Training Centre organises training for judges and, when needed, training on cybercrime can also be organised. Prosecutors are also given training, but in both cases training is not mandatory and covers a limited number of practitioners. Having prosecutors specialised in cybercrime could strengthen Latvia's capacity to fight this phenomenon. Police officers, however, are well trained. The State Police College offers police officers a comprehensive cybercrime training programme with different modules. Joint training courses involving the State Police and the judiciary could help to spread knowledge of cybercrime and function as a platform for the exchange of experiences, with topics such as the possibilities and techniques available to the police or issues relevant for judges and prosecutors in criminal proceedings related to cybercrime.

With limited resources, Latvia maximises its performance in the joint fight against cybercrime by integrating available resources from outside public administration as much as possible. A clear example is the creation of the Cyber Defence Unit of the National Guard, which will serve as a capacity buffer, composed of Latvian private sector experts, in the event of a cyber crisis. Another example is the use of young people and other volunteers, for example in awareness-raising initiatives. On top of that, the use of peers (young people talking to other young people in their language) in prevention and awareness campaigns has also proven to be a very effective method of actually reaching the target audience. A third example is the good cooperation with NGOs in the cyber field, such as Latvian Safer Internet. To keep up this good cooperation, consideration could be given to providing enough feedback to NGOs on the results of their cooperation.

The strategy in Latvia is obviously to make the country unattractive to cybercriminals and to make preparations for a possible crisis. In view of the existing structures, the level of effort invested by the country in the fight against cybercrime, and the effectiveness of that investment, the opinion of the evaluators is clearly positive.

2. INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[1], a mechanism was established to evaluate the application and implementation at national level of international undertakings in the fight against organised crime. In line with Article 2 of the Joint Action, the Working Party on General Matters including Evaluations (GENVAL) decided on 3 October 2013 that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of EU policies on preventing and combating cybercrime.

The choice of cybercrime as the subject for the seventh round of mutual evaluations was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas: cyber-attacks, child sexual abuse/pornography online, and online card fraud. It should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation, and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[2] (transposition date 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems (transposition date 4 September 2015), are particularly relevant in this context.

1 Joint Action of 5 December 1997 (97/827/JHA), OJ L 344, 15.12.1997, p. 7.
2 OJ L 335, 17.12.2011, p. 1.
3 OJ L 218, 14.8.2013, p. 8.

Moreover, the Council Conclusions of June 2013[4] on the EU Cybersecurity Strategy reiterate the objective of ratifying the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] of 23 November 2001 as soon as possible and emphasise in their preamble that 'the EU does not call for the creation of new international legal instruments for cyber issues'. This Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.[6]

Experience from past evaluations shows that Member States will be in different positions as regards the implementation of the relevant legal instruments, and the current evaluation process could also provide useful input to Member States that may not have implemented all aspects of the various instruments. Nonetheless, the evaluation aims to be broad and interdisciplinary, and to focus not only on the implementation of various instruments relating to the fight against cybercrime, but also on the operational aspects in the Member States.

Therefore, in addition to cooperation with prosecution services, this will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3 and how feedback from those organisations is channelled to the appropriate police and social services. The evaluation focuses on the implementation of national policies to suppress cyber-attacks, fraud and child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to those who fall victim to cybercrime.

4 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

5 CETS no 185; opened for signature on 23 November 2001, entered into force on 1 July 2004.

6 CETS no 189; opened for signature on 28 January 2003, entered into force on 1 March 2006.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. Latvia was the twentieth Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, a list of experts in the evaluations to be carried out has been drawn up by the Presidency. Member States have nominated experts with substantial practical knowledge in the field pursuant to a written request to delegations made by the Chairman of GENVAL on 28 January 2014.

The evaluation teams consist of three national experts, supported by two staff from the General Secretariat of the Council and observers. For the seventh round of mutual evaluations, GENVAL agreed with the proposal from the Presidency that the European Commission, Eurojust, ENISA and Europol/EC3 should be invited as observers.

The experts charged with undertaking the evaluation of Latvia were Mr Geert Schoorens (Belgium), Mr Søren Palsgaard (Denmark) and Mr Marcin Golizda-Bliziński (Poland). Two observers were also present: Mr Tomas Zbihlej (Eurojust) and Mr Sławomir Buczma (General Secretariat of the Council).

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Latvia between 8 and 11 March 2016, and on Latvia's detailed replies to the evaluation questionnaire and to subsequent follow-up questions.

3. GENERAL MATTERS AND STRUCTURES

3.1. National cyber security strategy

The Cyber Security Strategy of Latvia 2014-2018 (CSS) was adopted by the Cabinet of Ministers (government) in January 2014. The aim of the cybersecurity policy is to create a secure and reliable cyberspace which ensures a safe, reliable and continuous supply of services essential for the state and society. The implementation of the cybersecurity policy is based on the principles of development, cooperation responsibility and openness.

The rule of law in cyberspace and the reduction of cybercrime is one of the five key action areas (subsection 4.2). It is stated that reducing cybercrime requires two basic types of action:

— preventive work to limit criminal offences;

— effective combating of crime.

3.2. National priorities with regard to cybercrime

A. National priorities

The national priorities which refer to cybercrime are set out in various policy planning documents (including sectoral documents).

A.1. Policy-planning documents on cybersecurity, including cybercrime

A.1.1. Cyber Security Strategy of Latvia 2014-2018 and amendments (including an action plan)

According to the CSS, e-evidence-related capacities should be enhanced with a view to combating cybercrime. Cybercrime investigation and the collection and assessment of e-evidence and understanding of the concept of *"significant damage"* require special knowledge; it is crucial for law enforcement officials, prosecutors and judges to have sufficient expertise, to ensure the rule of law in cyberspace. Taking this into account, the CSS sets out the following required measures:

I Legislative actions

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

II Capacity-building and training actions

- assess and develop the existing e-evidence acquisition and analysis capacities in the cybercrime investigation process (by developing the State Police's competence and improving cooperation with the Information Technology (IT) Security Incidents Response Institution (CERT.LV);
- develop methodical material on the ICT sector to increase the knowledge of police officers, officials directing criminal proceedings and judges;
- in addition, implement an in-depth training programme on combating cybercrime.

III Measures to prevent and combat cybercrime

- establish a special unit dealing with cybercrime under the State Police;
- combat and investigate cybercrime by assessing and improving the existing resources, procedures and cooperation mechanisms and their efficiency.

IV Public-awareness-raising (and preventive) measures

- enhance the competence of educational institutions and teaching staff and their contribution to educating children and young people on ICT security (by integrating these issues into the education process and organising relevant learning activities to boost their understanding of information security, privacy protection and the use of e-services); additionally, ensure that children and young people are able to report violations on the internet and to receive support from a psychologist, and organise continuous training for teaching staff on cybersecurity;
- develop educational and informative materials on cybersecurity (for educational institutions and interest groups) which are easily accessible and adapted to various age groups;
- create an ICT security laboratory and organise scientific conferences on topical issues related to cybersecurity and cybercrime (in cooperation with universities and scientific institutes);
- implement educational and informative campaigns and other measures for the overall enhancement of awareness and understanding in society on cybersecurity, cybercrime and existing threats.

V International cooperation actions

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

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

At the time of the on-site visit the establishment of a special unit dealing with cybercrime under the State Police was mentioned. After the on-site visit the evaluation team was informed that the Action plan (approved on 03.05.2016) of the new government does not foresee establishment of a special unit dealing with cybercrime within the State Police. However, this is envisaged in the State Police development concept (policy planning document), approved by the government on 06.04.2016.

A.2. Sectoral policy (home affairs) planning documents related to cybercrime

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

The State Police Strategy 2014-2016 states that the use of high technology to combat offences must be improved.

According to its 2016 Working Plan, combating all types of cybercrime is one of the State Police's top four priorities. The State Police should carry out activities aimed at enhancing the implementation of the Criminal Procedure Law provisions (to simplify investigations and enhance their effectiveness).

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

The Action Plan provides that the work of law enforcement agencies and the relevant security agencies should be enhanced. In addition, increased awareness and knowledge of new trends and dynamics and of the threat level of organised crime (including cybercrime) is required.

A.2.3. State Police Crime Prevention Strategy 2014-2017

The Strategy outlines the main principles, objectives, strategic directions, priorities and approaches regarding crime prevention (situation prevention, social prevention). According to the Strategy, internet safety is one of the five priority areas in crime prevention.

A.3. Other sectoral policy-planning documents related to cybercrime

A.3.1. Intellectual Rights Protection and Enforcement Guidelines for 2015-2020

The Guidelines emphasise the necessity of establishing a special unit under the State Police to deal with cybercrime (including copyright offences).

A.3.2. Guidelines for the prevention of juvenile delinquency and the protection of children from crime 2013-2019

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

A.3.3. Guidelines for the Prevention of Trafficking in Human Beings 2014-2020

The Guidelines provide for cases in which victims or potential victims are recruited through internet social networks to be notified, as well as for information to be provided on potential human trafficking cases or attempts.

B. Links 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 the fight against organised crime 2014-2016: (1) trafficking in human beings; (2) excise fraud and MTIC fraud; (3) synthetic drugs; (4) heroin; (5) cybercrime; and (6) organised property crime.

Latvia participates in those EU priorities which pose the greatest threat on the ground at national level, in EU priorities where Latvia is directly involved in a specific phenomenon (for instance, trafficking in human beings), and in the implementation of those strategic goals and specific OAP activities which are linked to national priorities, measures and activities (as set out in the State Police Strategy 2014-2016, the State Police Working Plan 2016, the Action Plan on the fight against organised crime 2014-2016, and the State Police Crime Prevention Strategy 2014-2017). Latvia participates in all three cybercrime OAPs.

3.3. Statistics on cybercrime

3.3.1. Main trends leading to cybercrime

The main trends observed by the Latvian authorities in 2015 and 2016 with regard to cybercrime are as follows:

- extortion related to DDoS and ransomware attacks against the private sector (merchants);
- use of Latvian hosting possibilities – due to the very high internet speed and very good connection quality in Latvia, Latvian internet connections are increasingly being used to commit criminal offences from abroad (this refers in particular to CSE and malicious software); there is also an anonymity issue which should be highlighted (reselling IP ranges to private internet service providers (ISPs) which are not registered as electronic communications merchants);
- spreading of child pornography and paedophilic material on the internet (a trend which 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.

In 2015, a total of 47 406 criminal proceedings were initiated in Latvia, 453 of which were related to cybercrime. Cybercrime therefore accounted for 0.96 % of all criminal proceedings. Of these criminal proceedings, the State Police initiated 44 900, 427 (0.95 %) of which were related to cybercrime. Cybercrime in a broader context (cyber-enabled and cyber-related crime) accounts for 1.54 % of all criminal proceedings in Latvia.

3.3.2. Number of registered cases of cyber-criminality

Law enforcement statistics

All law enforcement agencies have access to the Integrated Interior Information System (IIIS), a register held and managed by the Information Centre of the Ministry of the Interior. The IIIS consists of several sub-information systems, including the Punishment Register, which contains, inter alia, data on initiated criminal proceedings, criminal offences and accused persons, and specific information on criminal proceedings (from KRASS). Information is provided by the authorities which, according to the Criminal Procedure Law, are authorised to carry out criminal proceedings. Authorised users have direct access to the IIIS.

The Information Centre of the Ministry of the Interior also holds and manages the Criminal Procedure Information System (KRASS), which includes information on initiated criminal proceedings, detected criminal offences, officials directing proceedings, individuals entitled to assistance from a defence counsel, and victims. Information in KRASS is entered online no later than the next working day following a procedural action, the registration of an act or the coming into effect of a court judgement.

Judicial statistics

Judicial statistics are kept separately from law enforcement statistics.

The Court Information System (TIS) is managed by the Ministry of Justice. Its aim is to facilitate record registration, to store, process and exchange judicial information, and to gather statistics. Law enforcement authorities can access judicial statistics.

The Latvian authorities reported that it is not possible to obtain an entire data set (from the initiation of a criminal proceeding to data on conviction) under one information system. However, some of the systems are interlinked (for instance, TIS is linked to KRASS (to ensure data exchange, except for statistics), and KRASS is linked to the IIIS Punishment Register).

Role of the private sector

The private sector does not provide input into statistics on cybercrime. However, CERT.LV gathers statistics which are based, inter alia, on data submitted by the private sector.

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 finalised within one or two years; hence, for instance, a final conviction delivered in 2015 may refer to a criminal offence registered earlier than 2014.

Criminal Law	Initiated criminal proceedings (in total)[23]		Criminal proceedings initiated by the State Police		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

[23] Total number of criminal proceedings initiated by the State Police, Security Police and Public Prosecutor's Office of the Republic of Latvia.
[24] Incitement of national, ethnic and racial hatred.
[25] Violation of 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, the restriction of entertainment of an intimate nature and the handling of material of a 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 related to financial instruments and means of payment.
[30] Arbitrary accessing of automated data processing systems.
[31] Interference in the operation of automated data processing systems and illegal actions using the information included in such systems.
[32] Illegal operations with devices influencing automated data processing system resources.
[33] Acquisition, development, alteration, storage and distribution of data, programs and equipment for illegal activities using electronic communications network terminal equipment.
[34] Incitement of national, ethnic and racial hatred.

3.4. Domestic budget allocated to the prevention of and fight against cybercrime, and support from EU funding

Since there are several State Police entities involved in the prevention of and fight against cybercrime, there are no budgetary allocations dedicated specifically 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.

The EU is funding a two year 'Capacity building to prevent and fight against cybercrime' project, expected to commence in April 2017. The project is one of the national priorities within the Internal Security Fund. There are plans to use this funding (expected to total EUR 865 775) for acquiring technical equipment (e.g. in order to ensure also remote expertise), for training of forensic experts and other officials, and for prevention activities, including awareness raising (covering a wide range of interest groups).

3.5. Conclusions

- Latvia has adopted a Cyber Security Strategy together with an action plan for its implementation. The Strategy provides for a number of steps, which are being taken with the aim of enhancing Latvia's existing operational capabilities in the fight against cybercrime. The Strategy is structured around five main areas where improvements are to be made, namely: legislative actions; capacity-building and training actions; measures to prevent and combat cybercrime (aimed at establishing a focal point in the State Police to deal with cybercrime and improving the existing procedures and cooperation mechanisms); public-awareness-raising measures; and international cooperation actions (aimed at improving cooperation with various international organisations).

- The Ministry of Defence is responsible for the implementation of the Cyber Security Strategy, coordinates the development and implementation of the IT security and protection policy, and deals with international cooperation. However, the fight against cybercrime falls within the exclusive competence of the Ministry of the Interior (see the information on the State Police).

- The main trends observed by the Latvian authorities in 2015 and 2016 with regard to cybercrime are as follows: extortion related to DDoS and ransomware attacks against the private sector (merchants); use of Latvian hosting possibilities; spreading of child pornography and paedophilic material on the internet (a trend which has developed over a longer time period); phishing attacks and malicious software (malware); malware attacks on banking systems and e-bank users; and 'card sharing'.

- While the State Police is responsible for the investigation of most types of crimes falling under or associated with the cybercrime category, the investigation of one form of cybercrime is singled out and entrusted to the Security Police – namely, the investigation of 'hate speech', meaning the dissemination of racist or xenophobic material through IT systems. As was reported to the evaluation team, this stems from the historical context and the need to protect the state against external attacks by radical opponents of Latvia's independence.

- However, the statistics show that very few hate crimes are registered, and it seems that an even smaller number of these cases were actually submitted to the prosecutor's office in 2014 and 2015. After the on-site visit the evaluation team was informed that in 2016 significant rise of hate crimes was noted.

- Furthermore, practitioners met during the evaluation visit mentioned problems with the delineation of jurisdiction between the State and the Security Police in this area. It seems that further delineation of their jurisdiction could be beneficial and raise the efficiency of prosecution of this type of cybercrime.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecution and courts)

4.1.1. Internal structure

a) Courts

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

There are no special (extraordinary) courts in Latvia. Article 1(5) 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 of this Article, are not allowed and shall not be established'. Hence, in Latvia cyber-dependent crime cases and cyber-enabled crime cases are heard by ordinary district (city) courts and regional courts as well as the Supreme Court.

There are no judges specialised in cybercrime cases.

b) 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 supervises the observance of law within the scope of the jurisdiction determined by the law. The Prosecution Service is composed of the Office of the Prosecutor-General; Offices of Prosecutors of judicial regions; Offices of Prosecutors of districts (cities); specialised Offices of Prosecutors; and the Service of the Administrative Director. There are no prosecutors specialised in cybercrime cases.

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

Cybercrime	**Entity which supervises pre-trial investigations, conducts criminal prosecution and maintains state charges**
Cybercrime within the territory of the 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
Cybercrime where computer/IT systems were involved as tool or target (of Article 177[1](3) of the Criminal Law)	Prosecutor's Office for Organised Crime and Other Branches
Other cybercrime	Prosecutor's Office of general jurisdiction

4.1.2. Capacity and obstacles for successful prosecution

The Latvian authorities stressed that the Office of the Prosecutor pays particular attention to the training of prosecutors and that efforts in this regard are to be intensified. To strengthen the capacity of prosecutors, they are covered by training organised in Latvia and abroad.

In 2014 and 2015, prosecutors participated in the following training activities:

- 'Cybercrime' (organised by the Office of the Prosecutor in cooperation with the Latvian Judicial Training Centre; 54 participants);
- 'Cybercrime and electronic evidence' (organised by the Office of the Prosecutor in cooperation with the Latvian Judicial Training Centre; 57 participants);
- 'Cybersecurity crisis management' (organised by CERT.LV; one participant);
- 'Judicial and technical aspects of cybercrime' (organised by ERA, Trier, Germany; three participants).

- 'Planning and justifying the search and seizure of electronic evidence: practical implications for legal practitioners in criminal proceedings before presenting evidence in court' (organised by the Academy of European Law in cooperation with the Latvian Judicial Training Centre; five participants);
- 'Basic course on judicial and technical aspects of cybercrime' (organised by the Academy of European Law, Trier, Germany; two participants);
- 'Digital piracy – investigation and prosecution' (Hungary; one participant).

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

- electronic communications merchants have a duty to ensure the retention and storage of data for 18 months as well as the transfer of such data (including to the Office of the Public Prosecutor), but in some complicated and drawn-out cases 18 months is too short a period of time for data to be stored;
- anonymous internet service provision (pre-paid internet, WiFi, one IP address for several devices);
- electronic communications merchants' inability to submit requested information in a timely manner;
- possibility of one IP address being used by thousands per day (agreements on IP address usage);
- long delays in receiving IT forensic examination results (since there is a lack of experts in Latvia and existing experts are overloaded);
- the possibility of receiving IP addresses registered outside Latvia in a timely manner is very limited.

4.2. Law enforcement authorities

The following State Police departments are responsible for the prevention of and fight against cybercrime:

- the Central Public Order Police Department – prevention of cybercrime;
- the Central Criminal Police Department – fight against cybercrime.

a) Prevention

The Crime Prevention Unit (CPU), which is an integral part of the Central Public Order Police Department, is responsible for the coordination and implementation of crime prevention activities. Four police officers at the CPU are specifically designated to implement prevention measures in the following fields: (1) drugs; (2) violence (in schools and domestic violence); (3) property crimes; (4) cybercrimes. Each officer, in his or her respective field, is in charge of enhancing cooperation with the relevant state and municipal institutions, NGOs and other stakeholders, as well as of obtaining additional funding.

The CPU has established valuable cooperation with the relevant units of the Central Criminal Police Department, for instance with the Economic Crimes Enforcement Department, which consults the CPU officers on new developments and other relevant issues relating to cybercrime. There are also plans to increase the involvement of civil society through a volunteer programme launched by the State Police in 2016, where volunteers raise awareness and spread information to the wider public on a number of topical issues, including internet safety.

In addition, certain prevention tasks are implemented at the level of five regional state departments and districts (with inspectors specialised in various areas).

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

b) Fight against cybercrime

There are five departments at the Central Criminal Police Department. Two of them deal directly with the 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 and credit institutions;
- Unit 3: Unit for combating fraud, malfeasance, money counterfeiting and unlicensed business;
- Unit 4: Cybercrime Enforcement Unit (CEU).

The CEU has 13 officers in total. Their tasks are divided as follows: fighting crimes against automated data processing systems group (three officers); operational analysis group (one officer); technical support, internet intelligence, crimes against online child sexual abuse group (two officers); intellectual property protection group (two officers); and investigative capacity (three officers).

On the basis of recent amendments to Cabinet Regulation No 568 on salaries and premiums of those officials who work in authorities subordinated to the Ministry of the Interior (7 April 2015), officials who work in the field of the fight against cybercrime may be awarded a bonus (of up to EUR 400) based on individual performance.[7]

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

[7] After the on-site visit the evaluation team was informed that as from January 2017 CEU (Unit 3, previously Unit 4) is also dealing with online and payment card fraud as well as industrial property issues. The total number of officers has increased; CEU currently has staff of 20 officials. Also ranks of the officials has been increased and premium system maintained. In addition, each region (5) has designated a contact/support officer; they are under the "supervision" of the CEU, which has an authority to require support in specific priority issues.

The Forensic IT Unit is a part of the Forensics Department of the State Police. As regards human resources, at the time of the on-site visit four certified experts were hired by the Forensic IT Unit, which provides support to investigators. The certified experts have higher education qualifications in the IT field.

In autumn 2015, the process of setting up a specialist IT group was started. The aim of this group is to deliver high-quality support to investigators before an expert examination is determined. At the time of the on-site visit two specialists were receiving training from the experts at the Forensic IT Unit. Further extension of the group was planned in late 2016 (two more specialists).

The State Police has identified the following main challenges in fighting cybercrime: improving the capacity and training of the CEU; technical capabilities and equipment (for instance, regarding evidence-fixing on the spot); rapid technological developments (for instance, in encryption); IT forensics as regards content (challenges relate to malware and cyber-attacks in particular; CERT.LV as a specialist provides valuable contributions, which cannot however be presented as evidence in criminal proceedings, since according to the Criminal Procedure Law, evidence in criminal proceedings 'may be the conclusion of an expert [...] regarding facts and circumstances that has been provided by an expert [...] involved in concrete criminal proceedings'); and IT forensics as regards timing (forensic examination is usually carried out within one to two months).

The operational 24/7 contact point (CP) is the Operational Coordination and Information Provision Unit (OCIPU) of the International Cooperation Bureau of the State Police Central Criminal Police Department. The Unit acts as an international criminal judicial cooperation 'front office', providing a single point of contact (SPOC) by coordinating all international information exchanges 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.

There are 16 employees at the OCIPU: ten duty officers, four police officers (who carry out administrative tasks during working hours) and one civilian staff member (dealing with international projects). Only police officers are employed as duty officers at the CP (10 police officers working shifts).

The CP's main tasks are as follows:

- providing and exchanging information between Latvian and foreign law enforcement agencies 24/7;
- assisting Latvian and foreign law enforcement agencies in combating and preventing organised crime, cybercrime and illegal immigration;
- dealing with the identification of persons, document checks, searches for wanted and missing persons, and searches for stolen vehicles and items;
- coordination of the authorities involved in cases of prevention and investigation of cross-border crimes, including police cooperation in the framework of the Schengen Convention (for instance, Articles 40 and 41);
- general police cooperation (Article 39 of the Schengen Convention);
- the Swedish initiative (Council Framework Decision 2006/960/JHA);
- Prüm hit follow-up procedure.

The CP's officers have investigative powers and apply any investigative measures related to activities within criminal cases. In addition, they collect electronic evidence in relation to various types of offences. Most of the CP's officers have attended the basic course ('New technologies in police work') organised by the State Police College.

4.3. Other authorities/institutions/public-private partnership

Besides the judiciary and law enforcement agencies, the role of the following entities in preventing and combating cybercrime should be underlined:

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

National IT Security Council

This is a central platform for information exchange and cooperation between public and private authorities. It is composed of representatives of a number of institutions, such as the Ministry of Defence, the Bank of Latvia, the Ministry of Justice, the Financial and Capital Markets Commission, etc. (For more information, please refer to 4.4.1.)

CERT.LV

Since 1 February 2011 CERT.LV has been tasked with promoting IT security in Latvia. It operates under the Ministry of Defence and its powers are governed by the Law on the Security of IT. The main tasks of CERT.LV are to maintain and update information on IT security threats, provide support during IT security incidents, advise governmental institutions, and organise informative and educational activities for government employees, IT security professionals and the general public.

CERT.LV also supports the IT and Information Systems Security Experts Group 'DEG' and the safer internet environment initiative 'Responsible ISP' and maintains the website esidross.lv ('Be safe' in English) which is aimed at a wide audience and provides guidance on how to protect computers and stay safe on the internet.

***Net-Safe Latvia* Safer Internet Centre**

The *Net-Safe Latvia* Safer Internet Centre (the Centre) is the national contact point for the EU *Safer Internet* Programme's Insafe network. Its main tasks involve informing and educating (target groups: children, adolescents, teachers and parents); reporting illegal online content and breaches (reporting is anonymous; reports are processed and, if necessary, sent to the State Police for examination); and providing a State Inspectorate for Protection of Children's Rights helpline, 116111 (for more information, please refer to 6.2.3).

4.4. Cooperation and coordination at national level

4.4.1. Legal or policy obligations

According to the CSS, the Ministry of Defence (MoD) coordinates the development and implementation of the IT security and protection policy, and deals with international cooperation. Hence, in the context of cybersecurity as such, the MoD has the main coordinating role. However, the fight against cybercrime falls within the exclusive competence of the Ministry of the Interior (mainly the State Police and, in specific cases, also the Security Police).

The State Police is responsible for fighting offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices); computer-related offences (computer-related forgery, computer-related fraud); content-related offences (offences related to child pornography); and offences related to infringements of copyright and related rights.

The Security Police is responsible for combating the dissemination of racist and xenophobic material through computer systems.

As regards prevention, several ministries are involved in cybercrime prevention measures:

- the Ministry of the Interior (the State Police, the Security Police) focuses on raising public awareness and running campaigns (covering issues such as new trends in cybercrime, and risks and how to avoid them);
- the Ministry of Education and Science, within its remit, promotes knowledge and understanding of cyberspace and how to use it securely;
- the Ministry of Welfare implements social policy and policies on the protection of children's rights.

Coordination is based on the mutual cooperation principle, whereby each institution or entity in performing its functions cooperates with the other parties involved either directly or through the National IT Security Council (the Council). The Council was 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. The Council's operation is ensured by the National Cybersecurity Policy Coordination Section of the MoD. The following institutions and entities currently participate in the Council:

1) the Ministry of Defence;
2) the Ministry of Foreign Affairs;
3) the Financial and Capital Markets Commission;
4) the Bank of Latvia;
5) the Ministry of Economics;
6) the Ministry of the Interior, the State Police and the Security Police;
7) CERT.LV;
8) the Ministry of Education and Science;
9) the Ministry of Welfare;
10) *Net-Safe Latvia* Safer Internet Centre;
11) the State Chancellery;

12) the National Armed Forces and the Cyber Defence Unit of the National Guard;

13) IT-sector NGOs;

14) the Ministry of Transport;

15) the Constitution Protection Bureau;

16) the Ministry of Justice and the Data State Inspectorate;

17) State Joint Stock Company 'Latvian State Radio and Television Centre';

18) the Ministry of Environmental Protection and Regional Development.

In the context of coordination, the National Cyber Security Policy Coordination Section of the MoD regularly informs the Cabinet of Ministers (by submitting progress reports) and the Latvian Parliament *(Saeima)* on the state of play of the implementation of the CSS. The Parliament is thus fulfilling its supervisory function in this regard. The *Saeima* takes a rather active role and puts forward a number of topical issues, including related to collaboration and cooperation between various state bodies (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 department).

4.4.2. Resources allocated to improve cooperation

The State Police makes wide use of the training opportunities provided by CEPOL, Europol and other entities to increase police officers' capacities. Forensic experts also participate in training courses. However, according to the Latvian authorities, this training should be intensified due to rapid developments in IT.

As regards the examination of illegal use of payment cards and skimmers, it was reported that the Forensic IT Unit (the Forensic Department of the State Police) has the necessary technical and human resources. However, it was noted that the technical equipment (i.e. the software and technical resources) used by the CEU needed improving, as did the unit's knowledge of the newest technologies. Using the existing resources, efforts are made to enhance cooperation with the private sector.

4.5. Conclusions

- According to Article 82 of the Constitution, courts are separated into district (city) courts, regional courts and the Supreme Court. There are no special courts dedicated to cybercrime in Latvia. Cybercrime cases are heard by ordinary courts. Judges exchange their experiences of specific types of cases via email through organised groups. Furthermore, the central judicial database of judgments helps to keep the different judges informed of judgments handed down by the other courts, which contributes to the fair distribution of justice and legal certainty.

- Judges would, however, welcome the possibility of exchanging information on how to proceed in the most difficult cybercrime cases, specifically those with an international dimension. In the opinion of the evaluators, creating a network of judges with relevant experience in handling complicated cybercrime cases at EU level could contribute to an efficient and effective distribution of justice.

- The Office of the Prosecutor is an institution of judicial power, which independently supervises the observance of law within the scope of the jurisdiction determined by law. The Office of the Prosecutor is not a member of the National IT Security Council.

- The Office of the Prosecutor is involved in handling cybercrime cases (e.g. through the Prosecutor's Office of Investigation of Finance and Economic Crimes, the Prosecutor's Office for Organised Crime and the Prosecutor's Office of general jurisdiction). Most cybercrime cases seem to be handled by the Regional Prosecution Offices. However, there are no prosecutors specialised in handling cybercrime cases. Therefore, in the opinion of the evaluators, specialisation within the prosecution service should be considered, for instance by designating a prosecutor within each district to specialise in the field of cybercrime or by issuing internal guidelines to all prosecutors on criminal policy related to cybercrime or on issues of criminal procedure, such as the gathering of e-evidence (cell phone searches, network searches, covert operations on the internet).

- The State Police and the Security Police are responsible for the fight against cybercrime. Within the State Police, the Central Public Order Police Department is responsible for the prevention of cybercrime and the Central Criminal Police Department is responsible for the fight against cybercrime.

- Due to its varied nature, cybercrime is handled by multiple units within the State Police: the Criminal Investigations Department, the Economic Crime Department and the International Cooperation Bureau. Responsibility for cybercrime is also spread amongst multiple units within these various departments.

- At the time of the on-site visit the Action plan of the Latvian government provided for the establishment of a single unit within the State Police to fight cybercrime. Currently it is envisaged in the State Police development concept. The evaluators consider this to be an important step in improving limited police capacities in cybercrime. However, additional resources should make it possible for this central unit to have the operational and technical capacity to deal autonomously with the most complex forms of cybercrime (e.g. intrusions into protected networks, organised crime), as well as substantial capacity to support regional police in dealing with the more common forms of cybercrime. Therefore, consideration should be given to how to maintain and increase resources at the State Police, and thus to strengthen the national capacity to fight cybercrime. Consideration could also be given to building sufficient intelligence capacity within the police as regards cyber threats and criminal groups in the field of cybercrime. Therefore, the goal of streamlining and simplifying the structure and spread of functions of the various State Police units to achieve the greatest possible return on investment is commendable. Careful consideration should be given to the possibility of concentrating the responsibilities for cybercrime in one State Police unit, with dedicated support from the Forensic IT Unit.

- The forensic side of investigations is handled by the Forensic IT Unit, which is also responsible for providing support on IT-related issues to all other State Police units, as well as to the Military Police, the courts and other bodies outside the State Police. It seems, in view of the lack of resources allocated to the fight against cybercrime, that clear priorities should be identified to build basic forensic capacities at the regional police level (e.g. cell phone analysis), to alleviate the work of the Forensic IT Unit of the Central State Police and to enable them to focus their limited resources on more complex forensic issues. In the evaluators' view, sufficient and up-to-date technical equipment (both hardware and software) is essential, to allow the limited human resources to be used as efficiently as possible.

- The evaluation team was informed that, despite limited financial resources within the State Police, salary bonuses are granted to police officers working in the cybercrime field. In the evaluators' view, this is an example of best practice, since it promotes knowledgeable and skilled staff and helps to prevent them from looking for a new job.

- The State Police Information Bureau has set up an automated system of communication with domestic internet service providers, using fixed forms and a Single Point of Contact (SPOC), to ensure that requests for digital evidence data are executed efficiently. The system prevents misunderstandings, delays and confusion between police officials and ISPs, and guarantees a quick and accurate response to sometimes urgent requests**.**

- The National IT Security Council provides a platform for communication between the governmental and non-governmental bodies in charge of implementing the Cyber Security Strategy of Latvia. Although the Council is not empowered to give 'orders' to its members, it functions as an important coordination and discussion forum. Policies and their implementation are discussed and common solutions are developed and agreed upon. Furthermore, the representatives met by the evaluation team confirmed that any disagreements can easily be escalated to the political level, where they can be solved comparatively swiftly and solutions can be implemented. This results from involving the Latvian Parliament in its work. Given that several ministries are involved in cybercrime prevention, the ability to swiftly and efficiently coordinate policy as well as to swiftly secure a political consensus where necessary seems especially important. However, in the opinion of the evaluators, Latvia should further increase its use of the existing structures and channels, to enhance coordination.

- Consequently, the National IT Security Council should make optimal use of its capabilities and its position of authority, *inter alia* by increasing the involvement of private stakeholders in the coordination process. The National IT Security Council should consider involving specific private partners for specific coordination projects, such as in the field of prevention, to avoid gaps or overlaps in the fight against cybercrime.

- CERT.LV plays a very important role in Latvia's strategy to tackle cybersecurity. It provides highly valuable expertise to all governmental bodies active in the field, and acts as a key partner to all the most affected spheres of the private sector. It monitors all cyber incidents and also provides testing and technical exercises to increase cybersecurity and facilitate the prevention of cybercrime. It also actively participates in exercises and cooperation at the international level, for example in NATO exercises and Cyber Europe (ENISA-led training). CERT.LV is also active in prevention and awareness-raising, amongst both the general public and IT professionals. In the opinion of the evaluators, CERT.LV seems to be a very efficient and flexible organisation with the ability to adapt to the fast-changing landscape of cybersecurity and to provide much-needed support to all public and private bodies concerned.

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

5.1.1. Council of Europe Convention on Cybercrime

Latvia 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 on 1 June 2007.

5.1.2. Description of national legislation

A/ Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems

Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU have been transposed into the Latvian legal system through amendments to the following acts:

- Criminal Law, including amendments to the Criminal Law adopted on 25 September 2014 (Articles 144, 241, 243 and 244);
- Procedures for the Coming into Force and Application of the Criminal Law;
- Criminal Procedure Law;
- Operational Activities Law;
- Latvian Administrative Violations Code;
- Electronic Communication Law;
- Law On Information Society Services;

- Law on the Security of IT;
- Personal Data Protection Law;
- Law on Pornography Restrictions;
- Protection of the Rights of the Child Law;
- Law on Judicial Power;
- Office of the Prosecutor Law.

There is extensive legislation in place in the Criminal Law regarding cybercrime[8]. The following acts are criminalised therein: illegal interception (Article 144); the obtaining, manufacture, distribution, utilisation and storage of data, software and equipment for illegal acts with financial instruments and means of payment (Article 193[1]); the arbitrary accessing of automated data processing systems (Article 241); interference with the operation of automated data processing systems and illegal actions using the information included in such systems (Article 243); illegal operations with devices influencing automated data processing system resources (Article 244); the acquisition, development, alteration, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment (Article 244[1]).

The law stipulates that attempts to commit such offences are also punishable. Incitement, aiding and abetting are also criminalised under Latvian law. Legal entities, including state or local government capital companies, as well as partnerships, may be criminally liable for offences perpetrated in the performance of their activities, in their interest or on their behalf.

There is no definition of cybercrime in the Criminal Code. The terms cyber-dependent crime and cyber-enabled crime (or crime with an online element) are used.

[8] Due to the large number of pages involved, no description has been included in the report. For more information, see Annex D.

B/ Directive 2011/92/EU on combating sexual abuse and sexual exploitation of children and child pornography

Latvia has fully transposed Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography through amendments provided for in the Criminal Law (Articles 48, 159-162[1], 164-166). This resulted in the criminalisation of the act of encouraging participation in sexual acts (Article 162[1]) and of the violation of provisions regarding the demonstration of a pornographic performance, the restriction of entertainment of an intimate nature and the handling of material of a pornographic nature (Article 166)[9].

Latvia pointed out that it has an advanced legal framework on pornography and thus there are no major qualification issues. For instance, unlike in other countries, in Latvia it was possible to commence a criminal proceeding on the *Shreck* pornography case, which contained a sound recording/talk/animation of a pornographic nature. According to the Law on Pornography Restrictions, 'material of a pornographic nature' is a 'composition, printed matter, image, computer program, film, video or sound recording, television programme, or radio programme, other material in any form or type [...]'.

C/ Online card fraud

The following acts have been criminalised to punish online card fraud:
Illegal activities involving personal data of natural persons (Article 145):
For *illegal activities involving personal data of natural persons* which have caused substantial harm, the applicable punishment is either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine (Article 145(1));

[9] Due to the large number of pages involved, no description has been included in the report. For more information, see Annex D.

For *illegal activities involving personal data of a natural person* performed by a personal-data-processing administrator or operator for the purpose of vengeance, acquisition of property or blackmail, the applicable punishment is either deprivation of liberty for a term of up to four years, temporary deprivation of liberty, community service or a fine (Article 145(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 to perform illegal activities involving personal data of a natural person, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine (Article 145(3)).

Fraud in an automated data processing system (Article 177^1) where a person knowingly enters 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, to influence the operation of the resources thereof (computer fraud) (Article 177^1(1)):

- for *computer fraud committed by a group of persons pursuant to prior agreement*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine, with or without confiscation of property (Article 177^1(2));

- for *computer fraud committed on a large scale or by an organised group*, the applicable punishment is either deprivation of liberty for a term of between two and ten years or a fine, with or without confiscation of property and with or without police supervision for a term of up to three years (Article 177^1(3)).

D/ Other cybercrime phenomena

Article 78(2) (incitement of national, ethnic and racial hatred) of the Criminal Law: for such acts [*acts intended to incite 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 they are committed using an automated data processing system*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine.

Article 88(2) (terrorism) refers to cyberterrorism: for destruction of or damage to physical objects, *automated data processing systems, electronic networks*, and other objects located in the territory or the continental shelf of the state, if such activities are committed for the purpose provided for in Article 88(1), the applicable punishment is either life imprisonment or deprivation of liberty for a term of between eight and twenty years, with or without confiscation of property and with probationary supervision for a term of up to three years.

Article 148 (infringement of copyright and neighbouring rights):

- for the *infringement of copyright or neighbouring rights* which has caused *substantial harm to rights and interests protected by law of a person*, the applicable punishment is either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine (paragraph 1);
- for the criminal offence provided for in Article 148(1), if it has been committed *by a group of persons pursuant to prior agreement*, the applicable punishment is either deprivation of liberty for a term of up to four years, temporary deprivation of liberty, community service or a fine (paragraph 2);
- for the infringement of copyright or neighbouring rights committed *on a large scale or by an organised group, or by compelling, by means of violence, threats or blackmail, joint authorship or the renouncing of authorship,* the applicable punishment is deprivation of liberty for a term of up to six years, with deprivation of the right to engage in specific employment for a term of up to five years, and with or without police supervision for a term of up to three years (paragraph 3).

Article 182 (arbitrary consumption of electricity, thermal energy and gas, arbitrary utilisation of electronic communications services):

- for the arbitrary consumption of electricity, thermal energy or gas services or the *arbitrary utilisation of electronic communications services*, if *substantial material damage* has been caused thereby, the applicable punishment is either temporary deprivation of liberty, community service or a fine;
- for the arbitrary consumption of electricity, thermal energy or gas services or the arbitrary utilisation of electronic communications services committed on a *large scale* or *by a group of persons pursuant to prior agreement,* the applicable punishment is either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine.

Article 245 (violation of safety provisions regarding information systems):

- for the violation of provisions regarding *information storage and processing, which have been formulated in accordance with an information system or the protection thereof, or the violation of other safety provisions regarding computerised information systems, where committed by a person responsible for compliance with these provisions*, if such has been the cause of theft, destruction or damage of the information, or other *substantial harm* has been caused thereby, the applicable punishment is either temporary deprivation of liberty, community service or a fine.

Pursuant to Article 204 of the Latvian Administrative Violations Code, in the case of violation of the prohibition on sending commercial information ('spam') as specified in the law, a warning is to be issued or a fine imposed on natural persons in an amount from EUR 140 to 500, and on legal persons in an amount from EUR 700 to 7100. The competent supervisory authority is the Data State Inspectorate (DSI).

5.2. Procedural issues

5.2.1. Investigative Techniques

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 to 185 further specify the procedure to be followed and other relevant issues. Article 186 states that 'seizure is an investigative measure involving the removal of objects or documents significant to a case, if the performer of the investigative measure knows where the concrete object or document is located or by whom it is held and a search for such object or document is not necessary, or such object or document is located in a publicly accessible place'.

Submission of objects and documents requested by a person directing proceedings

According to Article 190 of the Criminal Procedure Law, a person directing proceedings is entitled, without conducting the seizure provided for in Article 186, 'to request from natural or legal persons, in writing, objects, documents and information regarding facts that are significant to criminal proceedings, including in the form of electronic information and documents which are 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 proceedings during the term specified by such person directing proceedings, the person directing the proceedings shall conduct a seizure or search in accordance with the procedures laid down in [...] [the Criminal Procedure] Law'.

Moreover, 'the heads of legal persons have a duty to perform a documentary audit, inventory, or departmental or service examination within the framework of their competence and on the basis of a request from a person directing proceedings, and to submit documents, within a specific term, together with the relevant annexes 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 proceedings *may charge* [...] *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 which 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 further term of up to thirty days'.

Disclosure and issue of data stored

According to Article 192 of the Criminal Procedure Law, the 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';
- *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';
- *in adjudicating a criminal case* – 'a judge or the court panel may request that a merchant of electronic communications disclose and issue 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'.

Monitoring of means of communication *(a special investigative measure)*

Article 218 of the Criminal Procedure Law states that 'the monitoring of telephones and other means of communication 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 relevant to circumstances to be proven, and if the acquisition of necessary information is not possible without such operation'. The monitoring of telephones and other means of communication with the written consent of a member of a conversation, or the sender or recipient of information, is to be performed if there are grounds to believe that a criminal offence may be directed against such persons or a relative thereof, or if such person is involved or may be enlisted in the committing of a criminal offence.

Investigation of data located in automated data processing systems *(a special investigative measure)*

Article 219 of the Criminal Procedure Law states that 'search of an automated data processing system (or a part thereof), the data accumulated therein, the data environment, and the access thereto, as well as the removal thereof without the notification 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 relevant to circumstances to be proven'.

It further explains that 'a person directing proceedings may request, for the commencement of an investigative measure, 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 investigated unavailable to other users' and that 'a person directing proceedings may prohibit such person to perform other actions with data subject to investigation, and shall notify such person regarding the non-disclosure of investigative secrets'. In a decision on investigation of data present in an automated data processing system, an investigating judge may allow a person directing proceedings to remove or otherwise store the resources of an automated data processing system, as well as to make copies of these resources.

Investigation of the content of transmitted data *(a special investigative measure)*

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 notification 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 relevant to circumstances to be proven'.

5.2.2. Forensics and Encryption

1. State Police

Forensic examination is carried out by the Forensic IT Unit of the Forensics Department of the State Police. Forensics refers to both cybercrime and other criminal offences where electronic evidence is present. The analysis of seized objects is carried out in a laboratory. The Forensic IT Unit carried out 290 forensic examinations in 2014, and 200 in the first ten months of 2015.

Forensic examinations involve the following main tasks: identification and search of network settings; recovery of deleted documents; information search and recovery of deleted information; recovery of deleted graphic files; search, export and recovery of graphic and video files (with regard to pornography, child sexual abuse and other offences); search of banknote images in data devices; search and recovery of deleted e-signatures; search of information regarding emailing services (usage, visits); history exports (regarding internet visits) and recovery of deleted history; confirmation regarding file downloads/uploads; search and recovery of credit card data; analysis of various operating systems (mainly Windows, Linux, Unix and Mac OS); analysis of Microsoft Windows operating system register; file carving/recovery; log file analysis; file and file container password cracking/removal; tasks related to data-hiding and encryption software; spyware detection and log analysis; tasks related to remote-management software and analysis of log files; tasks related to viruses; search (and conversion) of data; 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 the recovery of information from damaged data devices and information retrieval from damaged mobile phones/smartphones and tablets.

As part of the IT inspection (or 'pre-analysis' prior to the forensic examination), the following activities are carried out: export of existing documents; search/selection (through keywords) of relevant documents (doc, xls, pdf and others); export of existing graphic files; export of emails; export and recovery of chat correspondence.

The Economic Crimes Enforcement Department (Unit 4 – Cybercrime Enforcement Unit) of the State Police carries out internet intelligence (known as 'live/network analysis').

Regarding encryption, the Forensic IT Unit of the State Police Forensic Department has the necessary equipment to determine the form of encryption and to access the encrypted information. However, there is limited computation capacity, which prevents the unit from achieving better results (hence, if the password is technically advanced and cannot be retrieved in a reasonable period of time, the encryption process is ceased). In this regard, Latvia sees clear added value in EC3's encryption/decryption platform. In view of the encryption issue, Latvia also highly values the availability of the Europol Platform for Experts. The Forensic IT Unit does not cooperate with private companies. However, experts may inform the person directing the proceedings that it is necessary to involve the private sector to gain the additional information required.

2. ***State Forensic Science Bureau (SFSB)***

SFSB is an institution supervised by the Ministry of Justice which provides forensic investigation services to law enforcement agencies (where requested) as well as to other legal and natural entities. IT/computer forensics is one of the areas in which the SFSB provides its services (for instance, information search, recovery of deleted documents, analysis of documents on hard drives, flash drives, CDs and other electronic data devices).

5.2.3. e-Evidence

Terms such as 'automated data processing system', 'publicly unavailable data', and 'ICT and electronic communications network terminal equipment' are used in the Criminal Law, although no definitions are provided. The Electronic Communications Law contains the following definitions: electronic communications merchant, electronic communications service, electronic communications service provider, electronic communications network, access, terminal equipment, identifiable terminal equipment, end-user, access to data flow, traffic data, location data, location information database, and data to be retained.

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 which has been processed, stored or broadcast with automated data processing devices or systems'. In addition, Article 135(2), which refers to the term '*document*', explains 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 practical arrangements and good practices for electronic evidence, a single contact point has been designated at the State Police, which is in charge of both requesting and receiving the necessary data from electronic communications merchants (meaning that there is established centralised cooperation between the State Police and electronic communications merchants). For this purpose, a specific database has been designed. The single contact point is available 24/7 and receives requests from all State Police departments (there is a designated contact person in each regional State Police entity).

Article 130 of the Criminal Procedure Law on *admissibility of evidence* (which 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 any of the following manners 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 an operation; (3) allowing the violations specifically indicated in[...] [the Criminal Procedure] Law that prohibit the use of a concrete piece of evidence; (4) violating the fundamental principles of criminal proceedings'.

At the same time, the Article states that 'information regarding facts that has been obtained by allowing other procedural violations shall be considered *restrictedly admissible*, and may be used as evidence only in cases where the allowed procedural violations are not essential or may be prevented, or where such violations have not influenced the veracity of the acquired information, or where 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 is obtained according to Chapter 83: 'Request to a Foreign State regarding the Performance of Procedural Actions' of the Criminal Procedure Law).

5.3. Protection of Human Rights/Fundamental Freedoms

Legal requirements

Fundamental rights and freedoms are protected by the **Constitution** of the Republic of Latvia. Article 89 of the Constitution declares that the state must recognise and protect fundamental human rights in accordance with the Constitution and the 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'.

More specific safeguards are envisaged in the **Criminal Procedure Law** (please refer to 5.2.1). 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 that 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 with law of the actions of the officials of the body performing the operational activities, or the person may bring an action in court'.

Data State Inspectorate

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

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'. It further explains 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 […] [the Criminal Procedure] Law according to the character and danger of the criminal offence'. It 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 criminal proceedings has a *duty to protect the confidentiality of the private life of a person* and the commercial confidentiality of a person' and 'information regarding such confidentiality shall be obtained and used only in cases where such information is necessary 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 fiancé(e), 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*'.

Investigative judge

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 [...] *to monitor the observance of human rights in criminal proceedings*'. An investigative judge may carry out the following measures during an investigation and prosecution:

- applying compulsory measures in the cases provided for by law;
- deciding on the application of a suspect or an accused person regarding the amendment or revocation of the security measures that have been applied by decision of the investigating judge;
- examining complaints regarding a security measure applied by the person directing the proceedings;
- deciding on the performance of procedural actions;
- deciding on complaints in relation to an unjustified violation during criminal proceedings of confidentiality that is protected by law;
- deciding on the request of a person who has the right to assistance from a defence counsel to give a discharge of payment regarding the use of the assistance of an advocate.

As long as a case is pending before a court, the investigative judge may decide on:

- the application of an accused person regarding the amendment 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 be acquainted with the materials of a criminal case, with special investigative actions that are not attached to a criminal case (primary documents).

However, the investigative judge is not permitted to replace the person directing the proceedings or the supervising public prosecutor in pre-trial criminal proceedings by giving instructions regarding the direction of an investigation and the performance of investigative measures.

5.4. Jurisdiction

5.4.1. Principles applied to the investigation of cybercrime

According to Article 4 of the Criminal Law (on the 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 in which it is committed'.

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 in which it is committed, the coercive measures provided for in [...] the Criminal Law may be applied to the legal person'.

Foreigners who do not have permanent residence permits for the Republic of Latvia and who have committed, in the territory of another state, serious or especially serious crimes directed against the Republic of Latvia or against the interests of its inhabitants, will be held criminally liable in accordance with [...] [the Criminal] Law, irrespective of the laws of the state in which the crime has been committed, provided that they have not been held criminally liable or summoned 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, shall, irrespective of the laws of the state in which the offence has been committed, be held liable in accordance with [...] [the Criminal] Law, provided that they have not been held criminally liable for such offence or summoned to stand trial in the territory of another state'.

5.4.2. Rules in case of conflicts of jurisdiction and referral to Eurojust

In general, conflicts of jurisdiction are resolved via a consultation process (in accordance with the Council of Europe legal instruments) and the Eurojust coordination meetings. However, the Prosecutor-General's Office has not experienced any such conflicts in the field of cybercrime.

Thus, the provisions related to Council Framework Decision 2009/948/JHA of 30 November 2009 on the prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings in relation to cybercrime case have not yet been used.

5.4.3. Jurisdiction for acts of cybercrime committed in the 'cloud'

No specific problems have been encountered or solutions found with regard to the 'cloud' issue in Latvia. In Latvia's view, this is a global challenge which could – and should – be addressed at the EU level.[10] Similarly to other countries, if the provider of a 'cloud' service is registered in Latvia, investigative measures are carried out in accordance with the relevant national legislation. If the service is registered outside the criminal jurisdiction of the Republic of Latvia, a request for criminal legal assistance is used.

The State Police referred to a good cooperation experience with Microsoft (it had received positive responses to a number of requests).

[10] After the on-site visit the evaluation team was informed that Latvia is currently in process to amend the Criminal Procedure Law foreseeing the deletion of the reference to the territory of Latvia (Article 220 "Control (investigation) of the content of transmitted data" which is a special investigative measure). This would allow to obtain data from "clouds" based outside Latvia. Thus – if the person has the relevant authorisation tools, it should be made possible for the competent authorities to obtain data belonging to that person (hence, there would be no link to the country in which the "cloud" is based.

5.4.4. Latvia's perception of the legal framework for combating cybercrime

With regard to cybercrime and electronic evidence (data storage requests in particular), timing plays a crucial role. In most cases, requests for criminal legal assistance are unfortunately not fulfilled in a timely enough manner (for instance, in one cybercrime case the request sent by the State Police was fulfilled after two years). The general observation is that the 'request for criminal legal assistance' instrument does not correspond to the actual investigation and prosecution needs in the digital age. The implementation procedure of the 'request for criminal legal assistance' instrument should be reviewed to take into account cybercrime.

5.5. Conclusions

- Latvia has ratified the Budapest Convention. Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA have been transposed in the Criminal Law. Therefore, the offences provided for in the Convention and the EU legislation exist in the national legislation.

- Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and the sexual exploitation of children and child pornography has been implemented. Combating credit card fraud is provided for in the Criminal Code.

- The evaluation team was informed that the Security Police and the State Police are both empowered to investigate hate crimes (Articles 78, 149[1] and 150 of the Criminal Law). There is a legal division of competences to be found in the Criminal Procedure Law. If a discussion related to competence arises, the investigating institution is determined by the Prosecutor General (Article 387 of the Criminal Procedure Law). However, in practice the delineation of competences between both police forces remains at times unclear when such crimes are to be investigated. Without clearer guidelines there is a danger that some examples of hate crimes will escape the notice of the relevant authorities.

- The Ministry of Justice, in cooperation with the courts, seems to actively monitor the situation in the fight against cybercrime. The Ministry of Justice showed willingness to actively adopt, where needed, new rules to facilitate the prosecution of cybercrime offences.

- The Ministry of Justice operates two working groups aimed at prosecuting crime, with the participation of academia and the national chamber of advocates. The working groups are currently working on proposals which should facilitate faster prosecution of crimes. However, at the time of on-site visit no specific solution how to facilitate the prosecution and investigation of cybercrimes was presented.

- E-evidence is defined in Article 136 of the Criminal Procedure Law; however, there are no special admissibility rules related to e-evidence. E-evidence is subject to the same rules of evidence as paper documents. The Electronic Communications Law contains several definitions relating to data communication.

- The practitioners met by the evaluation team mentioned that the annulment of the Data Retention Directive had had a negative impact on the ability to secure e-evidence in the EU Member States. It was stressed that this development had had a serious negative impact on the ability of the Latvian investigative authorities to investigate cybercrime and other crime where e-evidence and internet or telecommunications data would greatly contribute to the successful identification of the perpetrators. In the opinion of the Latvian authorities, there would be added value in having a new instrument at the EU level to harmonise data retention periods.

- Encryption is considered to be a challenge. The Forensic IT Unit of the State Police Forensic Department has the necessary equipment to determine the form of encryption and access the encrypted information. However, there is limited computation capacity, which prevents the unit from achieving better results.

- During the on-site visit the evaluation team was informed that, as a general practice, computer hardware containing e-evidence is physically seized. It may be cumbersome for a victim of cybercrime to accept the loss of his or her digital equipment seized for the duration of the investigation. It may be perceived by such persons to be secondary victimisation. If national legislation pertaining to the seizure of digital materials by documented mirror copying were introduced, this could encourage people to cooperate with law enforcement more willingly. Therefore, mirror copying could be a way of securing digital material.[11]

- Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings has been transposed into national law. No conflicts of jurisdiction have been registered so far.

[11] After the on-site visit the evaluation team was informed that Latvian institutions and entities reviewed the legislation and assumed no need for any legal amendments in the Criminal Procedure Law. The identified issue is currently addressed by changing the practice of the competent authorities through returning the object (the computer hardware) to the owner or lawful possessor and making the mirror copy of the digital material.

6. OPERATIONAL ASPECTS

6.1. Cyber-attacks

6.1.1. Nature of cyber-attacks

CERT.LV is in charge of monitoring cyber-attacks in Latvia and publishes month-by-month statistics on both high- and low-priority cyber incidents once a quarter.

In 2015 200-300 high-priority incidents and on average 50 000 low-priority incidents were registered each month. According to CERT.LV's incident classification, such elements as the information source and the 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 processed by hand, whereas low-priority incidents are processed automatically. The incidents are either notified to the State Police or managed according to the CERT.LV internal procedures.

Attacks targeting Latvia's cyberspace are becoming increasingly sophisticated and thoroughly planned. The Latvian financial and public sectors are the usual targets of cyber-attacks. The spectrum of cyber-attacks is very wide, ranging from system intrusions to web page defacement, banking trojans, denial of service attacks and very sophisticated advanced persistent threat (APT) attacks. The resolution of these incidents and attacks is part of CERT.LV's normal duties and is carried out according to its policies and best practices.

CERT.LV values the information-sharing with other EU Member States facilitated by the Computer Security Incident Response Team (CSIRT) cooperation (either bilaterally on a case-by-case basis or by using CSIRT cooperation formats such as TF-CSIRT). At the national level, CERT.LV sets great importance on cooperation with law enforcement and intelligence agencies.

The evaluation team was informed that in November 2015 a memorandum of understanding had been signed between the CERT units of all three Baltic states pledging to step up cooperation on cyber-attacks and the protection of IT systems and networks.

6.1.2. Mechanism to respond to cyber-attacks

General overview on the response mechanism

According to Article 4(5) of the Law on the Security of IT, in case of danger to the state, the Cabinet of Ministers (government) may decide to transfer 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 and reports to the Cabinet of Ministers (government), where the necessary decisions are made.

Cyber Defence Unit

Taking into account the existing security threats and concerns as well as the limited state resources, a reserve unit – the 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 a crisis situation (namely, if the capabilities of the National Armed Forces and CERT.LV appear to be insufficient). The CDU is developed on the basis of the National Guard, which ensures a legal basis and procedures for using highly qualified IT experts from the private sector to fulfil defence tasks in an organised manner. There are currently more than 70 volunteers in the CDU (its full operational capacity is 94 volunteers and four professional soldiers).[12] Currently, within the CDU, IT experts work on improving knowledge, organising and participating in cyber-attack prevention training and, where necessary, providing assistance to both the public and the private sector. The main tasks of the CDU are:

- to recruit IT experts;
- to elaborate a development and work plan for the CDU;
- to ensure initial military and further professional training for the national guards involved;

[12] After the on-site visit the evaluation team was informed that the number of volunteers at the CDU is growing and currently exceeds 80 persons.

- to plan, organise and ensure participation in national and international training courses (for instance, regular participation in cyber defence training in NATO, EU, bilateral and regional formats, including the NATO Cooperative Cyber Defence Centre of Excellence, and organisation of regular training at national level);
- to perform expert examinations in collaboration with military CERT experts from the National Armed Forces and CERT.LV[13], to participate in new security solution testing and evaluation, and to provide proposals for the improvement of cyber defence;
- to prepare and participate in NATO, EU or regional cyber defence units or reserves;
- to promote civil-military collaboration and public-private partnerships in the field of cyber defence;
- to promote understanding and knowledge of cyber threats among IT experts and society; to involve the Young Guard, to promote the education of young people and interest them in getting involved in the field of IT security and defence.

Critical IT infrastructure

For each critical IT infrastructure, the owner or legal manager designates a person responsible for IT security. The designated person cooperates with CERT.LV and the Constitution Protection Bureau to ensure that critical IT infrastructure is protected in accordance with the rules set out by the Cabinet of Ministers. Moreover, the following measures are taken to minimise cyber-attack threats and mitigate their effects: coherent IT security documentation, risk analysis, contingency planning, penetration testing and incident response.

[13] At the beginning of 2016 the Ministry of Defence also established a Military Computer Emergency Readiness Team (MilCERT) which closely cooperates with CERT.LV.

6.2. Actions against child pornography and sexual abuse online

6.2.1. Software databases to identify victims and measures to avoid re-victimisation

Latvia has no national software database specifically designed to identify victims. However, to reinforce its capacity to tackle offences related to child sexual abuse online and child pornography, the State Police actively uses international databases and tools such as:

- **Child Protection System (CPS)** – a database of persons who regularly violate provisions regarding the handling of child pornography material (also within the territory of Latvia);
- **Voyager One** – a comprehensive web platform which enables the State Police to detect networks of criminal organisations, as well as child abusers;
- **ICACCOPS** – a web-based database which allows for the identification of IP addresses which share and upload illegal material (it is possible to see Gnutella, Emule, IRC, Gigatribe, TOR, Bittorrent and Freener net IP addresses);
- **Biometric Data Processing System (BDPS)** – a database consisting of biometric data (facial images, ten pressed fingerprints, ten rolled fingerprints and palm prints) from individuals involved in criminal proceedings – suspects, detainees and convicted persons. BDPS also includes comparative samples (biological material taken from victims and from persons arrested, suspected, accused or convicted, as well as from unidentified bodies and biologically close relatives of missing persons (children, parents) to ascertain the source of the biological traces) which enable the State Police to identify a missing person or an unidentified body.

From 30 June 2016 the State Police also began to use Interpol's International Child Sexual Exploitation (ICSE) database.

According to the Criminal Procedure Law (Article 239(4)), during the course of an inspection of the location of an event, the performer of the operation may remove objects presenting traces of a criminal offence (including hardware). After the final conviction, material evidence (the circulation of which is prohibited by law) must be transferred to the relevant institutions or destroyed according to a decision of the person directing the proceedings. Hardware containing images or videos related to child sexual abuse online and child pornography are always destroyed (if not fully, then partly, by erasing material with illegal content).

To fully implement 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), amendments to the Criminal Procedure Law have been submitted for adoption by the Parliament. A new chapter on victims in need of special protection is to be introduced, and new measures implemented. These include, for instance, 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 victims are 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 are 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). In addition, measures are to be implemented to ensure that victims may be heard in a courtroom without being present, in particular through the use of appropriate communication technology.

6.2.2. Measures to address sexual exploitation and abuse online, sexting and cyber-bullying

As regards sex exploitation and abuse online and sexting, Article 162 of the Criminal Law criminalises acts by which a person, using information or communication technologies or another means of communication, encourages another person under sixteen years of age to take part in sexual acts or encourages such person to meet with the aim of committing sexual acts or entering into a sexual relationship.

With regard to cyber-bullying, there is no legal definition in place; cyber-bullying as such may range from criminal to non-criminal behaviour (depending on the consequences) and therefore every case has been treated individually. There are several articles in the Criminal Law that may apply in cases of cyber-bullying, such as Article 150, 'Incitement of religious hatred', Article 157, 'Defamation' and Article 145, 'Illegal activities involving personal data of natural persons'.

6.2.3. Preventive measures against sex tourism, child pornographic performance and others

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

The Criminal Law does not provide a legal definition of child sex tourism or the advertising thereof. However, in practice, if a person organises or advertises such travel, he or she can be considered to be a perpetrator of the relevant criminal offence in the Criminal Law (for instance, Article 162).

In the context of practical measures, on 17 and 18 September 2014 the State Police (six officers), customs authority (four officers) and State Border Guard (eight officers) participated in the international 'HAVEN' operation (Halting Europeans Abusing Victims in Every Nation). The goal of the operation was to support the EU Member States in detecting and intercepting child sex offenders travelling to abuse children.

The following special preventive measures have been put in place to prevent sex tourism and child pornographic performance:

Hotlines (helplines) and specific information on how to register a complaint

Cybercrime can be reported by calling 112 or 110, or by filling in an online registration form. To simplify the procedure, which can be used to report any type of criminal offence, including cybercrime, all the necessary information is displayed on 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 a helpline or, for cyber-attacks, CERT. LV.

Information tools for children (and parents) on safe use of the internet and harmful or illegal behaviour online

1. State Police measures

Overall, the State Police organised 61 prevention initiatives related to internet safety in 2014 and 312 in 2015. These included:

- providing information on the **'ten most significant internet communication provisions'** on the website of the State Police, to protect individuals, including children, from potential abusers on the internet;
- organising **training** on internet safety for **inspectors working on juvenile cases,** in close cooperation with the *Net-Safe Latvia* Safer Internet Centre;

- developing **games for children** ('*Sivēns lielpilsētā*', '*Sivēna ziemas diena*') linked to child safety on the internet and social networks (profile creation, photo galleries, how to react to messages from unknown senders and negative comments);
- organising **seminars for children**; the State Police produces material on cyber safety for children of different ages, emphasising the dangers that they may encounter. The main goal is to make children understand the risks related to seemingly commonplace activities on the internet; the material includes basic advice on how to protect themselves from cybercrime. The State Police has also developed a brochure for children and adults in Braille;
- publishing **brochures for parents** on how to better protect their children from sexual harassment online;
- in 2015, three important **press releases** were prepared in response to sexual offences committed in cyberspace.

2. *Net-Safe Latvia* Safer Internet Centre measures

The *Net-Safe Latvia* Safer Internet Centre (the Centre) is the national contact point for the EU *Safer Internet* Programme's Insafe network. The project is co-financed by the European Commission (50 %). It was scheduled for 18 months (from 1 January 2015 until 30 June 2016).[14] The coordinating institution of the Centre is the Latvian Internet Association, in cooperation with the State Inspectorate for the Protection of Children's Rights (the Inspectorate) and the Municipal Governments Training Centre of Latvia. The Centre's work is focused on the following three areas:

- **informing and educating** (target groups: children, adolescents, teachers and parents; content: safety of internet content and potential threats (incitement to hatred, racism, child pornography and paedophilia, emotional harassment on the internet, identity theft and data abuse));

[14] After the on-site visit the evaluation team was informed that on 7.10.2016 an agreement on the continuation of the project was signed. The new project "SIC Latvia "Net-safe II"" (supported in the framework of the European Commission's Connecting Europe Facility) will last from 01/07/2016 until 31/08/2018.

- **operating hotline and ensuring for the society to report on illegal online content and breaches** (reporting is anonymous; reports are processed and, if necessary, sent to the State Police for further examination);
- **operating the Inspectorate's 116111 helpline** (to give everyone, but especially children and young people, somewhere to turn for help on any internet-related issue).

- During the three years' period (2014 – 2016) the hotline has received 1 968 electronically submitted reports on illegal online content and breaches.[15]

In 2015, the helpline received calls from more than 670 children and young people on internet-related issues (including cyber-bullying, online pornography and the sexual exploitation of children), twice as many as in 2014. Various educational initiatives have also been launched:

- to educate children and young people on internet safety, the Inspectorate, in cooperation with the Centre, has created videos reflecting three situations which children and young people may experience or may already have experienced in real life, and has also created a book on internet safety for 5-7 year olds;
- for parents, instructions on safe internet use have been created;
- for individuals working with children (teachers, social workers), free training has been provided.

15 Additionally the evaluation was informed that in 2016, 53 reports that contained child sexual exploitation were hosted on servers in Latvia; these reports were forwarded to the State Police for investigation. 134 reports containing child sexual abuse materials that were not hosted in Latvia were submitted to the INHOPE association data base (for the relevant countries to delete this material from public access). In 2016, due to good cooperation between the Centre, the State Police and the Latvian ISPs, all child sexual abuse materials that were hosted in Latvia and reported to the Latvian hotline were deleted from public access.

Other relevant measures

To prevent child pornography and sexual exploitation on the internet, the State Police has created a video file ('police to peer project') that will automatically appear when image or video files containing child pornography and sexual exploitation are downloaded. In the video file a police officer informs the abuser that the police have detected his or her IP address and that the process of identification has been launched, and provides information on criminal charges.

6.2.4. Actors and measures countering websites containing or disseminating child pornography

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

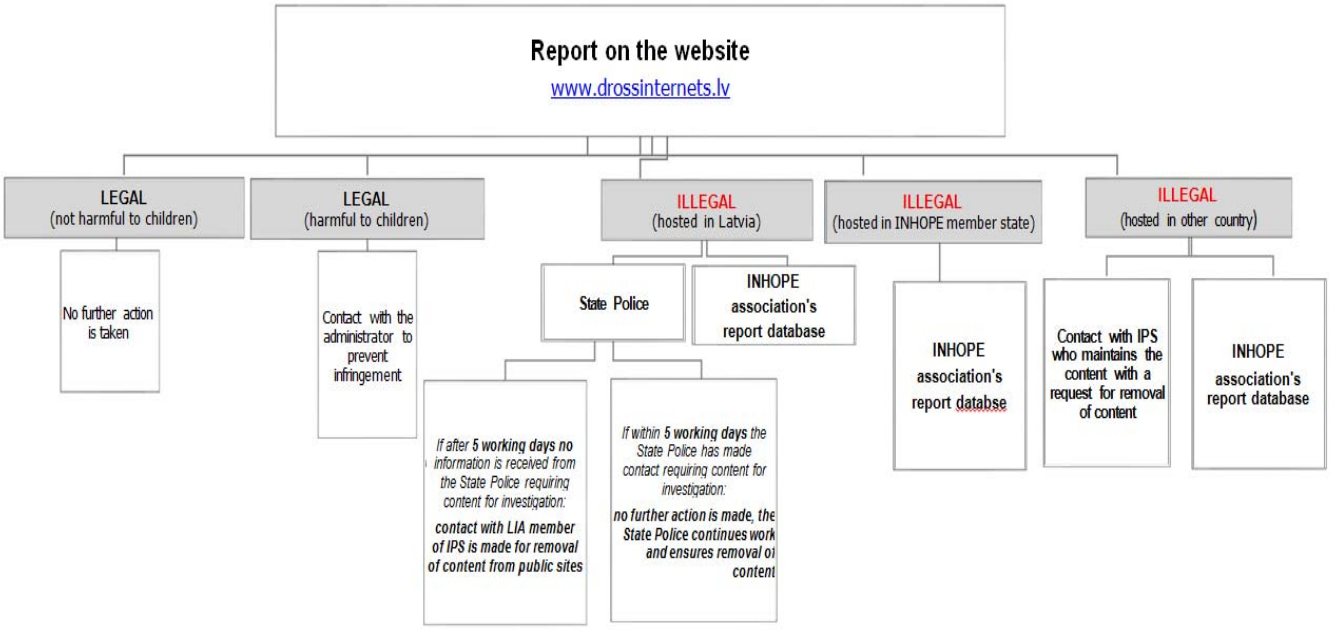
There are no technical tools to filter websites for child pornographic material. However, the State Police cooperates with the Centre in this regard. The official, who is authorised to perform criminal proceedings, can also authorise the removal of web page content.[16]

Electronic communications service providers have no legal obligation ex officio to block access, remove content or take down web pages. However, some providers (for instance, the national social media platform www.draugiem.lv) cooperate with law enforcement agencies on a voluntary basis (by reporting illegal content they identify and blocking or removing it).

16 After the on-site visit the evaluation team was informed that the State Police has created technical tools to filter websites for child pornographic materials. Those tools are currently being tested.

Moreover, the Centre, as a member of INHOPE, processes the reports received and, if necessary, sends them to the State Police for further examination.

Please see the diagram below for information on the cooperation between the Centre and the State Police:



The Criminal Procedure Law stands for the principle of equality, supporting a uniform procedural order for all persons involved in criminal proceedings. Therefore, no separate procedure has been introduced for urgent cases. However, the 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 must take priority.

Cases in which the server is located outside the territory of Latvia are solved according to the Convention on Cybercrime and by using the Interpol and Europol information channels.

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

6.3. Online card fraud

6.3.1. Online reporting

There is an obligation in place to report all card fraud offences to the State Police. Reports are mostly submitted via a universal phone number or by email to kanc@vp.gov.lv. However, in practice commercial banks often do not report offences to the law enforcement agencies, due to the risk of losing their credibility.

6.3.2. Role of the private sector

The Latvian authorities perceive the cooperation with the private sector to be effective. As an example, the State Police (Cybercrime Enforcement Unit of the Economic Crimes Enforcement Department) holds a regular dialogue with the Association of Latvian Commercial Banks (which brings together, on a voluntary basis, banks registered in Latvia and branches of foreign banks) and actively participates in a tripartite cooperation platform together with banks' security units and CERT.LV.

In practice, commercial banks in Latvia change ATM components periodically to limit the possibility of skimming. This procedure has also been put in place at automatic service (petrol) stations. Moreover, several commercial banks have taken additional steps to ensure the safety of online payments. In addition, to warn and protect potential victims, the police and commercial banks regularly provide information to the public about the risks of cyber-criminality and how to protect personal data.

6.4. Conclusions

- A response mechanism is in place to fight cyber-attacks. In the event of danger to the state, the Cabinet of Ministers (government) may decide to transfer the tasks, rights and resources of CERT.LV to the National Armed Forces. In less severe cases, CERT.LV reports to the Ministry of Defence, which further consults the National IT Security Council and reports to the Cabinet of Ministers (government), where the necessary decisions are made. Specific legislation for critical IT infrastructure is in place in Latvia. Incident response exercises are organised by CERT.LV, addressed to IT experts not only at the technical level but also at management level.

- CERT.LV plays an important role in the cybersecurity structure, acting as an intermediary between the private sector, academia and the police. It is a well-staffed, skilled and willing partner to public institutions and society at large. It is very active in the public debate on cybersecurity. It also deals with the bulk of security incidents and has agreements with all major electronic communications providers to inform victims swiftly and efficiently (backed up by the CERT.LV call centre).

- The obligation for key players such as state institutions, national critical infrastructure and internet service providers to report significant cybersecurity incidents, based on the Law on IT Security, is reinforced by agreements with CERT.LV on more extensive voluntary reporting and voluntary cooperation by other sectors, such as the banking sector. Latvia is thus able to neutralise to a great extent underreporting due to fears of reputational damage, and to provide fairly comprehensive statistics on the number of cybersecurity incidents.

- Worth mentioning too is Latvia's close cooperation with neighbouring countries. In November 2015, a memorandum of understanding was 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.

- Special mention should be made of the Cyber Defence Unit, a newly organised volunteer body which provides support to the National Armed Forces in responding to IT security incidents and mitigating the consequences thereof. It cooperates closely with the Ministry of Defence and with CERT.LV. It provides a very innovative approach in terms of the exchange of expertise between the private and public sectors, since volunteers from the private sector bring with them knowledge and experience, and interact and exchange this experience with their counterparts in the public sector. Since participation is voluntary, the costs and resource investment return are very positive for the public institutions. The volunteers, with their new training capacity, contribute to making cyberspace safe in Latvia and also provide a pool of resources to draw upon when needed with minimal investment from public bodies.

- The non-governmental organisations that the evaluation team met during the on-site visit, such as the Digital Security Alliance and Net-Safe, also play an important role in cybercrime prevention. These organisations are very active in the field of cybercrime prevention and actively cooperate with affected industrial sectors and vulnerable groups. The role of Net-Safe in particular in preventing cybercrime and providing support in cases of child sexual abuse online and pornography should be highlighted as an example of best practice.

- Some issues were raised, especially by associations of private organisations, including banks, regarding the handling of incidents of phishing and/or minor cybercrimes. The fact that a criminal investigation cannot be launched unless it is possible to clearly identify sufficient damage, even when it is clear that illegal activity is taking place, was repeatedly flagged as a problem. This stops many from reporting attempts at cybercrime, like phishing, which – unless successful – do not end up causing damage to their victims. Even if losses can be identified, they are not considered sufficient for the alleged crime to be reported to the competent authorities. This hinders early detection of these forms of cybercrime and allows them to continue until there actually is a victim who suffers serious damage.

- Perceptions of the success of the cooperation between the private and the public sector seem to differ from one to the other. Whereas the public institutions perceive the existing cooperation as excellent and sufficient, the associations paint a less positive picture. Although still very welcoming of the existing venues and channels for cooperation, the private entities would clearly welcome additional steps to make the prosecution of cybercrime easier and less expensive for the victims. There seems to be scope to strengthen cooperation between the private and the public sector, e.g. with the financial sector at the national level.

- Moreover, it seems that private entities often do not share information about cyber-attacks either with the State Police or among themselves. This again impairs the successful prevention, identification, investigation and prosecution of cybercrime. Therefore, in the opinion of the evaluators Latvia should consider introducing a legal obligation to report cyber-attacks for the most affected and vulnerable sectors, such as the banking sector, internet service providers and services processing large amounts of personal data, even if they are not part of the critical infrastructure.

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

7.1.1. Formal requirements to cooperate with Europol/EC3, Eurojust, ENISA

There are no formal cooperation requirements between the Latvian authorities and Europol/EC3, Eurojust and ENISA in relation to cybercrime cases.

7.1.2. Assessment of the cooperation with Europol/EC3, Eurojust, ENISA

EUROPOL/EC3

The number of cases where Latvia would require assistance from Europol/EC3 is limited. However, the number of cases is increasing. In 2015, the State Police received and processed 54 requests (sent by Europol/EC3). Moreover, Latvia has expressed its willingness to continue providing the required assistance to other EU Member States and the relevant third countries.

- Latvia greatly values the implementation of the EU policy cycle on organised and serious international crime and OAPs in the cybercrime priority. Latvia participates in all the sub-priorities.
- It also sees clear added value in the focal points (Terminal, Cyborg and others), the J-CAT and the Europol Platform for Experts (which is a valuable source/tool for gaining additional knowledge and information on the latest cybercrime trends).

In addition, one State Police expert is delegated to participate in the EC3 platform aimed at analysing malware (the European Malware Analysis Solution, which 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 investigatory capacity.

Latvia has good experiences cooperating with Europol and Interpol in certain targeted cases, for instance through an operative meeting held at Europol on a criminal group formed in Latvia which was setting up ATM skimmers in the Baltics, the UK, Poland and Russia. As a result, several members of this criminal group were detained in Sweden and Russia.

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

Furthermore, in 2014 the State Police took part in the international 'HAVEN' operation (Halting Europeans Abusing Victims in Every Nation), the goal of which is to support the EU Member States in detecting and intercepting child sex offenders travelling to abuse children.

Eurojust

The Prosecutor-General's Office in particular values the assistance provided by Eurojust (especially regarding more timely fulfilment of legal assistance requests in complicated cases). The Latvian authorities highlighted the added value of coordination meetings as a tool contributing to more effective investigation and evidence gathering. In 2014 and 2015, the Prosecutor-General's Office did not submit any requests to Eurojust for assistance in cybercrime cases.

The State Police participated in Eurojust's tactical meeting on territorial jurisdiction of cybercrime and evidence-related issues. This experience is regarded as being professionally valuable.

ENISA

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

7.1.3. Operational performance of JITs and cyber patrols

Latvia has not yet participated in any JITs concerning cybercrime. However, the Latvian authorities believe that tools such as JITs and cyber patrols are valuable cooperation instruments and that increased use should be made of them.

7.2. Cooperation between the Latvian authorities and Interpol

The involvement of the Latvian authorities in cooperation with Interpol in cyber cases is less regular than with Europol/EC3. The State Police receives Interpol Cyber Fusion Centre activity reports, which undoubtedly contribute to its overall work. At the time of the on-site visit there were plans to provide access to the ICSE database until 30 June 2016 (with two connection points planned and training scheduled for six officials).

7.3. Cooperation with third states

When addressing requests for legal assistance to Latvia, third countries often use Europol as a channel. Latvia values the coordinating role of Europol in this regard. The Budapest Convention, the European Convention on Mutual Assistance in Criminal Matters and bilateral agreements provide the legal basis.

Cooperation with the USA is based on the Agreement on MLA between the Government of the Republic of Latvia and the United States of America. It was applied to the extradition of a Latvian citizen accused of cybercrime.

7.4. Cooperation with the private sector

When local branches (of companies of which the main headquarters are located in a third country) are officially registered in Latvia (in the Enterprise Register or the Commercial Register), information exchange and/or procedural activities (including coercive measures) are carried out according to national legislation.

Before pre-trial investigations, Europol, Interpol and the police cooperation information communication channels are used. During pre-trial investigations, the relevant MLA instruments and possibilities provided by Europol and Eurojust, including JITs, are explored.

7.5. Tools of international cooperation

7.5.1. Mutual Legal Assistance

There is no specific legal basis in Latvia for the provision of MLA for cybercrime. The rules set out in the Criminal Procedure Law (Part C, International cooperation in the criminal-legal field) and bilateral agreements apply in this area. According to the Criminal Procedure Law (Article 846 on the competent authorities in the examination of a request from a foreign state):

- *in pre-trial proceedings*: the Prosecutor-General's Office examines and decides on requests from foreign states; up to the commencement of criminal prosecution, this may also be carried out by the State Police;
- *after a case has been transferred to a court*: the Ministry of Justice examines and decides on requests from foreign states.

I. Statistics on the number of requests received

Prosecutor-General'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 bases for the 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 between the Government of the Republic of Latvia and the United States of America on mutual legal assistance (20);

— Agreement between the Republic of Latvia and the Republic of Belarus on mutual legal assistance and legal relations in civil, family and criminal matters (3);

— Agreement between the Republic of Latvia and the Republic of Moldova on mutual legal assistance and legal relations in civil, family and criminal matters (1);

— Agreement between the Republic of Latvia and the Russian Federation on mutual legal assistance and legal relations in civil, family and criminal matters (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 bases for the 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 between the Government of the Republic of Latvia and the United States of America on mutual legal assistance (19);

— Agreement between the Republic of Latvia and the Republic of Belarus on mutual legal assistance and legal relations in civil, family and criminal matters (3);

— Agreement between the Republic of Latvia, the Republic of Estonia and the Republic of Lithuania on mutual legal assistance (Lithuania – 58, Estonia – 6);

— Agreement between the Republic of Latvia and the Republic of Poland on mutual legal assistance and legal relations in civil, family, labour and criminal matters (97);

— Agreement between the Republic of Latvia and the Russian Federation on mutual legal assistance and legal relations in civil, family and criminal matters (10);

— Agreement between the Republic of Latvia and the Republic of Uzbekistan on mutual legal assistance and legal relations in civil, family, labour and criminal matters (1).

II. Statistics on the number of requests sent

Prosecutor-General's Office:

Criminal Law					
Year	**Article 243**	**Article 162**	**Article 166**	**Article 177[1]**	**Article 193[1]**
2014	1	0	0	1	0
2015	0	1	2	4	7

Legal bases for the cooperation:

— Agreement between the Government of the Republic of Latvia and the United States of America on mutual legal assistance (5);

— Agreement between the Republic of Latvia and the Russian Federation on mutual legal assistance and legal relations in civil, family and criminal matters (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**	**Article 166**	**Article 177[1]**	**Article 193[1]**	**Article 241**	**Article 243**	**Article 244**	**Article 244[1]**
2014	5	1	1	13	0	1	0	0
2015	4	2	4	33	1	0	1	3

Legal bases for the 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 between the Government of the Republic of Latvia and the United States of America on mutual legal assistance (12);

— Agreement between the Republic of Latvia, the Republic of Estonia and the Republic of Lithuania on mutual legal assistance (Lithuania – 5, Estonia – 1);

— Agreement between the Republic of Latvia and the Russian Federation on mutual legal assistance and legal relations in civil, family and criminal matters (7);

— Agreement between the Republic of Latvia and Ukraine on mutual legal assistance and legal relations in civil, family, labour and criminal matters (1).

At the trial stage, no legal assistance has been requested or received regarding cybercrime. There are no specific procedures or conditions that need to be fulfilled to send an MLA request. The average response time is two months; however, urgent requests are processed as soon as possible (this does not apply to the trial stage, since no legal assistance has been requested).

Since MLA with respect to cybercrime is not distinguished from other criminal offences, Latvia ensures cooperation according to the Criminal Procedure Law. The following action 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; and other action provided for in international treaties. The most common reasons for MLA requests are information requests from electronic communications merchants and credit institutions to help them better prepare for interrogation.

Requests for criminal-legal assistance relating to cybercrime are used. However, according to the Latvian authorities the process is lengthy and rather cumbersome. Latvia expressed the opinion that MLA instruments as such are not designed to meet the needs of the digital age.

7.5.2. Mutual recognition instruments

In the last two years, the Prosecutor-General's Office has executed orders freezing property or evidence three times. Other EU mutual recognition instruments have not been used.

7.5.3. Surrender/Extradition

The extradition procedure in Latvia is governed by Chapter 65 on extradition of a person to Latvia and Chapter 66 on extradition of a person to a foreign state of the Criminal Procedure Law. Hence, all cybercrime acts covered by the Criminal Law fall within 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).

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

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

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	Criminal Law Article 166	Criminal Law Article 193[1]
2014	5	0	1
2015	1	1	2

On 2 December 2012, the United States of America, in accordance with the Agreement between the Government of the Republic of Latvia and the United States of America on mutual legal assistance, submitted a request to the Prosecutor-General's Office for the extradition of a Latvian citizen accused of cybercrime. On 23 August 2012, the US District Court Southern District of New York accussed a Latvian citizen of 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 between the Government of the Republic of Latvia and the United States of America on MLA, submitted an extradition request to the Prosecutor-General's Office. On 6 December 2012, the City of Riga Central District Court issued an extradition arrest. On 20 December 2012, the Prosecutor-General's Office decided that the grounds for the extradition were admissible; on 31 January 2013, its decision was endorsed by the Supreme Court of the Republic of Latvia. 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 (the Convention) and to obtain information on human rights guarantees in the US, to avoid any possibilities of human rights violations. On 4 July 2013, the US Embassy in Latvia replied that, in the event of the extradition of a Latvian citizen to the US, universal human rights would be granted (including, for instance, the right to legal aid and a defence attorney). On 31 May 2013, the Constitutional Court of the Republic of Latvia ruled that there were 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 and was sentenced to imprisonment equal to the time already spent in custody.

7.6. Conclusions

- Europol and Eurojust are known to practitioners who participate in the investigation and prosecution of cybercrime. The cooperation with these EU agencies is considered satisfactory by all the relevant state bodies. As criminal investigations in the area of cybercrime are mainly carried out by the State Police, it is the State Police that utilises the possibilities for cooperation these EU bodies offer.

- The State Police expressed its appreciation for the topical meetings organised by Eurojust, which allow for an exchange of experiences relating to investigative methods and judicial cooperation instruments with practitioners from the EU Member States. The cooperation with Europol/EC3 has been extensively and successfully utilised by the State Police in investigations of cybercrime and is considered as very useful. However, the practitioners met mentioned that they would greatly appreciate it if a forum were to be set up where experience could be exchanged on the subject of cybercrime prosecution on a more regular basis between the competent authorities of the EU Member States.

- The practitioners met mentioned the need to establish at EU level an effective way of communicating and executing MLA requests from the EU Member States to major internet service providers located outside of the EU. A framework for transmitting such requests directly to the relevant non-EU ISPs under a harmonised set of conditions would significantly enhance cooperation. It would also be appreciated if the EU agencies could provide information on the possibilities for cooperation with third countries and the associated requirements and experiences.

- Latvian practitioners make use of all the available channels to provide legal assistance: bilateral relations, liaison officers, liaison magistrates and EU agencies. It was stressed that the cooperation possible under the existing legal assistance instruments is often too slow to address those forms of cybercrime which are especially sensitive to fast securing of e-evidence. Without swift action – within a day or two of the crime being committed – it often may not be possible to secure enough evidence for successful investigation and prosecution. The slow execution of the currently available instruments of judicial cooperation was identified as one of the main hurdles to successful prosecution. Therefore, in the opinion of the evaluators, the EU should consider how it could help speed up the legal and judicial cooperation procedures between EU Member States and third countries.

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

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 special attention paid to subjects on and improvements to the quality of court judgments as well as to quality work within the legal system of the EU.

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 attended the 'Cybercrime I' and 'Cybercrime II' training courses (90 minutes each) and two judges participated in a two-day seminar entitled 'Planning and justifying the search and seizure of electronic evidence: practical implications for legal practitioners in criminal proceedings before presenting evidence in court' (organised by the Academy of European Law in Riga).

The Judicial Qualification Board evaluates the professional work of a judge once every five years (following the approval of the judge for the office with an unlimited term). As part of the evaluation process the Judicial Qualification Board is also obliged to analyse judges' participation in measures aimed at improving their qualifications. Some training courses are also available online.

Law enforcement

Training of law enforcement staff is provided by the State Police College, an educational institution under the authority of the State Police. It provides professional training and continuing training to the State Police staff. As regards continuing training in 2015:

- 133 officials/police officers participated in the informal education programme 'Using the newest IT in police work' (eight academic hours), which continues to run in 2016;
- 65 officials/police officers took part in the programme 'Electronic communication methods on the internet: types, usage and ways of controlling them' (eight academic hours);
- 42 officials/police officers participated in the programme 'Using electronic communication merchants' data in investigating criminal offences' (eight academic hours).

In addition, a professional development programme on 'IT usage in the fight against crime' has been put in place, covering the following specialisations:

- IT specialist (120 academic hours);
- information processing and analysis specialist (120 academic hours);
- IT specialist in the 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) cooperates with various Latvian IT companies and software producers on a daily basis.

State Police officials (IT-forensic examiners and cybercrime investigators) participate in continuous training provided by the State Police College as well as in training courses provided by CEPOL, Europol and other entities.

CEPOL

State Police officials frequently participate in CEPOL training.

In 2014, seven State Police officials participated in training courses on cybercrime and nine officials followed the courses online. In 2015, seven State Police officials participated in training courses on cybercrime and three officials followed the courses online.

In March 2015 the Latvian Presidency of the Council of the EU, in cooperation with CEPOL, organised a conference entitled 'Cybercrime – Strategic', which focused on improving cooperation methods 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 the EU and Eastern Partnership countries to tackle cybercrime; and identifying current challenges to improve partnerships with the private sector.

ECTEG

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

Europol/EC3

State Police officials regularly participate in training activities provided by Europol/EC3. For instance, in 2015, State Police officials participated in training activities and expert meetings including '16th Europol training course on combating online sexual exploitation of children', 'Europol annual expert seminar on child sexual exploitation' and 'Fighting Internet Paedophilia Project (FIIP)'.

Academia

Academia provides valuable input, such as, for instance, a comprehensive cybercrime investigation manual and significant academic analysis by the Constitutional Court. At the time of the on-site visit, the State Police College had not established cooperation with university academics (for instance, from the University of Latvia or Riga Technical University); however, this possibility is currently being explored.

Other training

State Police officials have also participated in training provided by the Marshall Centre. In 2014, one official participated in the 'Programme on cybersecurity studies' training course. In 2015, one official took part in a seminar on cybersecurity entitled 'Cyber alumni community of interest (workshop challenges: practitioner action)' and two officials participated in the 'Programme on cybersecurity studies' training course.

Financing

Training costs are covered by several State Police budgetary lines. It is therefore not possible to estimate the total annual costs of regular training modules/programmes provided by the State Police College or other entities (such as CEPOL).

8.2. Awareness-raising

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

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

As part of the *Digital Europe* priority the Latvian Presidency organised 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), which focused on the development of the Digital Single Market and issues such as trust, ensuring access and connectivity, building the digital economy for businesses and consumers, and promoting e-society and digital skills;

— *EU-28 Cloud Security Conference* (in cooperation with ENISA; June 2015), which focused on topics such as legal and compliance issues, technical advancements, privacy and personal data protection, critical information infrastructure and cloud certification;

— *conference on information and communication technologies (ICT) for information accessibility in learning* (May 2015), which focused on how the use of ICT in the learning process makes information more accessible, including for people with special needs;

— *seminar on the cybersecurity framework* (May 2015), at which the national strategies of different EU Member States were assessed and best practices shared (for instance, regarding responsible incident detection policy);

— *'e-Skills for jobs 2015' conference* (March 2015), at which the acquisition of digital skills and the creation of new jobs to promote European economic growth were highlighted (and the Riga Declaration was also adopted).

CERT.LV and the State Police

CERT.LV raises awareness not only of cybercrime but also on broader topics such as security and privacy and on a number of specific issues (passwords, authentication, others) and particular threats (phishing, malware, email attachments, identity theft). In 2014, CERT.LV was involved in organising 95 events with almost 6 000 participants, and in 2015, 104 events with 6 680 participants. A broad range of participants have taken part in these events (from schoolchildren to IT security professionals and managers).

The State Police has an active Facebook page with more than 10 300 subscribers and a Twitter account with 43 100 followers. Information related to cybercrime is regularly disseminated through these social media platforms.

NGOs contributing to awareness-raising

'Latvian Information and Communication Technology Association' (LIKTA)

LIKTA was founded in 1998 and brings together leading industry companies and organisations, as well as ICT professionals. LIKTA's goal is to foster growth in the Latvian ICT sector by promoting the development of an information society and of ICT education, thus increasing Latvia's competitiveness on a global scale.

There are also 11 working groups established within LIKTA, including an education/professional education development working group, a data protection and copyright working group and a working group on safety and legal issues in the digital environment. In addition, LIKTA presents an annual award to the best e-teacher. In assessing the candidates, the following elements are evaluated: development of e-skills and enhancement of the information society (as such); inclusiveness (regional aspect and the social groups involved); 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 had also previously been included in the list of the top 500 most innovative IT teachers (Microsoft 'Partners in Learning' programme).

'Latvian Internet Association' (LIA)

Founded in 2000, it focuses on promoting internet accessibility in Latvia, and strengthening, developing and popularising its use. LIA is the coordinating body of *Net-Safe Latvia* Safer Internet Centre with the main focus on educating children on safe and responsible use of the internet and operating the hotline to ensure possibility for the society to electronically report illegal online content and breaches.

'Digital Safety Alliance' (DDA)

Launched on 9 February 2016 (during the Safer Internet Day), DDA aims to raise awareness about internet safety (in user-friendly language), focusing in particular on children and young people (social media), and the safety of e-banking and e-commerce.

Events

Cybersecurity month (each October)

During cybersecurity month, a number of activities are organised. For instance, in 2015 a conference entitled 'Cyber chess. Strategy and tactics in a virtual environment' was organised (by CERT.LV in cooperation with a number of partners). It focused on matters such as secure, stable and resilient identifier systems and cyberterrorism, and included various workshops.

Moreover, every year since 2012 CERT.LV has run the *Datorologs* scheme, which gives everyone the possibility to have their PC, tablet or smartphone checked by IT specialists free of charge, to 'cure' them from viruses and receive consultations on internet safety.

E-skills week (since 2012)

Latvia actively participates in the e-skills week; in 2016, the campaign focussed on topics such as digital skills for employment and employability, and ICT security and data protection. In 2016 the e-skills week took place from 7 to 11 March; the national coordinators are LIKTA and the Ministry of Environmental Protection and Regional Development. The following main activities were organised: activities for schoolchildren and young people; teacher training; digital day for entrepreneurs; and regional seminars across Latvia.

Safer Internet Day

Each year on Safer Internet Day a number of awareness campaigns and events are organised in Latvia. For instance, a special seminar for school teachers was organised on 9 February 2016 covering, among other topics, challenges with the 'millennium generation' and relevant teaching methods.

5. The Ministry of Education and Science

The Ministry of Education and Science pays particular attention to the integration of ICT knowledge in education. For instance, a pilot project on e-skills (the '*Datorika*' programme) has been implemented in 157 schools; in 2018/2019, a standard on digital skills (based on the results of the pilot project) will be implemented in primary schools; digital teaching materials and resources are being developed; a new curriculum is being drafted in line with the latest ICT development tendencies, and will contain requirements on digital and media skills (including e-safety); students are being encouraged to choose careers in ICT; and teachers' e-skills are being enhanced.

The Ministry of Education and Science and its dependent institutions have developed very good cooperation with the private sector, for instance with LIKTA. In February 2016, the National Centre for Education concluded a memorandum on cooperation aimed at improving the integration of ICT knowledge in education and linking it more effectively to the labour market.

8.3. Prevention

8.3.1 National legislation/policy and other measures

The State Police is developing a website www.sargi-sevi.lv ('protect/guard yourself' in English), which will be an information platform on security and prevention issues, including cybercrime. Children and young people will be one of the target groups; for each age group the main security threats and concerns will be listed and explained. This goal should be achieved by involving children and young people in preventive activities as trainers for their peers (peer-level training). In the view of the evaluators this could be a good way to maximise the efficiency of preventive measures with limited resources.

Latvia greatly values the ongoing regional cooperation between the Baltic states (with Estonia and Lithuania). For instance, experience in the area of prevention is actively shared between the competent police authorities.

8.3.2 Public Private Partnership (PPP)

According to Article 1 of the Law On Public–Private Partnership (PPP), PPP cooperation between the public and private sectors is characterised by the simultaneous presence of the following features:

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

Latvia does not use PPP in preventing and combating cybercrime as defined in the Law on PPP (where a specific understanding on the PPP concept is envisaged). However, the State Police has signed a cooperation agreement with CERT.LV and a cooperation agreement with the Latvian Internet Association (on illegal internet content). The agreements set out, for instance, terms regarding information exchange, knowledge exchange/training and specific issues such as blocking access of end users and removing illegal internet content.

8.4. Conclusions

- The Judicial Training Centre, an NGO with which the government has concluded a long-term agreement to provide training for the judiciary, offers a short non-compulsory training course on cybercrime for judges. It provides continuing training for judges and court employees. It seems to be able to organise and provide training where necessary for interested judges. Some training courses are also open to other legal professions, such as public prosecutors. The Prosecutions Office considered the existing training possibilities to be sufficient and did not see the need for any joint training with either judges or police officers in the cybercrime area. However, the evaluators observed that no sufficient practical training is provided to judges and prosecutors.

- On the other hand, the State Police College offers a comprehensive cybercrime training programme covering various modules to State Police staff. It seems to be very extensive and varied, covering a whole range of topics ranging from cyber investigative methods to the best way to capture e-evidence. This shows that a substantial amount of knowledge is passed on to active police officers, in addition to the more extensive training offered to specialised officers dealing with cybercrime.

- The State Police especially expressed appreciation for the topical meetings and training provided by both Europol and Eurojust in the area of cybercrime investigation and prosecution. Moreover, the practitioners met highlighted the importance of knowledge-sharing at the EU level. This was considered as especially vital when it comes to cybercrime, which is an area in which experiences and solutions evolve very quickly.

- Though many training initiatives are in place for the State Police and some are addressed to the judiciary, training is given separately to judges, prosecutors and the State Police. Providing joint training between all the authorities involved in investigating, prosecuting and handling cybercrime cases could greatly facilitate the efficiency and speed of the process as well as help in identifying any necessary legislative activity or changes in practice. In addition to transmitting knowledge to the participants, common training courses may create an informal network of people who are responsible for tackling cybercrime. It could contribute to making the whole process of fighting against cybercrime better organised and lead to better outcomes for the whole country.

- As regards training and prevention, the evaluators observed little cooperation between public administration and academia. The evaluators believe that enhancing this cooperation may help strengthen the authorities' capacity to fight cybercrime. One way of doing so might be by creating and supporting a multidisciplinary Cyber Centre of Excellence where academia and field experts from the public and private sectors can meet, exchange experiences and knowledge and thus promote scientific insights in the field. Another way might be to encourage academia to consider developing education programmes in the field of cybersecurity, to ensure a sufficient influx of qualified professionals.

- The Cybercrime Enforcement Unit of the State Police actively pursues cooperation with non-governmental organisations and private sector projects to keep vulnerable social groups, especially minors and teenagers, informed of the dangers of the internet. The evaluation team was also informed that, depending on its resources, the CEU intends to assess whether it needs to widen its focus to other vulnerable groups, such as seniors. Since early prevention greatly contributes to lowering the number of successful cybercrime cases, especially when it comes to identity theft and phishing, investing resources in this area seems to be a very prudent and commendable measure to enhance the fight against cybercrime. Therefore, in the opinion of the evaluators, it would be useful to assess to which other vulnerable groups beside minors and teenagers preventive measures could be targeted, to ensure optimum use of the available resources and the most effective return on investment.

- Incident response exercises addressed to IT experts at both the technical level and the management level are organised by CERT.LV.

- Many preventive measures have been put in place by various public bodies in Latvia, but they are not coordinated. In the evaluators' view, appointing a single point to coordinate preventive activities among ministries and with other relevant bodies would lead to cost savings and avoid duplication of efforts. Preventive projects should take other initiatives into account, since some cover the same topics or have the same target group.

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Latvia

The Latvian authorities perceive their general capabilities to be sufficient. The challenges identified are being addressed. Latvia greatly values the regional cooperation with its Baltic neighbours (Lithuania and Estonia) on cybercrime prevention, and the cooperation between their CERTs. Moreover, cooperation with the US government and big companies registered in the US is also regarded as an important measure in stepping up the fight against cybercrime. 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 additional impetus to the EU's efforts to continue work on the issues identified (encryption, e-evidence, 'cloud' issues, jurisdictional issues and data retention in particular).

The Latvian authorities also mentioned that, due to the interest of the Saeima in the work of the National IT Security Council, there is a quick legislative response to the problems and challenges identified in practice.

9.2. Recommendations

As regards the practical implementation and operation of the Framework Decision and the Directives, the expert team involved in the evaluation was able to satisfactorily review the system in Latvia.

Latvia should conduct a follow-up on the recommendations given in this report 18 months after the evaluation and report on the progress to the Working Party on General Affairs, including Evaluations (GENVAL).

The evaluation team thought it fit to make a number of suggestions for the attention of the Latvian authorities. Furthermore, based on the various good practices, related recommendations to the EU and its institutions and agencies, Europol in particular, are also put forward.

9.2.1. Recommendations to Latvia

1. Should consider enhancing cybercrime specialisation within the Prosecution Service (cf. 4.1.1 and 4.5);

2. Should make even greater use of the existing structures and channels to enhance coordination between actors involved in cybersecurity, in particular by optimising the use of the capabilities and the authoritative position of the National IT Security Council (cf. 4.4.1 and 4.5);

3. Should consider involving specific private partners for specific coordination projects within the structure of the National IT Security Council, such as in the field of prevention, to avoid gaps or overlaps in the fight against cybercrime (cf. 4.2, 4.5 and 6.4);

4. Should be encouraged to establish at the level of the State Police one unit responsible for cybercrime issues to support and coordinate the efforts of all police units and to conduct proper investigations, especially in the most serious cybercrime cases (cf. 4.2 and 4.5);

5. Should be encouraged to put continuous focus on maintaining and increasing dedicated resources to strengthen the national capacity to combat cybercrime, especially at the central and regional levels of the State Police (cf. 4.4.2 and 4.5);

6. Should further develop guidelines how to apply the existing rules on the allocation of the competences for investigating hate crimes (cf. 3.5 and 5.5);

7. Should consider improving the procedures for seizing digital data by introducing mirror copying as a standard practice, to encourage people to cooperate with law enforcement more willingly (cf. 5.2.1 and 5.5);

8. Should consider expanding preventive activities to vulnerable groups other than minors and appointing a single point to coordinate preventive activities with other relevant actors, such as NGOs (cf. 6.2.3 and 6.4);

9. Should consider enhancing the relations between public administration and academia, to strengthen its capacities to fight cybercrime (cf. 6.4, 8.1 and 8.4);

10. Should continue organising practical training for judges and prosecutors to raise their level of expertise, and consider developing a joint training/experience-sharing concept involving all groups involved in tackling cybercrime (prosecutors, judges and police officers) (cf. 8.1 and 8.4).

9.2.2. Recommendations to the European Union, its institutions and other Member States

1. Member States are recommended to make the most of available civilian resources to enhance their cyber defence abilities, both in peacetime and in crisis situations, as Latvia does through the Cyber Defence Unit (cf. 6.1.2 and 6.4);

2. Member States are recommended to develop close relations between actors involved in cybersecurity representing different specialisations and profiles and dedicated to serving society at large, such as CERT.LV in Latvia (cf. 4.3, 4.5, 6.1.2 and 6.4);

3. Member States are recommended to use tools to counter child abuse and child pornography online by developing tools that allow illegal content on the internet to be reported, such as the *Net-Safe Latvia* Safer Internet Centre project (cf. 6.2.3 and 6.5);

4. Member States are recommended to work on solutions to improve and speed up the execution of MLA requests related to cybercrime (cf. 7.3 and 7.6);

5. EU institutions should address the issue of data retention (cf. 5.2.1 and 5.5);

6. The EU should consider coordinating efforts to establish an effective way of communicating and executing MLA requests from its Member States to non-EU countries, or establishing a framework for direct cooperation with relevant non-EU ISPs (cf. 7.6).

9.2.3. Recommendations to Eurojust/Europol/ENISA

1. Eurojust or Europol are encouraged to create a platform which would make available to all relevant actors involved in fighting cybercrime all the information necessary to submit an MLA request to other EU Member States or to neighbouring states (cf. 7.6);

2. Eurojust/EJN are encouraged to make efforts to provide a forum where experience with prosecuting cybercrime and using judicial cooperation instruments as well as formal requirements for these could be exchanged on a regular basis (cf. 7.6).

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

MINISTRY OF THE INTERIOR OF THE REPUBLIC OF LATVIA

7TH ROUND OF MUTUAL EVALUATIONS

The practical implementation and operation of EU policies on preventing and combating cybercrime

VISIT TO LATVIA

7 – 11 March 2016

Monday 7 March		
	Arrival	
19.30	Informal meeting *Radisson Blu Rīdzene Hotel* *Reimersa iela 1*	Representatives from the Ministry of the Interior (MoI)
Tuesday 8 March		
10.00 – 10.30	Opening by the MoI *Čiekurkalna 1. līnija 1, k. 2*	*Mr Dimitrijs Trofimovs,* Deputy State Secretary, MoI Representatives from the MoI and the State Police

10.30 – 12.30	Meeting with the State Police *Čiekurkalna 1. līnija 1, k. 2*	*Mr Gatis Švika,* Head, Cooperation and Development Bureau, Central Administrative Department, State Police *Ms Brigita Lasenberga,* Deputy Head, Criminal Intelligence Department, Central Criminal Police Department, State Police *Mr Andis Rinkevics*, Head, Crime Prevention Unit, Central Public Order Police Department, State Police *Ms Dina Tarāne*, Deputy Director,
		State Police College *Mr Aleksandrs Bebris*, Lecturer, State Police College
12.30 – 13.30	Lunch provided by the MoI and the State Police *Čiekurkalna 1. līnija 1, k. 2*	

13.30 – 16.00	Meeting with the State Police *Čiekurkalna 1. līnija 1, k. 2*	*Ms Aleksandra Tukiša,* Head, Operational Coordination and Information Provision Unit, International Cooperation Bureau, Central Criminal Police Department, State Police *Mr Deniss Belouss,* Acting Head, Forensic IT Unit, Forensics Department, State Police Economic Crime Enforcement Department, State Police: Unit 4: – *Mr Dmitrijs Homenko,* Head – *Mr Jānis Tikums,* Senior Inspector – *Mr Aleksandrs Bebris*, Senior Inspector – *Mr Dzintars Vikšers,* Senior Inspector Unit 1: – *Ms Inese Gise*, Head – *Mr Jānis Barens,* Senior Inspector
18.00	Dinner provided by the Deputy State Secretary, MoI *'Kolonāde' restaurant, Brīvības bulvāris 26*	

Wednesday 9 March

10.00 – 12.00	Meeting at the Ministry of Defence (MoD) and CERT.LV	*Mr Einārs Leps,* Senior Expert, National Cybersecurity Policy Coordination Section, MoD
	Kr. Valdemāra iela 10/12	*Mr Edgars Tauriņš,* IT Security Expert, CERT.LV
12.30 – 13.30	Lunch provided by the MoD *'Amarone' restaurant, Jura Alunāna iela 2*	
14.00 – 15.00	Meeting with the *Net-safe Latvia* Safer Internet Centre *Brīvības gatve 214M – 206*	*Ms Maija Katkovska,* Director *Ms Anita Ērgle*, Expert, Family Support Department, the State Inspectorate for Protection of Children's Rights *Ms Anda Sauļūna*, Expert, Family Support Department, the State Inspectorate for Protection of Children's Rights
15.30 – 16.30	Meeting with the Latvian Information and Communication Technology Association *Stabu iela 47*	*Mr Andris Melnūdris*, Director

Thursday 10 March

9.30 – 12.00	Meeting at the Ministry of Justice (MoJ) *Brīvības bulvāris 36*	*Ms Ilze Vanaga*, Judge, City of Riga Zemgale Urban District Court *Ms Kristīne Pommere*, Director, Department of European Affairs, MoJ *Mr Uldis Zemzars,* Legal Adviser, Department of Criminal Law, MoJ *Ms Elīna Feldmane,* Legal Adviser, Department of Criminal Law, MoJ *Mr Viktors Makucevičs*, Legal Adviser, Department of Judicial Cooperation, MoJ *Ms Dārta Mestere,* Legal Programme Officer, Latvian Judicial Training Centre
12.30 – 13.30	Lunch on behalf of the Prosecutor's General Office (PGO) *Radisson Blu Hotel Latvija* *Elizabetes iela 55*	

14.00 – 16.00	Meeting at the PGO *Kalpaka bulvāris 6*	*Ms Una Brenča*, Head Prosecutor, International Cooperation Division, PGO *Ms Dagmāra Skudra*, Prosecutor, International Cooperation Division, PGO *Mr Mārcis Viļums,* Prosecutor, International Cooperation Division, PGO *Mr Gatis Doniks*, Prosecutor, Methodology Division, PGO *Mr Ingemārs Masaļskis*, Head Prosecutor, Specially Authorised Prosecutors' Division, PGO *Mr Kaspars Cakuls*, Prosecutor, Prosecution Office of Riga Judicial Region *Mr Mairis Mackēvičs*, Prosecutor, Prosecution Office of Riga Judicial Region

Friday 11 March

9.30 – 10.00	Meeting with the Digital Security Alliance *Čiekurkalna 1. līnija 1, k. 2*	*Ms Sanita Igaune,* Director Representative from *Swedbank*
10.00 – 12.00	Overview of the evaluation visit (wrap-up session) *Čiekurkalna 1. līnija 1, k. 2* Departure	Representatives from the MoI and the State Police

ANNEX B: PERSONS INTERVIEWED/MET

Meetings on 8 March 2016

Venue: Ministry of the Interior

Person interviewed/met	Organisation represented
Mr Dimitrijs Trofimovs	Deputy State Secretary Ministry of the Interior
Ms Anete Valaine-Elsone	Legal Adviser, Ministry of the Interior
Ms Asnāte Kalniņa	Legal Adviser, Ministry of the Interior
Mr Gatis Švika	Head, Cooperation and Development Bureau, Central Administrative Department of the State Police
Ms Brigita Lasenberga	Deputy Head, Criminal Intelligence Department, Central Criminal Police Department of the State Police
Mr Andis Rinkevics	Head, Crime Prevention Unit, Central Public Order Police Department
Ms Dina Tarāne	Deputy Director, State Police College
Mr Aleksandrs Bebris	Lecturer, State Police College Senior Inspector, Group 2, Unit 4, Economic Crime Enforcement Department
Ms Aleksandra Tukiša	Head, Operational Coordination and Informative Provision Unit, International Cooperation Bureau, Central Criminal Police Department
Ms Olga Trocka	Head, Legal Assistance Request Unit, International Cooperation Bureau, Central Criminal Police Department
Mr Deniss Belouss	Acting Head, Forensic IT Unit, Forensics Department
Mr Dmitrijs Homenko	Head, Unit 4, Economic Crime Enforcement Department

Mr Jānis Tikums	Senior Inspector, Group 1, Unit 4, Economic Crime Enforcement Department
Mr Dzintars Vikšers	Senior Inspector, Group 3, Unit 4, Economic Crime Enforcement Department
Ms Inese Gise	Head, Unit 1, Economic Crime Enforcement Department
Mr Jānis Barens	Senior Inspector, Unit 1, Economic Crime Enforcement Department

Meetings on 9 March 2016

Venue: Ministry of Defence

Person interviewed/met	**Organisation represented**
Ms Ieva Ilves	Head, National Cyber Security Policy Coordination Section
Mr Einārs Leps	Senior Expert, National Cyber Security Policy Coordination Section
Ms Elīna Neimane	Senior Desk Officer, National Cyber Security Policy Coordination Section
Mr Ēriks Dobelis	Member of the Cyber Defence Unit National Guard
Mr Edgars Tauriņš	IT Security Expert, CERT.LV

Venue: Net-Safe Latvia Safer Internet Centre

Person interviewed/met	**Organisation represented**
Ms Maija Katkovska	Director
Ms Anita Ērgle	Expert, Family Support Department
Ms Anda Sauļūna	Expert, Family Support Department

Venue: Latvian Information and Communication Technology Association (LIKTA)

Person interviewed/met	Organisation represented
Ms Māra Jākobsone	Vice President
Mr Andris Melnūdris	Managing Director
Mr Toms Pēcis	IT risk manager, Lattelecom

Meetings on 10 March 2016

Venue: Ministry of Justice

Person interviewed/met	Organisation represented
Ms Ilze Vanaga	Judge, City of Riga Zemgale Urban District Court
Mr Uldis Zemzars	Legal Adviser, Department of Criminal Law, Ministry of Justice
Ms Elīna Feldmane	Legal Adviser, Department of Criminal Law, Ministry of Justice
Mr Viktors Makucevičs	Legal Adviser, Department of Judicial Cooperation, Ministry of Justice
Ms Dārta Mestere	Legal Programme Officer

Venue: Prosecutor-General's Office

Person interviewed/met	Organisation represented
Ms Una Brenča	Head Prosecutor, International Cooperation Division, Prosecutor-General's Office
Ms Dagmāra Skudra	Prosecutor, International Cooperation Division, Prosecutor-General's Office
Mr Gatis Doniks	Prosecutor, Methodology Division, Prosecutor-General's Office
Mr Ingemārs Masaļskis	Head Prosecutor, Specially Authorised Prosecutors' Division, Prosecutor-General's Office

Person interviewed/met	Organisation represented
Mr Kaspars Cakuls	Prosecution Office of Riga Judicial Region

Venue: CERT.LV

Person interviewed/met	Organisation represented
Ms Baiba Kaškina	Director
Mr Varis Teivāns	Deputy Director
Mr Edgars Tauriņš	IT Security Expert

Meetings on 11 March 2016

Venue: Ministry of the Interior

Person interviewed/met	Organisation represented
Ms Sanita Igaune	Director, Digital Security Alliance
Mr Vitālijs Kuzmins	IT risk manager, Swedbank
Name and surname not to be disclosed	Security Police
Mr Gatis Švika	Head, Cooperation and Development Bureau, Central Administrative Department
Ms Brigita Lasenberga	Deputy Head, Criminal Intelligence Department, Central Criminal Police Department
Ms Inga Šamarova	Head, Information Bureau, Central Criminal Police Department
Mr Jānis Kruks	IT security administrator
Ms Aleksandra Tukiša	Head, Operational Coordination and Information Provision Unit, International Cooperation Bureau, Central Criminal Police Department

Person interviewed/met	Organisation represented
Mr Deniss Belouss	Acting Head, Forensic IT Unit, Forensics Department
Mr Dmitrijs Homenko	Head, Unit 4, Economic Crime Enforcement Department
Mr Jānis Tikums	Senior Inspector, Group 1, Unit 4, Economic Crime Enforcement Department
Mr Dzintars Vikšers	Senior Inspector, Group 3, Unit 4, Economic Crime Enforcement Department
Mr Mārtiņš Brižs	Senior Inspector, Unit 4, Economic Crime Enforcement Department
Ms Inese Gise	Head, Unit 1, Economic Crime Enforcement Department

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	LATVIAN OR ACRONYM IN ORIGINAL LANGUAGE	LATVIAN OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
BDPS	*BDPS*		Biometric Data Processing System
CEU	*CEU*		Cybercrime Enforcement Unit
CPU	*CPU*		Crime Prevention Unit
CSS	*CSS*		Cyber Security Strategy of Latvia 2014-2018
DDA	*DDA*		Digital Safety Alliance
DSI	*DSI*		Data State Inspectorate
HAVEN	*HAVEN*		Halting Europeans Abusing Victims in Every Nation
IIIS	*IIIS*		Integrated Interior Information System
KRASS	*KRASS*		Criminal Procedure Information System
LIA	*LIA*		Latvian Internet Association
LIKTA	*LIKTA*		Latvian Information and Communication Technology Association
OCIPU	*OCIPU*		Operational Coordination and Information Provision Unit
TIS	*TIS*		Court Information System

Under the **Criminal Law**, the following acts are criminalised:

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

— for *intentional violation of the confidentiality of personal correspondence*, the applicable punishment is either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine (Article 144(1));

— for *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 either deprivation of liberty for a term of up to three years, temporary deprivation of liberty, community service or a fine (Article 144(2));

— if the acts provided for in Article 144(1) or (2) are committed *for the purposes of acquiring property*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine (Article 144(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 *obtaining or distribution of such data as enable illegal utilisation of financial instruments or means of payment*, the applicable punishment is either deprivation of liberty for a term of up to three years, temporary deprivation of liberty, community service or a fine (Article 193^1(1));

— for *utilisation of such data as enable illegal utilisation of financial instruments or means of payment, or manufacture or adaptation of software or equipment for the commission of the crimes provided for in Article 193 of the Criminal Law, or obtaining, storage or distribution of such software or equipment for the same purpose*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine, with or without confiscation of property (Article 193^1(2));

— if the acts provided for in Article 193^1(1) or (2) *are committed by a member of an organised group*, the applicable punishment is deprivation of liberty for a term of between two and ten years, with or without confiscation of property and with police supervision for a term of up to three years (Article 193^1(3));

3) the arbitrary accessing of automated data processing systems (Article 241):

— for *arbitrary accessing of an automated data processing system, if it is related to a breach of system protective measures 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 either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine (Article 241(1));

— for the criminal offence provided for in Article 241(1), if it has been committed *for the purposes of acquiring property*, the applicable punishment is either deprivation of liberty for a term of up to four years, temporary deprivation of liberty, community service or a fine, with or without confiscation of property (Article 241(2));

— for the acts provided for in Article 241(1), *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 either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine, with or without confiscation of property (Article 241(3));

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

— for *unauthorised modification, damage, destruction, impairment or concealment 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 either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine (Article 243(1));

— for *knowingly interfering in the operation of an automated data processing system by entering, transferring, damaging, erasing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused*, the applicable punishment is either deprivation of liberty for a term of up to three years, temporary deprivation of liberty, community service or a fine (Article 243(2));

— for the criminal offence provided for in Article 243(1) or (2), if it has been committed *for the purposes of acquiring property*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine, with or without police supervision for a term of up to three years (Article 243(3));

— for the acts provided for in Article 243(1) or (2), *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 of up to seven years, with or without confiscation of property and with or without probationary supervision for a term of up to three years (Article 243(5));

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

— for *illegal manufacture, adaptation for utilisation, sale, distribution or storage of a tool (device, software, computer password, access code or similar data) intended to influence the 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 the purposes of committing a criminal offence*, the applicable punishment is either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine (Article 244(1));

— for the same acts, *if serious consequences have been caused thereby*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine (Article 244(2));

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

— for *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 the 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 either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine.

Content-related acts, in particular those related to child sexual abuse

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

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

— if the acts provided for in Article 162[1](1) are *committed against an underage person,* the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine, with probationary supervision for a term of up to five years (Article 162[1](2));

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

— for *violation of provisions regarding the demonstration of a pornographic performance, provisions regarding the restriction of entertainment of an intimate nature, or provisions regarding the handling of material of a pornographic nature, if substantial harm has been caused by the commission thereof*, the applicable punishment is either deprivation of liberty for a term of up to one year, temporary deprivation of liberty, community service or a fine (Article 166(1));

— for *visiting or demonstrating such pornographic performance or handling materials of a pornographic nature which contain child pornography, sexual activities of people with animals, necrophilia or sexual gratification in a violent way*, the applicable punishment is either deprivation of liberty for a term of up to three years, temporary deprivation of liberty, community service or a fine, with or without confiscation of property and with probationary supervision for a term of up to three years (Article 166(2));

— for *involvement, forced participation or utilisation of minors in a pornographic performance or the production of material of a pornographic nature, or for encouraging their participation therein*, the applicable punishment is deprivation of liberty for a term of up to six years, with or without confiscation of property and with probationary supervision for a term of up to three years (Article 166(3));

— for *involvement, forced participation or utilisation of persons who have not attained the age of sixteen in a pornographic performance or the production of material of a pornographic nature, or for encouraging their participation therein*, the applicable punishment is deprivation of liberty for between three and twelve years, with or without confiscation of property and with probationary supervision for a term of up to three years (Article 166(4));

— if the acts provided for in Article 166(3) or (4) are 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 between five and fifteen years, with or without confiscation of property and with probationary supervision for a term of up to three years (Article 166(5)).

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', and further explains 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 *direct or indirect intent*'. It further explains that a criminal offence is considered to have been committed with:

— *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 has been aware of the harm caused by his or her act or failure to act, has foreseen the harmful consequences of the offence and has desired them.

— *indirect intent* if the person has been aware of the harm caused by his or her act or failure to act, has foreseen the harmful consequences of the offence and, although not desiring 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 is 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 their 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, even though according to the actual circumstances of the offence he or she should and could have foreseen such harmful consequences.

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 must be taken into account.

Article 47 sets out the following circumstances which are to be considered as *mitigating* the liability:

— if the perpetrator of the criminal offence has admitted his or her guilt, has freely confessed and has regretted the criminal offence committed;

— if the 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;

  — if the criminal offence was committed:
- as a result of unlawful or immoral behaviour by the victim;
- exceeding the conditions regarding necessary self-defence, extreme necessity, detention of the person committing the criminal offence, justifiable professional risk, or the legality of the execution of a command or order;
- by a person in a state of diminished mental capacity.

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

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

— if the criminal offence was committed:

- while in a group of persons;
- by 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 by taking advantage of the helpless condition or infirmity due to old age of a person;
- by taking advantage of a person's official, financial or other dependence on the offender;
- with particular cruelty or with humiliation of the victim;
- by taking advantage of the circumstances of a public disaster;
- using weapons or explosives, or in some other generally dangerous way;
- out of a desire to acquire property;
- under the influence of alcohol or of narcotic, psychotropic, toxic or other intoxicating substances;
- for racist, national, ethnic or religious motives;

  — if the criminal offence:

- has caused serious consequences;
- constitutes *recidivism* of criminal offences;
- was related to violence or threats of violence, or if the criminal offence against morality and sexual inviolability was committed against a person to whom the perpetrator is related in the first or second degree of kinship, against the spouse or former spouse, against a person with whom the perpetrator is or has been in an unregistered marital relationship, or against a person with whom the perpetrator has a joint (single) household;

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

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'.

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, instigators and abettors* are joint participants in a criminal offence'.

Attempt

According to Article 15 on completed and uncompleted criminal offences, 'a conscious act (failure to act), which is directly dedicated to the 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'.

'Serious' or 'large-scale' cyber-attack

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 as specified in the Republic of Latvia at that time'. The Article further explains 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 one of the following consequences has been caused:

— financial loss which at the time of committing the crime has not been less than five times the minimum monthly wage (in total) as determined at the time in the Republic of Latvia, *and* if other interests protected by law have been threatened;

— financial loss which at the time of committing the crime has not been less than ten times the minimum monthly wage (in total) as determined at the time in the Republic of Latvia;

— other interests protected by law have been significantly threatened.

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, which at the time of committing the crime has not been less than fifty times the minimum monthly wage (in total) as determined at the time in the Republic of Latvia, have been inflicted, or other serious harm has been caused to the interests protected by law.[17]

[17] The criteria for the specification of the level of seriousness of bodily injury are provided for in annexes to this Law.