# NATIONAL
# CYBERSECURITY
## STRATEGY II
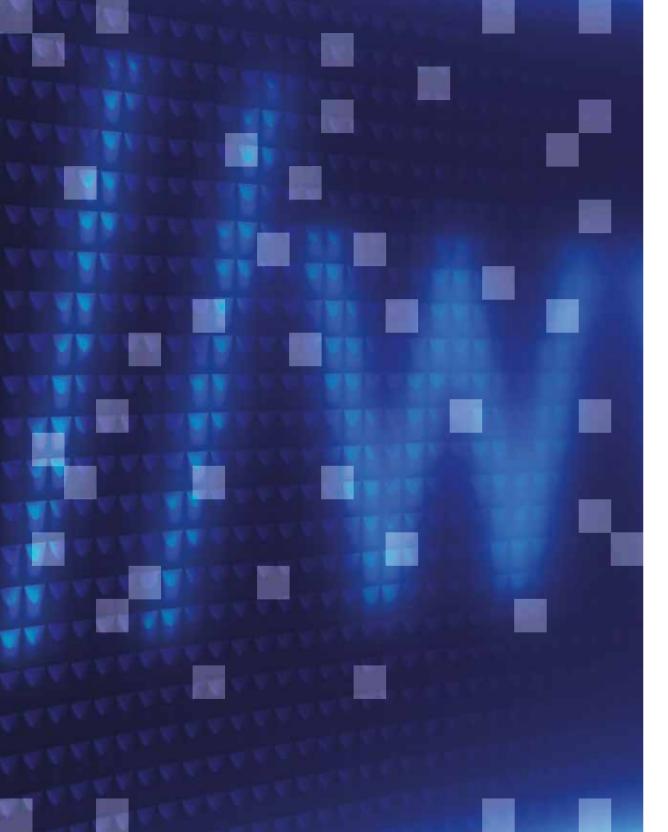
# *NATIONAL CYBERSECURITY* *STRATEGY II*

Approved and made enforceable by the Government Council on 27.03.2015

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

## *FOREWORD OF THE PRIME MINISTER, MINISTER OF STATE*

You have in your hands the second version of the national cybersecurity strategy approved by the Government on 27th March 2015. The task force in charge of revising the first version of 2012 operated under the authority of the High Commissioner for National Protection and was composed of representatives of the State's Information Technology Centre, the government CERT, the Department of Media and Communications, the Ministry of the Economy, the Government Communications Centre, the Intelligence Service, the Grand Ducal Police Force and the Army. First of all, the task force assessed the impact of the strategy which was adopted in 2012 and then made the amendments that were required in light of the conclusions of this assessment.

The introduction of seven objectives, complemented by action plans resulting in specific timelines and the identification of actors responsible for the implementation of approximately forty different actions, should ensure adequate implementation of this new national cybersecurity strategy by the end of 2017.
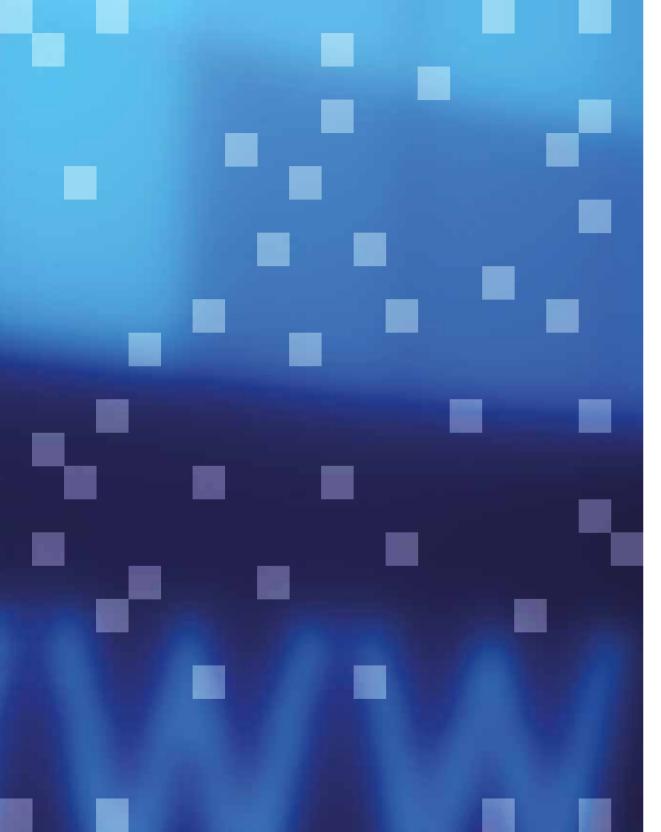
The adaptation of this strategic document is in line with the focus areas that were defined in 2012 and reflects Luxembourg's willingness, and even determination, to provide the country with electronic communication infrastructures that meet international security standards. It is a prerequisite for the development of a digital society, in the same spirit of the "Digital Lëtzebuerg" initiative, as having a safe technological environment will build up the trust of citizens and companies in these technologies, and this will, in turn, ensure that our country's objectives of economic growth are met.

Xavier Bettel

# TABLE OF CONTENTS

## INTRODUCTION

The 2013 government programme emphasises the importance of cybersecurity for the well-being of society. Aware of the risks associated with information and communication technologies (ICTs), the Cyber Security Board (CSB) developed a national strategy on cybersecurity in 2012. On 11th March 2014, the Cyber Security Board established a task force composed of representatives of the State's Information Technology Centre, the government CERT, the Department of Media and Communications, the Ministry of Economy, the Government Communications Centre, the Intelligence Service, the Grand Ducal Police Force and the Army, operating under the authority of the HCPN, to develop a new version of the said strategy.

Cybersecurity has become a critical asset for the attractiveness of our economy. For this reason, the government is determined to review its strategy on a recurring basis, update its governance tools and ensure to remain sovereign with respect to certain critical services related to security.

The government understands that information security is a societal challenge that needs to be addressed jointly by engaging in appropriate behaviours and implementing effective and efficient organisational and technical measures while complying with principles of proportionality and necessity.

The government promotes national and international cooperation, and is determined to democratise information security by identifying potential synergies while reducing the costs and complexity of procedures for all stakeholders.

# SITUATIONAL ANALYSIS OF THE CYBERSECURITY STRATEGY I

## SITUATIONAL ANALYSIS OF THE CYBERSECURITY STRATEGY I

The cybersecurity strategy I provides for a regular review of its procedures. This chapter is dedicated to this task.

### Axis 1: Ensuring the Operational Protection of Communication and Information Processing Infrastructures and Information Systems

*Preventive Operational Strand*

Luxembourg has many initiatives under way in the field of prevention. These initiatives are coordinated by the Cyber Security Board (CSB) and most of them are executed by public actors. In the preventive field, priority was given to organisational security measures:

• The government has identified risk analysis as a priority. Indeed, it is only after such an analysis that an entity may identify the organisational and technical measures required. This analysis ensures that the measures put in place comply with the principle of proportionality and necessity. As a result, CASES developed an optimised approach to risk analysis based on a common taxonomy, taking advantage of the sectoral knowledge bases and offering great synergistic potential: the MONARC optimised risk analysis methodology.

• The CTIE, GOVCERT and CIRCL conducted internal risk analyses.

• An inventory of databases dealing with personal data under the responsibility of the State has been compiled by the CSB's "Database" working group.

• The CSB instructed a "Mobile devices" working group to prepare a proposal to equip members of the government with secure mobile communication devices. The findings were presented to the CSB.

• With regards to risk treatment, CASES has developed several good practice guides that are made available to all the entities concerned.

• As for the identification of threats, tools for exchanging information on indicators of compromise have been developed and made available to all parties concerned.

Several national actors (CSSF, ILR, NCDP, ILNAS and HCPN in the future) require from their constituent a risk analysis according to specific criteria for the sectors and assigned missions. The government must strive to improve the harmonisation of the approaches as well as frames of reference for requirements in order to reduce the individual effort of regulated entities. The government's ambition is to turn risk analysis into a governance tool which complies with the principles of proportionality and necessity.

### *Defensive Operational Strand*

- Cyber plan: On 19th March 2014, the government adapted the emergency intervention plan in the event of an attack against information systems or of a technical fault of information systems ("PIU Cyber"). This plan is regularly tweaked during European cyber exercises in which Luxembourg participates actively.

  "PIU Cyber", developed under the authority of HCPN, sets out government action in the event of significant issues with information systems of the public or private sector that may cause a major malfunction, or the unavailability of these systems, which would threaten the vital interests or the basic needs of the country or the Grand Duchy's population, in full or in part. It should be noted that routine incidents are managed by operational CERTs.

  The plan first determines the crisis management bodies, such as the crisis unit, the operational unit, the cyber risk assessment unit and the communication/information unit. It then lays down the process to alert the authorities and release information to the public, emergency measures, related actions as well as the respective officials and actors. During the implementation of the various measures of prevention and protection, ministries, administrations and services of the State can be assisted by the government CERT (primarily focused on the public sector and critical infrastructures) and, if necessary, by the CIRCL (primarily focused on the private sector).

- In addition to the CIRCL, which consists of a CERT dedicated to the private sector and communes, several private and public sector CERTs were created: GOVCERT.LU for government and critical infrastructures, RESTENA-CSIRT in charge of the education and research sector, as well as HealthNet-CSIRT covering the health sector. It is up to these CERTs to support their respective constituent.

- Similarly, to increase the attractiveness of the economy, Luxembourg CERTs offer specialised services in the field of information security:
  - Tools to create health indicators of Luxembourg networks. These include BGP-Ranking[1] and passive DNS[2] projects which allow incident management to be more prompt and efficient.
  - Tools for the exchange of compromise indicators specific to threats considered dangerous, including the MISP platform and the DMA dynamic analysis[3] tool. These indicators allow all relevant entities to detect any incidents in their networks.
  - Tools to provide individual information to interested parties regarding the vulnerabilities of products they use.

## Axis 2: Modernising the legal framework

### *"Legal monitoring"*

The legal framework has several levels, namely:

- at national level:

Regular meetings take place between the Prosecution service, the GOVCERT, the Grand Ducal Police, the CSIRT RESTENA, the CIRCL, the Ministry of the Economy, the SRE and the NCDP in order to discuss the evolution of threats and possible solutions.

In this regard, it is appropriate to mention the law of 18th July 2014 on:

- The approval of the Council of Europe's Convention on Cybercrime opened for signature in Budapest on 23rd November 2001.

- The approval of the Additional Protocol to the Convention on Cybercrime on:
  - the criminalisation of acts of a racist and xenophobic nature committed via computer systems, done in Strasbourg on 28th January 2003,
  - the amendment of the Criminal Code,
  - the amendment of the Code of Criminal Procedure,
  - the amendment of the amended Act of 30th May 2005 on the protection of privacy in the electronic communications sector.

Following the ratification of the Budapest Convention in August 2014, adaptations were made to the Luxembourgish legal framework. An article containing all the texts in question was published in the journal of Luxembourg courts[4].

 On the other hand, along with the NCDP, the government considered the possibility of creating a software platform that would allow all the entities concerned to perform PIAs (Privacy Impact Assessments) as requested by the European texts on the protection of personal data.

- at community level:

Reviews and text proposals were drawn up regarding projects of directives developed by competent community bodies (EFMS; FOP). Examples include Directive 2013/40/EU of the European Parliament and of the Council of 12th August 2013 on attacks against information systems and replacing Council framework decision 2005/222/JHA of 24th February 2005, or the Council and Parliament's proposal for a directive on measures to ensure a common high level of safety of information networks within the Union.

## Axis 3: Developing national and international cooperation

Over the past few years, Luxembourg has given special attention to national and international cooperation in cybersecurity. Examples include:

- An active participation in the 2012 and 2014 Cyber Europe exercises of the European Union.

- The participation in NATO's CC13 and CC14 Cyber Coalition exercise as an observer.

- The signature of a MoU on cybersecurity between the HCPN and NATO's Cyber Defence Management Board (CDMB).

- The designation of two contact points for cybersecurity at the GOVCERT.LU in the context of the MoU with NATO.

- The establishment of a 24/7 service responsible for national and international contact-making for the treatment of cyber crisis computer emergencies, the management of which is provided in collaboration with the NATO Computer Incident Response Capability on their platform for sharing information on cyber incidents.

- The participation of the CIRCL in the development of computer software that facilitates the sharing of information on indicators of compromise: Malware Information Sharing Platform (MISP). Said software was made available to all NATO allies and used by almost all CERTs in Europe.

- Active participation of Luxembourg CERTs in international networks (TF-CSIRT, FIRST, etc.); Luxembourg CERTs enjoy a very good reputation.

- Luxembourg's collaboration with Germany and Belgium with respect to risk management.

- The establishment of a cyber risk assessment unit ("CERC") by the PIU Cyber, framing the cooperation between, in particular, the HCPN, CTIE, SRE and the CERTs concerned in the event of a significant incident. Said assessment unit is chaired by the GOVCERT.LU.

- GOVCERT.LU's participation in conferences bringing together the GOVCERTs of Europe.

- The participation of Luxembourg CERTs in various European research projects, particularly in the field of phishing and the fight against "botnets".

4  The ratification of the Budapest
   Convention on Cybercrime by
   Luxembourg; Max Braun; journal
   of Luxembourg courts; No. 35, 5th
   October 2014.

## Axis 4: Informing, educating and raising awareness about the risks involved

### *Objectives of educating, informing and raising the awareness of end users*

Luxembourg understands that awareness and education are essential for all persons concerned to adopt adequate behaviour patterns in the field of information security. Many threats aimed at exploiting human vulnerabilities exist. It is important to reduce these vulnerabilities by training all the persons concerned and raising their awareness:

• With respect to users/Internet users, the following actions were undertaken:
  - Existing websites and websites to come:

    · www.govcert.lu
    · www.circl.lu
    · www.bee-secure.lu
    · www.cases.lu
    · www.police.lu
    · Government portal on cybersecurity.

  - Recurring articles in the press (by the CIRCL, CASES, BEE SECURE or the Grand Ducal Police, depending on the case in question).
  - Annual awareness campaigns of CASES and BEE-SECURE.
  - Alerts (from the CIRCL, CASES, BEE SECURE, the Grand Ducal Police or the Ministry of the Economy, depending on the case in question).
  - More technical reports and communications by the GOVCERT and CIRCL[5] or savvy users and IT professionals.

• For students, parents, educators and teachers, the authorities organised:

  - Compulsory BEE-SECURE training sessions (two hours in all classes of 7th secondary and technical secondary).
  - Optional BEE-SECURE training sessions (two hours in basic education classes).
  - Evening meetings with parents of pupils (with some success).
  - Training sessions for educators (with an average success).
  - Training sessions for teachers (with little success).

The government is determined to expand its training and raising awareness offers. Given the great need for IT experts in the next few decades, the government continues its efforts to stimulate young people's (boys and girls) interest in computing and programming.

---

5   http://circl.lu/pub/

• Civil servants and public employees benefit from:

  - Optional CASES training sessions (three hours organised by the INAP on its own premises). It consists of three sessions per year. For the moment, these training sessions are not compulsory for all new government officials.
  - Optional CASES training sessions (three hours organised by the INAP on the premises of the administration). These training sessions have been fairly successful: 4-5 administrations per year rely on them.
  - Specialised CASES training sessions (very little success).
  - GOVCERT training sessions for new data protection officers.
  - Warnings and information provided by the GOVCERT.
  - Publication of the CTIE's IT Charter.

Very few applications come from small and medium enterprises. The government has implemented a price-regulated and very advantageous awareness service, provided by private CASES-certified experts.

### *Objectives of educating, informing and raising the awareness of service providers*

Many of the actors who are subject to a regulatory regime are obliged to attend training sessions. However, a good overview is not yet available.

Obligations can derive from:

• certification standards such as ISO/IEC 27001 (ISO/IEC 27002) to which certain enterprises are subject;

• requirements of regulators:
  - the CSSF for certain types of PSF as well as for banking institutions;
  - the ILNAS for Public Key Infrastructures (PKIs) as well as for dematerialisation and electronic archiving service providers;
  - the NCPD for processing security (Articles 22 and 23 of the law of 27 July 2007).

GOVCERT.LU, CIRCL and CASES offer training sessions to businesses. In the case of CASES, the training sessions are not free and they are offered by trainers from certified specialised companies.

CASES makes available to enterprises a catalogue of governance and risk analysis services, as well as a platform including tools associated therewith:

http://my.cases.lu/.

In the context of coordination and computer incident response, the CIRCL provides companies and especially computer teams with proactive tools and services to make operational and reactive security more effective and efficient:

http://circl.lu/services/ and http://circl.lu/projects/.

## Axis 5:
## Developing and implementing norms and binding standards

• A new regulator for operators of critical infrastructures:

The bill of law on national protection provides for the establishment of the High Commissioner for National Protection as new cross-regulator, responsible for all operators of critical infrastructures in the areas of physical security as well as the security of information systems. Thus, in the future, operators will be required to provide to the High Commissioner for National Protection all data requested for the purposes of census, designation and protection of critical infrastructure. This data includes all the information needed in the context of crisis prevention or management.

Data relating to critical infrastructures which are subject to registration, communication, statement, census, filing, permission or notification imposed by the law or relevant regulations are communicated to the High Commissioner for National Protection, upon his request, by the ministerial departments, administrations and government services that hold such data.

The owner or operator of a critical infrastructure is required to develop a plan of security and continuity of the activity, which includes security measures for the protection of the infrastructure. The High Commissioner for National Protection addresses recommendations regarding these safety measures to the owner or the operator of a critical infrastructure, allowing the latter improve resilience and facilitate crisis management.

The owner or operator of a critical infrastructure is also required to appoint a security officer whose role is to be the contact person of the competent authority for issues relating to the security of the infrastructure.

The owner or operator of a critical infrastructure must ultimately notify the High Commissioner for National Protection of any incident which had a significant impact on the security and continuity of the infrastructure's operation.

• The management of PSDCs (dematerialisation and storage service providers).

*Conclusions of the Analysis of the Cybersecurity Strategy I*

When drafting the Cybersecurity Strategy I, the competent body at inter-ministerial level was the CSB. With regards to the execution of tasks, it turned to the creation of ad hoc working groups within the CSB, respectively to the assignment of missions to members of the CSB.

In any case, while the CSB is the appropriate forum for discussions and decisions of a strategic nature, it seems hardly suitable to perform all the work required in the context of the implementation of a cybersecurity strategy. These tasks could be better coordinated by a permanent operational body.

Therefore, in the future, emphasis will need to be placed on supervising the new strategy and on the modalities of the implementation, rather than on a thorough reform of the objectives and areas that remain relevant.

## Cybersecurity Strategy I in the Image of Other National Strategies

The vast majority of nations have a cybersecurity strategy. Several international organisations[6], consulting firms and universities have compiled comparisons. For this analysis, two documents were selected, the Dutch strategy (NCSS2[7]) and a comparison of strategies of European Union member states edited by ENISA.

### "ENISA National Cyber Security Strategies Checklist"

An analysis of the 2012 cybersecurity strategy via an ENISA[8] questionnaire reveals that the current text has two weaknesses that need to be remedied in the future: on the one hand, the definition of the term "cyber security" and, on the other, the dialogue with the academic and industrial world.

### The Dutch Strategy

The second version of the 2013 "NCSS2" Dutch strategy is in line with the objectives of the first version, further developing its implementation. Emphasis is placed on cooperation with the private sector and on the accountability of all stakeholders (government, citizens and economic actors). A joint action plan with a timeline over two years is presented in detail in the new text.

### Findings of the Comparison

The comparative analysis reveals that it would be useful to develop the following elements to a greater extent in the new text:

- Introduce a definition of cybersecurity;
- Initiate dialogue with the academic and industrial world;
- Introduce the concept of cyberdefence;
- Formally instruct a body to handle the coordination of the new strategy's implementation;
- Set up action plans.

6  The OECD, OSCE, ENISA (European Network and Information Security Agency)
7  NCSS2: National Cyber Security Strategy 2
8  http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

# CYBERSECURITY STRATEGY II

# *CYBERSECURITY STRATEGY II*

### Definition of Cybersecurity[9]

*"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user assets. Organisation and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user assets against relevant security risks in the cyber environment. The general security objectives comprise the following:*

- *Availability;*
- *Integrity, which may include authenticity and non-repudiation;*
- *Confidentiality."*

### Objectives of the Cybersecurity Strategy II

In broad terms, this cybersecurity strategy is designed to protect the public and private actors against cyber threats while promoting economic and social development in cyberspace.

The government recognises that information security should not be considered as a burden, but rather as an opportunity. It is about democratising information security by promoting collaboration while reducing the complexity and costs to all stakeholders.

The government intends to achieve this goal by defining the following objectives and action plans:

### *Objective 1: Strengthen National Cooperation*

The need for a comprehensive approach raises the issue of government coordination so that all stakeholders can collaborate consistently, avoiding duplication of functions and promoting the development of synergies and the consolidation of initiatives with a view to maintaining, or even to developing a high-quality image both nationwide and internationally.

> The government recognises that information security should not be considered as a burden, but rather as an opportunity. It is about democratising information security by promoting collaboration while reducing the complexity and costs to all stakeholders.

At national level, increased cooperation between all stakeholders is a prerequisite to implement the strategy consistently. The methodology of governance must be based on concepts defined in risk management, as proposed by ISO/IEC 27005: 2011, i.e. establishing the context, estimating risks, assessing risks, treating, accepting and finally communicating risks; all in a context of continuous improvement.

An important objective for the government is to increase the attractiveness of the economic position by introducing adaptable, flexible and modern governance tools. Governance must be risk-orientated.

The following are affected by this approach:

- government bodies (HCPN, GOVCERT, SRE, CTIE, Army);
- prosecuting authorities (Grand Ducal Police and the Prosecution service);
- independent national authorities concerned (ILR, CSSF, NCDP);
- sectoral actors (CIRCL, RESTENA, private CERTs);
- public-private partnerships (PPP).

*The creation of a national agency for the security of information systems (ANSSI) will facilitate the implementation of the contemplated action plans.*

The creation of a national agency for the security of information systems (ANSSI), decided by the government when adopting the draft Grand Ducal Decree on this matter in its sitting of 21st January 2015, will facilitate the implementation of the contemplated action plans.

The ANSSI's mission is to define policies and guidelines for the security of classified and unclassified information, ensure that norms and standards are established, that the necessary measures regarding the security of information systems are implemented and that their application is guaranteed, certify the means of processing of unclassified information (digital systems, services, infrastructures), and finally to act as national CERT and ensure the government CERT's hosting (GOVCERT.LU). It will bring together under a single line of command all active players in the field of cybersecurity in relation to the public sector and critical infrastructure, and will have to cooperate with all suitable private sector stakeholders, if necessary by means of formalised cooperation agreements.

## Action Plan Objective 1

| # | Action | Note | Responsible party, Actor(s) | Schedule |
|---|--------|------|------------------------------|----------|
| 1 | Creation of an ANSSI | | HCPN, PGD, SMILE, GOVCERT, CTIE/CCMD, SRE/ANS | 2015 |
| 2 | Identification and allocation of human and budget resources needed for the proper functioning of an ANSSI | | HCPN, Ministry of State | 2015-2016 |
| 3 | Set up a cooperation agreement between the ANSSI and the SRE | Formalise the exchange of information and cooperation between the two entities. | ANSSI, SRE | 2015 |
| 4 | Set up a cooperation agreement between ANSSI and SMILE | Ditto | ANSSI, SMILE | 2015 |
| 5 | Promote cooperation with ISPs | | ANSSI, CERTs | 2015-2017 |
| 6 | Merger of CTIE and GCC operators | Creation of a single operator for classified and unclassified State networks | Ministry for Public Function and Administrative Reform, CTIE, CCG | 2015 |
| 7 | Establishment and operation of a single website on the topic of cybersecurity | | ANSSI, GOVCERT, SMILE, CTIE, SIP, SMC | 2015-2016 |
| 8 | Clarify the CSB's missions after creating an ANSSI | | CSB, SMC | 2015 |
| 9 | Adopt a system for the management of risks related to the security of information systems based on the ISO/IEC 27005:2011 standard | | ANSSI, SMILE | 2015-2016 |
| 10 | Set up a "Governance" working group for the purpose of perfecting the governance model at national level | | CSB | 2015-2016 |

*Objective 2: Strengthen International Cooperation*

*Active cooperation with the international community is imperative*

The need for cooperation between all those involved both nationally and internationally, stems from the supra-national nature of communication networks. Therefore, active cooperation with the international community is imperative, in particular at the level of CERTs and law enforcement agencies. The purpose of this cooperation is to lead to an exchange of information and mutual assistance between the competent services of the different countries and in international fora, as well as to the creation of common solutions and approaches.

However, international cooperation must not be limited to the exchange of operational information. It must also focus on methodological aspects and tools in the field of incident management, on systems for detecting abnormalities, early warning systems, risk management, security policies, raising awareness and education.

At international level, cooperation can take the form of bilateral contacts or rely on multilateral exchanges within institutions/groups/communities, such as (non-exhaustive list):

- the Benelux
- the European Union
  - ENISA, NIS platform, EFSM and other high-level groups
  - TF-CSIRT, EGC, CERT-Verbund, CLUSIx, R2GS clubs and other technical groups
- Germany: BSI
- Switzerland: ISB
- Austria: Ministry of Finance, A-SIT
- France ANSSI
- the Council of Europe
- NATO/CCDCoE/CDMB
- OECD/OSCE
- Europol/Interpol/FBI
- FIRST (and other specialised communities of the CERT sphere)

*Action Plan Objective 2*

| # | Action | Notes | Responsible party, Actor(s) | Schedule |
|---|--------|-------|------------------------------|----------|
| 1 | Establish an inventory of all the agreements, collaborations and participations at bi- or multi-national level. | | CSB | 2015 |
| 2 | Identify good practices for cooperation (in Europe and internationally) and participate in groups, respectively establish key partnerships. | | ANSSI, CERTs, SRE, Army | 2015-2017 |

## *Objective 3: Increase the resilience of the digital infrastructure*

> *The security of the digital infrastructure lies in its ability to guarantee a certain level of availability, integrity and confidentiality.*

The security of the digital infrastructure lies in its ability to guarantee a certain level of availability, integrity and confidentiality. The security of the digital infrastructure carries a cost and requires the know-how of experts. For this reason, it is advised to make the most of synergies that may arise and to pool as much as possible risk analysis, the establishment of situational analysis and the setting up of measures to handle risks and incidents.

### *Preventive Operational Strand*

In accordance with the principle of proportionality and necessity, the government should encourage all parties concerned to implement preventive measures. Information, training, guides to good practice as well as methodologies will be made available to stakeholders. The system of governance implemented by the government will help private and public actors as well as regulators to identify necessary treatments and to respectively define frames of reference for requirements in the field of cybersecurity. The principles of necessity and proportionality are essential to fulfil the needs of cost-effectiveness, which, in turn, has a great impact on the attractiveness of the economic position.

In the preventive sphere, it is possible to capitalise on a large number of synergies:

- Governance tools for analysis, risk management, as well as metrics of threats and vulnerabilities (made available to CERTs) may be used by regulators and private and public actors.
- Frames of reference for requirements developed by regulators will be harmonised through the use of taxonomy and common methodology.
- In terms of risk management, contextualised approaches will be offered that will substantially reduce the effort and investment in risk analyses.
- With regards to the treatment of risks, the pooling of certain security measures is planned.
- In terms of CERTs, threats and vulnerabilities are monitored. The result of such monitoring is made available to all Luxembourg actors and used in the context of governance and risk management tools.

### *Defensive Operational Strand*

It must be acknowledged that no information system, regardless of its level of protection, is perfectly secure. Therefore, sufficient capacity is necessary to detect intrusions, but also to react once an incident is detected, to handle the issue efficiently and restore the operability of the systems affected.

In this context, three types of operational measures are intended to achieve this objective, i.e.:

- sharpen operational aspects in the implementation of the Cyber PIU for significant cyber incidents;
- create simulations and/or sectoral and national exercises on the response to incidents affecting the security of sensitive or critical information and communication systems, and participate in international exercises in this area;
- improve cooperation between CERTs when handling routine incidents through cooperation agreements and the establishment of an information exchange platform.

*Action Plan Objective 3*

| # | Action | Notes | Responsible party, Actor(s) | Schedule |
|---|--------|-------|------------------------------|----------|
| 1 | Propose tools for sectoral risk management | | ANSSI, CASES, research | |
| 2 | Develop good sectoral practices | | ANSSI, CASES, CERTs | |
| 3 | Intensify pooling of security measures | | ANSSI, ILR, CERTs, private sector | 2015-2017 |
| 4 | Develop performance indicators for security, monitor these indicators | | CERTs | 2015-2017 |
| 5 | Implement tools and detailed procedures to manage significant incidents | Implementation of the PIU Cyber. | HCPN, ANSSI, CIRCL, GOVCERT, CTIE, PGD, SRE | 2016 |
| 6 | Develop a military doctrine for the cyber sphere | | EMA | 2016 |
| 7 | Participation in the preparation and execution of the EU's "Cyber Europe 2016" exercise. | | HCPN, CERTs, private sector | 2016 |
| 8 | Participation in the preparation and execution of NATO's "Cyber Coalition 2015" exercise | | EMA, HCPN, CERTs | 2015 |
| 9 | Implement national exercises including the private sector | | HCPN, CERTs | 2016 |
| 10 | Develop good practices, methods and tools for readiness at different levels (critical infrastructure, telecom operators/providers, large companies, administrations, SMEs) | | ANSSI, CERTs | 2015-2017 |

*Objective 4: Fight cybercriminality*

The fast evolution of digital infrastructure continuously generates new threats. It is therefore important to regularly assess if the legal bases in force are still adapted and if they allow to prosecute and sanction new forms of cybercrime.

Legal monitoring must identify the contradictions or discrepancies in laws, regulations and circulars, and harmonise the approach of all state actors.

The need for legal monitoring still derives from the cross-border nature of criminal acts which calls into question, to some extent, the principle of territorial application of legal rules. In fact, when it comes to crimes committed using a computer system or network, the number of places and countries involved in such fraudulent acts is likely to increase. The offence can be partly committed in a country and partly in another, or even in a third, while the offender can be located practically anywhere in the world. Therefore, the evolution of technologies and fraudulent behaviours needs to be closely monitored.

In order to be effective, legal monitoring should include the follow-up of initiatives launched amongst communities or even internationally. Indeed, the global nature of networks and systems requires a global response and any purely national approach would be doomed to failure.

*The fast evolution of digital infrastructure continuously generates new threats. It is therefore important to regularly assess if the legal bases in force are still adapted and if they allow to prosecute and sanction new forms of cybercrime.*

*Action Plan Objective 4*

| # | Action | Notes | Responsible party, Actor(s) | When |
|---|--------|-------|----------------------------|------|
| 1 | Continue the work of the "Cybercrime" working group. | | Prosecution service, PGD, ANSSI, CIRCL, GOVCERT. LU, RESTENA CSIRT, NCDP, SRE | 2015-2017 |
| 2 | Creation of a legal WG with the following missions:<br>• Analysis of the current legal framework<br>• Analysis of the provisions in force abroad<br>• Transposition of European directives and adaptations of the national legal framework | | Ministry of Justice, Prosecution service, SMC, NCDP, ANSSI, PGD, SRE | 2015-2017 |
| 3 | Continue international cooperation in the fight against cybercrime (EC3 Europol) | Purpose:<br>• Facilitate joint actions in the fight against cybercrime<br>• Data-merging Centre | PGD | 2015-2017 |
| 4 | Continue the cooperation with the EUCTF (European Cybercrime Task Force) | | PGD | 2015-2017 |
| 5 | Continue the cooperation with Interpol | via Europol | PGD | 2015-2017 |
| 6 | Continue the cooperation with the FBI | Via the Liaison Officer in Brussels | PGD | 2015-2017 |

*Objective 5: Inform, train and raise awareness of the risks involved*

Raising the awareness of public and private sectors of the risks involved and means of protection is an essential element of the strategy, which largely contributes to reducing potential vulnerabilities and motivating actors to participate actively in the strengthening of security. It is important to make all the actors concerned come to the realisation that they can amply protect themselves against threats and potential dangers by adopting a responsible behaviour.

In the medium term, improved security in cyberspace will not happen without fostering the accountability of all the actors of the sectors in question. A large proportion of the vulnerabilities exploited by cybercriminals are made possible by negligence in the design and use of systems that are on the market. For example: the late publication and application of corrigenda, the non-compliance with procedures and the prevalence of convenience over security. The legislator, owners and operators of infrastructures as well as the users and providers of IT solutions will have to join efforts in order to secure the cyberspace for the benefit of all.

Any awareness-raising, education and information related process should be addressed to all the actors, namely:

• End users and more specifically:
  - children and young people;
  - students, parents, educators, teachers;
  - civil servants and public employees;
  - private employees;
  - freelancers and other professionals;
  - IT professionals, specialists and other ICT experts.

• Decision-makers and private executives with responsibilities
  - of the private sector.

• Providers
  - of physical hosting services (data centres);
  - of communication services;
  - of cloud computing services;
  - of electronic signature services;
  - of dematerialisation and electronic archiving services;
  - of integration and ICT equipment supplying services;
  - of ICT consultancy services;
  - of information security services.

- Operators of critical infrastructures:
  - decision-makers;
  - operators of infrastructures;
  - IT professionals;
  - non-expert employees/users.

The constant evolution of the threat means that citizens and enterprises must regularly be informed of the extent and nature of ongoing attacks, but also of the tools to be implemented and procedures to be applied in order to be effectively protected.

Training will allow interested parties to update their knowledge of potential threats and means of protection.

*The constant evolution of the threat means that citizens and enterprises must regularly be informed of the extent and nature of ongoing attacks, but also of the tools to be implemented and procedures to be applied in order to be effectively protected.*

## Action Plan Objective 5

| # | Action | Notes | Responsible party, Actor(s) | Schedule |
|---|--------|-------|-----------------------------|----------|
| 1 | Make the CASES training compulsory for each new civil servant | | CSB and MFPRA, CASES, external service provider | 2015 |
| 2 | Include methodological aspects in the CASES training programme | | CASES, external service provider | 2016 |
| 3 | Introduce compulsory training in primary and secondary education | | CASES, Ministry of National Education, Childhood and Youth | 2016 |
| 4 | Establish an inventory of training obligations incumbent on service providers | | CASES, professional associations in the field of ICT and/or information security | 2015-2016 |
| 5 | Develop an attractive training programme for SMEs | | CASES, Chamber of Trades | 2015-2016 |
| 6 | Promote post-secondary training in the field of security | | UNI, MESR | 2015-2017 |
| 7 | Develop a raising-awareness/training programme for decision-makers | | CASES, Chamber of Trades, Chamber of Commerce, Fedil | 2015-2016 |
| 8 | Develop a training programme for operators of critical infrastructures | | ANSSI, GOVCERT, CASES, CI operators | 2016-2017 |

*Objective 6:*
*Implement norms, standards, certificates, labels and frames of refer-*
*ence for requirements for the government and critical infrastructures*

Information security requires actors to have a suitable behaviour as well as the implementation of appropriate organisational and technical measures. Prior to the establishment of preventive security measures, a risk analysis must be performed to assess potential losses related to a compromised availability, integrity or confidentiality of assets. It must also be borne in mind that the major impact is often the loss of trust and reputation.

Implementing consistent and effective secure systems within the State requires the existence of methods of risk analysis, policies and security standards which are consistent and adapted to specific contexts. Organisational and technical security measures described in these policies and standards must be applied by the different administrations.

*Implementing consistent and effective secure systems within the State requires the existence of methods of risk analysis, policies and security standards which are consistent and adapted to specific contexts.*

Similarly, critical or sensitive infrastructure operators will be invited to comply with a number of frames of reference, respectively to target sectoral certification so as to prove their maturity in terms of security.

*Action Plan Objective 6*

| # | Action | Notes | Responsible party, Actor(s) | Schedule |
|---|--------|-------|------------------------------|----------|
| 1 | Risk analysis for priority sectors | | HCPN, ANSSI, SMILE | 2015-2017 |
| 2 | Implementation of SSI norms and standards for classified and unclassified networks of the public sector and critical infrastructures | | ANSSI, HCPN | 2015-2017 |
| 3 | Establish an inventory of standards and good practices in the different sectors | | ANSSI,CSSF, ILR, NCDP, ILNAS | 2015-2016 |

*Objective 7:*
*Strengthen cooperation with the academic and research sphere*

The University and public research centres specialised in ICT have developed cutting-edge skills in the security of information systems, "big data" and the use of information systems for the purpose of controlling the quality of services.

It is appropriate to systematically put these skills to use for the benefit of improving the national cybersecurity environment, both through research per se and training.

In this same context, it must be ensured that these skills continue to be developed in close consultation with the private sector and government authorities, while promoting international cooperation academically.

In the medium term, University courses or training modules could be developed at the University of Luxembourg, together with all actors – private and public – to adopt a response to cybersecurity needs while taking into account national specificities.

*It must be ensured that these skills continue to be developed in close consultation with the private sector and government authorities, while promoting international cooperation academically.*

*Action Plan Objective 7*

| # | Action | Notes | Responsible party, Actor(s) | Schedule |
|---|--------|-------|------------------------------|----------|
| 1 | Develop protocols and cryptographic algorithms | | UNI, CRPs | 2015-2017 |
| 2 | Develop a cybersecurity training programme | | UNI, CRPs | 2015-2017 |

## Implementation

This strategy defines the objectives which are important to achieve in the next three years. Each objective is complemented by an action plan outlining concrete measures to be implemented following a definite time frame, as well as the actors called on to contribute to their implementation.

The cybersecurity strategy is intended to evolve over time. It will be periodically revised in order to be adapted to new realities.

*The cybersecurity strategy is intended to evolve over time. It will be periodically revised in order to be adapted to new realities.*

# GLOSSARY

# GLOSSARY

**ANSSI**
National Agency for the Security of Information Systems: national authority for the security of classified and unclassified information systems installed and operated by the State and operators of critical infrastructures for their specific needs.

**BEE SECURE stopline**
Centre for reporting illegal and/or harmful online content.

**CASES**
Cyberworld Awareness & Security Enhancement Services: programme of the SMILE economic interest grouping.

**CC13**
Cyber Coalition: NATO annual cyber-defence exercise.

**CCDCoE**
Cooperative Cyber Defence Centre of Excellence: NATO Centre of Excellence for Cyber Defence in Tallinn (Estonia).

**CDMB**
Cyber Defence Management Board: body of NATO in charge of cyberdefence affairs of the alliance.

**CE2012**
Cyber Europe 2012: bi-annual exercise of the EU.

**CERC**
Cyber Risk Assessment Unit: group of cyber experts created in the context of the PIU Cyber.

**CERT**
Computer Emergency Response Team: team taking charge of cyber security incidents.

**CIRCL**
Computer Incident Response Centre Luxembourg: CERT in charge of cyber incidents in the private and communal sectors, operated by the SMILE grouping of economic interest.

**CSB**
Cybersecurity Board: Created by decision of the Governing Council on 18 July 2011. It is the Luxembourg Cybersecurity Board's mission to develop the national strategic plan to combat cyber attacks. It is chaired by the Minister of Communications and Media.

**CSIRT**
Computer Security Incident Response Team, synonym of CERT.

**CSSF**
Financial Sector Supervisory Commission.

**CTIE**
State Information Technology Centre.

**EC3**
European Cybercrime Centre.

**EFMS**
European Forum for Member States on CIIP.

**EMA**
Army Chief of Staff.

**ENISA**
European Network and Information Security Agency.

**EUCTF**
European Cybercrime Task Force.

**FOP**
Friends of the Presidency.

**GOVCERT**
Government CERT: CERT taking charge of cybersecurity incidents in the public sector and critical infrastructures. Created by Grand-Ducal Decree of 30th July 2013 determining the organisation and powers of the Government computer emergency treatment centre, also referred to as "Computer Emergency Response Team Gouvernemental".

**GT**
Working group.

**HCPN**
High Commissioner for National Protection.

**ICT**
Information and Communication Technology.

**ILNAS**
Luxembourg Institute for Standardisation, Accreditation, Security and the Quality of Products and Services.

**ILR**
Luxembourg Institute of Regulation.

**ISP**
Internet Service Provider.

**MISP**
Malware Information Sharing Platform.

**MONARC**
CASES methodology of risk analysis.

**MoU**
Memorandum of Understanding.

**NCSS2**
National Cyber Security Strategy 2.

**NCDP**
National Commission for Data Protection.

**PGD**
Grand Ducal Police.

**PIU**
Emergency response plan.

**PSF**
Professionals of the Financial Sector.

**PKI**
Public Key Infrastructure - LUXTRUST in this case.

**RESTENA**
Teleprocessing Network of National Education and Research.

**SMC**
Media and Communications service.

**SMILE**
"Security Made In Lëtzebuerg": economic interest grouping of major operators of the BEE SECURE, CASES and CIRCL governmental initiatives. SMILE is composed of three members: the State (represented by three Ministries: the Ministry of the Economy, the Ministry of the Family, Integration and the Greater Region, the Ministry of National Education, Childhood and Youth), the SYVICOL (Trade Union of Cities and Communes of Luxembourg) and the SIGI (Intercommunal Trade Union of Computer Management).

**SSI**
Security of information systems.