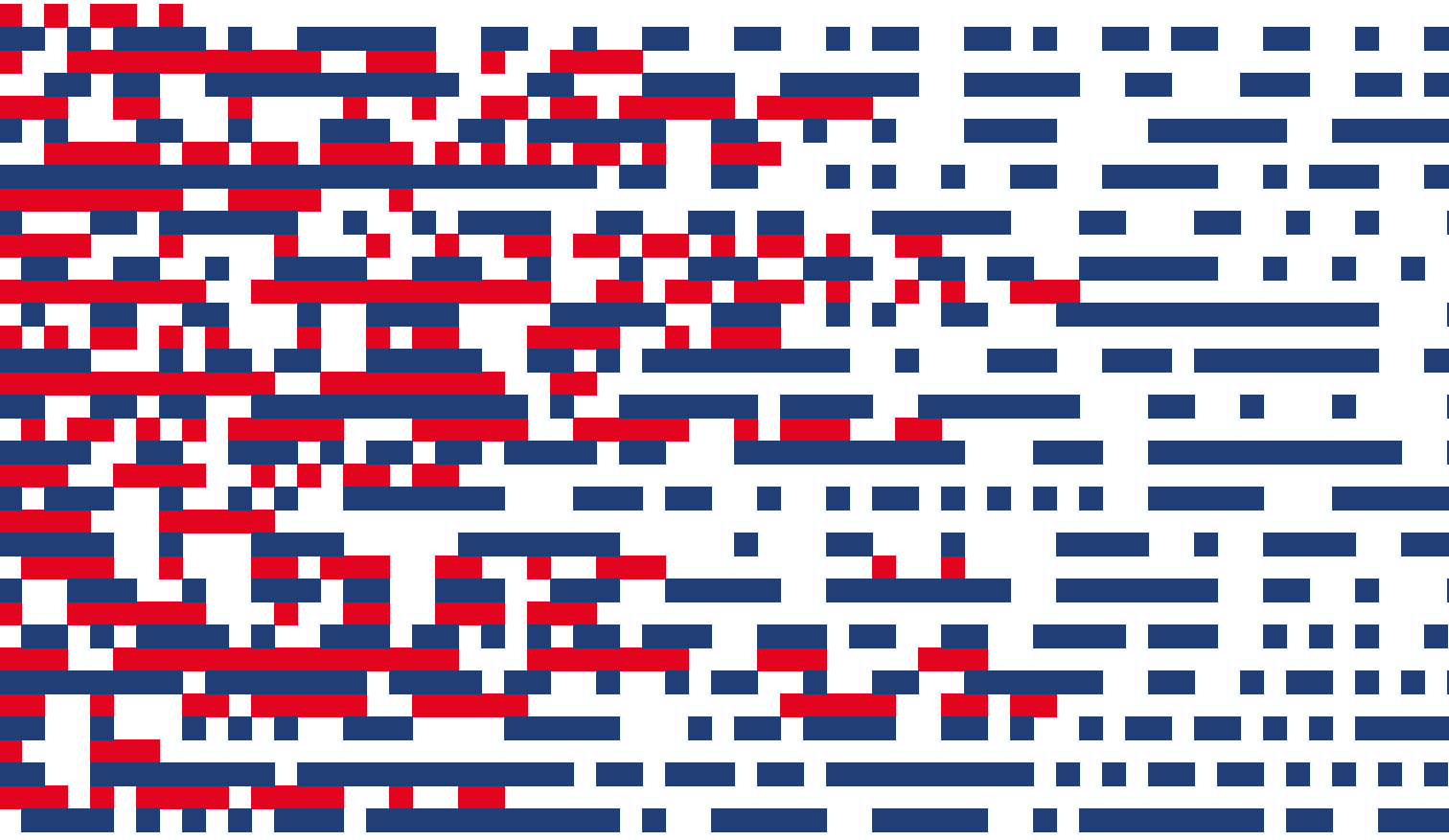
NATIONAL CYBERSECURITY STRATEGY III



ENGLISH VERSION

Approved and made enforceable by the Government Council on january 26, 2018.

· FOREWORD BY THE PRIME MINISTER, MINISTER OF STATE ·

I am pleased to submit to you the new national cybersecurity strategy for the 2018-2020 period. It illustrates the Government's intentions in response to the changes and challenges that characterize a digital environment in constant change.

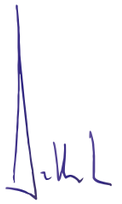
The strategy has been developed by a task force under the leadership of the High Commissioner for National Protection. The task force is composed of representatives of the State's Information Technology Centre, the Governmental Computer Emergency Response Centre (GOVCERT), the National Agency for the Security of Information Systems (ANSSI), the Media and Communication Unit, the Ministry of Economy, the Ministry of Foreign and European Affairs, the Luxembourg Defence, the State Intelligence Services and the Grand Ducal Police Force.

It reflects, at national level, the objectives of the cybersecurity package that the European Commission has just published and is part of the continuity of a series of measures recently adopted by the Government, whether at the level of cyber attack management procedures, cybersecurity governance or the promotion of cybersecurity to companies with the inauguration of the "Cybersecurity Competence Centre". It is worth mentioning, in this context, that as a result of the ambitious digital agenda that the Government has been pursuing in recent years, the report of the World Economic Forum has ranked Luxembourg number 1 among 137 countries as part of an assessment based on technological skills.

This third strategy takes into account the experience gained in the context of the implementation of the second strategy adopted in March 2015, and the conclusions drawn from a general analysis of the cyber threat. It sets the framework within which full advantage is taken of new digital opportunities, while providing a response to the risks associated with ever-growing connectivity.

To this end, in line with the "Digital Lëtzebuerg" initiative, the strategy seeks first and foremost to strengthen public confidence in the digital environment, in order to allow citizens to enjoy it to the fullest. It is also aimed at enhancing the security of information systems, improving the ability to identify cyber attacks, protecting critical digital infrastructure and raising stakeholders' awareness of resilience. Finally, it does not only focus on security and raising awareness, but also takes into account strategic issues of the digital infrastructure for our economy and turns cybersecurity into an economic attractiveness factor.

Xavier Bettel



NATIONAL CYBERSECURITY STRATEGY III

TABLE OF CONTENTS

INTRODUCTION

NATIONAL CYBERSECURITY STRATEGY III

· INTRODUCTION ·

The evolving nature that characterizes the digital environment in broad terms and in particular information and communication technologies, has a direct impact on our daily lives. Nowadays, we are accustomed to the emergence and the large-scale and especially very fast development of new technologies, as well as the new risk vectors that accompany this evolution. The adaptation of our society to the massive transformations that accompany this constantly changing digital landscape remains a complex process.

In the run-up to the end of the period covered by the second national cybersecurity strategy, in order to develop a new national cybersecurity strategy, the Cybersecurity Board (CSB) commissioned a task force operating under the authority of the High Commissioner for National Protection (HCPN) and composed of representatives of the State's Information Technology Centre (CTIE), the Governmental Computer Emergency Response Centre (GOVCERT), the National Agency for the Security of Information Systems (ANSSI), the Media and Communication Unit, the Ministry of Economy, the Ministry of Foreign and European Affairs, the Ministry of Defence, the State Intelligence Services and the Grand Ducal Police Force. The aim is to respond to the far-reaching changes referred to above and consolidate public confidence in new technologies, notwithstanding the emergence of more and more cyber attacks of a very varied nature, often organized on a transnational level. Another concern which is inherent in the strategy is to create an environment that allows – for the sake of the development of digital economy – to support actively the fact of delving deeper into new topics such as the internet of things, artificial intelligence, the technology of advanced algorithms or the ubiquity of potential dual-use technologies.

The new national cybersecurity strategy shows that the government is aware of both the opportunities and risks which are inherent in new technologies. It is in this context that the strategy, which covers the 2018-2020 period, is structured around the three following main guidelines:

- **the strengthening of public trust in the digital environment** in order to allow Luxembourg's digital transition towards a "Smart nation" model, which will be sustainable from an economic, social, environmental and political point of view, particularly in respect of the UN sustainable development programme targets for 2030;
- **the protection of digital infrastructure**, in order to ensure the availability of essential services, as well as information integrity and confidentiality, and finally
- **the promotion of the economy**, particularly by creating an environment that is conducive to the establishment and development of companies which are active in the digital field.

NATIONAL CYBERSECURITY STRATEGY III

NATIONAL CYBERSECURITY STRATEGY III

NATIONAL CYBERSECURITY STRATEGY III (NCSS III)

The new version of the national cybersecurity strategy takes into account the feedback of the strategy covering the period 2015-2017, the details of which are included in the appendix from page 21, and the findings of a general analysis on cyber threats which is appended from page 26.

The topic of cybersecurity covers a wide range of measures which could be taken to improve the resilience and defence of computer systems and networks, on the one hand, and of digital technologies in general terms, on the other hand, against a very wide variety of cyber attacks.

The Government has set up an interministerial coordination committee in order to sustain cybersecurity governance and facilitate the implementation of the NCSS III objectives. A number of objectives of the second strategy remain relevant and are therefore included herein, but are adapted to the current environment.

DEFINITION OF CYBERSECURITY[1]

"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies can be used to protect the cyber environment, its organization and its user's assets. Organization and user's 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 organization and user's 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."

[1] *Recommendation ITU-T X.1205 in accordance with UN resolution 181 (Guadalajara/2010)*

1. CYBERSECURITY GOVERNANCE

The current and future challenges related to cybersecurity can only be tackled by means of efficient and effective national cyber governance. Considering Luxembourg's cyber defence commitments at the level of NATO and the European Union, European and international cooperation and information-sharing agreements at different levels, the impact of the implementation of the EU Directive on the security of networks and information systems, as well as the horizontal character of topics pertaining to cybersecurity, the existing governance model will be strengthened by the setting up of an interministerial cyber prevention and cybersecurity coordination committee.

MAIN STATE BODIES INVOLVED IN NATIONAL CYBERSECURITY

As a result of the large number of sectors and areas affected by cybersecurity policies, the topic is subject to the accountability and the responsibility of several state bodies.

- The Ministry of Economy is responsible, pursuant to the Grand Ducal Decree of 28 January 2015 on the constitution of ministries, for computer security, risk awareness and private sector vulnerabilities. In this context, the economic interest grouping "Security Made in Luxembourg" (GIE Smile) – a platform promoting cybersecurity – notably operates initiatives of CASES (promotion of information security in companies), C3 (National Centre for Cybersecurity Skills) and the CIRCL (Coordination and Post-Incident Action Unit), the latter also acting as CERT for private and non-governmental entities and communes.
- The Luxembourg Defence (Ministry of Foreign and European Affairs (MAEE) - Defence Management and the Luxembourg army) is in charge of any cybersecurity elements that fall within national responsibilities and obligations generated within NATO and the EU.

- The Ministry of State - Media and Communication Unit follows the Telecom Council which discusses at European level, both the European cybersecurity strategy and the "cybersecurity package". The Media and Communication Unit also coordinates the work of the Cybersecurity Board which, under the Grand-Ducal Decree of 28 January

2015 on the constitution of ministries, is subject to the responsibility of the Ministry of State.

- The Ministry of Foreign and European Affairs coordinates the work of the horizontal "Cyber" work group of the Council of the European Union, which has just developed the "cyber diplomatic toolbox" adopted in June 2017, which is likely to evolve, while the international dimension of threats, as well as the response to any such threats, will be amplified.

- The State Information Technology Centre has its mission governed by the amended organic law of 20 April 2009. Its mission is, among other things, to ensure, as part of its responsibilities, computer security, the management of electronic and computer equipment and appropriate security, the administration of the state's computer network, as well as the production of secure administrative documents.

- As for the State Intelligence Service, its mission is to search, analyse and process information on cyber threats insofar as they may be related to espionage, intrusion, terrorism, extremism with a violent tendency and the proliferation of weapons of mass destruction or defence-related products and technologies related thereto.

- The High Commissioner for National Protection is involved in the management of a cyber crisis. Its action is established on the basis of the plan for emergency response in the face of attacks against information systems, from the moment the crisis is likely to have serious consequences for a part of the territory or the population of the Grand Duchy. It also acts as the National Security Agency for Information Systems, the mission of which is to establish guidelines for information security (ANSSI). The Governmental Computer Emergency Response Centre (GOVCERT), which also acts under the responsibility of the High Commissioner for National Protection, is involved in the management of major security incidents affecting networks and communication systems.

- The mission of the above entities is, of course, complemented by the actions of judicial authorities and services of the Grand-Ducal Police, which are particularly involved in the fight against cybercrime.

INTERMINISTERIAL COORDINATION COMMITTEE FOR CYBER PREVENTION AND CYBERSECURITY

Given that the cybersecurity topic covers a wide range of areas and falls within the assignment of several state entities, on 13th December 2017, the Government decided to bring together key players to set up an interministerial committee in charge of cybersecurity coordination at national level. The committee shall coordinate, alongside the Cybersecurity Board – which plays a rather strategic role –, pragmatic initiatives as part of cyber security.

To this end, the committee's mission is as follows:

- to ensure the consistency of actions and initiatives in the areas of cyber prevention and cybersecurity;

- to coordinate the implementation of initiatives and measures decided at European and international level with respect to cyber prevention and cybersecurity;

- to monitor the implementation at national level of policies decided at European and international level;

- to advise the Government on cyber prevention and cybersecurity by identifying issues and priorities for further investigation in this area, as well as players in charge of their implementation;

- to discuss the positions to be adopted by national representatives in European and international forums on cyber prevention and cybersecurity.

The committee consists of members of the main state entities involved in national cybersecurity, and the committee is chaired by the High Commissioner for National Protection. The High Commissioner also acts as secretariat.

2. GUIDELINES OF THE NATIONAL CYBERSECURITY STRATEGY

The priority objectives are listed in the following three guidelines:

- **BUILDING PUBLIC CONFIDENCE IN THE DIGITAL ENVIRONMENT**
- **PROTECTING DIGITAL INFRASTRUCTURES**
- **PROMOTING THE ECONOMY.**

GUIDELINE NO. 1: STRENGTHENING PUBLIC CONFIDENCE IN THE DIGITAL ENVIRONMENT

Each citizen must be able to take full advantage of the opportunities offered by information and communication technology (ICT). In this context, it is important to maintain the confidence of users in these technologies at a high level, while knowing that this trust is influenced by external factors (e.g. cyber attacks, online sale frauds, etc.).

Digital confidence-building depends on a good perception of risks associated with the use of ICT, while being able to estimate its interest and opportunities. The consolidation of public trust depends on a good command of the digital value chain, which can only be guaranteed by ensuring ICT quality and security. It is important, in this context, to successfully combine respect for privacy and information security with the development of strategic areas such as cloud computing, big data and the Internet of things. It is also with this in mind that it is in Luxembourg's best interest to follow, or even contribute to the development of the state of the art in the key area of artificial intelligence (AI).

THE IMPLEMENTATION OF GUIDELINE NO. 1 DEPENDS ON THE ACHIEVEMENT OF FIVE OBJECTIVES.

OBJECTIVE 1 : KNOWLEDGE-SHARING BETWEEN ALL STAKEHOLDERS

There are too many users – both natural and legal persons – who are victims of the most common computer attacks. In spite of the multiple efforts made to raise awareness in recent years, it will be necessary to further raise users' awareness of the potential consequences of a digital threat.

Good practice guides, including behavioural, organizational, and technical measures will be drawn up and published in several languages.

OBJECTIVE 2 : DISSEMINATING INFORMATION ON RISKS

All interested parties will be informed appropriately on the level of risk applicable to the specific environment in which they operate. The Government thus intends to disseminate information on websites that users can access and which are adapted to the various target audiences.

The purpose is to inform the different categories of users on the latest developments with respect to threats, vulnerabilities and the effectiveness of security measures; information that is essential for the achievement of objective and comparable risk analysis.

Systematic dissemination of information on threats, vulnerabilities and common security measures should allow information security managers to draw conclusions for a given field of activity, in view of identifying measures that are appropriate for a specific threat, while being proportionate compared to the level of safety to be achieved. In addition, such information could be used usefully, for example, by the insurance industry to create new products meeting the needs of citizens and the SME sector.

OBJECTIVE 3 : RAISING AWARENESS OF ALL THE PARTIES CONCERNED

Raising awareness of information security is a process with multiple tasks. Many initiatives and efforts have already been initiated in this context. However, a significant part of the population is still not aware enough of the risks and weaknesses in the digital world.

Alongside knowledge sharing and the dissemination of information, efforts to raise awareness will be intensified, both with regards to young people and adults, both in the private and public sector, with special emphasis on businesses that will be appointed operators of critical infrastructures, in accordance with the law of 23 July 2016 for the establishment of a High Commissioner for National Protection.
Efforts to popularise information on information security will continue, in order for users to grasp the subject more easily.

Outreach programs will also be made available through various media: websites, print-outs, presentations, animations, videos and interactive media.

OBJECTIVE 4 : RESPONSIBLE DISCLOSURE

A model of "responsible disclosure", allowing the disclosure of a detected computer vulnerability, while giving the parties concerned a deadline to correct the vulnerability prior to its disclosure, will be implemented in Luxembourg. This could be of interest, especially in the field of academic and private research: the development of a work environment with specific rules to increase legal certainty for the benefit of researchers in the field of information security.

OBJECTIVE 5 : COMBATING CYBERCRIME

Public confidence in the digital environment is enhanced in the presence of a successful fight against illegal digital activities.

In the face of the continued growth of cybercrime in Europe and across the world, Luxembourg will remain vigilant in its fight against abuse and theft of digital tools, and will continue to implement the necessary measures to protect its digital infrastructure.
Strengthening police training and training magistrates specialized in the fight against cybercrime is being envisaged.

Cybercrime increasingly takes advantage of organised crime structures and in particular of their networks and financial systems. To limit and put an end to the development of online fraud, collaboration between the world of computer security experts (CERTs, etc.) and the financial sector (banks, CSSF, etc.) will be intensified. Stakeholders will examine the opportunity of setting up a specialized unit aimed at proposing measures to dismantle the financial structures of cybercrime.

Since national judicial authorities are competent in the event of attacks made through servers located in Luxembourg, even though the victim, respectively the offender, are not established in Luxembourg, there are also plans to strengthen cooperation between technical and legal experts in order to develop the necessary expertise in this field. The implementation of enhanced cooperation among technical specialists and legal experts will not only allow more effective analysis to be conducted, but also simplify highly complex records. Last but not least, such exchanges between experts will finally be put to good use to develop new training plans.

GUIDELINE NO. 2: DIGITAL INFRASTRUCTURE PROTECTION

More and more business processes of all sectors rely on infrastructure and digital services provided by specialized players. The transformation of Luxembourg into a digital nation speeds up that development and increases the need for security of infrastructure and services, in terms of confidentiality, integrity and availability. As a result, digital infrastructures play a quintessential role for the protection of the country's vital interests, because they replicate computer vulnerabilities in the physical world. That is why the Government pays special attention to the resilience of the digital infrastructure.

THE IMPLEMENTATION OF GUIDELINE NO. 2 DEPENDS ON THE ACHIEVEMENT OF SEVEN OBJECTIVES.

OBJECTIVE 1 : CENSUS OF ESSENTIAL AND CRITICAL DIGITAL INFRASTRUCTURE

The Government will be in charge of identifying critical IT infrastructures, to ensure the implementation of an adequate level of protection. The specific needs of protection will be, as appropriate, developed in close collaboration with operators and users of those infrastructures. The census will be done online with the transposition of the EU Directive on security of networks and information systems (NIS Directive), and pursuant to the provisions of the law of 23 July 2016 establishing a High Commissioner for National Protection.

OBJECTIVE 2 : SECURITY POLICIES

The application of information security policies (PSI-LU), which have been developed under the responsibility of the National Agency for the Security of Information Systems (ANSSI), will be recommended to critical IT infrastructure. Performing analysis of specific risks based on the ISO 2700x methodology will also be suggested to them. The CASES optimized method of risk analysis (MONARC methodology) will be offered to operators who have not yet implemented a risk management process.

OBJECTIVE 3 : CRISIS MANAGEMENT

The emergency response plan to attacks against the information systems or in the event of vulnerable technical information systems (Cyber ERP) has been tested within the framework of the management of recent digital incidents. The Cyber ERP will continue to be adapted in the light of developments in the digital environment.

The new technical procedures and measures included in the emergency response plan will be implemented as a priority. To this end, the High Commissioner for National Protection and the Cyber Risk Assessment Unit will contact public and private sector operators that are considered essential for the management of certain types of crisis, in order to develop operational plans per measure (OPMs). The OPM has a contact list of persons involved in crisis management. It then lists a series of predefined measures that need to be activated in the event of a crisis. Finally, it includes a description of the possible impact of activating a measure predefined on other systems. OPMs allow operators to implement predefined measures swiftly and efficiently in the event of a crisis associated with them.

OBJECTIVE 4 : STANDARDIZATION

Standardization determines common technical language, both at European and international level. If applied to the field of cybersecurity, this unifying capability allows us to set definitions and needs, the state of the art in this area as well as reference architecture, while establishing by consensus requirements and specifications required to ensure a suitable level of security. This constantly evolving whole facilitates digital ownership, especially for Smart ICT developments (Cloud Computing, Big Data, the Internet of things, Blockchain, etc.).
National monitori
ng and investment in the development process of standards related to the field of cybersecurity will be strengthened, specifically in order to convert it into a strategic tool for the development of national digital confidence.

This approach will be carried out for formal technical standardization (ISO, IEC, ETSI, CEN-CENELEC, ITU-T), while taking into account the work developed by relevant fora and consortia identified in the context of cybersecurity.

The ILNAS (Luxembourg standardisation body) will unify and develop this strategic monitoring in order to report it at national level, in the interest of the implementation of a “smart nation”.

OBJECTIVE 5 : STRENGTHEN INTERNATIONAL COOPERATION

Close collaboration will be continued and strengthened at international level, on the one hand to exchange information on threats, vulnerabilities and the effectiveness of processes and, on the other hand, for effective prevention, reliable detection and efficient mitigation. At European level, the transposition of the NIS directive in all Member States will lead to harmonisation in the field of cybersecurity.

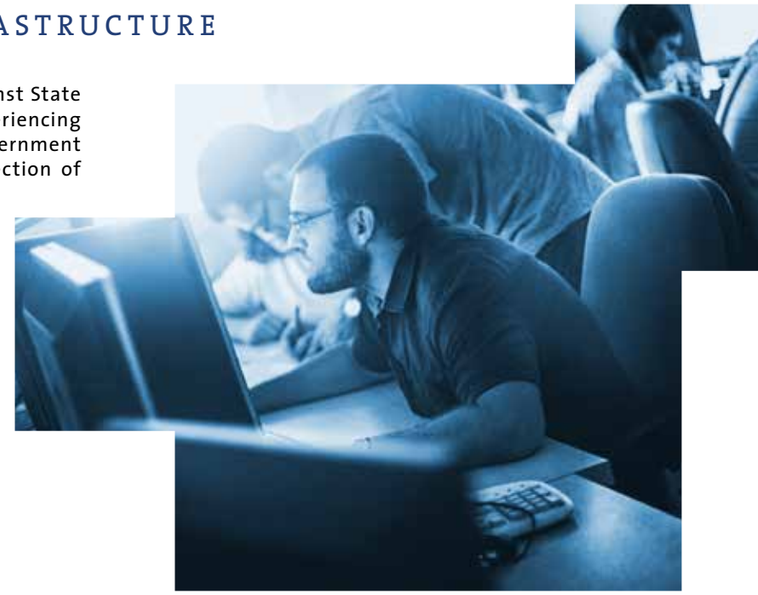
The latter should also be sought regarding the management of risk, norms and standards, accreditation and certification systems, as well as in the field of compliance management. Minimum harmonisation among European systems will be supported to facilitate free trade in services and products.

OBJECTIVE 6 : CYBER DEFENCE

In July 2017, the Government approved the guidelines of the cyber targets for 2025 and beyond. Further development of skills and abilities in the field of cyber defence has been retained among the objectives. The Luxembourg Defence will continue working on the definition and implementation of elements under its responsibility with respect to national and international cybersecurity strategies.

OBJECTIVE 7 : STRENGTHENING THE RESILIENCE OF THE STATE’S DIGITAL INFRASTRUCTURE

For some time, targeted attacks against State digital infrastructures have been experiencing significant growth in Europe. The Government will ensure a high standard of protection of State digital infrastructure.



GUIDELINE NO. 3
PROMOTION OF THE ECONOMY

Nowadays, cybersecurity has become a factor of economic attractiveness. It represents a competitive advantage. Faced with the professionalism of cybercriminals and the rapid evolution of technology and corollary threats, such intense and efficient collaboration between all public and private stakeholders is a guarantee of security.

The Government intends to implement the necessary measures to continue democratizing access to information security, including by pooling certain services and capitalizing on existing synergies. This approach is expected to reduce the complexity and costs associated with cybersecurity and consequently increase the attractiveness of an investment. This new guideline fits perfectly into the Government's "Digital Luxembourg" ambition, also confirmed in the context of the "TIRLUX"[2] strategy, i.e. to turn Luxembourg into a "Smart nation" by transforming digital-related challenges into opportunities for the country. Cybersecurity fits into this ambition through the Cybersecurity Competence Centre, set up and managed by SECURITYMADEIN.LU.

THE IMPLEMENTATION OF GUIDELINE NO. 3 DEPENDS ON THE ACHIEVEMENT OF 10 OBJECTIVES.

OBJECTIVE 1 : CREATING NEW PRODUCTS AND SERVICES

Luxembourg will continue to invest heavily in information technology infrastructure, clouds, fintech, biotech, spacetech and autonomous driving. The involvement of Luxembourg as a leader in the IPCEI project ("Important Project of Common European Interest"), High Performance Computing and Big Data[3] simply underlines Luxembourg's ambition to further diversify its economy towards digitalisation.

Public-private partnerships are strengthened. These partnerships allow us to combine the skills and expertise of stakeholders, in order to create products and services of high added value. They facilitate the creation of security services that comply with principles of proportionality and necessity, which are suitable in terms of complexity and the costs involved.

Along the same lines, the Government will offer new innovative services. Thus, offers composed of very high quality digital services and guarantees based on international conventions such as the Vienna Convention on diplomatic relations will be created. The development of products and services based on cryptographic technology will be promoted. They are essential for trusted third parties in the field of personal data management, as well as for strong authentication systems, electronic signatures and blockchain technology.

To pool risks and encourage victims of digital cyber incidents to seek help from experts to manage the incident and restore a system affected by a malicious act, insurance com-

[2] *See "Rifkin study"*

[3] *https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/white-paper-big-data-1-2.html*

panies will be encouraged to create specific products for the area of cyber insurance.

Probe services and products (intrusion detection systems) will be developed with a view to preparing situational reports on traffic in networks, so as to identify any anomalous or suspicious activity. These products and services will be developed in a spirit of "privacy by default" and "security by design".

The cybersecurity ecosystem will be federated actively and will address businesses, start-ups, incubators, financial players and regulators; the aim being to respond in a nifty and coordinated way to rapidly evolving threats, through qualitative, affordable and innovative products and services.

OBJECTIVE 2 : POOLING SECURITY INFRASTRUCTURES

Certain attacks, such as distributed denial of service (DDOS) attacks, have reached a level of disturbance so high that they call for national measures. These attacks require coordinated action from service providers. It is recommended to coordinate detection tools and poo infrastructures to some extent.

In order to mitigate a "denial of service" attack, an operator must be able, at the time of an attack, to instruct upstream operators to adapt their routing rules with the help of the Border Gate Protocol. At the same time, it must filter illicit communications belonging to the attack which has reached its network. The State considers, in this context, the possibility of investing in a national scrubbing centre (filtering of illegal communications infrastructure) that will be used when the filtering means of local operators are no longer sufficient.

OBJECTIVE 3 : REQUIREMENT BENCHMARKS AND CONTRACTOR

Recurring errors made in the design or configuration of computer systems are the source of many problems related to information security. The Government will release standard requirement benchmarks for the most widely operated systems. The contractor, or failing that, the buyer, will be encouraged to enforce the requirement benchmarks by the various parties involved.

OBJECTIVE 4 : CREATION OF THE CYBERSECURITY COMPETENCE CENTRE (C3)

The Ministry of the Economy and the economic interest grouping SECURITYMADEIN have a large reservoir of experiences, operational information and knowledge of threats, vulnerabilities and the effectiveness of protection measures that are implemented for the benefit of the entire economy through partnerships with the private sector. The latter should allow the development of innovative products and services in the field of information security.

The Cybersecurity Competence Centre will implement the necessary measures to support the development of three types of services: "Observatory", "Training" and "Testing", in close collaboration with private and public partners:

- "Observatory" services will focus on elements of a knowledge-driven economy in the field of cybersecurity, bringing together public and private efforts to provide information and trends in this area. Creating such services will greatly reduce the individual efforts and costs of cybersecurity, while increasing the effectiveness of protection measures. Thus, the Centre provides, in collaboration with its partners, not only technical information, but also an overview of contextualized and specific trade-specific threats, as well as protection mechanisms, metrics and key figures, which are necessary for good governance. The interpretation of threats in a specific context (ISAC: information sharing and analysis centre) is considered to be a new economic model to be developed with partners specialized in different areas such as finance, the Internet of things, the health sector or even space.

- Training-type services will allow us to go beyond what is currently available in terms of training centres in Luxembourg. Businesses and other players will be able to train their staff in an immersive environment, simulating computer incidents. This way, participants will be immersed in a concrete context to learn to work in multidisciplinary teams in order to acquire the legal, technical, organizational and behavioural skills necessary to identify and stem digital and business risks associated therewith. They will also learn to make notifications to respective regulators.

- Testing-type services will provide clients and partners with new possibilities of digital application testing. Thus, the "honeypots" networks of SECURITYMADEIN.LU will be made available to test software. Companies and partners will be able to test security management systems as part of scenario-based exercises. Start-ups will have access to the centre's testing infrastructure at low cost in order to validate their technology or service via a test environment simulating the real environment in which their product will have to survive, once manufactured.

OBJECTIVE 5 : RISK MANAGEMENT AND INFORMED GOVERNANCE

Risk management, as introduced since the second national cybersecurity strategy, is recognized as being the appropriate tool for good governance of cybersecurity. Indeed, it complies with the principles of proportionality and necessity, while it offers a risk and security analysis based on different points of view (companies, natural persons, clients). It allows us to understand and take into account the specific needs of the various stakeholders involved in the development of digital society.

This is why the Government will publish objective metrics invaluable to carry out objective risk analysis. This situational awareness will also facilitate the implementation of internal management governance based on metrics adapted to the circumstances.

With informed governance, through decisions based on objective and realistic situational reports, Luxembourg will be able to position itself as a modern, open, resilient and trustworthy digital nation.

OBJECTIVE 6 : TRAINING AND TRAINING AID

The Government intends to set up a university course in the field of information security in order to mitigate the risk of having a lack of experts in information security, which would constitute an obstacle to the development of our security's ecosystem.

There are plans to offer aid for specific training in the field of information security. Such aid will be associated with the lifelong training of experts, so as to encourage them to attend, for example, conferences and other relevant events.

The development of specialised training aimed at multidisciplinary teams will be considered with a view to addressing the shortage of experts in the security field, while taking into account the interconnectivity of tools.

OBJECTIVE 7 : COLLABORATION BETWEEN PARTIES IN CHARGE OF INFORMATION SECURITY

The opportunity of appointing a person in charge of information security within each state entity will be considered. A training plan for these people will be set up if necessary and exchange platforms for these experts will be created.

In the private sector, leaders will be encouraged to provide information security managers with resources to implement effective protection measures. Efforts will have to be made to improve communication and collaboration between teams in charge of different missions: information security, compliance, management, customer management, etc.

The Government will encourage cooperation between technical security and business process experts in order to create and exchange contextualized risk reports according to key areas.

OBJECTIVE 8 : COLLABORATION BETWEEN EXPERTS IN INCIDENT RESPONSE

The existence of numerous private and public entities specialized in the field of incident management is already an asset for Luxembourg. The Government will support the strengthening of cooperation between these specialized entities, which will facilitate the management of cross-sector or large-scale incidents.

To execute the requirements listed in the new regulations and directives (RGPD, Telecom, NIS), regulators will, in the future, have to become more involved in the management of incidents, which will result in more cooperation between regulators and specialized teams. This cooperation should increase the confidence of users in existing structures and thus improve the quality of digital incident management.

In addition, the Government will continue to promote the exchange of information between CERTs. The four public CERTs (GOVCERT. LU, circl.lu, HealthNet CSIRT and RESTENA-CSIRT) are known and contacted by their respective audiences. They have a large reservoir of information on existing threats and vulnerabilities, as well as on the actual effectiveness of security measures. The CERTs' good reputation contributes to the attractiveness of Luxembourg's economy.

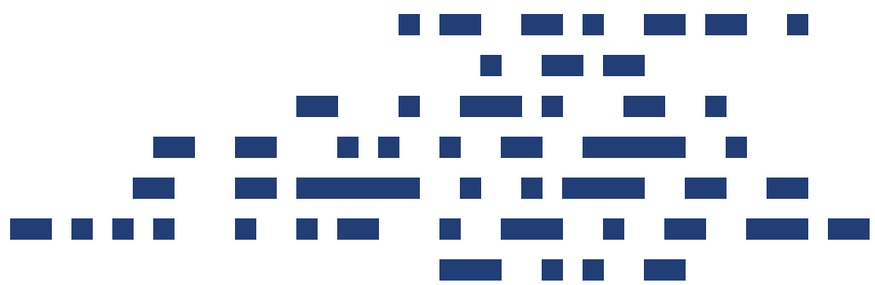
OBJECTIVE 9 : PRIORITY FOR RESEARCH: START-UPS

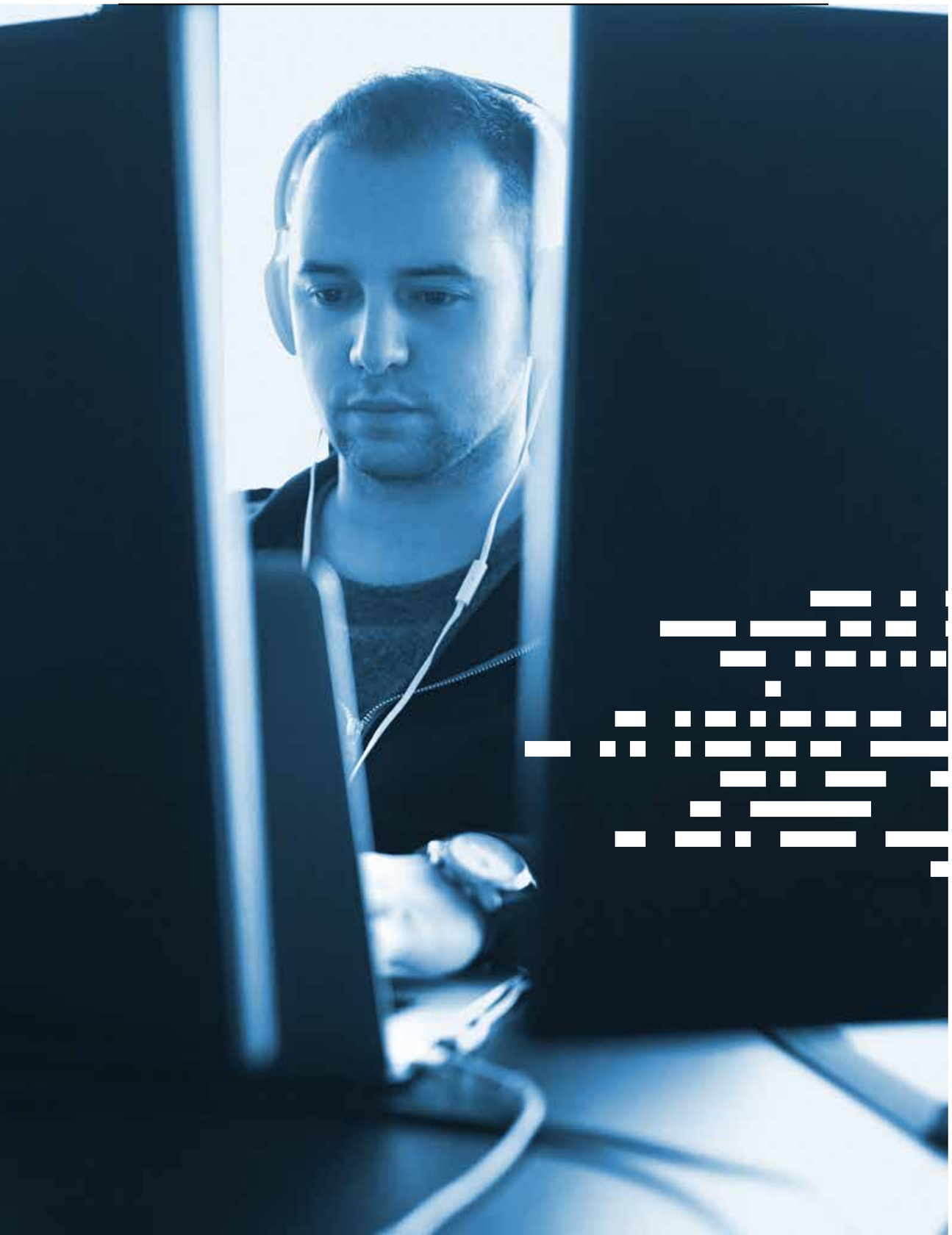
Start-ups offering innovative solutions feature among the needs identified within the Luxembourg digital security ecosystem. It will be taken into account for priorities in the field of research, by promoting the creation of start-ups.

OBJECTIVE 10 : CODE DISASSEMBLY AND IDENTIFYING VULNERABILITIES

It is intended to establish a framework to allow code disassembly ("reverse engineering") in Luxembourg, as well as penetration tests for the purpose of identifying vulnerabilities. These abilities will be useful to improve the interoperability of systems and to help ensure a higher level of security by identifying malicious software, spyware software, and so forth.

If serious vulnerabilities are published, public CERTs are allowed – at national level – to identify Internet-connected devices with these vulnerabilities and notify officials (e.g. Heartbleed vulnerability in OpenSSL).





NATIONAL CYBERSECURITY STRATEGY III

IMPLEMENTATION OF THE SCNS III

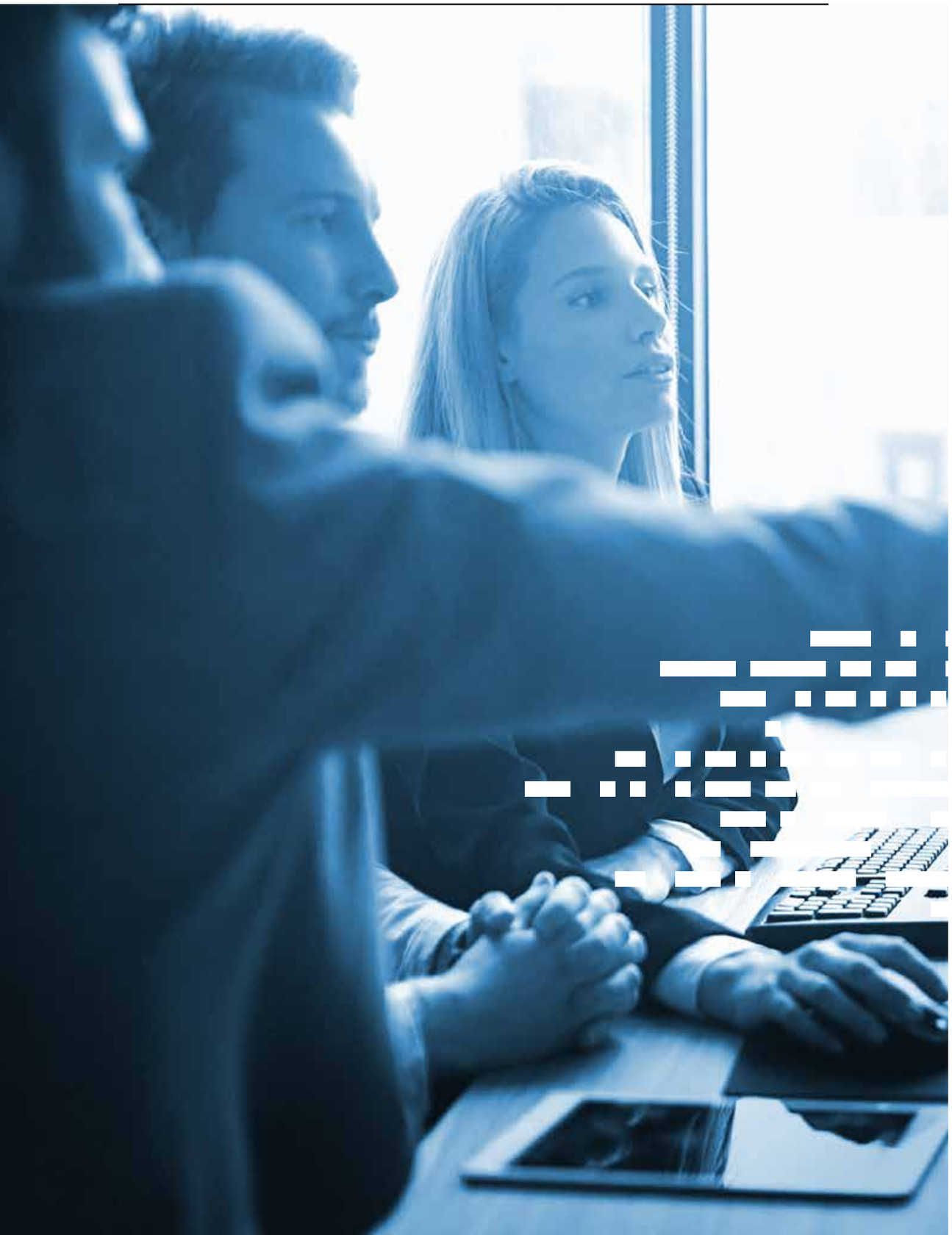
This strategy defines the objectives which are important to achieve in the next three years.

These objectives will be 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 action plan is available upon request to the High Commissioner for National Protection (e-mail: info@hcpn.etat.lu; Subject: #NCSS action plan).

The Cybersecurity Board and the interministerial coordination committee for cybersecurity accompanies the execution of the action plan.

The national cyber strategy is intended to evolve over time. Thus, the action plan will be periodically revised within the interministerial coordination committee, in order to remain relevant in a digital environment in constant change.



3. APPENDIX

FEEDBACK ON THE NATIONAL CYBERSECURITY STRATEGY II

The NCSS II had placed emphasis on information security as a challenge faced by society as a whole. Whether it is a company, public services or a citizen; each party bears responsibility for the construction of a secure digital society.

This appendix gives an update on the progress and implementation of the action points of the NCSS II, while it is clear that some of the actions are recurrent given that cybersecurity represents a continuous and dynamic process with an evolutionary character.

OBJECTIVE 1 : STRENGTHEN NATIONAL COOPERATION

Many initiatives have been taken at national level in order to intensify collaboration – both in terms of organisation and operations – between actors. Regular exchanges took place between the ANSSI, regulators and relevant ministries in order to establish a security policy for information at the level of the public sector and operators of critical infrastructures.

Frequent exchanges have been held about the protection of personal data in the field of cybersecurity, two intimately related topics that deserve to be partially addressed together.

At the operational level, ongoing exchanges took place between CERTs, thanks to modern and efficient collaboration tools. Incidents reported to the national CERT are managed through the joint efforts of the GOVCERT and CIRCL. Moreover, joint efforts to raise awareness have been organized to address decision-makers in the public and private sector about the importance of information security already bear their first fruits. Close collaborations to raise the awareness of children, teenagers, adults and the elderly, as well as that of supervisors have also been very successful. Since its implementation in 2015, the ANSSI has developed a security policy of General information for the State (PSI-LU). It also entered into cooperation agreements with various actors at national level.

The State Information Technology Centre (CTIE) and the Government's Communications Centre (CGC) have merged so as to improve

the provision of services with regards to the management of State secure communications. The information security portal www.cybersecurity.lu has been online since July 2017. It introduces the different actors of the sector and their respective sites. Its main purpose is to be the “single window” for information security.

Tools such as the Malware Information Sharing Platform (MISP) and the Analysis of Information Leaks (AIL) created by the CIRCL, or the CASES Diagnostics and MONARC risk analysis developed by CASES, contribute to greater collaboration and exchange on digital threats and vulnerabilities between the parties concerned. They also allow to gather information on the different degrees of maturity on the ground in the private and public sectors, for informed cybersecurity governance.

The use of risk analysis as a basic method for managing information security has now become standard in the Luxembourg. Several tools are available, including the MONARC tool which was released as an open source method. Towards the end of 2017, the ANSSI initiated a broad risk analysis project with State entities.

OBJECTIVE 2 : STRENGTHEN INTERNATIONAL COOPERATION

Luxembourg is represented in major information security groups and associations. Luxembourg entities have established close contacts internationally and entered into key partnerships with their counterparts in partner countries. The development of collaboration agreements with the BSI (Germany), the A-SIT (Austria), and the BSI (Switzerland) was possible and the agreements will be signed in 2018. Other agreements, including with France and Belgium, will be finalized in the first quarter of the year 2018. In the same vein, the GOVCERT and the CIRCL joined the CSIRT network and are part of the FIRST (Forum of Incident Response and Security Teams).

International cooperation has been successful, which was noticeable on the occasion of the Luxembourg Presidency of the Council of the European Union during which the GOVCERT was given the task to protect – alongside its international partners – the State’s digital infrastructure.

OBJECTIVE 3 : INCREASE THE RESILIENCE OF THE DIGITAL INFRASTRUCTURE

Luxembourg entities now have several modern risk analysis tools at their disposal.

Since March 2017, the MONARC method has been accessible to all in open source. Some metrics necessary for the implementation of objective risk analysis have been published. Depending on the degree of maturity and competence of organizations, different models of risk assessment are available.

Certain good sector practices have been developed. They were published through MONARC risk management models, respectively via security policies issued by the ANSSI. In addition, sites of state actors such as CASES offer both specific and general practices.

For several years, data has been collected on trends of threats, vulnerabilities and the effectiveness of security measures. This data, along with data acquired from diagnostics and risk analysis, provides information on the level of maturity of the various entities. They constitute a solid base to draw up reports of situational awareness. They can be used to contribute to governance (informed governance).

The cyber emergency response plan developed by the HCPN is operational. The plan has been updated by the HCPN on a regular basis as a result of the lessons learned from exercises and actual crises.

Luxembourg participated in the Cyber Europe 2016 exercise organised by ENISA (European Network and Information Security Agency). Luxembourg also contributed to NATO’s 2016 Cyber Coalition exercise as an observer, in close cooperation with Germany, and participated actively in it in 2017.

OBJECTIVE 4 : FIGHT AGAINST CYBERCRIME

Cybercrime-related work carried out by the cybercrime working group, chaired by the Public Prosecutor of Luxembourg, helped foster national cooperation and provided contextually important information to all entities involved.

Stakeholders indicated that they were satisfied with such good mutual collaboration, which has led to significant successes of investigation. Stakeholders unanimously agree that existing laws will have to be applied and adapted to the reality of the digital environment, and that cybercrime investigation procedures will have to be improved, especially in the context of electronic evidence manipulation, while the sharing of information between actors will have to be facilitated.

Thanks to good cooperation between the various actors involved and Europol’s support, police intervention in international cybercrime has become faster and more efficient.
As an extension of measures initiated in the context of the NCSS II, it will be essential to continue strengthening the capacity for action of judicial authorities, notably with respect to transnational cybercrime. In line with their respective mandates and assignments, the Prosecutor’s Office, the judicial investigation office and specialist services (investigation and computing expertise) of the judicial police must be able to investigate and prosecute cases of cybercrime, but also any other ICT-related offence. The following measures will be necessary to ensure effective action against acts of cybercrime:

- d’adapter les instruments d’entraide judiciaire internationale à la volatilité des preuves sur internet,
- adapting instruments of international legal assistance to the volatility of evidence on the internet,
- proceeding, to the extent possible, to a minimum harmonisation of the duration of data retention which varies strongly from one State to another,
- taking into account encryption possibilities given by appropriate tools and technology that may be used to ensure anonymity, making it difficult to identify a suspect (e.g. TOR, DARKNET),
- finding a solution with regards to the new means of payment (cryptocurrencies such as Bitcoin and derivatives) that allow criminals to easily evade authorities and hide transactions,
- creating opportunities to deal with the large volume of data to be analysed.

OBJECTIVE 5 : INFORM, TRAIN AND RAISE AWARENESS ON THE RISKS INVOLVED

Since the end of 2015, the CASES training has become mandatory for new government employees and officials, for all careers. This training course includes general methodological elements, such as the classification of information and risk analysis.

In addition to this basic training course, specialized and non-mandatory training courses are available from the INAP upon request.

Training courses are compulsory for schoolchildren and high school students. They focus on the "behavioural" aspects of information security and explain current good practices.

Together with its partners, CASES offers a wide range of training courses to professional audiences (users, managers, IT staff, trainers, etc.).

Specific training courses for decision-makers are also available.

Among the measures that were included in the second strategy and that will be taken up in the new strategy, it is worth mentioning the training programme for operators of critical infrastructures.

In Luxembourg, access to information security is largely facilitated by the State. Free or affordable training courses are offered for a very diverse audience. Much effort has been put into raising citizens' awareness, for example through workshops at lunchtime on weekdays, in the evening or at the weekend.

In line with the government's "Digital Luxembourg" strategy, notably the objective of raising the awareness of students to the appeal of new technologies and encourage their creativity, the "makerspaces" have been set up in co-curricular and educational institutions in order to spark the interest of young people for new information technologies since 2015. Some of these areas, including the "Base1" at the Geesseknäppchen Forum, can accommodate young people outside their school schedule. A few other projects are worth noting to highlight the Government's commitment to the development of digital skills in Luxembourg, which is a priority area. "Cryptoparty", "coder dojo", "Mak@ons", "hack4kids" and "Luxembourg Tech School". These "makerspaces" are grouped in the BEE CREATIVE initiative.

The "Kniwwelino" initiative has been launched recently. It is a microprocessor developed in Luxembourg and distributed to children and young people to familiarize them with the concept of programming and code security (for more information, go to: www.bee-creative.lu).

OBJECTIVE 6 : IMPLEMENT STANDARDS, NORMS, CERTIFICATES, LABELS AND FRAMES OF REFERENCE FOR REQUIREMENTS FOR THE GOVERNMENT AND CRITICAL INFRASTRUCTURES

Both in the public and private sector, risk analysis according to ISO/IEC 27005 has become the golden standard for managing information security. MONARC analysis were conducted in various priority sectors and there are plans to have the same exercises again at the pace of three tests per year. The risk management approach will be gradually generalized and extended to all sectors.

Security standards and guidelines for information systems have been implemented. They are published via the security policies issued by the ANSSI and will be finalized following the conclusions on the pilot project, which was carried out within the CTIE.

An inventory of standards and norms of information security has been developed. As this inventory is a living document, this action item will be incorporated into the new strategy.

OBJECTIVE 7 : STRENGTHEN COOPERATION WITH THE ACADEMIC AND RESEARCH SPHERE

A cross-cutting approach is required for the development of a cybersecurity training programme. Programmes have been created by many Luxembourg actors. The coordination of initiatives in this area will be further strengthened in the coming years.

The strengthening of cooperation in the development of cryptographic protocols and algorithms will be included in the new strategy, in order to clarify the means at Luxembourg's disposal to certify products in this area. In the absence of appropriate certification laboratories, partnerships with foreign organizations (neighbouring countries) are being pursued.

NATIONAL CYBERSECURITY STRATEGY III

ANALYSIS OF NATIONAL THREATS TO CYBERSECURITY

In recent years, entities with responsibilities in the area of cybersecurity have gained experience in observing and analysing a large number of attacks on computer systems. These observations allowed the actors to have a global view on the development of attacks over time. This analysis, which is not intended to be exhaustive, allows us to describe current and future cyber threats.

- **RANSOMWARES**

  At this time, the actors noted a significant increase of attacks with a purely financial goal, including attacks carried out through ransomware, i.e. malware introduced into a system to encrypt the digital files it contains, in order to sell the decryption key to the victim. Such illegal activities are facilitated by the emergence of virtual currencies such as Bitcoin, Ethereum, etc. One of the last major attacks by way of ransomware (Notpetya) has also revealed that it is possible to conceal a cyber sabotage attack by making it appear as ransomware.

- **ATTACKS BY DISTRIBUTED DENIAL OF SERVICE (DDOS) VIA THE INTERNET OF THINGS**

  The impact of DDoS attacks is more and more significant. This form of attack has now reached unprecedented significance as a result of the internet of things. Via tools like MIRAI, poorly secured internet-connected objects can easily be tracked and manipulated for very large-scale DDoS attacks. These tools are freely available on the internet, and they are often used for blackmail purposes. Such tools also allow to track and jeopardise internet-connected objects to perform mass surveillance or some kind of industrial espionage.

- **“BRICKERBOT”**

  Unlike other attacks such as DDoS attacks that prevent services from working for a while, “BrickerBots” are designed to destroy Internet-connected objects. These attacks can be very stealthy and difficult to detect. They are aimed at objects with poor protection and attempt, after successful authentication, to change the system settings so as to make the object unusable[4].

- **RISKS INHERENT IN THE DEVELOPMENT OF SMART CITIES AND HOME AUTOMATION**

  More and more components, which are part of our daily lives and are used to provide high-value services, are using information from real-time digital infrastructure. Smart cities are equipped with sensors collecting data and rely on information systems to optimize services that are characterized by their high degree of connectivity. The attacks against these infrastructures are likely to multiply in the presence of authentication systems and cryptographic protocols, which often do not meet the highest security level.

- **FAILURE TO COMPLY WITH MINIMUM SECURITY STANDARDS**

  A worrying element, which is currently felt in the cybercrime sphere, is the failure by the publisher of a software or a com-

[4] *https://arstechnica.com/security/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/*

puter tool, to comply with standards and better security objectives with regards to development. Computer security is not always a priority in the production of software and IT tools. Often distributed to millions of users such software is likely to be hacked in order to be manipulated and constitutes a real threat to a country's economy and security.

- **THREATS TO THE BUSINESS PROCESS**

  Recent attacks have shown that criminals are diversifying their actions and targets. Rather than harming by way of blackmail, exfiltration or data sabotage, they are now also targeting the business process. The shortage of skilled human resources in the field of IT must be considered as a vulnerability in this context. As a result, a vast number of companies have no choice but to outsource their IT systems to major players specialised in the field. It follows that the staff of these companies no longer have the skills necessary to protect business or industrial processes. This vulnerability can be exploited by the intrusion of malicious software that is used as a spying tool to provide its author with a company's internal details. The cybersecurity package presented by the European Commission in September 2017 seeks to address many of these threats.

- **REGULATORY THREATS**

  With "WannaCry", the massive resurgence of computer worms was felt across the entire world. The attack also showed that a risk can come from very strict regulatory obligations, which can give a false sense of security while linking major resources to ensure compliance with process standards.

  Alternatively, cyberspace is at risk of not being sufficiently regulated in some places because the law is not always able to keep pace with new technologies, which results in legal limbo situations where malicious activities thrive

- **DISCLOSURE OF INFORMATION ON SOCIAL NETWORKS AND SOCIAL ENGINEERING**

  Nowadays, the use of social networks is ever-increasing. Users disclose ample information on their private lives. The technique of social engineering is designed to access confidential information stored by companies in order to use it for criminal purposes or even espionage or sabotage. For example, some "all-cloud" companies migrate all data to a cloud, but do not have any secure procedures to contact the cloud service provider. Through social engineering, such flaws can easily be used by criminals, while strong authentication systems that would prevent this are not really common in cloud environments.

- **THREATS FROM A LARGE NUMBER OF INTERNET ACCESS TOOLS**

  Today, users frequently use their mobile phones to access the internet and carry out online transactions. Some smartphones are unfortunately difficult to protect and therefore represent an ideal target.

- **USE OF DIGITAL TOOLS AS A MEANS OF DESTABILIZATION**

  One of the threats that has recently had a great impact is the fact that digital tools are being used as a means of destabilization. It is worth mentioning here the group of hackers Shadow-brokers, who managed to steal a large number of computer tools from a security authority, tools used by it to access certain systems and networks. The use of such a weapon could have very serious consequences. This new threat aligns with situations that could paralyse the country and even entire regions. The idea of the digital sabotage and shut-down of an entire country through digital means is becoming more and more realistic. Armed forces around the world are preparing for such scenarios. The manipulation of elections by revelations from digital attacks or broadcasting false information through social networks has been seen in some countries over the past years, in the context of hybrid attacks, which partly falls within the scope of cybersecurity.

- **THREATS INHERENT IN THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE**

  Generally speaking, artificial intelligence will emerge in the context of designing and executing malicious software. It is currently a research subject in the world of academia and will soon be mature enough to be implemented in real malware, which will have the ability to adapt dynamically to security measures put in place by teams defending the networks and infrastructure of organizations.

GLOSSAIRE

AIL
Analysis of Information Leaks *(analyse des fuites d'information)*

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.*

BEESECURE stopline
Centre for reporting illegal and/or harmful online content

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

CC
Cyber Coalition*: annual Cyber Defence NATO 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 cyber defence affairs of the alliance.*

CE2012
Cyber Europe 2012*: biannual EU exercise.*

CERC
Cyber Risk Assessment Unit*: group of cyber experts created in the context of the Cyber Emergency Response Plan (ERP).*

CERT
Computer Emergency Response Team*: team in charge of cybersecurity 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

ENISA
European Network and Information Security Agency

ERP
Emergency Response Plan

EUCTF
European Cybercrime Task Force

FIRST
Forum of Incident Response and Security Teams

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 30 July 2013 determining the organisation and assignments of the Governmental Computer Emergency Response Team.*

GT
Working group

HCPN
High Commissioner for National Protection

Hybrid threat
In general, a hybrid threat is a combination of different types of threats, used together to achieve a common goal. In this document, the term exclusively refers to hybrid threats with a cyber element.

ICT
Information and Communication Technology

ILNAS
Luxembourg Institute for Standardization, 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

NCDP
National Commission for Data Protection

OPMs
Operational plans per measure

PGD
Grand Ducal Police

PKI
Public Key Infrastructure - *LUXTRUST in this case*

PSI-LU
Luxembourg information security policies

RGPD
General regulation on the protection of personal data

Smart nation
A multilingual, cosmopolitan, hyperconnected, enterprising and very well-trained nation.

SMC
Media and Communication Unit *("Service des Médias et des Communications")*

SMILE
"Security Made in Lëtzebuerg" *g.i.e. (economic interest grouping): major operators of the BEE SECURE, CASES and CIRCL governmental initiatives. SMILE consists of three members: the State (represented by three ministries: the Ministry of Economy, the Ministry of the Family, Integration and the Greater Region and the Ministry of National Education, Childhood and Youth), SYVICOL (trade union of cities and communes of Luxembourg) and SIGI (intercommunal trade union of computer management).*

SSI
Security of information systems

VERSION FRANÇAISE