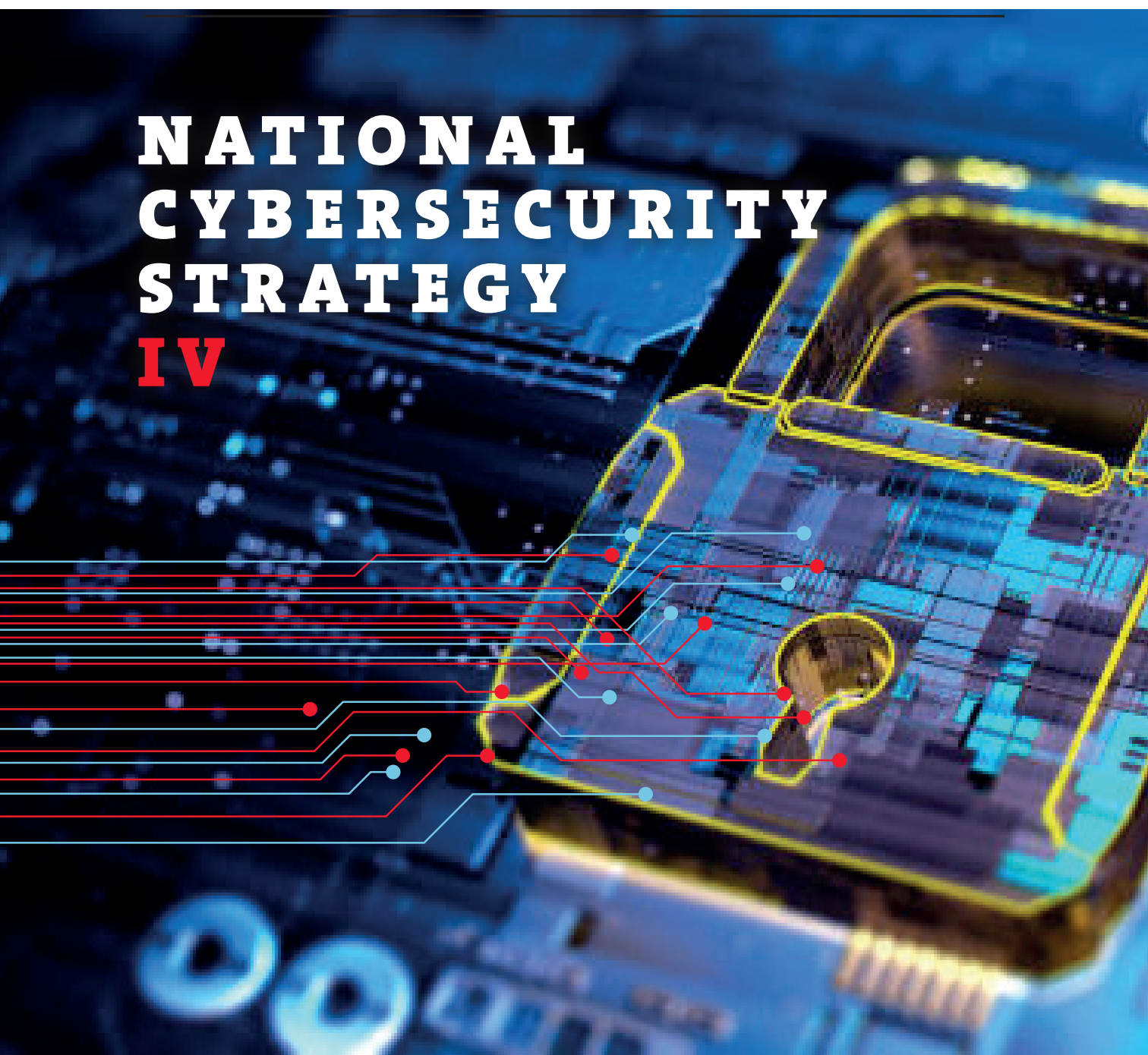# NATIONAL CYBERSECURITY STRATEGY IV

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

TABLE OF CONTENTS

· FOREWORD OF XAVIER BETTEL, PRIME MINISTER, MINISTER FOR COMMUNICATIONS AND MEDIA ·

The national cybersecurity strategy for the period up to 2025 sets out the guidelines underlying the projects that the Government intends to implement in order to secure cyberspace at all levels. It goes hand-in-hand with the digital transformation that characterises our economy and our society.

We are going through exceptional times in more than one way. We are witnessing the large-scale deployment of new technologies such as the fifth generation of mobile networks or new applications in the field of artificial intelligence. Existing digital infrastructures in Luxembourg, Europe and the world have been consolidated, enabling greater connectivity for more people with undeniable gains in reliability and availability, even though much remains to be done to ensure that no one is left behind in this digital revolution. At the same time, cybercriminals and other threat actors are taking advantage of these changes and using the new developments to increase attempts at intrusion, sabotage or online theft.

Building on the experience acquired in the context of the third strategy adopted in April 2018 and mindful to taking into account the numerous facets of cybersecurity, the new strategy was drawn up by a multidisciplinary working group chaired by the High Commission for National Protection and consisting of rep-

resentatives of the Ministry of Foreign and European Affairs, the Ministry of Economy, the EIG SECURITYMADEIN.LU, the Department of Media, Telecommunications and Digital Policy (SMC), the State Intelligence Service, the Luxembourg Regulatory Institute (ILR), the Directorate of Defence, the Government IT Centre (CTIE), the governmental CERT (GOVCERT) and the National Agency for Information Systems Security (ANSSI).

The aim of the cybersecurity strategy is to enable all actors to participate fully in a digital society and to access the new technologies in a secure environment. The measures that will be implemented in this context are designed in the first place to ensure that Internet users are aware and to strengthen their trust in the digital world. Furthermore, they consist in consolidating and strengthening the security and resilience of digital networks and infrastructures. Lastly, the strategy seeks to take account of cybersecurity as a factor of economic attractiveness and to complement the strategy of dynamisation that characterises the digital sector towards the continued development of a high-performance digital economy.

Xavier Bettel

INTRODUCTION

· INTRODUCTION: MAIN TRENDS AND THREATS ·

The world in 2021 is facing a multitude of international crises, ranging from the health crisis due to the COVID-19 pandemic, to the climate crisis, but also a deep crisis related to the social contract and political confidence in many countries. All these crises have complex but undeniable relationships with information and communication technologies and systems: society's dependence on the Internet and connectivity is growing. At the same time, the attack surface is becoming more diverse with the introduction of new technologies, while geopolitical rivalries are impacting the security of the digital space. Malicious acts are undertaken by a multitude of state and non-state actors against diverse targets: government administrations, businesses and citizens are victims of such acts.

With the massive introduction of fifth generation (5G) mobile data transmission, which promises to revolutionise connectivity worldwide, both for industrial and mission-critical applications and users/citizens, society will benefit from unprecedented speed of access to information and data availability, through a sharp increase in data rates, increased responsiveness thanks to a sharp reduction in latency and a significant improvement in connectivity capabilities. The transition to increasingly mobile technologies – the widespread use of smartphones and other portable, ever more affordable technologies is just one example – and the ever-increasing reliance on cloud computing solutions, as well as the continued development of the Internet of Things mean that human societies are increasingly connected but at the same time increasingly dependent on the availability and reliability of their data. Advances in quantum computing research suggest that the race between encryption and decryption technologies will continue.

This underlines the collective responsibility of political actors, ICT experts and industry, as well as citizens of all ages to become more independent and to use technology wisely, and even to demand trusted services and tools that meet their needs.

The dissemination of disinformation, hate speech or conspiracy theories undermines citizens' trust in their governments and often threatens social peace. Influencing operations – for political destabilisation purposes as well as for the purpose of increasing private income – such as micro-targeting on social networks, were unimaginable a few years ago: they have now become commonplace in the contemporary landscape of threats.

The development of a new national cybersecurity strategy is a prime opportunity to review the state's posture on information security awareness. In a spirit of openness and collaboration, the new strategy has been submitted for consultation to stakeholders at the national level: relevant ministries and administrations, private companies, professional information security researchers and civil society organisations.

While technological progress harbours risks, it also bears opportunities to be seized. The use of blockchain technology for many different applications makes it possible to develop trust solutions in political contexts where trust can be a scarce commodity. This Cybersecurity Strategy outlines how an integrated and comprehensive information security approach enables the government, private enterprises and citizens to fully seize the opportunities offered by the digital revolution. Improvements in the performance of cyber intrusion warning and response systems offered by, among other things, advanced algorithmic applications make life more difficult for advanced persistent threat groups; measures for mitigating denial of service attacks help thwart or cushion the disruptive effect on networks, applications, or other digital services.

Luxembourg will engage more proactively in positive cooperation initiatives at global level, such as in the United Nations Secretary-General's Digital Cooperation Action Plan. At European level, the EU's digital hub is in a process of consolidation in the Grand Duchy of Luxembourg. The national cybersecurity ecosystem is booming. This strategy is part of a continuous process of improving coordination and procedures in the field of information security and builds on the lessons learned from the three previous national strategies.

II.
NATIONAL CYBERSECURITY STRATEGY IV (2021-2025)

1.
OBJECTIVES AND PRIORITIES OF THE NCSS IV

STRATEGIC OBJECTIVES:

Luxembourg's fourth national strategy builds on the foundations of the three previous strategies. It comprises three strategic objectives, which each have several strategic priorities. Multiple concrete and measurable actions, which are set out in an internal monitoring table (available upon request from info@hcpn.etat.lu), are grouped under each priority.

I.   **Building trust in the digital world and protecting human rights online**

II. **Consolidating the security and resilience of digital infrastructures in Luxembourg**

III. **Developing of a reliable, sustainable and secure digital economy**

1.1 OBJECTIVE I: BUILDING TRUST IN THE DIGITAL WORLD AND PROTECTION OF HUMAN RIGHTS ONLINE

The first obligation of the State is to protect its citizens and guarantee their fundamental rights and freedoms. In a society that is permanently connected to the Internet and multi-dependent on computer networks and systems, there are many risks and threats to living together and to the rights of each individual. The protection of this civic space in line with all human rights – civil, political, economic, social, cultural, and environmental – is the first objective of this strategy. As formulated by the United Nations in its 2030 Agenda for Sustainable Development, "leaving no one behind", this fundamental principle of the social contract applies both in cyberspace and in the physical world. This pillar encompasses both data protection and privacy as well as the security of – already omnipresent – virtual meeting places, which have become truly indispensable in the era of the COVID-19 pandemic.
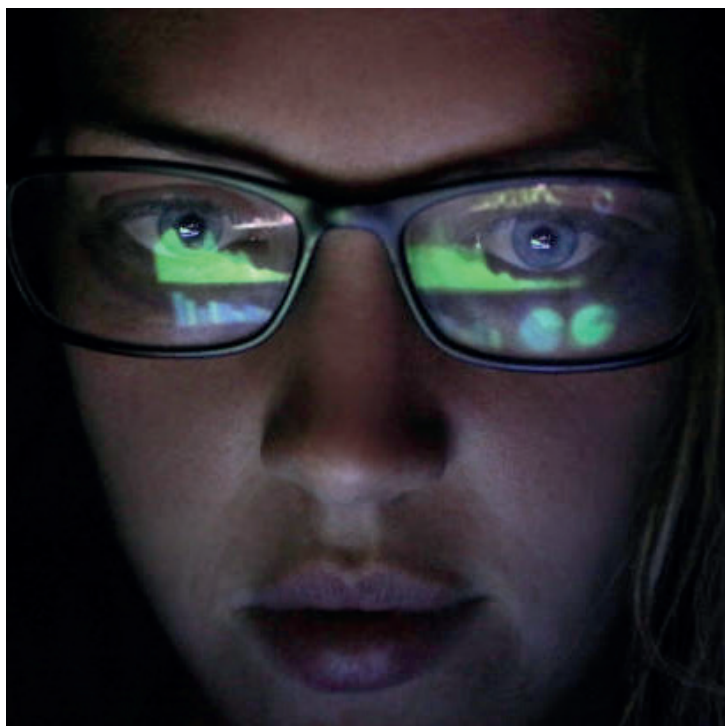
I.1 PROTECTION OF HUMAN RIGHTS ONLINE

- Inter-ministerial coordination will be strengthened in existing forums to conceptualise and tackle human rights risks (Inter-ministerial Human Rights Committee; Digital Inclusion Working Group; AI4GOV Inter-ministerial Coordination Group; etc.).

- Reflections on the regulation of surveillance or intrusion technologies will be undertaken, taking into account international discussions, in particular at the level of the European Union and the United Nations, and in compliance with international and Community law.

- Documentation and tools for digital security (e.g. security and encryption of communications, data protection, etc.) through the improvement of the cybersecurity skills of independent non-governmental organisations working in the field of human rights and humanitarian workers (e.g. CiviCERT) will be developed and made available.

I.2 PROTECTION OF CHILDREN AND YOUNG PEOPLE'S RIGHTS

- Efforts to protect children and young people's rights online, notably through raising awareness of cyber threats, will be continued, notably through the governmental initiative BEE SECURE, founded in 2010, which is operated by the 'Service National de la Jeunesse' (SNJ) and the 'Kanner a Jugendtelefon', and which develops important measures to raise awareness of the population in general, focusing on young people and children in particular.

I.3 SAFE DIGITAL INCLUSION

- Diversity and inclusion will be promoted in the field of cybersecurity, in support of initiatives such as Women in Digital Empowerment or civil society projects, in particular to encourage people from population groups that are under-represented in the sector (including women and girls, as well as people of migrant backgrounds or beneficiaries of international protection) to pursue training or careers in cybersecurity.

- Cybersecurity and online safety awareness will find their place in the context of the inter-ministerial working group for digital inclusion, which targets audiences that are far from the digital sphere. The subject is also addressed in the "digital confidence" strategic focus of the national action plan for digital inclusion and is a fundamental element of education for digital citizenship.

I.4 CYBERSECURITY EDUCATION AND VOCATIONAL TRAINING

- Cybersecurity awareness, education and training will be addressed more strategically. Developing professional curricula adapted to today's society and raising awareness of cybersecurity professions makes this area tangible for citizens. This will make it easier for young people in the process of obtaining their certificates or studies, as well as for adults in the process of retraining, to design a digital career and project themselves into the future. Curricula and research plans are developed under points 4 and 5 of this strategy.

I.5 PEN-TESTING, BUG BOUNTIES AND RESPONSIBLE DISCLOSURE OF VULNERABILITIES

- The Government will propose the necessary legislative changes and initiatives to make possible or deepen different approaches in order to improve cybersecurity by using the collective intelligence of security researchers, private companies active in the search for vulnerabilities and any users who discover a security breach. The possibility of creating, in the near future, a platform at GOVCERT.LU that encourages researchers to report bugs, especially those associated with vulnerabilities, will be analysed.

I.6 COMBATING CYBERCRIME

- A coordination body will be established between law enforcement and cybersecurity entities, in accordance with their respective mandates and missions. This forum will, inter alia, provide an avenue for strategic and operational analysis of the impact of the threat of organised crime and cybercrime activity and the interrelationship between cybercrime and cybersecurity. It will also seek synergies in combating different forms of Internet crime, including the fight against sexual exploitation and abuse of children.

- Cooperation with Europol/EC3, as well as with other relevant international organisations (e.g. Interpol, UNODC) will be strengthened, taking into account the needs and capacities of the different actors involved.

I.7 SECURE DEMOCRATIC AND CIVIC PARTICIPATION

- Emphasis will be placed on the prevention of influence operations and disinformation conveyed by digital means (hybrid threats). Guidelines will be drawn up for businesses to detect and counter the consequences of crises caused by such campaigns.
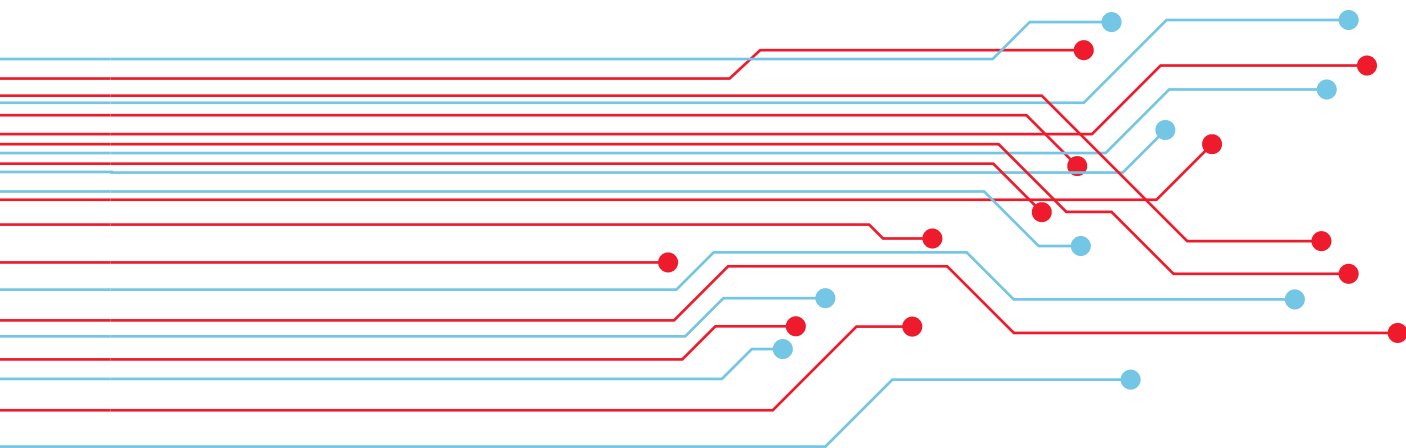
1.2 OBJECTIVE II: STRENGTHENING THE SECURITY AND RESILIENCE OF DIGITAL INFRASTRUCTURES IN LUXEMBOURG

The availability, integrity and confidentiality of data are the objectives of cybersecurity: faced with the numerous cyber incidents observed daily, as well as the risks and threats observed on the horizon, the Government has chosen to prioritise strengthening the security and resilience of digital infrastructures as a second strategic objective. The protection of vital infrastructures and essential services is one of the key activities of this objective, as is the wide range of activities of the various operational entities.
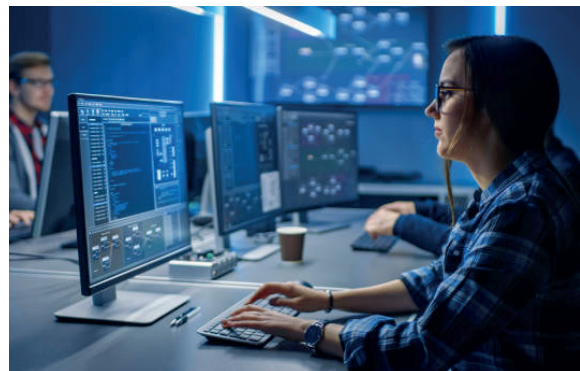
II.1 STRENGTHENING THE SECURITY AND RESILIENCE OF THE STATE'S DIGITAL PROCESSES AND INFORMATION AND COMMUNICATION SYSTEMS

- The security and resilience of digital processes and the underlying critical information and communication systems will be strengthened:
  - the information portal guichet.lu and myguichet.lu
  - the State's electronic messaging platform
  - the videoconferencing system
  - the remote access system
  - fixed and mobile terminal equipment
  - the DNS system.

- The opportunity of implementing an encryption solution for the exchange of sensitive messages, classified up to RESTRICTED level, will be evaluated as part of a Proof of Concept.

- The opportunity of implementing a national secure instant messaging solution, initially intended for government departments and agents, will be examined as part of a Proof of Concept. The "LuxChat" solution will be based on a federated architecture with end-to-end message encryption and will be implemented via open-source software.

II.2 SECURE AND CONTROLLED USE OF THE PUBLIC CLOUD AT STATE LEVEL

- In order to respond to the challenges of digital technology in a coordinated and thoughtful manner, the government adopted a cloud strategy in 2016. Investments and the establishment of central services at State level and making them available to State customers via private cloud services such as "Govcloud", are the preferred route.

- Given the advances in the world of digitalisation, the use of the public cloud is becoming essential in certain areas. The governance framework for the use of public Cloud services at State level or in the provision of public services will be defined, considering, in particular, the aspects of security, data protection, location and retention, dependencies and the potential risks of infringement upon government sovereignty and essential services.

II.3 ENSURING DIGITAL SOVEREIGNTY

- In cooperation with its partners in the European Union, the Luxembourg government will continue its efforts to ensure digital sovereignty at national and European level. Reflections on this subject will be conducted among all public sector stakeholders, involving, according to their needs and mandates, stakeholders from industry, research, or civil society.

II.4 CONTINUOUS IMPROVEMENT OF INCIDENT DETECTION AND MANAGEMENT

- The capacity to prevent and detect intrusions into State networks and information systems will be improved and gradually extended to all critical systems and networks.

- The capacity to process and analyse security logs will be strengthened. The collection, analysis and correlation of security events are essential for the early detection of attacks, for rapid responses in the event of a compromise, and for subsequent investigation in the event of an incident. The architecture and capabilities of the logging system and GOVCERT's management processes will be continuously adapted to the development of the State's information systems.

- Systematic recourse to teleworking significantly increases the area of exposure to attacks. In the event of a security incident and in order to minimise the risks of malicious propagation and data leakage, the use of remote analysis and diagnostic tools will be promoted.

II.5 CYBER SITUATIONAL ANALYSIS (CYBER WEATHER) AND CYBER INTELLIGENCE

- Better shared situational awareness will enable all stakeholders to act in an informed and concerted manner to ensure a level of security appropriate to the current state of threat.

- Within the framework of the Cyber Weather initiative launched by GOVCERT, the Luxembourg CERTs, based upon a dynamic analysis of notified incidents, regularly constitute an inventory at the national level. In close collaboration with all the players involved, the inventory will be gradually expanded by incorporating information from other available sources (sectoral ISACs, SOCs, intrusion detection probes, risk analyses, etc.).

- The systematic analysis of the information gathered, combined with the analysis of the modus operandi of the attacks, will enable a better understanding of the state of the threat (cyber intelligence) and the identification of concrete and actionable recommendations for prevention and preparedness.

- The State entities concerned will ensure coherent and exploitable dissemination of current threats to public and private operators and professionals in the ICT sector on the one hand, and, on the other hand, will ensure the dissemination of security warnings with mitigation recommendations to the general public.
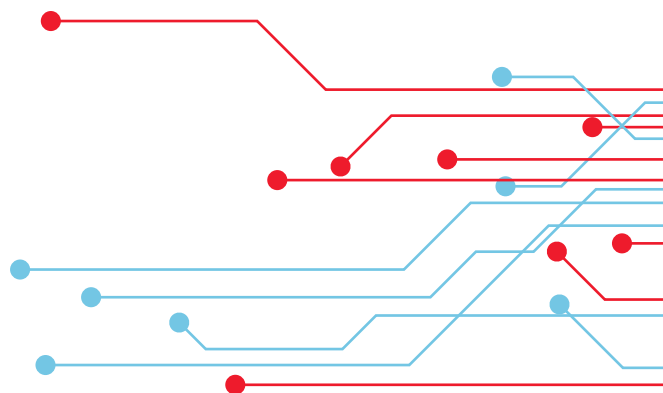
II.6 RISK ASSESSMENT AND MANAGEMENT

- Since the first national cybersecurity strategy, the government has actively promoted a risk management culture based on risk analysis and the application of security measures adapted to the level of risk involved. The scope of this approach will be extended to all sectors and the risk analysis tools made available will be adapted to the specific needs of the sectors.

- Aggregating risk assessments at the sector and national level will help to identify systemic risks within sectors and at national level and to define scenarios for assessing such systemic risks. These scenarios will be made available to the sectors for inclusion in their risk analyses.

- The identification and exchange of relevant risk scenarios and metrics is a collective activity that will be coordinated at State level and documented in the Risk Scenario Sharing Platform (MOSP). This will be accessible as a public service, which in the medium term will substantially contribute to increasing the quality of governance (informed governance) and resilience, and thus the attractiveness of Luxembourg.

II.7 CRITICAL INFRASTRUCTURE PROTECTION

- The National Filtering Centre for Distributed Denial of Service Attacks (DDOS) will be responsible for systematically monitoring national and global DDOS developments and trends and developing recommendations and best practices for critical infrastructure in the prevention, detection and response to DDOS attacks.

- A security operations centre for critical infrastructure will be set up.

- For the purpose of protecting against known and emerging threats — of the systematic dissemination of information on exploitable threats, attacks and intrusion attempts, and of building up shared situational awareness using metrics — it is envisaged to deploy a national network of probes installed at voluntary critical infrastructures in partnership with private sector actors.

- GOVCERT will continue to strengthen its capacities, skills and pen testing team. The service currently offered to State administrations and services will be extended to critical infrastructures.

II.8 SECURITY OF THE NETWORKS AND INFORMATION SYSTEMS OF ESSENTIAL SERVICE OPERATORS

- The ILR, as the competent national authority and single point of contact, ensures that operators of essential services manage the security of their networks and information systems. In close cooperation with essential service operators, the ILR will develop the SERIMA risk analysis and management platform, develop sector-specific best practices, initiate awareness campaigns and organise incident management exercises.

II.9 CYBERSECURITY IN THE HEALTH SECTOR

- Cybersecurity will accompany the accelerated digitalisation of health services, particularly in the light of developments initiated in the context of the COVID-19 pandemic. Ensuring the security of information and communication systems, medical devices, and more specifically patient data (e.g. the Shared Patient Record) has become a strategic issue.

- In close consultation with stakeholders, collaboration with stakeholders in the sector will be intensified, the security and resilience of key information systems and networks will be strengthened, a centralised Security Event Management System (SIEM) will be implemented, the HealthNet CSIRT will be strengthened, collaborative information sharing on cybersecurity in the health sector will be institutionalised (ISAC) and the implementation of an operational Security Management Centre (SOC) for the entire health sector will be envisaged.

II.10 IMPROVEMENT OF NATIONAL AND INTERNATIONAL CYBER CRISIS MANAGEMENT PROCESSES AND PROCEDURES

- Luxembourg will continue to participate regularly in international cyber crisis management exercises (e.g. with the EU and NATO). Lessons learned from the exercises will be implemented at the national level. The procedures and decision-making structure for diplomatic response to cyber incidents, specifically in the context of EU cooperation and the Cyber Emergency Response Plan will be reviewed. At the national level, exercises for the management of major cyber incidents impacting critical infrastructures will be carried out making use of the national simulation platform (cyber-range).

II.11 PROMOTION OF COLLABORATION AND INFORMATION EXCHANGE BETWEEN THE PUBLIC AND PRIVATE SECTORS

- In close cooperation with ICT Luxembourg and the federations represented there, the State will set up a transversal working group (cyber TWG) to organise, structure and boost exchanges and mutual assistance in the cyber field. The aim of this cyber TWG is to exchange information proactively and rapidly on attacks with a high propagation potential.

- If necessary, the cyber TWG will also coordinate the various private incident management teams to boost mutual support.

If necessary, the coordination may also be taken over by CIRCL or, in the event of a crisis, by the cyber crisis unit set up by the HCPN.

- The Threat Intelligence Sharing Platform (MISP), the Risk Scenario Sharing Platform (MOSP) and any other tools or services identified as necessary, will serve as platforms for information exchange and support a dynamic and rich exchange on threats, vulnerabilities, and any measures to be implemented.

II.12 SECURITY OF TELECOMMUNICATIONS NETWORKS AND SERVICES

- Security of telecommunications networks and services Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code will be transposed into national law. Exchange

and coordination with telecommunications network operators will be developed, notably with a view to implementing the security measures of the 5G toolkit.

II.13 SUPPLY CHAIN SECURITY

- The State's responsible entities will continue to work to improve detection and response capabilities to risks and threats throughout the hardware, software, and services supply chain. To this end, they will

base themselves on the recommendations and good practices for the State, critical infrastructure operators, OSEs, etc. in this area.

II.14 SECURING E-MAIL COMMUNICATIONS AT THE NATIONAL LEVEL

- E-mail is the major attack vector for specific actions that target users, such as phishing. A set of specific measures will be implemented to further secure e-mail services:
  - Encouraging e-mail service providers to raise awareness among their customers and offer them the spambee.lu national spam notification solution

- Development of an offer to assess the security of e-mail servers by the C3
- Promotion and support for the implementation of the standard for domain protection and authentication of e-mail -DMARC

II.15 SECURING COMMUNICATIONS AND DATA THROUGH THE USE OF QUANTUM TECHNOLOGIES

- In June 2019, Luxembourg signed a cooperation declaration to explore together with the European Commission and the European Space Agency (ESA) the feasibility of implementing a secure communication infrastructure based on quantum technology. This infrastructure will consist of a terrestrial part and a space part. Faced with the threat to the integrity of encrypted communications posed by the power of the quantum computer, the "Quantum Communication Infrastructure" (QCI) could be the answer, enabling the secure exchange of encryption keys (quantum key distribution, QKD). This infrastructure will be developed and implemented at the national level and then integrated into the European infrastructure. The QCI is initially aimed at users in the public sector with the aim of extending it to the private sector. The following potential uses have been identified:
  - Critical infrastructures (energy, transport, water supply, etc.)
  - Data centres
  - Additional level of protection for the "Meluxina" HPC
  - European Institutions.

II.16 OPERATIONALISATION OF THE NATIONAL CYBER DEFENCE STRATEGY

- The Defence Directorate of the Ministry of Foreign and European Affairs together with the Luxembourg Army have mapped Luxembourg's cyber defence obligations and national priorities in order to establish a framework to facilitate the transformation of Luxembourg's defence force into one of the most cyber-secure armed forces by 2030.

- By developing cybersecurity capabilities for information and communication systems, Luxembourg's defence force is working to become a point of reference and to strengthen its image as a reliable partner for national entities and international organisations. This long-term objective is supported by strategic objectives such as the cultivation of talent, the strengthening of cooperation in the field of cybersecurity at both national and international level, the integration of Cyber/CIS security in all Luxembourg Defence activities, and research and development.
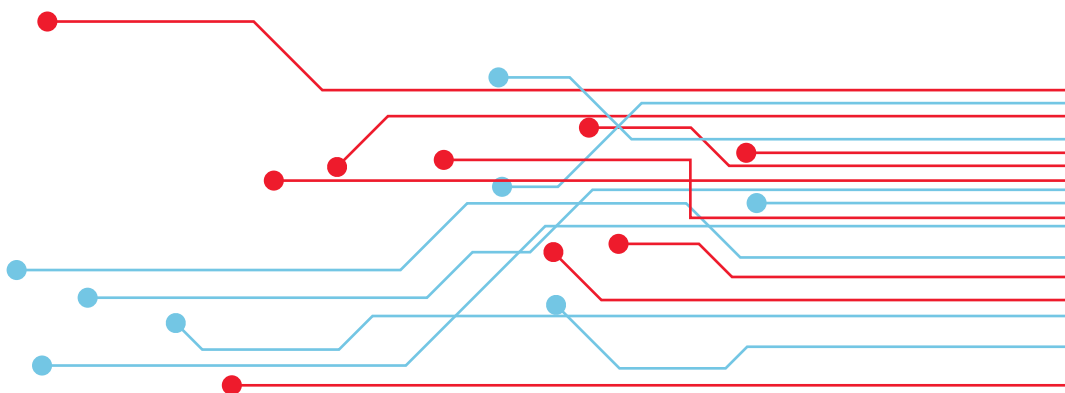
1.3 OBJECTIVE III: DEVELOPING A RELIABLE, SUSTAINABLE AND SECURE DIGITAL ECONOMY

"Openness, dynamism and reliability": the Luxembourg Government's strategy of economic dynamism and diversification is largely based on the continuous development of a high-performance digital economy. Cybersecurity is essential for the smooth functioning of the relations, transactions, services and other interactions that underpin the digital economy. Relationships based on trust operate at several levels: between the State and citizens, between users and technological tools, and finally between economic partners. The various growth sectors of the Luxembourg economy – industry, finance, technology, knowledge and logistics – all rely on high-performance and reliable IT networks and systems.

III.1 FEDERATION OF THE LUXEMBOURG CYBERSECURITY ECOSYSTEM

- In close collaboration with the Ministry of the Economy and Luxinnovation, SECURITYMADEIN.LU will continue to manage the directory of cybersecurity stakeholders in Luxembourg in order to identify and promote the services available in Luxembourg, to intensify collaboration between stakeholders and to promote this sector at international level.

- Luxinnovation and the Ministry of the Economy can, in a targeted manner, attract companies offering specific services that are not yet available in Luxembourg.

III.2 FEDERATION OF THE LUXEMBOURG CYBERSECURITY RESEARCH ECOSYSTEM

- Through its C3 department (Cybersecurity Competence Center) and in collaboration with relevant research and state actors. SECURITYMADEIN.LU will define cybersecurity research priorities and coordinate research players. Collaboration with research centres in the Greater Region is being intensified. This will also respond to the proposal for a European regulation COM (2018) 630 which provides for the reorganisation of the allocation of European research funds in the field of cybersecurity.

III.3 DEVELOPMENT OF CERTIFICATION, TESTING AND STANDARDISATION METHODOLOGIES

- The Luxembourg Institute for Standardisation, Accreditation, Safety and Quality of Products and Services (ILNAS) has been appointed as the National Cybersecurity Certification[1] Authority (NCCA) in Luxembourg within the framework of Regulation (EU) 2019/881 on Cybersecurity ("Cybersecurity Act – CSA"). In this context, the ILNAS will be in charge of supervision and will ensure that the rules relating to cybersecurity certification schemes, for the purpose of monitoring that ICT products, ICT services and ICT processes comply with the requirements of the European cybersecurity certificates issued on the national territory. Where appropriate, the ILNAS will also be responsible for monitoring compliance with the obligations of manufacturers or suppliers of ICT products, ICT services or ICT processes that are established on the national territory, and which carry out conformity self-assessments.

- Depending on the identified national needs, the government may decide to appoint another national cybersecurity certification authority to carry out the certification tasks and/or tasks directly related to this.

- The ILNAS takes part in various meetings of the European Cybersecurity Certification Group established in 2018 by the EU Cybersecurity Act to take into account any information relevant to its supervisory tasks.

[1] **Levels of insurance**
A European cybersecurity certification scheme may specify one or more of the following levels of insurance for ICT products, ICT services and ICT processes: "basic", "substantial" or "high". The level of insurance corresponds to the level of risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the likelihood and impact of an incident.

Self-assessment
A European cybersecurity certification scheme can allow conformity self-assessments to be carried out under the sole responsibility of the manufacturer or supplier of ICT products, ICT services or ICT processes. Conformity self-assessments are only permitted for ICT products, ICT services and ICT processes that present a low risk, a scheme corresponding to the so-called "basic" level of insurance. The manufacturer or supplier of ICT products, ICT services or ICT processes shall keep at the disposal of ILNAS the European Union declaration of conformity, the technical documentation and all other relevant information relating to the conformity of the ICT products or ICT services with the European certification scheme concerned for the period specified in the scheme.

Certification
For basic or substantial levels of assurance, certification is carried out by a conformity assessment body (CAB), unless a scheme provides that only a public body may issue certificates in duly justified cases (Art. 56.5). CASES, the department of SECURITYMADEIN.LU, the mission of which is to secure SMEs, will serve as the CAB for the elementary level.

III.4 CREATION OF THE FIRST CYBERSECURITY DATA SPACE IN EUROPE

- SECURITYMADEIN.LU will create the first cybersecurity data space in Europe and will thus encourage the actors of the Luxembourg ecosystem and the greater region to exchange and make data available for research and the creation of new cybersecurity products and services.

III.5 CAPITALISATION ON THE CYBERSECURITY COMPETENCE CENTRE (C3)

- The scope of ROOM#42, the cyber-incident simulator for training incident response teams, will be extended to allow its use in distributed mode, through a dedicated electronic platform.

- The deployment of ROOM#42 in the form of a platform will make it possible to interconnect with cyber-range infrastructures, allowing the development of more complex scenarios, bringing the technical teams to deal with simulated incidents closer to their operational realities.

- The C3 will continue to develop partnerships at both national and international level, following the opening of a first "franchise" in Toulouse in May 2019.

- In addition to ROOM#42, the C3 will develop a method for creating and implementing crisis management exercises involving players with heterogeneous levels of competence. The corresponding tools will also be made available to the ecosystem.

- A national cybersecurity skills and competence framework will be established to facilitate the development of cybersecurity skills by economic actors, in particular SMEs. This framework will describe generic roles and corresponding competences and will include a decision support tool. Other services consistent with this framework will be created.

- The public-private partnership for the C3 "testing" platform will be developed to help organisations identify areas for improvement from a skills perspective. It should enable the testing of infrastructures, organisations, as well as individuals. It must also be accompanied by tools and documentation to help understand and interpret the test results. This platform will also be made available to the Luxembourg European Digital Innovation Hub, operated by Luxinnovation, to offer a "test before invest" service.

- A C3 observatory will be set up, in order to:
  - Centralise all monitoring, cyber-weathering and information sharing efforts and analyse the data collected;
  - Produce a regular "bulletin" on relevant and topical subjects for Luxembourg;
  - Provide information that can be used as a reference for decision-makers in organisations when making choices about resource allocations for cybersecurity.

III.6 EUROPEAN CYBERSECURITY EXPERTISE COMMUNITY

- Designation of the national coordination centre and contribution to the achievement of the objectives of the European Centre of Industrial Technological and Research Competence in Cybersecurity, notably by actively taking part in the activities of the European Cyber Skills Network.

III.7 CAPACITY BUILDING AT NATIONAL AND INTERNATIONAL LEVEL

- State actors will continue to work towards the provision of tools, methods, and documentation to facilitate the appropriation of security technologies by the economic sector and civil society in the least developed countries, specifically through cooperation for the development of local skills (capacity building).

- Intra-governmental "Digital 4 Development" efforts will be coordinated by the MAEE Development Cooperation Directorate. The development of Luxembourg's expertise in capacity building and skills transfer to the countries and regions most in need will be pursued through the established channels of Luxembourg Cooperation, as well as through public-private partnerships; the C3 will continue its active participation in the consortium for the establishment of the European Union platform for capacity building on cybersecurity for developing countries (EU CyberNet: https://www.eucybernet.eu);

- MILCERT.LU strengthens cooperation efforts in the network of military CERTs, particularly in the field of cybersecurity training for military personnel in Luxembourg.

- Luxembourg will participate in the Global Forum on Cyber Expertise (GFCE) and other international cooperation initiatives in the field of the provision of cyber expertise.

III.8 INTENSIFYING PARTNERSHIPS WITH INDUSTRY, RESEARCH, AND CIVIL SOCIETY

- Research projects will be promoted for the development of secure software and hardware with the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg.

- Creation of partnerships to foster the emergence of economically viable cybersecurity innovations. This should involve providing the various partners with a portfolio of services and business models adapted to the nature of the services or products they intend to develop or promote.
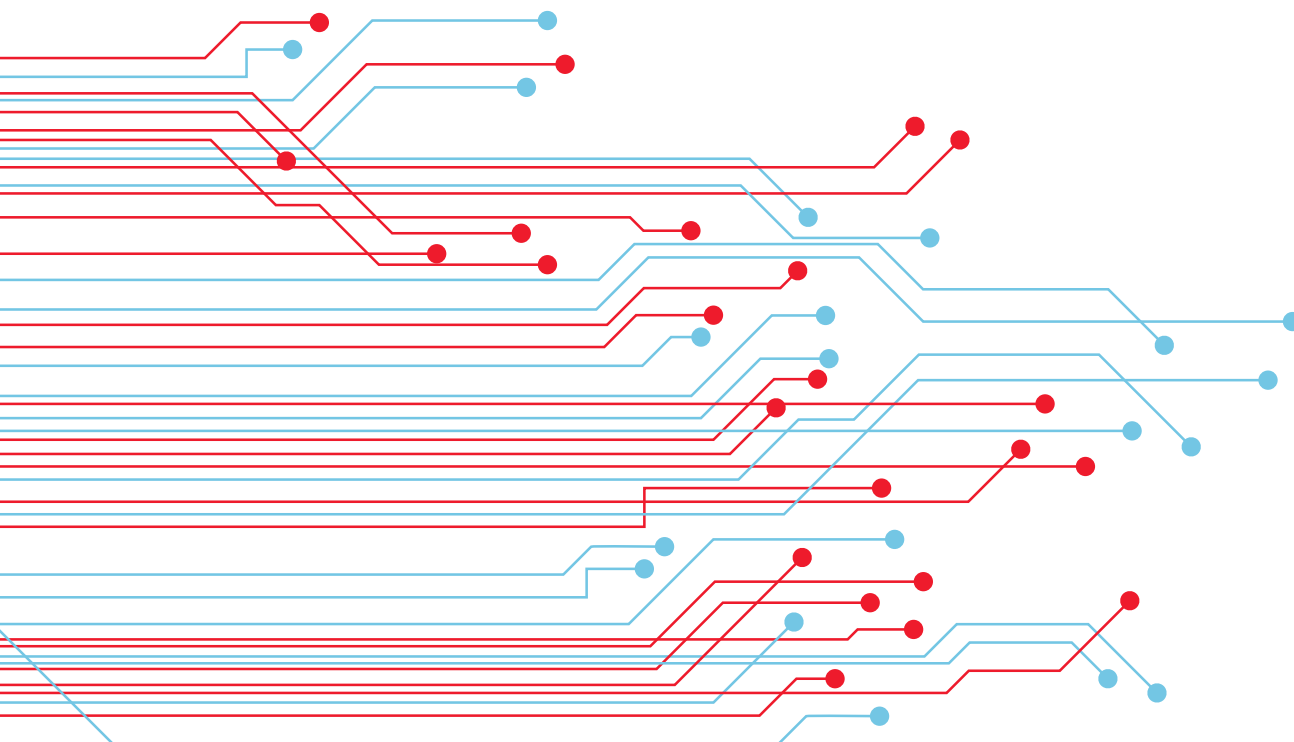
2.
NATIONAL CYBERSECURITY GOVERNANCE FRAMEWORK

2.1 INTER-MINISTERIAL CYBER PREVENTION AND CYBERSECURITY COORDINATION COMMITTEE

- On 6 December 2017, the Government Council approved the creation of an inter-ministerial committee responsible for ensuring national coordination in the field of cyber prevention and cybersecurity (CIC-CPCS). The committee's task is to ensure the pragmatic and swift coordination of initiatives that are part of cyber-attack prevention and cybersecurity.

- The CIC-CPCS, which meets on a regular basis under the chairmanship of the High Commissioner for National Protection, has as its mission, in accordance with the specific competences and responsibilities of the entities described below, to:
  - Ensure the coherence of actions and initiatives undertaken in the fields of cyber-prevention and cyber-security;
  - Coordinate the implementation of European and international initiatives and measures in the field of cyber-prevention and cybersecurity;
  - Monitor the implementation at national level of policies decided at European and international level;
  - Advise the Government on cybersecurity and cyber-prevention by identifying the topics and priorities to be developed in this field and the actors responsible for their implementation;
  - Discuss the positions to be taken by national representatives in European and international fora on cybersecurity and cyber prevention.

2.2 KEY STATE ENTITIES INVOLVED IN NATIONAL CYBERSECURITY GOVERNANCE

- The High Commission for National Protection (HCPN) is involved in the management of a cyber crisis. Its action is defined through the emergency response plan for attacks against information systems as soon as the crisis is likely to have serious consequences for some of the territory or population of the Grand Duchy of Luxembourg. It also acts as the National Agency for the Security of Information Systems (ANSSI), the mission of which is to define information security guidelines and ensure that measures concerning the security of information systems are put in place. The Government Centre for Computer Emergency Response (governmental CERT/GOVCERT), which also operates under the responsibility of the HCPN, is involved in the management of large-scale security incidents affecting networks and communication systems.

- The Ministry of the Economy is responsible for information security, risk awareness and vulnerabilities in the private sector. In this context, the Economic Interest Group – Security Made in Luxembourg (EIG SECURITYMADEIN.LU), a platform for the promotion of cybersecurity, operates among others the CASES (promotion of information security in companies), the C3 (national centre of expertise in cybersecurity) and the CIRCL (Computer Incident Response Center Luxembourg) initiatives, the latter also acting as a CERT for private and non-governmental entities and municipalities.

- The Ministry of State – Department of Media, Telecommunications and Digital Policy (SMC) follows the European Council's Working Party on Telecommunications and Information Society and its preparatory meetings. It covers the subject of cybersecurity strategy, particularly in the field of electronic communications networks, under the banner of the Minister for Communications and Media, on behalf of the Ministry of State.

- Within the Ministry for Digitalisation, the mission of the Government IT Centre (CTIE) is governed by its amended organic law of 20 April 2009. Within the framework of its remit, its mission includes ensuring the security of information technology, the management of electronic and computer equipment and appropriate security, the administration of the State's computer network and the production of secure administrative documents.

- The mission of the State Intelligence Service is to seek, analyse and process intelligence relating to cyber threats insofar as it may be related to espionage, interference, terrorism, extremism with violent propensity, proliferation of weapons of mass destruction or defence-related products and related technologies.

- Two directorates of the Ministry of Foreign and European Affairs are concerned:
  - The Directorate of Political Affairs coordinates work on cyber diplomacy. This includes following the activities of the Horizontal Working Party on Cyber Issues of the Council of the European Union, the "EU Cyber Diplomacy Toolbox" and the cyber-sanctions regime, as well as other cyber diplomacy activities at international level, in particular within the framework of the United Nations.
  - The Directorate of Defence is committed to this topic because cyber defence is one of NATO's core tasks, as cyberattacks are an important part of hybrid warfare. It should also be noted that NATO and the European Union signed a cyber defence cooperation agreement in February 2016 to address the common challenges faced by both organisations.

- The Luxembourg Institute of Regulation (ILR) is the single point of contact for Luxembourg in the implementation of the European Directive on security of networks and information systems (NIS Directive) and the competent authority for all sectors referred to in the NIS Law except for the financial sector which remains under the aegis of the Financial Sector Supervisory Commission ("CSSF"). Within this framework, the Institute has been entrusted with new competences in the field of network and information system security as well as in the context of cybersecurity. In concrete terms, the Institute's role as a competent authority is to ensure that the sectors under its responsibility (energy, transport, health, drinking water, digital infrastructure, and digital service providers) achieve a high common level of security in order to assume responsibility for computer incidents or cyberattacks and thus prevent incidents with a significant impact on the availability, confidentiality and integrity of essential services.

2.3 CYBERSECURITY LUXEMBOURG, LUXEMBOURG'S CYBERSECURITY ECOSYSTEM

The CYBERSECURITY LUXEMBOURG initiative was launched by the Ministry of the Economy to consolidate and improve public-private cooperation in the field of cybersecurity.

As the national label of Luxembourg's cybersecurity ecosystem, CYBERSECURITY LUXEMBOURG brings together and supports all relevant actors from the private and public sectors in the field of cybersecurity, in order to consolidate this crucial pillar of the national economy and to facilitate the international opening of Luxembourg's cybersecurity expertise. Endorsed by all market players, the CYBERSECURITY Luxembourg brand represents a common platform at the national and international level.

CYBERSECURITY LUXEMBOURG is managed and operated by three entities:

- **HCPN** – as chair of the inter-ministerial committee for ensuring national coordination in the field of cyber prevention and cybersecurity (CIC-CPCS) and coordinator of the national cybersecurity strategy, the HCPN leads the initiative by integrating it into the national strategy and liaising with other relevant public entities. The ANSSI,the national authority for the security of classified and unclassified information systems operated by the State, which is dependent on the HCPN, will organise the collection and collation of information from the public entities involved (e.g. CTIE) and will lead the online platform that covers its sphere of competence.

- **SECURITYMADEIN.LU** – The cybersecurity agency for the Luxembourg economy and municipalities will be in charge of the overall coordination of the initiative. SECURITYMADEIN.LU will organise the collection and collation, as well as the management of information on the essential services provided by the ecosystem. It will map their availability among the players in the ecosystem and improve the potential collaboration between them. It will also promote, in collaboration with Luxinnovation, the ecosystem within the Greater Region and in Europe. It will co-manage the e-platform and contribute communication and promotional tools, such as the cybersecurity breakfasts, the cybersecurity week, etc.

- **LUXINNOVATION** – this government agency provides companies and public research organisations with a wide range of services to foster innovation and thus support the Government's economic development objectives. The agency ensures that Luxembourg continues to attract investments, companies and knowledge that are perfectly in line with the country's context. Luxinnovation contributes its expertise in terms of market knowledge and promotion of the ecosystem at both the national and international level. As coordinator of the L-DIH (Luxembourg Digital Innovation Hub) initiative, it will bridge the gap between needs and expertise in cybersecurity (contributing to the relevant parts of the online platform).

2.4 BEE SECURE GOVERNMENT INITIATIVE

Founded in 2010, the BEE SECURE government initiative is operated by the 'Service National de la Jeunesse' (SNJ) and the 'Kanner-Jugendtelefon', in partnership with SECURITYMADEIN.LU, the Grand-Ducal Police and the Public Prosecutor's Office of the Grand Duchy of Luxembourg. The ministries involved are the Ministry of National Education, Children and Youth, the Ministry of the Economy and the Ministry of Family and Integration.

BEE SECURE is also the Luxembourg representative of the Safer Internet Center (SIC) co-funded by the European Commission and as such is supported by a network of international counterparts and partners: INSAFE (awareness centres and helplines) and INHOPE (reporting centres for illegal content).

Thanks to its experience on the ground in Luxembourg and its established network of partners, BEE SECURE is able to contribute in a concrete way to the empowerment of the user.

AIMS OF BEE SECURE:

To promote a safer, responsible, and positive use of new information technologies among the general public and, in particular, among three distinct groups of people:
- To assist children and young people in their education related to use of new technologies.
- Support parents, teachers, and educators as a reference/role models for children/young people.
- Support seniors, for whom demand is growing increasingly (https://silversurfer.lu/).

FIELDS OF ACTION:

1. Awareness raising and information: BEE SECURE disseminates information and advice on responsible use of the Internet. BEE SECURE therefore systematically organises training courses in schools and high schools. BEE SECURE regularly publishes information packs on hot topics (including cyber bullying, disinformation, cyber risks, radicalisation, learning how to use IT tools in a balanced way, etc.) as well as practical guides for children, young people, and their peers. BEE SECURE makes this information available to the general public through its websites, social networks and the national press.
2. Guidance and advice: The BEE SECURE Helpline is a contact point for questions related to online safety and the responsible use of new communication technologies. It is aimed at the general public and especially to children, young people, parents, seniors as well as teachers and educators. The Helpline is a free service, with anonymous and confidential treatment of information.
3. Reporting illegal content: Through the BEE SECURE Stopline, illegal online content can be reported anonymously and confidentially. These reports can be classified in one of three categories: child sexual abuse material (CSAM); discrimination, racism or revisionism; or terrorism. The alerts are analysed and, if necessary, will be forwarded to the relevant authorities.
4. Watch: Regular exchange with children and young people during training courses, analysis of requests on the BEE SECURE Helpline and collaboration with the "Youth and Kids Panels" discussion groups enables BEE SECURE to follow trends closely. The exchange with different national and international partners completes the trend monitoring. The results of the trend monitoring will be shared through BEE SECURE 'RADAR'.

3.
PREPAREDNESS, RESPONSE AND RECOVERY MEASURES

3.1 PRESENTATION OF THE CYBER EMERGENCY RESPONSE PLAN

Cyber emergency refers to a situation caused by an incident or an attack that could lead to a major malfunction or even unavailability of communication and information processing systems that threatens the vital interests or essential needs of all or part of the country or the population of the Grand Duchy of Luxembourg.

In principle, crisis management bodies become aware of a cyber incident or attack either through the analysis of information available at the national level or through international channels following existing agreements.

As soon as it becomes aware of a cyber incident, the Cyber Risk Assessment Unit (CERC) is alerted and carries out an assessment of the available information. If the incident is likely to have a significant impact, the High Commissioner for National Protection is alerted and informs the Prime Minister, Minister of State, who decides whether to activate the Crisis Unit.

The Crisis Unit may delegate to an operational unit, in particular the execution, implementation and monitoring of the measures and activities ordered.

In the cyber context, the functions of the Operational Unit are generally assumed by the Cyber Risk Assessment Unit (CERC).

3.2 PRESENTATION OF CERT'S ACTIVITIES

Luxembourg has an active community of public and private Computer Alert and Response Centres (CERT/CSIRTs), which cooperate at the national and international level to respond rapidly to incidents.

The governmental CERT is integrated into the High Commission for National Protection (Ministry of State) and provides a range of services for the public sector and critical infrastructure in order to further increase the resilience of IT systems in its constituency. The governmental CERT also operates a military CERT that promotes synergies, especially in the field of cybersecurity exercises and vulnerability and intrusion testing.

The CIRCL (*Computer Incident Response Centre Luxembourg*), CERT for the private sector managed by the Ministry of Economy, operates various services in the field of threat prevention, detection and mitigation, including the Malware Information Sharing Platform (MISP).

CIRCL acts as a clearinghouse for information sharing on cyber threats for various sectors, providing tools, community leadership, best practices, exchange standards and data for a wide range of communities, placing Luxembourg in a central position for this global threat information sharing. In addition, the CIRCL also acts as a trusted host for several leading information sharing communities, offering hosting and management of dedicated central hubs as well as support and training opportunities for these communities.

3.3 THE SCRUBBING CENTRE

In 2018, Luxembourg created an ambitious public-private partnership to set up a centre for protection against sophisticated Distributed Denial of Service (DDoS) attacks. This public-private partnership ensures advanced detection of DDoS incidents and allows the filtering of non-legitimate requests in order to ensure the continuity of IT services and the accessibility and reliability of data in the event of an attack.

3.4 CYBERSECURITY EXERCISES

Luxembourg participates in large-scale exercises organised by its multilateral partners, notably at EU level (CyberEurope) and NATO level (Locked Shields and Cyber Coalition).

A "Cyber Range" platform will be introduced to conduct national and international exercises and to complement the cyber training programme by developing an advanced training centre.
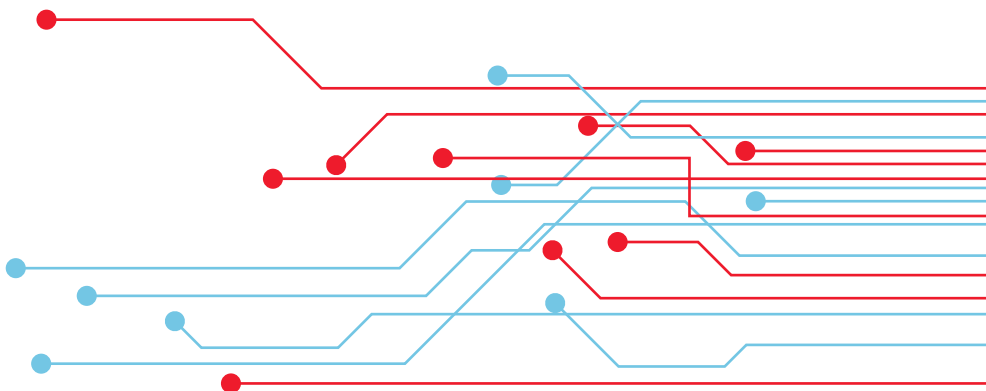
3.5 INTERNATIONAL COOPERATION AND CYBER DIPLOMACY

In the field of diplomacy and international relations, Luxembourg is a long-standing advocate of the multilateral method and works for positive international cooperation within the framework of international law and international humanitarian law. International cooperation in the field of standard-setting makes it possible to discuss and deepen the norms of responsible behaviour of states in cyberspace, following the example of the efforts currently underway at UN level: engaging in good faith in these international negotiations is one of the strategic elements promoting greater collective security.

- At UN level, Luxembourg follows in particular the activities currently underway in the General Assembly, within two bodies set up in 2019: on the one hand, through active participation in the work of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, and on the other hand, by following the work of the Group of Governmental Experts on Promoting the Responsible Conduct of States in Cyberspace in the Context of International Security.

- The European Union is the most advanced regional integration organisation in the world: Luxembourg participates in the various cooperation mechanisms set up in the framework of (EU) Directive 2016/1148 on the security of networks and information systems, as well as in cooperation forums for policy formulation and crisis management.
  - The NCSS IV will have to take on the mission of transposing European obligations at the national level, in particular in regards to the use of the EU diplomatic toolbox to respond to malicious cyber acts, as well as the operationalisation of the EU action plan ("Blueprint") for responses to large-scale cyber incidents.
  - Luxembourg should have a national policy and the necessary procedures for assigning responsibility for a cyber incident.

- The Organization for Security and Cooperation in Europe (OSCE) is one of the most advanced regional organizations in the development of confidence-building measures and cyber cooperation.

- The North Atlantic Treaty Organisation (NATO) has a sophisticated cooperative cyber defence capability.

3.6 COOPERATION AGREEMENTS AT BENELUX LEVEL

- The HCPN plans to strengthen strategic cooperation on cyber crisis management and cybersecurity capacity development with its Benelux counterparts.

4.
EDUCATION, TRAINING AND AWARENESS PROGRAMMES

In an effort to engage cybersecurity experts in the future, training curricula need to be updated to include the topic of cybersecurity. At the beginning of secondary school or even Cycle 4, initial introductions should be made to steer future experts in the right direction from the outset.
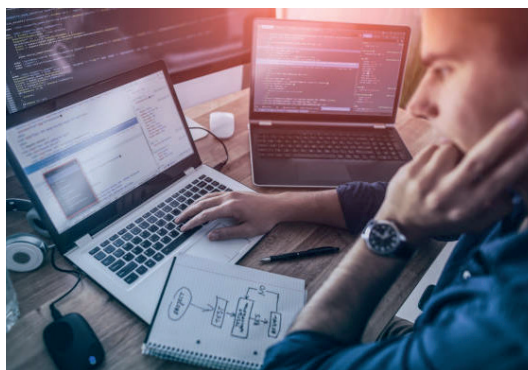
4.1 FORMAL EDUCATION

National education and inclusion in national curricula
- General framework for education to and through the media: the *Medienkompass (https://www.edumedia.lu/medienkompass/medienkompass/)*

• BEE SECURE
  BEE SECURE's objectives and areas of action include the promotion of a safer, responsible and positive use of new information technologies among the general public (children, young people, parents, teachers, educators, seniors). To achieve this, BEE SECURE
  - Disseminates information and advice on responsible use of the Internet;
  - Systematically organises training in schools and colleges;
  - Regularly publishes information packs on current topics and practical guides for children, young people and their families.

• BTS ("Brevet Technique Supérieur") diploma:
  - BTS Cloud computing – http://bts.lu/domaines/services/cloud-computing/
  - BTS "Internet of Things" – http://bts.lu/domaines/services/internet-things/
  - BTS Informatique – http://bts.lu/domaines/services/informatique
  - 2021/2022: creation of a BTS in the field of cybersecurity, with the aim of training professionals who have a technical profile and can take up operational positions such as SOC operator, incident analyst, cybersecurity officer or junior "penetration tester".

• University of Luxembourg:
  - Bachelor in Applied Information Technology (https://wwwen.uni.lu/studies/fstm/bachelor_in_applied_information_technology)
  - Master in Information System Security Management (https://wwwen.uni.lu/studies/fstm/master_in_information_system_security_management)

4.2 INITIAL AND ONGOING TRAINING; RE-SKILLING AND UPSKILLING

The growth of the digital market goes hand in hand with strong growth in the need for trainers and cybersecurity professionals. Training courses and professions are generally still little known or are misunderstood by the general public and young people when it comes to choosing their studies. They are also not really considered as an option when adults choose to retrain during their working life. In reality, however, there is a wide range of cyber-related professions; it is constantly changing due to the evolving nature of the digital society, and training and access to such professions are open to all kinds of people.

INAP

• Cyberattacks and information leaks are a reality. How to prepare? (Room #42)

• Information security – training for management of administrations

• Information security – tailor-made training by administration

• Information security – Initiation
  - This course will soon be available in e-Learning. It is part of the General State Training and is attended by every trainee civil servant and every employee on temporary duty.

• Training in reporting information security incidents to the government CERT

• ECDL Base – Web and Communication Basics

• ECDL Standard – Online collaboration

• ECDL Standard – IT Security

4.3 RE-SKILLING / UPSKILLING

• Cyberwayfinder.com

4.4 NON-FORMAL EDUCATION

• BEE CREATIVE / Maker Spaces

• Hack4kids.lu
  Since 2018, C3 has been organising the Lëtz Cybersecurity Challenge, an annual competition intended to detect young talents in the field of cybersecurity. During the LCSC,

HOUSE OF TRAINING

• The House of Training (https://www.houseoftraining.lu/) offers a number of training courses to companies, some of which are offered in partnership with SECURITYMADEIN.LU:
  - Personal data and information security – Legal issues and new EU rules
  - Cybersecurity – Raising employee awareness
  - Cybersecurity and SMEs – How to protect your business
  - Ethical Hacking – Fundamentals
  - Room#42 – Experience and learn to manage cyber incidents
  - Room#42 – Experience and cyber crisis management training

C3

• The C3 supports the development of a BTS Cybersecurity at the Lycée des Arts et Métiers.

• The C3 is strengthening the ROOM#42 simulation programme by developing a platform version of it, enabling teams spread geographically over several sites to be trained and tested.

• The C3 increases the interactivity of awareness training to help trained staff acquire basic self-protection gestures, particularly with respect to the use of mobile platforms (telephone, tablet, personal vehicle, household appliances) and social networks.
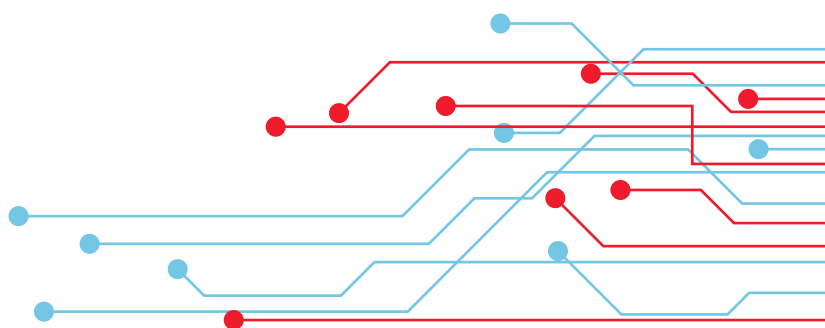
participants face multiple online challenges, specifically designed for them by C3 experts and partners. The most talented of them are selected to build the national team representing the Grand Duchy of Luxembourg at the yearly European Cybersecurity Challenge (ECSC).

4.5 AWARENESS-RAISING ACTIVITIES

BEE SECURE
https://www.bee-secure.lu/fr/

European Cybersecurity Month

- European Cybersecurity Month, or ECSM, is a European awareness raising event organised every year in October at the initiative of ENISA, the European Network and Information Security Agency. In Luxembourg, the contact point for ECSM is the Ministry of the Economy; the events take place during the 'Luxembourg week' organised by the Luxembourg cybersecurity ecosystem 'Cybersecurity Luxembourg' and various local partners.

Cybersecurity Week Luxembourg:
https://www.cybersecurityweek.lu/

- The Cybersecurity Week Luxembourg is an advocacy-campaign week featuring different events and workshops, aiming to raise awareness about cybersecurity risks, to promote cybersecurity among citizens and professionals, and to provide up-to-date information about training and sharing of good practice. During the highlight and closing event, the Gala and Awards Night, the CISO and DPO of the Year awards are given to the most outstanding candidates by a jury of experts and peers in the field.

Trustbox CASES:
https://trustbox.cases.lu

- Providing resources in digital form, such as training courses, documents, tutorials, and workshops, allows for better protection of the privacy and professional life of stakeholders. This is an important addition in some situations, containing documents, video game training, webcasts, and online courses, with the aim of deepening knowledge and spreading the message of cybersecurity.

ANSSI Cyber Security Portal:
https://cybersecurite.public.lu/fr.html

ANSSI extranet portal reserved for users of the governement information systems:
https://anssi.extranet.etat.lu

"National" campaigns

- IoT – a campaign as important as its subject matter
  - In the latest cybersecurity strategy, the campaign for the Internet of Things (IoT) and Smart Buildings has been defined and started. However, this remains an important campaign that will remain active for a longer period of time in view of the number of topics to be addressed. Moreover, even though ANSSI and CASES have started the campaign, more players will join and continue with awareness raising in order to explain a more general vision regarding cybersecurity for smart equipment.

- New cybersecurity campaign on equipment disposal
  - Even if this campaign is not as broad as the Internet of Things (IoT), there is still a lot of confusion about the disposal of smart devices, and how to properly erase data from storage before it is destroyed or redistributed and reused. Several players can join this campaign, such as Digital Inclusion, CASES, SuperDrecksKëscht, or other information security and destruction organisations and companies to provide the knowledge and best practices for each company, so that they can recycle their equipment without giving their information to third parties.

5.
RESEARCH AND DEVELOPMENT PLANS

5.1 UNIVERSITY OF LUXEMBOURG: INTERDISCIPLINARY CENTRE FOR SECURITY, RELIABILITY AND TRUST (SNT)

The *Interdisciplinary Centre for Security, Reliability and Trust* (SnT) at the University of Luxembourg conducts internationally competitive research in information and communication technology (ICT) with a focus on creating socio-economic impact. The centre attracts talented researchers from all over the world to work on collaborative projects within the industry and the public sector. Since its launch in 2009, SnT has established partnerships with more than 45 organisations.

SnT's strategic research priorities are: autonomous vehicles, cybersecurity, fintech, Internet of Things, secure and compliant data management, space systems and resources.

KEY FIGURES

PEOPLE

365
workforce

66
nationalities

36%
alumni who stay
in Luxembourg

PARTNERSHIPS AND INNOVATION

43%
of Doctoral candidates
on Industrial projects

56
partners

8м
partener annual
contribution in euros

5
spin-offs
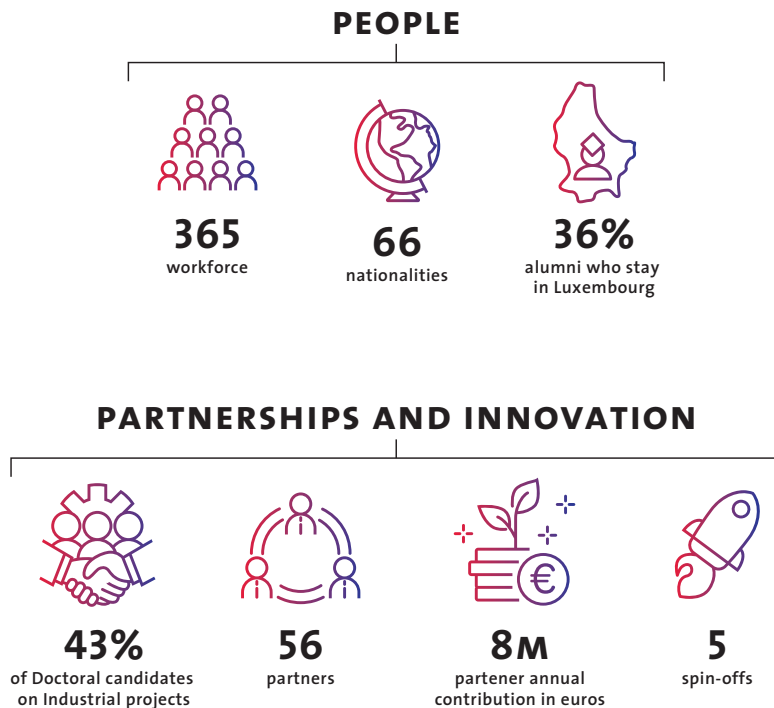
STRATEGIC RESEARCH AREAS

SnT has six research areas that define its work. While cybersecurity is one of SnT's focus areas, it is also a transversal topic across the most relevant industries in Luxembourg.

Fintech:
As regulations become increasingly complex, ICT tools are necessary for cost-effective, compliant solutions for the financial, legal, and insurance sectors. Our research teams develop solutions to ensure security and trust in these sectors.

Space systems:
The revolution in space technology is driving new and innovative business models. Our expertise in satellite communications, autonomous operations, and mission critical software makes us ideally placed to work with players establishing R&D activities in Luxembourg.

Autonomous vehicles:
Autonomous driving promises to be more efficient than traditional transport, introducing a new era of disruptive change in mobility. We are focused on creating secure and safe infrastructure solutions for this highly complex and dynamic technology.

Cybersecurity:
Security and trust are key words associated with doing business in Luxembourg, allowing the country to build a financial centre that manages assets many times the size of the national GDP. Cloud-based infrastructures are the future for much of the service-based economy, offering flexibility, scalability, and affordability. These systems must be designed to ensure resilience against faults and human error as well as to resist security attacks. Critical infrastructures present a special challenge, allowing researchers to push the envelope regarding security and resilience. Cybercrime and other forms of targeted and advanced persistent threats impose a permanent risk to these systems, and Luxembourg must be at the forefront of cybersecurity if it is to maintain and strengthen the country's position internationally.

Internet of Things:
Whether in use for smart homes, cities, or manufacturing, IoT offers tremendous opportunities to build services to improve our lives. To make this a reality, we are building smart, secure, and private IoT solutions and data analytics.

Secure and Compliant Data Management:
The new economy is data driven, and current data protection and privacy regulations create an opportunity for Luxembourg to establish itself in the domain. Our research into scalability, security, affordability, and compliance for the management and protection of data is crucial to this initiative.

PARTNERSHIP PROGRAMME

SnT is guided by the principle that excellent scientific research can address the most pressing challenges society faces, while supporting industry in developing solutions. This foundation defines its set-up. SnT has a partnership model that enables collaborative research with players from the private and public sector, addressing relevant challenges based on real-world data and systems. This approach creates a lively ecosystem that feeds the local talent pool and supports the local economy.

In the area of cybersecurity, SnT has partnerships with Huawei, CREOS, VAIL, Proximus, QRA, Ministry of Foreign Affairs (Department of Cooperation) and MEGENO.

Luxembourg/West Africa Lab for Higher Education Capacity Building in Cybersecurity (LuxWAyS) is the latest example of a partnership in cybersecurity. LuxWAyS is an ambitious project for higher education cooperation between Luxembourg and the target countries of Luxembourg cooperation. LuxWAyS aims at training cybersecurity experts (€ 1.5 M – ten PhD students over five years) within the West Africa sub-region in collaboration with the Université Cheikh Anta Diop de Dakar (UCAD), Senegal; Université Joseph Ki-Zerbo (UJKZ), Burkina Faso; and the Université Virtuelle du Burkina Faso (UVBF), Burkina Faso.

RESEARCH GROUPS

Teams across SnT currently execute more than 40 projects relating to cybersecurity.

Furthermore, SnT is the only organisation in Europe with a presence in three of the four H-2020 networks, underlining its reputation in the domain (CONCORDIA, Cybersecurity for Europe, SPARTA).

Among SnT's 15 research groups, five groups focus on cybersecurity:

CRITICAL AND EXTREME SECURITY AND DEPENDABILITY (CRITIX)

Interim head – Prof. Marcus Voelp

CritiX pursues state-of-the-art research in a problem area that may be described as extreme computing – computer science and engineering pushed to the extremes of functional and non-functional properties of systems. Amongst others, they investigate architectures, middleware, algorithms and protocols that may find applicability in distributed systems and networks, which, for example:

- Deploy extremely large-scale data sets, flows and computations – considering cloud, big data, complex event processing

- Withstand extreme levels of threat, such as advanced persistent threats – considering critical information infrastructures

- Need to have extremely low failure probability – considering high-criticality areas such as finance, energy, networking (SDN), or aerospace and autonomous vehicles

- Present extreme requirements with regards to data privacy and integrity – considering e-health, genomics, or business/finance

Resilient modular and distributed computing is a response to the need for a paradigm shift enabling a comprehensive approach to those extreme challenges, from first principles: architecting and designing for simultaneously coping with accidental and malicious disruptions; providing protection in an incremental way; and automatically adapting to a dynamic range of scale, severity, and persistence of threats, some of which may be unknown. Paradigms and techniques emerging from this research should endow systems with the capacity of defeating extreme adversarial power, accidental or malicious (severe and continued threats) and sustaining perpetual and unattended operation (in a systematic and automatic way).

CRITIX plans on addressing this level of threat drawing from and building on recent research on powerful and innovative automatic security and dependability techniques, such as fault and intrusion tolerance or Byzantine fault tolerance (BFT), trusted computing and architectural hybridisation, secret sharing and secure multi-party computation, self-healing and diversity, or post-compromise security. Furthermore, the research will leverage enhanced formal verification techniques such as interactive theorem proving, to achieve ultra-high reliance on software used behind roots-of-trust or TCBs.

Project acronym	Project name	Principal investigator	Funding body	SnT research group
HyLIT	Architectural Support for Intrusion Tolerant Operating-System Kernels	M. Voelp	FNR	CritiX
CyberSec4Europe	Cybersecurity Network of Competence Centres for Europe	P. Esteves Verissimo	EC	CritiX
ADMORPH	Towards Adaptively Morphing Embedded Systems	M. Voelp	EC	CritiX
GenoMask – PoC	Early stage read filtering and masking of genomic information POC	J. Decouchant	FNR	CritiX
IISD	Strategic RTnD Program on Information Infrastructure Security and Dependability	P. Esteves Verissimo	FNR	CritiX
SPARTA	Special projects for advanced research and technology in Europe	P. Esteves Verissimo	EC	CritiX
ByzRT	ByzRT: Intrusion resilient real-time communication and computation in autonomous systems	P. Esteves Verissimo	FNR	CritiX
ThreatAdapt	Adaptive Byzantine Fault and Intrusion Tolerance	P. Esteves Verissimo	FNR	CritiX
CritiX-CARS	Architectural Support for Efficient Domain-Specific Byzantine Fault and Intrusion Tolerance	P. Esteves Verissimo		CritiX

CRYPTOLUX

Prof. Dr. Alex Biryukov

CryptoLUX is a cryptology research group headed by Prof. Alex Biryukov.

The mission of the CryptoLUX group is to define, conduct, and disseminate leading-edge research in cryptology (and closely related fields), and to pass the knowledge gained from research on to students and industry partners. CryptoLUX is one of the few academic research teams worldwide that possesses expertise across the full spectrum of cryptology, ranging from theoretical foundations to implementation aspects and applications. Our mission and objectives are devised in accordance with the three main goals of the University of Luxembourg, which are teaching, research and knowledge transfer at the highest international level. Members of CryptoLUX collaborate with top research groups around the world and participate in activities of ECRYPT, the European network of excellence in cryptology. Our current research projects cover a wide variety of topics including algorithm design (block ciphers, hash functions, etc.), cryptanalysis, communication security and anonymity, efficient implementations, side-channel attacks, and reverse engineering.

Emerging information and communication technologies, such as cloud computing or the Internet of Things, pose a number of unique challenges related to the design and implementation of cryptographic primitives, which has initiated a large body of research in these areas. Nonetheless, the number of cryptanalytic attacks (both traditional ones as well as side-channel attacks) is steadily increasing, and many of these attacks have led to devastating security breaches with fatal consequences. We envisage CryptoLUX positioning itself at the forefront of an international research community that tackles these challenges and develops innovative solutions for complex security problems based on a solid cryptographic foundation. To achieve this, we strive for a greater understanding of how cryptosystems break (or otherwise fail) in the real world, how they can be designed and implemented to better resist attacks, and how they should be used to build secure systems and networks.

Project acronym	Project name	Principal investigator	Funding body
FinCrypt	Security, Scalability, and Privacy in Blockchain Applications and Smart Contracts	A. Biryukov	FNR
APLICA	Analysis and Protection of Lightweight Cryptographic Algorithms	A. Biryukov	FNR

## APPLIED SECURITY AND INFORMATION ASSURANCE (APSIA)

Prof. Dr. Peter Y.A. Ryan

The *Applied Security and Information Assurance Group* (APSIA) is headed by Prof. Dr. Peter Y. A. Ryan, Professor of Applied Security.

The APSIA Group specialises in the design and analysis of secure systems:

- Cryptographic Protocols (classical and quantum)

- Cryptographic Algorithms and Primitives

- Information Flow

- Verifiable Voting Schemes

- Socio-Technical Analysis of Security

- Privacy Enhancing Technologies

Project acronym	Project name	Principal investigator	Funding body
Q-CoDe	Quantum Communication with Deniability	P. Ryan	FNR
EquiVox	Secure, Quantum-Safe, Practical Voting Technologies	P. Ryan	FNR
FutureTPM	Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module	P. Ryan	EC
STV	Socio-Technical Verification of Information Security and Trust in Voting Systems	P. Ryan	FNR
SZK	Stateful Zero-Knowledge	A. Rial	FNR
SmartExit	Facilitating optimal containment and exit strategies with minimal disclosure access control and tracking	P. Ryan	FNR
SURCVS	Secure, Usable, Robust Cryptographic Voting Systems	P. Ryan	FNR
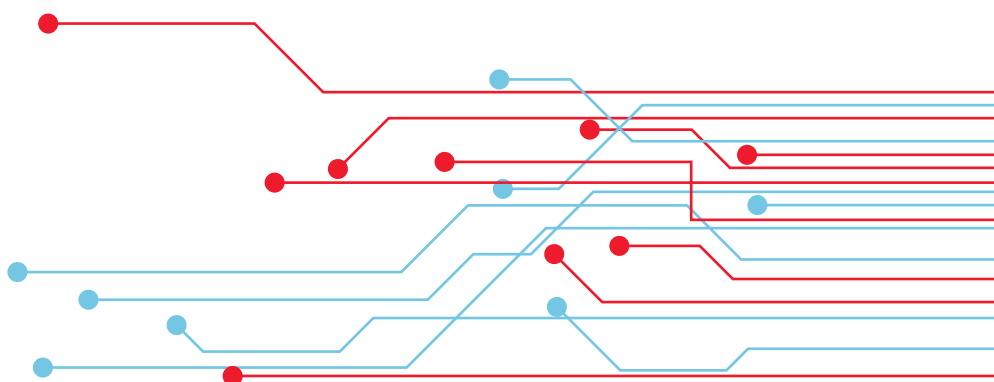
SOCIO-TECHNICAL CYBERSECURITY (IRISC)

Prof. Dr. Gabriele Lensing

The research group positions its research in the area of *sociotechnical cybersecurity*. Today, securing a system requires one to understand not only digital communications and protocols but also the human and legal reality where the system is deployed.

IRiSC's research recognizes this change in perspective: its focus on design and analysis of secure systems considers holistically both the technical, the social, and the legal frameworks. IRiSC's research is about, but not limited to, the following areas:

- Human-centred cybersecurity

- Usability security and user experience

- Cyberattacks and cyber defences

- Information and system security

- Data protection and legal compliance

- Ethics and human rights

IRiSC researchers follow methodologies that include formal computational methods, as well as quantitative and qualitative research methods. IRiSC researchers have an inter-disciplinary education, combining information security and social science, physics, or law. They all participate in the research of a cross-disciplinary nature.

Project acronym	Project name	Principal investigator	Funding body
NoCry PoC	No More Cryptographic Ransomware, Proof of Concept	G. Lenzini	FNR
ConGenIAL	Consent to turn Genome into Individual's Asset for a Lifetime	G. Lenzini	FNR
LEGAFIGHT	Legally Fighting Covid-19 – LEGAFIGHT	E. Poillot	FNR
LeADS – Resubmission 2	Legality Attentive Data Scientists – Resubmission 2	G. Lenzini	EC
SSh	Security in the Shell	J. Lagerwall	FNR

TRUSTWORTHY SOFTWARE ENGINEERING (TRUX)

Prof. Dr. Jacques Klein

TruX is a software engineering and software security research group that develops innovative approaches and tools to help the research and practice communities build trustworthy software. Trustworthy software has reduced vulnerabilities; when it fails, it can be repaired automatically; when it operates, it can justify its execution drives.

TruX explores the huge data on software development artefacts (including source code and textual information in repositories, such as bug reports, reviews, etc.) to derive knowledge on how to automate the analysis, construction, and repair of software programs. In particular, TruX conducts research in three main areas:

1. Software security: by developing new tools and approaches to assess and ensure security and privacy properties of software applications. Examples of research activities are the detection of privacy leaks in Android apps or the detection of vulnerabilities in open-source software at "commit time".

2. Software repair: by devising and implementing novel algorithms, methodologies, and tool support for automatically repairing programs. This is performed by identified bug or vulnerability locations and applying code change operations that will enable the programs to satisfy correctness criterion. TruX is particularly focused on inventing software repair solutions that are in line with practitioners' constraints.

3. Explainable software: by ensuring that software engineering solutions to business problems are not black-box solutions but, instead, provide explanations and contextual information to help end users. This research direction is in line with an emerging requirement in the field of artificial intelligence where models and techniques must be devised in such a way that the results of an AI solution can be understood by human experts. Given the use of AI algorithms in several of our research areas, we also investigate directions on making the analyses tractable.

Tools for practitioners: TruX aims at developing both practical and fundamental research solutions. Practical, because TruX directly targets practitioners with the ambition to release tools that are relevant for developers. Fundamental, because TruX investigates key open and hard software engineering problems such as the definition of code similarity (e.g. representation learning techniques for semantic code clone identification), the derivation of abstract repair operators that are less prone to test overfitting, etc.

Project acronym	Project name	Principal investigator	Funding body
CHARACTERIZE	Characterization of Malicious Code in Mobile Apps: Towards Accurate and Explainable Malware Detection	J. Klein	FNR
CatchMe	Android Malicious code Localisation: Catch Me if You can!	J. Klein	FNR
HitDroid	Hinting at Malicious Code in Android Apps Identifying Malicious Payloads in Malware at Market Scale with Graph and Data Clustering Techniques	J. Klein	UL
LuxWAys	Luxembourg/West Africa Lab for Higher Education Capacity Building in Cybersecurity and Emerging Topics in ICT4Dev	T.F.D.A. Bissyande	

Other teams also undertake research projects in the area of cybersecurity and the list below provides an overview of these projects:

Project acronym	Project name	Principal investigator	Funding body
CLOUDMAP	Cloud Computing via Homomorphic Encryption and Multilinear Maps	J. Coron	EC
SWITECH	Secure Software using Whitebox Technology – resubmission	J. Coron	FNR
PrivDA	Privacy-preserving Publication of Dynamic Social Network Data in the Presence of Active Adversaries	Y. Ramirez-Cruz	FNR
PriML	Privacy Attacks and Protection in Machine Learning as a Service	J. Pang	FNR
PandemicGR	Information Diffusion in Twitter during the COVID-19 Pandemic: The Case of the Greater Region	J. Pang	FNR
DGAP	Real time prediction and detection of malicious activities	R. State	FNR
CONCORDIA	Cybersecurity Competence for Research and Innovation	R. State	EC
FIN-TECH	A financial supervision and technology compliance training programme	R. State	EC
STARTS	Security Assessment of TrustZone-M enabled Software	A.K. Iannillo	FNR
Incident Management and Software Testing	Incident Management and Software testing	Y. Le Traon	UL
SATOCROSS	Support of Advanced Test Coverage Criteria for Robust and Secure Software	Mr. Papadakis	FNR
Fb testing and verification	Detecting (flaky) test failures of system user interactive tests	Mr. Papadakis	Other funding body
ONNIVA	Automatic Detection and Prevention of Deserialization Vulnerabilities	A. Bartel	FNR
EQUACS	Early Quality Assurance of Critical Systems	M. Sabetzadeh	FNR
FAQAS	Fault-based, Automated Quality Assurance Assessment and Augmentation for Space Software	F. Pastore	ESA
COSMOS	DevOps for Complex Cyber-physical Systems	L. Briand	EC

# 5.2 LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY (LIST)

The IT for Innovative Services (ITIS) department of the Luxembourg Institute of Science and Technology (LIST) combines both scientific and applied research activities with some 120 skilled engineers and highly qualified researchers. Within ITIS, the team involved in cybersecurity has a focus on data privacy and security, cyber system security and information security management. It comprises 10 researchers with a well-balanced mix of engineers, researchers holding a PhD as well as collaborators working on their PhD projects.

On the scientific side, the team focuses on modelling, designing, and analysing new algorithms, protocols, and systems for cyber-resilience. The research activities are mainly supported by funding from the FNR CORE/INTER and EU Horizon 2020 programmes.

On the applied side, the research focuses on practical cybersecurity challenges, e.g. application and development of crypto tools and privacy preserving technologies, design and implementation of blockchain technologies to solve security and privacy issues, support to regulator/regulated entities to comply with new and multiple regulations (risk management, compliance, data analytics). Such research activities are supported by private and public partners, FNR CORE/INTER, EU Horizon 2020 and Erasmus +, Connecting Europe Facility (CEF), Luxembourg's RDI Law, as well as in collaboration with industrial partners. In addition, researchers are involved in academic training, providing lectures in cybersecurity at Master level (University of Luxembourg, University of Lorraine, etc.) as well as in professional training.

The previously mentioned research activities of ITIS contribute to the whole National Cybersecurity Strategy. However, there is currently a particular focus on Guideline n°2 of the National Cybersecurity Strategy on Digital Infrastructure Protection. Nevertheless, others are addressed as well, in line with objectives such as creation of new products and services, risk management, training, etc.
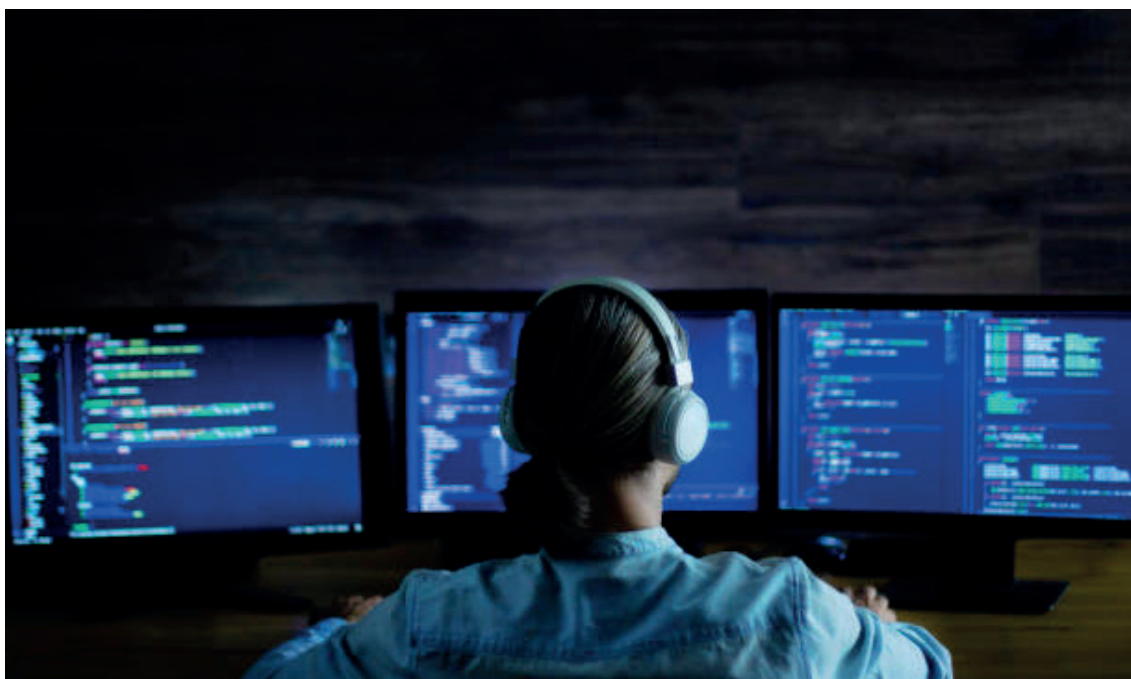
RESEARCH AREAS
DATA SECURITY AND DATA PRIVACY

LIST has extensive expertise in the foundations of data security and data privacy. Such expertise includes cryptographic algorithms and protocols as well as standard and emerging privacy enhancing technologies. Examples are statistical disclosure control and differential privacy. To this end, LIST consistently publishes new scientific results at conferences and in journals. Driven by the nature of RTO, LIST has used this expertise in areas of practical application. Notably, LIST is working on the design of efficient authenticated and key agreement protocols for IoT devices, the trustworthiness of machine learning solutions with a focus on data-oriented aspects (e.g. data poisoning and adversarial examples), and security and privacy issues for 5G ecosystems with a focus on API security. In addition, LIST is also working on the security and privacy aspects of Distributed Ledger Technologies (DLTs) and blockchain solutions, as well as the application of such technologies in domains such as dangerous goods transportation and housing.

The work carried out by LIST has made it possible to:

- Evaluate the security and privacy issues (and more generally trustworthiness) of existing ICT systems,

- Enhance the current systems with new algorithms (e.g. homomorphic encryption), protocols (e.g. privacy-preserving machine learning) and processes (e.g. how contact tracing is done),

- Apply new technologies such as machine learning and DLT/blockchain to new application scenarios in a responsible and accountable manner,

- File a patent (LU100580 – 12/2017) about a solution dedicated to the protection and valorisation of Internet user profiles.

CYBER SYSTEM SECURITY AND RESILIENCE

Research performed within this thematic is twofold. On the one hand, activities are centred around a full-spectrum cybersecurity awareness. LIST works on an approach to the modelling of the services, organisations, and infrastructures to enable security-related knowledge sharing, integration and better resilience of critical infrastructures and their related essential services. This approach relies on information security management outputs to enable continuous real-time incident prevention, detection, reaction, and mitigation. This allows increasing resilience to cybersecurity threats and potential cascading events, while ensuring a continuous alignment to cybersecurity requirements and finally feeding back information security risk analyses. This approach is based on the development of distributed technological artefacts, massive data exploitation and the use of artificial intelligence technologies for real-time cybersecurity protection.

On the other hand, LIST works on intelligent infrastructures with their IoT devices that are integrated into an edge-, fog- and cloud-computing concept, for which high-assurance of resilience against various types of attacks is crucial. In this sense, LIST identifies and specifies the key components, their functions and services, as part of an orchestration framework that are needed to ensure pre-defined security levels, and which take the heterogeneous setup of potential IoT infrastructures into account. Additionally, novel cryptographic mechanisms that will implement the privacy-by-design concept in the domain of intelligent infrastructures and IoT networks are evaluated and proposed. Blockchain/DLT are seen as the potential base of resilient infrastructures that targets distributed applications in an environment of partners which are not necessarily fully trusted. We are investigating use cases that could benefit most from the fundamental properties of blockchain/DLT and trying to create resilient solutions based upon the latest existing frameworks.

The work carried out by LIST has made it possible to:

- develop a risk-based methodology for real-time security monitoring of interdependent services in critical infrastructures,

- develop a distributed architecture allowing continuous real-time incidents prevention, detection, reaction, and mitigation for critical infrastructures,

- apply new technologies such as DLT/blockchain in order to create resilient infrastructures for certain use cases.

LIST is working on a security risk management framework that is directly linked to the work on resilience, and covers the entire regulatory cycle from the processing of security risk management by the regulated entities to the gathering and analysis of risk-related data by the regulator. The aim is to adopt a framework allowing integration of risk management specificities from various regulations and deal with all of them in an integrated manner. The framework has been implemented in a technological platform encompassing a risk management, an incident management, and a data analytics module. The outcome of this work is an improvement of the quality of risk management results and the reduction of the costs involved in compliance. Sector-based and systemic governance of cybersecurity are part of the key benefits of the approach.

A special focus in the next two years will be on the extension of models and best practices to the emergence of 5G and to the publication of the European Electronic Communications Code (EECC). In 2021, the regulatory platform will welcome around 100 companies from all sectors. A roadmap for improving methodologies and functionalities is also being developed over the next three years in collaboration with an industrial partner, the regulators (ILR in Luxembourg, BIPT in Belgium) and the companies concerned.

The work carried out by LIST has made it possible to build:

- a set of standard risk analysis models,

- a regulatory platform enabling all companies in the relevant sectors to manage their risks, report their risks to the regulator and notify incidents,

- data analytics capabilities at sectoral level for regulators.
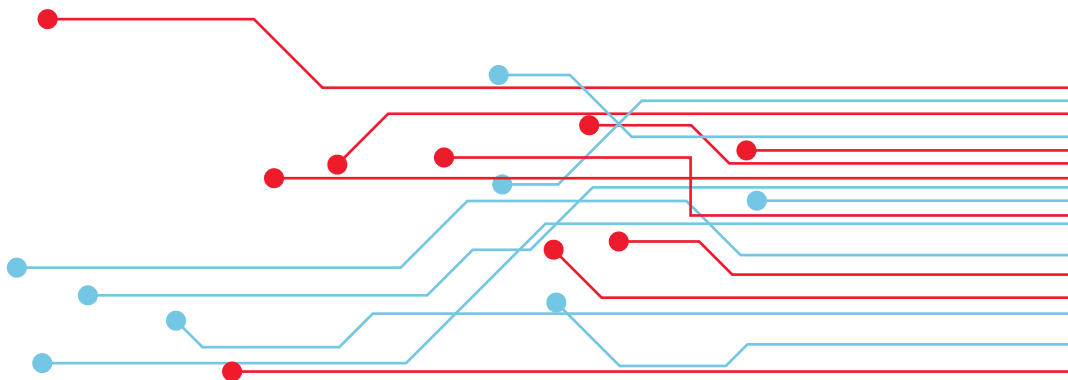
PROJECTS AND PARTNERS

PROJECTS:

EU PROJECTS

- **SPARTA (H2020)**: Developing a methodology enabling real-time critical infrastructures incidents prevention, detection, reaction and mitigation, and toolkits and frameworks supporting the design, development and verification of security-critical, large-scale distributed systems forming an Intelligent Infrastructure.

- **TOKEN (H2020)**: Providing enablers for the introduction of disruptive technologies (namely DLT and blockchain) that contribute to accelerating the transformation of public services towards an open government model based on the principles of collaboration, transparency, and participation.

- **NISDUC (CEF)**: Developing a set of activities aimed at raising awareness, competencies, and capabilities for NIS Directive actors (national authorities, operators of essential services, and digital service providers) together with SECURITYMADEIN.LU, ILR and IBPT.

- **Housing+ (Erasmus+)**: Improving academic training in the housing and real estate field among professionals, stakeholders, policymakers and academics through training materials with an interdisciplinary, international and new technologies content (i.e., DLT and blockchain), videos and gamification.

FNR:

- **DECEPTICON**: Developing procedures and tools to support various stakeholders in order to assess the presence of dark patterns in online services.

- **CATALYST**: Designing efficient authenticated and key agreement protocols for IoT devices and designing of privacy-preserving IoT data analysis protocols.

- **5G INSIGHT**: Designing novel security mechanisms ranging from attack detection to attack mitigation leveraging novel

tools and paradigms such as those based on machine learning (ML), particularly federated and deep learning, to blockchains and deception security, while considering the specific but highly sensitive (in terms of security) case of cross-border areas (i.e., the France-Luxembourg cross-border case).

- **REGTECH4ILR**: Developing a security risk management framework, comprising a regulatory authority part and a regulated entity part.

COLLABORATIVE PROJECTS:

- **DG-SEC (DoD)**: Developing a blockchain-based system to support the authorisation and improvement of security in the execution of the transport of dangerous waste across Europe.

- **NIS Cooperation (ILR)**: Work on developing and adapting a security risk management framework to include the sectors of the Law of 28 May 2019 transposing the NIS Directive, taking into account systemic risks in and between sectors.

RDI LAW PROJECT:

- **POST 5G Secure Experienc**e: Developing a 5G telecom security platform (a comprehensive Telecom Intrusion Detection System) over three years to protect the POST network and its users from exploits at infrastructure level against Telecom attacks such as SMS spoofing, call and SMS interception, signalling intrusion.

SERVICES AND TRAINING:

- **Consultancy on blockchain for INFRACHAIN** including the setup of an EBSI (European Blockchain Service Infrastructure) node for Luxembourg.

- **Professional trainings on security with Uni.lu**

INTERNALLY FUNDED PROJECTS:

- **PhD thesis on Blockchain in Dangerous Goods Transportation**

PARTNERS:

STAKEHOLDERS:

- **Regulation ecosystem** (regulators, regulated entities, and RegTech providers)
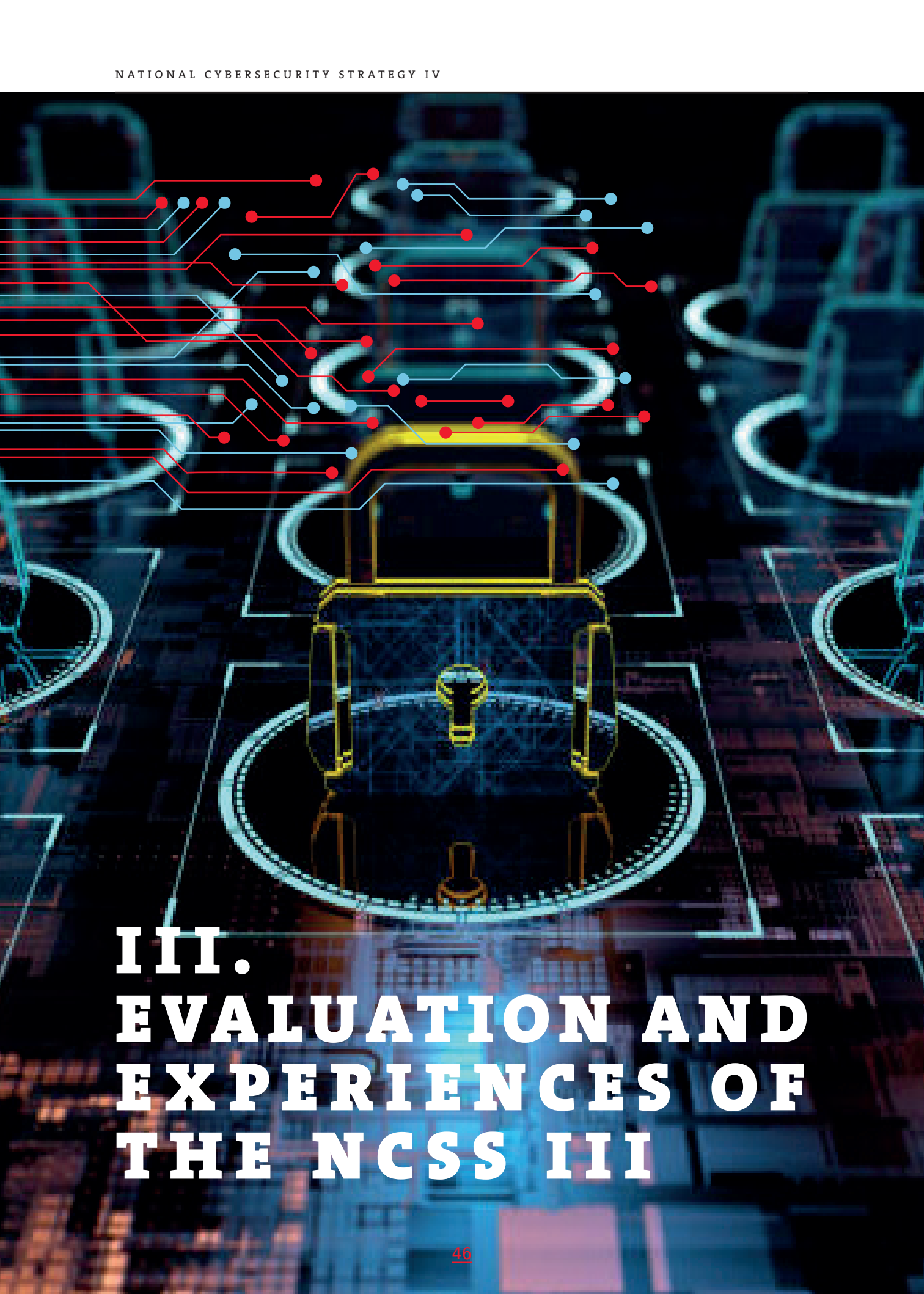
- **ICT organisations**.

COOPERATION PARTNERS (NATIONAL):

- **Authorities** (Ministry of Foreign and European Affairs – Defence, CIRCL)

- **Regulators** (ILR in Luxembourg and BIPT in Belgium)

- **Academia** (Uni.lu (MSSI Master, PhD supervision), SnT)

- **Technology providers** (Westpole, RoamsysNext, Post, Compellio)

- **Initiatives/Associations/Networks** (Infrachain, Luxembourg Blockchain Lab, CLUSIL, SDAM alliance)

COOPERATION PARTNERS (INTERNATIONAL):

- **H2020 consortia** across Europe

- **Academia** (University of Vienna and AIT), TNO (The Netherlands), SUTD (Singapore), University Paris Saclay (France)

III.
EVALUATION AND
EXPERIENCES OF
THE NCSS III

The third National Cybersecurity Strategy (NCSS III) was structured along three guidelines and its action plan listed 61 concrete actions, the vast majority of which have been implemented. The following is a selection of the results:

**FIRST GUIDELINE: STRENGTHENING PUBLIC CONFIDENCE IN THE DIGITAL ENVIRONMENT**

- To strengthen public confidence in the digital environment, the NCSS III has focused on collecting and sharing relevant information in the field of cybersecurity.

- On the side of collecting information on incidents and the threat landscape, the national CSIRTs cooperated within the national CERT.LU network. This has allowed it to gather and share information related to incidents at national level and to share it in the respective constituencies.

- Several strands of activities at international level (FIRST.org, TF-CSIRT, CiviCERT, OASIS Open, IETF, NIS CSIRT network, Europol) were pursued with a focus on technical and practical issues of information sharing, incident response and automation of relevant processes.

- The problems of cybercrime and disinformation campaigns were addressed in multidisciplinary working groups, set up on an ad-hoc basis and according to current events and international cooperation, particularly within the European Union. The securing of European elections or the response to extremist tendencies on social networks are two examples of cooperation. The organisations that have contributed to the achievement of the objectives under this guideline are mainly the Ministry of State, the National Youth Service, the Ministry of Education, the Ministry of the Economy, Security Made in Luxembourg, Kanner- a Jugendtelefon, the Ministry of the Family, BEE SECURE, GOVCERT, the High Commission for National Protection, the Ministry of European and Foreign Affairs, the Police and the Public Prosecutor's Office.

**SECOND GUIDELINE: PROTECTION OF DIGITAL INFRASTRUCTURES**

- With the transposition of the European Directive on security of networks and information systems (NIS) and the identification of critical infrastructure by the HCPN, a new foundation for strengthening the resilience of the State's digital infrastructure was established under the NCSS III. In the field, one of the concrete results was the implementation of the Distributed Denial of Service (DDoS) attack filtering centre, which mitigates such attacks at high volumes. Thus, additional protection for digital infrastructures and an increase in the resilience of the ICT sector at national level has been achieved.

- In the context of the refinement of our cyber crisis management procedures, relevant players have participated in major international cyber exercises organised by the European Union and NATO.

THIRD GUIDELINE: PROMOTION OF THE BUSINESS LOCATION

- In 2018, the Ministry of the Economy prepared a data-driven economy strategy (approved by the Government in Council on 26 April 2019). A legal analysis has been carried out in relation to the legislative work that still needs to be done. Since then, the Ministry has launched work on the establishment of a trusted third party in the field of pseudonymisation and anonymisation. This work is coordinated with the establishment of the European High Performance Computing Competence Centre (EuroHPC). Cooperation with the National Commission for Data Protection (CNPD) has been initiated to make available in Luxembourg an GDPR code of conduct for pseudonymisation and anonymisation.

- A new version of the MONARC platform has been developed and now also includes the possibility to link the risk analysis to requirements frameworks and to automatically create statements of applicability (SOA), as foreseen in the ISO/IEC 27001 standard.
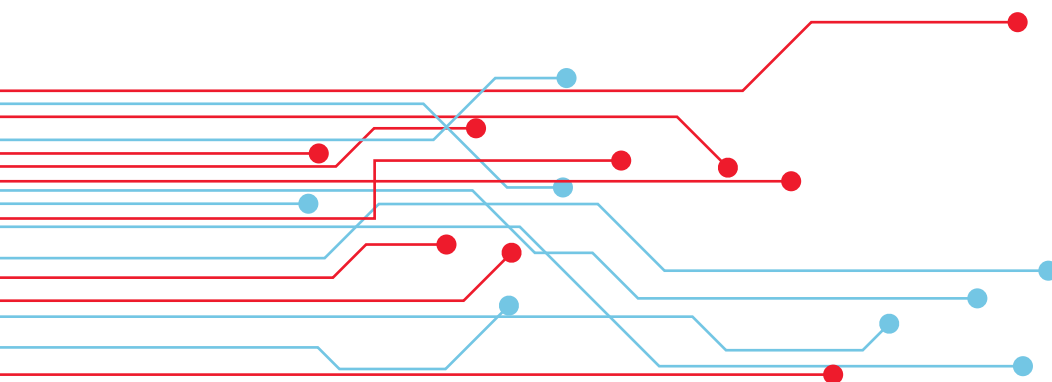
IV.
ACTION PLAN
(NON-PUBLIC)
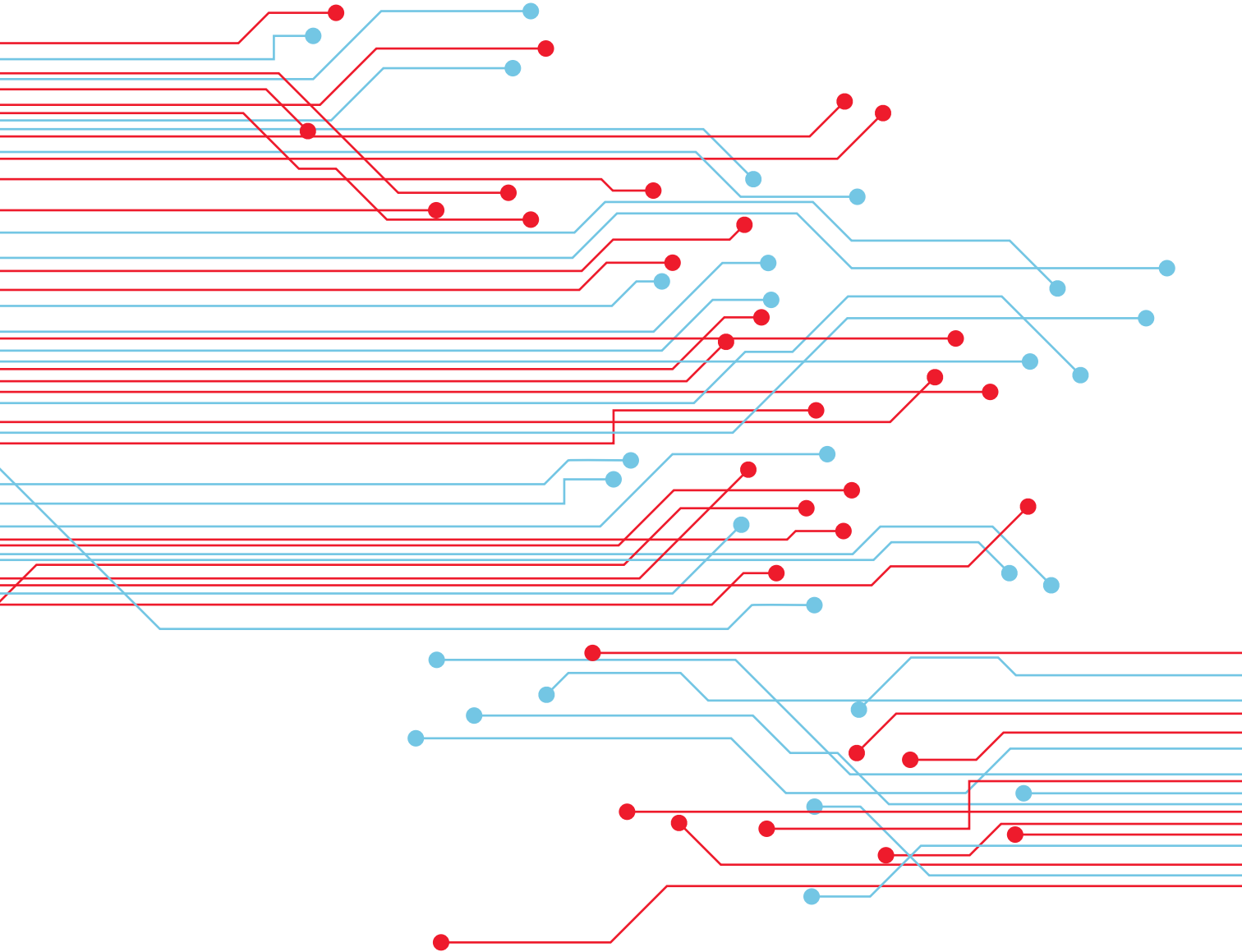
GLOSSARY

ANSSI

National Agency for Information Systems Security (*Agence nationale de la sécurité des systèmes d'information***):**
The National Agency for the Security of Information Systems is the national authority for the security of classified and unclassified information systems operated by the State. The Agency's main missions are to establish the general information security policy for the public sector, to define, in consultation with concerned players, information security policies and guidelines for specific domains, to define the information security risk management approach and to promote information security by awareness raising measures.
The function of National Agency for the Security of Information Systems is carried out by the High Commission for National Protection

CASES

Cyberworld Awareness & Security Enhancement Services*: department of SECURITYMADEIN.LU*

CERC

Cyber Risk Assessment Unit (*Cellule d'Evaluation du Risque Cyber***):**
Group of cyber experts created in the context of the "PIU Cyber"

CERT

Computer Emergency Response Team*: Team in charge of cybersecurity incidents*

CIRCL

Computer Incident Response Center Luxembourg*: department of SECURITYMADEIN.LU*

C3

Cybersecurity Competence Center*: department of SECURITYMADEIN.LU*

CNPD

National Commission for Data Protection (*Commission nationale pour la protection des données***)**

CSIRT

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

CSSF

Financial Sector Supervisory Commission (*Commission de surveillance du secteur financier*)

CTIE

Government IT Centre (*Centre des technologies de l'information de l'État*)

EC3

European Cybercrime Centre

ENISA

European Network and Information Security Agency

FIRST

Forum of Incident Response and Security Teams

GDPR

General Data Protection Regulation

GOVCERT

Governmental CERT:
The main missions of the Governmental CERT (GOVCERT) are to constitute a single point of contact dedicated to handling large-scale security incidents affecting the networks and information systems of State administrations and departments, to provide a watch for detecting, alerting and responding to large-scale IT attacks and security incidents, and to serve as the National CERT (NCERT.LU) and Military CERT (MILCERT.LU).
The Governmental CERT falls under the authority of the High Commission for National Protection.

HCPN

High Commission 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 addresses hybrid threats that include a cyber aspect.

ICT

Information and Communication Technology

ILNAS

Luxembourg Institute for Standardisation, Accreditation, Safety and Quality of Products and Services (*Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et de la qualité des produits et services*)

ILR

Luxembourg Institute of Regulation

MISP

Malware Information Sharing Platform

MONARC

CASES Risk Analysis Methodology

MOSP

MONARC Objects Sharing Platform

MoU

Memorandum of Understanding

PIU

Emergency Response Plan (*Plan d'intervention d'urgence*)

SECURITYMADEIN.LU

« Security Made in Lëtzebuerg » g.i.e. is the Cybersecurity Agency for the Luxembourg Economy and Municipalities. Its public mission aims to deliver high value-added services for the private sector, municipalities and other non-governmental entities, helping them to:
- detect and react to cyber attacks (CRICL);
- do governance and risk management (CASES) ;
- reinforce competence and capacity building (C3) ;
- federate and promote the ecosystem (CYBERSECURITY Luxembourg).

SMC

Department of Media, Telecommunications and Digital Policy (*Service des médias, des communications et du numérique*)