CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Cybersecurity Organisation: Luxembourg

Philippe Mitsuya Zotz
NATO CCDCOE Cyber defence expert

National Cybersecurity Governance Series

Tallinn 2021

About this study

This publication is part of a series of country reports offering a comprehensive overview of national cybersecurity governance by nation. The aim is to improve awareness of cybersecurity management in the various national settings, support nations enhancing their own cybersecurity governance, encourage the spread of best practice and contribute to the development of interagency and international cooperation.

Primarily focusing on NATO Nations that are Sponsoring Nations of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), each country report outlines the division of cybersecurity roles and responsibilities between agencies, describes their mandate, tasks and competencies and the coordination between them. In particular, it covers the mandates of political and strategic management; operational cybersecurity capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and management. It offers an introduction to the broader digital ecosystem of the country and outlines national cybersecurity strategy objectives in order to clarify the context for the organisational approach in a particular nation.

CCDCOE

The NATO CCDCOE is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 29 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the Tallinn Manual, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring the Centre hosts the International Conference on Cyber Conflict, CyCon, a unique event bringing together key experts and decision-makers of the global cyber defence community. Since January 2018, CCDCOE has been responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations, currently: Austria, Belgium, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

Reports in this series

National Cybersecurity Organisation in Czechia
National Cybersecurity Organisation in Germany
National Cybersecurity Organisation in Estonia
National Cybersecurity Organisation in France
National Cybersecurity Organisation in Hungary
National Cybersecurity Organisation in Italy
National Cybersecurity Organisation in Lithuania
National Cybersecurity Organisation in Luxembourg
National Cybersecurity Organisation in the Netherlands
National Cybersecurity Organisation in Poland
National Cybersecurity Organisation in Romania
National Cybersecurity Organisation in Spain
National Cybersecurity Organisation in Slovakia
National Cybersecurity Organisation in Turkey
National Cybersecurity Organisation in the United Kingdom
National Cybersecurity Organisation in the United States
China and Cyber: Attitudes, Strategies, Organisation
National Cybersecurity Organisation in Israel

Series editors: Kadri Kaska and Keiko Kono (CCDCOE)
Information in this document has been checked for accuracy as of March 2021.

Table of Contents

1. Digital society and cybersecurity assessment

Country indicators[1]

626.108	Population
93%	Internet users (% of population)
2,586	Area (km²)
120 980	GDP per capita (USD)[2]

International rankings

9th	ICT Development Index (ITU 2017)
18th	E-Government Development Index (UN 2018)
6th	Digital Economy and Society Index (EU 2019)
11th	Global Cybersecurity Index (ITU 2018)
32th	National Cyber Security Index (eGA 2019)

1.1 Digital infrastructure availability and take-up

Over 90% of Luxembourg households had a fixed broadband connection in 2020, and 45% had fixed broadband connections of 100Mbps or above. These numbers put Luxembourg above the EU average overall fixed broadband take-up, which is 78%. Fibre to the Premises (FTTP) coverage is reported at 68% of households, with fibre roll-out mainly performed by the state-owned company, POST.[3]

Luxembourg's wireless connectivity coverage for 4G reaches practically all of the country's households (98%), slightly above the European average (96%). By the end of 2019, Luxembourg had not made spectrum in the 700 MHz, 3.6 GHz and 26 GHz available for 5G,[4] but despite the COVID-19 pandemic, progress in this area was made in 2020. The national 5G strategy published in November 2018 by the Ministry of State's Department of Media, Telecommunications and Digital Policy (*Service des médias, des communications et du numérique*) stated that the 26 GHz band would be made available and 5G pilots would begin in 2020. In April 2020, a ministerial decision concerning the competitive selection by auction for the 700 MHz and 3.6 GHz ranges detailing the procedure and conditions was published.[5] Following the auction, a 15-year right of use period of the 700 MHz band was awarded to POST, Orange and Proximus while rights for the 3.6 GHz band were allocated to Luxembourg Online, Orange, POST and Proximus.[6] According to the *Digital Economy and Society Index 2020*, 5G will play a significant role for the 32% of households not connected to the fibre network, furthering connectivity.

[1] Grand Duchy of Luxembourg Statistics Portal, https://statistiques.public.lu/en/ (if not stated otherwise).
[2] OECD country data profile for Luxembourg, https://data.oecd.org/luxembourg.htm.
[3] Digital Economy and Society Index, Country Profile: Luxembourg (DESI 2020 Report), https://ec.europa.eu/digital-single-market/en/scoreboard/luxembourg.
[4] Digital Economy and Society Index, Country Profile: Luxembourg (DESI 2020 Report), https://ec.europa.eu/digital-single-market/en/scoreboard/luxembourg.
[5] 5G strategy for Luxembourg, Roadmap for the 5th generation of mobile communication in Luxembourg, 2018, https://digital-luxembourg.public.lu/stories/luxembourgs-5g-strategy.
[6] Service des médias, des communications et du numérique: Résultat des enchères en vue de l'octroi des fréquences destinées à la 5G (Communiqué du 22.07.2020), https://smc.gouvernement.lu/fr/actualites.gouvernement%2Bfr%2Bactualites%2Btoutes_actualites%2Bcommuniques%2B2020%2B07-juillet%2B22-resultats-5g.html.

1.2 Digital public services

Luxembourg ranks 14th in the European Union in digital public services, above the EU average, although the engagement of users with e-government services of 58% is still below the EU average of 67%.[7] Digitalisation is a central topic for Luxembourg, demonstrated by the establishment of a new Ministry for Digitalisation (*Ministère de la Digitalisation*) in 2018. The new Ministry has as its agenda to realise the action plan *Digital Luxembourg*, promote the digitalisation of administrative procedures and public service, develop digital infrastructure, promote digital inclusion and develop and realise an action plan for the internet of things.[8] *Digital Luxembourg* started in 2014 and focuses on promoting digital government, policy, infrastructure, ecosystem and skills. The initiative encompasses not only digital public services but projects like the country's open data platform (data.public.lu), a machine-readable legislation platform (legilux.public.lu), the world's first data embassy (in collaboration with Estonia), the digital administration portal *Guichet.lu* (guichet.public.lu) and others.[9]

The portal *Guichet.lu* allows Luxembourg's residents and non-residents working in or affiliated with Luxembourg access to a broad range of public services. It allows users to submit reports and applications including tax declarations, governmental student loans, declarations of stolen or lost items to the police, job applications, registration for seminars and requests for judicial records. *Guichet.lu* also allows access to personal data including residence certificates, driving licence penalty points, motor vehicles and licence plate records, the land registry, wage statements and health insurance reimbursement receipts. During the 2020 COVID-19 pandemic, the platform introduced several new processes including signing up for COVID-19 testing and applying for certificates required for travel.

Another effort for digitalisation is the online service and information platform *eSanté* (esante.lu), a result of a 2006 government initiative to provide a platform for healthcare providers to exchange data. It is an economic interest group involving, amongst others, the state, the national health fund (*Caisse nationale de santé*), the centre for social security (*Centre commun de la sécurité sociale*), associations of physicians and dentists, pharmacists and hospitals and the federation of Luxembourg medical laboratories.[10] The platform offers the public the option to share and manage their health records and health-related data digitally between stakeholders.[11]

Digital ID

Luxembourg has had an established legal framework for electronic signatures since the 2000 Law for e-Commerce.[12] Authentication comes in various ways: a one-time password generating token, Signing Stick (USB), Smartcard, smartphone applications and eID. Since 2012, Luxembourg's ID cards have been equipped with a chip that stores the data necessary for electronic authentication. Electronic certificates can be activated for ID cardholders over 15 years of age; the cards are meant for personal use.

Luxembourg's most common means of electronic authentication is provided by the trust service provider, LuxTrust. This is a public limited company where the government is the majority shareholder, with most of the remaining shares held by Luxembourg's financial sector. LuxTrust was set up in 2005 and its trust service is used for authentication in online banking and governmental services on *Guichet.lu*. LuxTrust is supervised by the Luxembourg Institute of Standardisation, Accreditation, Safety and Quality of Products and Services (*Institut luxembourgeois de la normalisation, de l'accréditation, de*

[7] Digital Economy and Society Index, Country Profile: Luxembourg (DESI 2020 Report), https://ec.europa.eu/digital-single-market/en/scoreboard/luxembourg.
[8] Arrêté grand-ducal du 5 décembre 2018 portant constitution des Ministères, http://data.legilux.public.lu/eli/etat/leg/agd/2018/12/05/a1099/jo.
[9] Digital Luxembourg: Progress Report spring 2018, https://digital-luxembourg.public.lu/sites/default/files/2018-06/DL_201804022_PROGRESS%20REPORT_08%20BAT.pdf.
[10] Agence eSanté, https://www.esante.lu/portal/de/ich-informiere-mich/die-agence-esante-259-323.html.
[11] Règlement grand-ducal du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé, http://legilux.public.lu/eli/etat/leg/rgd/2019/12/06/a909/jo.
[12] Loi du 14 août 2000 relative au commerce électronique, http://data.legilux.public.lu/eli/etat/leg/loi/2000/08/14/n8/jo.

la sécurité et qualité des produits et services or ILNAS). Its service complies with EU eIDAS Regulation 910/2014.[13]

AI and open data initiatives

Luxembourg wants to support human-centric AI development and promote AI. For government services, this would simplify administrative tasks like filling out forms and providing information for both administration and citizens. According to the national artificial intelligence strategic vision, services like *Guichet.lu* could see enhancements driven by AI in the future. A set of key actions ought to determine potential projects, collaborate with other EU member states and support AI tools for digital public services.[14]

Luxembourg ranks 19th in the EU for its use of open data.[15] The Digital Luxembourg initiative encourages making large amounts of public sector data available to the public and businesses to further transparency and openness. According to the Government's open data strategy, all data that is not subject to legal restrictions like intellectual property or matters of national security or personal information is considered open to the public.[16] The data strategy is executed and coordinated by Luxembourg's Information and Press Service (*Service Information et Presse*) and the open data platform data.public.lu. Its APIs are available to the public and businesses.

Education and research

The non-profit RESTENA Foundation provides the country's *National Research and Education Network* (NREN). Its board of directors consists of representatives of the Ministry of Education, Children and Youth (*Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse*), the Ministry of Higher Education and Research (*Ministère de l'Enseignement supérieur et de la Recherche*), the Ministry of Finance (*Ministère des Finances*), the *Centre de gestion informatique de l'éducation* (CGIE), the Government IT Center (*Centre des technologies de l'information de l'Etat* - CTIE) and the Department of Media, Telecommunications and Digital Policy (*Service des médias et des communications* - SMC). The RESTENA network not only connects schools, research facilities, museums and governmental entities, but also covers services related to education; for example, enabling the international research and education community roaming access service eduroam and e-mail and cloud services for students and teaching professionals.

Municipal digital services

On the communal level, a total of 101 municipalities with their respective inter-municipal unions, social offices and over 500 nurseries and childcare centres rely on the *Syndicat Intercommunal de Gestion Informatique* (SIGI). SIGI, established by a Grand-Ducal decree in 1982, supports the work of municipalities through digital means and promotes automation, collection and processing of data. SIGI also assists municipalities by supplying equipment, education and training and maintaining IT systems.[17]

---

[13] CERTIFICATE OF CONFORMITY for LUXTRUST by LSTI (Certificate LSTI 11085-124-V1.0), https://www.luxtrust.lu/upload/data/repository/certificate_lsti_ndeg_11085-1082_v4.0_luxtrust_1.pdf; Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC OJ L 257, 28.8.2014, p. 73–114, http://data.europa.eu/eli/reg/2014/910/oj.

[14] Artificial Intelligence: a strategic vision for Luxembourg, https://digital-luxembourg.public.lu/sites/default/files/2019-05/AI_EN.pdf.

[15] Digital Economy and Society Index, Country Profile: Luxembourg (DESI 2020 Report), https://ec.europa.eu/digital-single-market/en/scoreboard/luxembourg.

[16] Information and Press Service of the Luxembourg Government: The Government's Open Data policy (21.02.2018), https://gouvernement.lu/en/dossiers/2018/open-data.html#:~:text=According%20to%20the%20Luxembourg%20Government's,and%20data%20containing%20personal%20information.

[17] Arrêté grand-ducal du 31 mars 1982 autorisant la création d'un syndicat de communes pour l'organisation et la gestion d'un centre informatique intercommunal (S.I.G.I.), http://data.legilux.public.lu/file/eli-etat-leg-recueil-identification_numerique-20161227-fr-pdf.pdf.

While many SIGI services are for internal use, services like online building permits through SIGI platform Siginova or SMS2Citizen, a news service about municipal events via SMS and smartphone app, are intended for the public.

1.3 Digitalisation in business

Luxembourg ranks 19th in the EU for the integration of digital technology by businesses in DESI 2020 and is generally performing below the EU average. It performs well in electronic information sharing and enterprise social media use, but falls short in small and medium enterprises (SME) selling online. Less than a fifth of enterprises use big data and cloud services.[18]

The European Commission's publication *Digital Transformation Scoreboard 2018: EU businesses go digital: Opportunities, outcomes and uptake* describes Luxembourg as one of the EU leaders in digital transformation with an advantageous environment incentivising companies in digital business and technology. Luxembourg scored below the EU average in terms of entrepreneurial culture and digital transformation, but strongly in e-leadership, which is attributed to a high number of people with IT skills and companies providing ICT training to their employees, and to the reliable digital infrastructure providing access to broadband connections. There is also a positive trend in developing ICT start-ups and finance for digital transformation (20% and 30% above the EU average, respectively).[19]

Luxembourg's determination for digital transformation and industry digitalisation is expressed in several national strategies. In the *Research and Innovation Smart Specialisation Strategy (RIS3),* ICT is at the top of the six priority sectors in the economy domain and communications. A connected and efficient data-driven economy is expected to drive developments in the priority sectors identified. Support in terms of regulatory frameworks and public investments in cybersecurity, the internet of things, blockchain, big data, high-performance computing and other ICT technologies and infrastructure are considered crucial.[20] *The Data-Driven Innovation Strategy for the Development of a Trusted and Sustainable Economy in Luxembourg* includes three pillars: (1) boosting and assuring digital infrastructures; (2) experimenting innovating and uptake of new advanced digital technologies into the industry; and (3) ensure a robust regulatory, intellectual property, investment and financing environment. The strategy's priority sectors are Industry, Ecotech, Healthtech, Logistics, Space, Financial Services and ICT. According to the sector-specific innovation plan for the ICT sector, policy and investment measures will be taken by the Ministry of the Economy to allow Luxemburg to become the most trusted data-driven economy in the European Union by 2023. The measures consist of building a trusted business environment for data-centric businesses to develop internationally; fostering data innovation; establishing Luxembourg as a testbed for data business; Public-Private Partnerships (PPP) as catalysts to the adoption of the data-driven economy; acquiring data skills; and promoting Luxembourg as a data-driven economy internationally (6).[21]

The national artificial intelligence strategic vision intends to make use of AI to enable the country to become a data-driven and sustainable economy. Next to many AI projects undertaken through Luxembourg's National Research Fund in collaboration with researchers and companies, the country is making active, long-term investments and drawing up legal and ethical guidelines.[22]

[18] Digital Economy and Society Index, Country Profile: Luxembourg (DESI 2020 Report), https://ec.europa.eu/digital-single-market/en/scoreboard/luxembourg.
[19] Digital Transformation Scoreboard 2018–EU Businesses Go Digital: Opportunities, Outcomes and Uptake, https://op.europa.eu/en/publication-detail/-/publication/683fe365-408b-11e9-8d04-01aa75ed71a1.
[20] Luxembourg Ministry of the Economy: Research and Innovation Smart Specialisation Strategy (RIS3), http://www.fonds-europeens.public.lu/fr/publications/s/smart_spec_strategy_2017/ris3_2017.pdf.
[21] Luxembourg Ministry of the Economy: The Data-Driven Innovation Strategy for the Development of a Trusted and Sustainable economy in Luxembourg, https://gouvernement.lu/en/publications/rapport-etude-analyse/minist-economie/intelligence-artificielle/data-driven-innovation.html.
[22] Artificial Intelligence: a strategic vision for Luxembourg, https://digital-luxembourg.public.lu/sites/default/files/2019-05/AI_EN.pdf.

1.4 Cyber threat landscape and cybersecurity assessment

Analysis conducted for the third iteration of the national cybersecurity strategy shows that the country is concerned by similar cyber threats as many other nations. While ransomware, distributed denial-of-service (DDOS) attacks and IoT malware are common threats in the cyber threat landscape, risks inherent in the development of smart cities and home automation like attacks against digital infrastructure are also addressed. Regulatory threats are described as risks stemming from a lack of sufficient cyberspace regulation, or the false sense of safety brought through strict regulatory obligations. Information on social networks can be misused through social engineering by malicious actors to gain access to companies' confidential data and enable espionage and sabotage. Another threat described by the national cybersecurity strategy is the use of digital tools for destabilisation; this encompasses broadcasting false information through social media, manipulation of elections through digital attacks and digital sabotage of infrastructure and hybrid attacks.[23]

Luxembourg's Computer Emergency Response Team (CERT) for the private sector, CIRCL (*Computer Incident Response Center Luxembourg*, see Section 3.2) releases its operational statistics, giving insight into the threat landscape. Percentages of incident categories provided by CIRCL are based on reports and tickets and do not include data from intelligence sharing platforms. In 2020, the majority of reported incidents per sector were targeted towards individuals (54%), while finance (24%), institutions (12%) and industry (9%) made up the rest. In 2020, the share of reported incidents for the finance sector rose significantly compared to 2019 (from 8%).

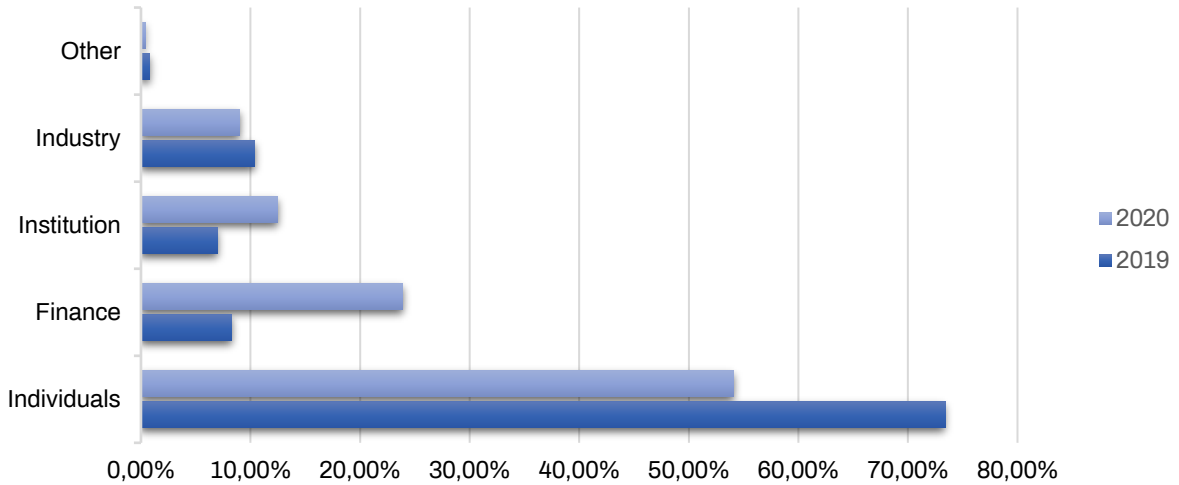

Figure 1. Simplified representation of CIRCL operational data according to Sectors of Activity
Source: *https://www.circl.lu/opendata/statistics/*

According to 2020 data, the majority of incidents were phishing (50%), followed by software/hardware vulnerabilities (23%) and data breaches (10%). The rest of the reported categories were made up of system compromise (6%), malware (6%) and scam (4%). The CIRCL has reported malware on mobile devices since 2016 and that international organisations in Luxembourg are also targeted by the same attacks as observed in other nations.[24]

[23] National Cybersecurity Strategy III, https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf.
[24] Computer Incident Response Center Luxembourg (CIRCL): Operational Statistics, https://www.circl.lu/opendata/statistics/.

2. National cybersecurity strategy and legal framework

The central document concerning cybersecurity in Luxembourg is its national cybersecurity strategy. In 2012, the first strategy was released, followed by the second in 2015[25] and the third in 2018. The fourth is planned for 2021.

Each iteration introduced a significant addition to the national cybersecurity landscape. The first introduced the Government CERT, while the second described the establishment of the National Agency for the Security of Information Systems (*Agence nationale de la sécurité des systèmes d'information*, ANSSI) (see Section 3.2). The third proposed the creation of the *Cybersecurity Competence Center* (C3) (see Section 3.5), the risk analysis methodology MONARC (Method for an Optimised aNAlysis of Risks) and the Interministerial Coordination Committee for Cyber Prevention and Cybersecurity (*Comité interministériel de coordination en matière de cyberprévention et de cybersécurité*). The responsibility for and coordination of the national cybersecurity strategy lies with the High Commission for National Protection (*Haut-Commissariat à la Protection nationale* - HCPN) situated under the Ministry of State.

2.1 National cybersecurity strategy

Luxembourg's first national cybersecurity strategy (*Stratégie nationale en matière de cybersécurité*)[26] was released in 2012 after the Government decided to establish a high-level document that deals with the cybersecurity and protection of infrastructure, communication systems and information processing. The first strategy's most significant impact was establishing the national CERT. The 2012 strategy comprised five axes containing objectives in the areas of infrastructure protection, legal framework, international cooperation, awareness-raising and establishing security standards.

The second version was published in the first quarter of 2015.[27] It featured an analysis of its predecessor's five axes, describing initiatives undertaken for each, and made a comparative analysis with other national strategies. The strategy defined seven objectives and contained an action plan detailing the implementation of the individual objective. The objectives focused on strengthening national and international cooperation; increasing the resilience of digital infrastructure and fighting cybercrime; training and awareness-raising; implementing minimum requirements for government and critical infrastructure; and strengthening cooperation with academia and research institutions.

To develop the third iteration of the strategy, the Cybersecurity Board (CSB) (see Section 3.1) commissioned a task force composed of relevant government bodies led by the HCPN. Three strategic guidelines were formulated, each with individual objectives. Unlike its predecessor, the action plan was not included in the strategy itself. However, an appendix provides feedback on the earlier edition and analysed national cybersecurity threats (see Section 1.4).[28]

(I) Guideline No. 1: Strengthening Public Confidence in the Digital Environment

The strategy outlines the effect of citizens being confident in using ICT systems and the effects of adverse external factors such as cybercrime. To reach an appropriate level of confidence and public trust, the risks associated with using ICT systems have to be considered and quality and security guaranteed. Five objectives were formulated to strengthen the public's confidence in the digital environment:

[25] National Cybersecurity Strategy II, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf.
[26] Stratégie nationale en matière de cybersécurité, https://cybersecurite.public.lu/dam-assets/fr/scs-1-2011.pdf
[27] National Cybersecurity Strategy II, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf.
[28] National Cybersecurity Strategy III, https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf.

(1) Knowledge-sharing between stakeholders;

(2) Disseminating information on risks;

(3) Raising the awareness of all parties concerned, including the general public, private and public organisations and critical infrastructure owners;

(4) Responsible disclosure; and

(5) Raising public confidence by combatting cybercrime, including specialised police training, enhancing collaboration between CERTs and the financial sector and promoting expert exchanges.

(II) Guideline No. 2: Digital Infrastructure Protection

Luxembourg's progress as a digital nation and the realisation that more citizens and companies depend on the digital infrastructure as the driver behind the second guideline: ensuring digital infrastructure resilience. Seven objectives support the goal expressed in that guideline:

(1) Census of essential and critical digital infrastructure, describing the Government's role to identify critical IT infrastructure and make sure that adequate protection measures are in place;

(2) Implementation of security policies for critical infrastructure, including ANSSI's security policies and ISO standards and the MONARC risk analysis methodology;

(3) Crisis management, dealing with adjustments and optimisation of the national crisis plan and developing customised operational plans by different sectors;

(4) Unifying and developing standards (see Section 2.3);

(5) Strengthening international cooperation;

(6) Cyber defence; and

(7) Strengthening the resilience of the state's digital infrastructure by ensuring a high standard of protection of the digital infrastructure to counter trends of increasing targeted attacks against government digital infrastructures.

(III) Guideline No. 3: Promotion of the Economy

The first and second strategy mentioned the protection of systems and infrastructures relevant to the economy; the economy's promotion is novel to the third strategy. The strategy claims that cybersecurity can be an economically attractive factor and that the government is set on democratising access to information security and the merging of known synergies. The third guideline is in line with other strategic documents such as *Digital Luxembourg* and highlights the Cybersecurity Competence Center and SECURITYMADEIN.LU (Security Made In Lëtzebuerg) roles (See Section 3.5).

Ten objectives have been formulated to achieve the third and most extensive guideline:

(1) Creating new products and services by investing in IT fields, strengthening PPPs, offering new digital services and encouraging insurance companies to create cyber insurance;

(2) Pooling security infrastructures by, *inter alia*, investing in a national scrubbing centre, a central point at which data traffic is analysed and sanitised for malicious activities so that internet service providers can be supported in their efforts;

(3) Requirement benchmarks and contractors to publish standard requirements for popular systems;

(4) Creation of the Cybersecurity Competence Center in conjunction with the Ministry of Economy and SECURITYMADEIN.LU to provide observatory services, training-type services and testing-type services;

(5) Risk management and informed governance;

(6) Training and training aid, working with universities in creating training programmes in the field of information security;

(7) Collaboration between parties in charge of information security to encourage the private sector, foster cooperation, provide information security managers with resources, and appoint people responsible for information security inside the state;

(8) Collaboration between experts in incident response;

(9) Creating start-ups as a priority for research; and

(10) Code disassembly and identifying vulnerabilities: The strategy intends to establish a framework allowing penetration testing and code disassembly in order to identify vulnerabilities.

2.2 Coalition agreement 2018-2023

In addition to the cybersecurity strategy, the government[29] emphasised the importance of cybersecurity by specifically addressing it in the coalition agreement 2018-2023, thereby showing its political commitment to fostering cybersecurity in the country.

Under the government's priorities for the financial sector, cybersecurity is cited as an example of new research approaches and in the context of business and competitiveness. As part of one of the eight axes of *The Data-Driven Innovation Strategy for the Development of a Trusted and Sustainable Economy in Luxembourg*, the regulatory framework for cybersecurity has a central role. To enhance Luxembourg's economic attractiveness, requirements in cybersecurity and digital data should be adopted. For the automotive industry in particular, a robust regulatory framework regarding new emerging technologies like 5G, AI and cybersecurity is addressed.

Luxembourg will support any initiatives that advance Europe in the field of cybersecurity, AI and high-performance computing.

An entire section of the coalition agreement is dedicated to cybersecurity. It states that protection mechanisms for citizens' and companies' data held by the state must be strengthened. The coalition also aims to establish Luxembourg as a haven for digital business and data and pledges ongoing investments in the security of critical IT infrastructures. Sensitisation of the private sector to threats of cyberattacks and industrial espionage are lines of effort the coalition is committed to.[30]

2.3 Cybersecurity legislation

Luxembourg's national cybersecurity framework relies on a broad range of laws. A law on electronic commerce,[31] adopted in 2000, established the free use of cryptographic techniques and created a legal basis for electronic signatures. A law on the organisation of the management of radio spectrum,[32] adopted in 2005 and amended in 2011,[33] sets the conditions for the use of the radio spectrum following international agreements. A 2011 law on electronic communications networks and services regulates access to electronic communications networks, ensures interoperability of electronic communications services and addresses network security and integrity obligations of communication network providers.[34]

The EU Network and Information Systems Security Directive (NIS directive) [35] was transposed by the Law of May 28, 2019transposing Directive (EU) 2016/1148 of the European Parliament and of the

[29] The current government is a coalition of the Democratic Party (*Demokratesch Partei* - DP), Luxembourg Socialist Workers' Party (*Lëtzebuerger Sozialistesch Aarbechterpartei* - LSAP) and The Greens (*déi Gréng*),.

[30] Les partis de la coalition DP, LSAP et déi Gréng: Koalitionsvertrag 2018-2023, https://gouvernement.lu/de/publications/accord-coalition/2018-2023.html.

[31] Loi du 14 août 2000 relative au commerce électronique, http://data.legilux.public.lu/eli/etat/leg/loi/2000/08/14/n8/jo.

[32] Loi du 30 mai 2005 portant organisation de la gestion des ondes radioélectriques., http://data.legilux.public.lu/eli/etat/leg/loi/2005/05/30/n2/jo.

[33] Loi du 27 février 2011 modifiant la loi du 30 mai 2005 portant organisation de la gestion des ondes radioélectriques. http://data.legilux.public.lu/eli/etat/leg/loi/2011/02/27/n2/jo.

[34] Loi du 27 février 2011 sur les réseaux et les services de communications électroniques, http://data.legilux.public.lu/file/eli-etat-leg-memorial-2011-43-fr-pdf.pdf.

[35] European Commission: Implementation of the NIS Directive in Luxembourg, https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-luxembourg.

Council of July 6, 2016 on measures to ensure a common high level of network and information system security in the European Union and amending Directive (EU) 2016/1148.[36] It amended earlier acts establishing the Center for State Information Technology and creating a High Commission for National Protection, making the Luxembourg Regulatory Institute (Institut Luxembourgeois de Régulation, ILR) the national point of contact. The ILR is responsible for the energy, transport, health, drinking water and digital infrastructures sector in the field of network and information systems security.[37] However, the CSSF (*Commission de surveillance du secteur financier*) is the competent authority for network and information systems security covering credit institutions and financial market infrastructure.[38]

Critical infrastructure[39]

According to the *Law of 23 July 2016 creating a High Commission for National Protection*, 'critical infrastructure' is defined as any asset, system or part thereof which is indispensable for safeguarding the vital interests or essential needs of all or part of the country or population or which is likely to be subject to a particular threat. Critical infrastructure protection and resilience is a broad and holistic concept where the security of the network and information systems is but one aspect among many. The term only applies if the infrastructure has been designated as such by Grand-Ducal decree. The competent administration for the initiation, coordination and execution of activities and measures relating to identifying, designating and protecting critical infrastructures is the HCPN (see Section 3.1).[40] A 2018 Grand-Ducal Regulation sets out more precise criteria given the potential impact. When identifying potential critical infrastructure, the HCPN typically performs an impact analysis considering the potential number of victims, economic impact, environmental impact and impact on the population in case of disruption.[41]

To be distinguished from critical infrastructures are essential services falling under the competency of the ILR introduced by the NIS directive (see above) which cover not only the sector of digital infrastructure but also energy, transport, health, drinking water and their respective sub-sectors.[42]

Computer-related offences

Articles about computer-related offences were introduced by the *Law of July 15, 1993, tending to reinforce the fight against economic crime and computer fraud* which modified Luxembourg's Penal Code by adding a new Section VII.[43] The Section, titled *Certain computer-related offences* (Art. 509-1 to Art. 509-7), addresses offences involving fraudulent access, impediment or distortion of computer

[36] Law of May 28, 2019 transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 on measures to ensure a common high level of network and information system security in the European Union and amending Directive (EU) 2016/1148.

[37] Further, ILR is tasked with specific responsibilities regarding oversight of NIS obligations of essential service providers under the national transposition of the NIS directive for various sectors and sub-sectors as defined by a national regulation, see: Règlement ILR/N19/1 of 5 November 2019, http://legilux.public.lu/eli/etat/leg/rilr/2019/11/05/a768/jo.

[38] Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 (NIS Directive) du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'Information de l'État et la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, http://data.legilux.public.lu/eli/etat/leg/loi/2019/05/28/a372/jo.

[39] Note: A law is currently worked on which will have impact on the HCPN, ANSSI, GovCERT and legal aspect concerning critical infrastructure. See: https://www.chd.lu/wps/portal/public/Accueil/TravailALaChambre/Recherche/RoleDesAffaires?action=doDocpaDetails&id=7670.

[40] Loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, http://legilux.public.lu/eli/etat/leg/loi/2016/07/23/n1/jo.

[41] Règlement grand-ducal du 21 février 2018 déterminant les modalités du recensement et de la désignation des infrastructures critiques, http://legilux.public.lu/eli/etat/leg/rgd/2018/02/21/a152/jo.

[42] Institut Luxembourgeois de Régulation - Règlement ILR/N19/1 du 5 novembre 2019 portant sur la fixation des services essentiels - Service NISS, http://legilux.public.lu/eli/etat/leg/rilr/2019/11/05/a768/jo.

[43] Loi du 15 juillet 1993 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique, http://data.legilux.public.lu/file/eli-etat-leg-memorial-1993-63-fr-pdf.pdf.

systems and insertion, deletion, modification and interception of data. The production, sale, procurement, holding, importing, distribution or the act of making available a means to commit one of the offences or committing these acts regarding electronic keys enabling access to a computer system is punishable by law. Participating in an organised group or acting under an agreement to prepare offences detailed in section VII of the penal code can be punished more severely.[44] Luxembourg is a signatory to the Council of Europe Convention on Cybercrime since 2003 and implements the mechanisms detailed in the treaty since 2015.[45]

3. National cybersecurity governance

3.1 Strategic leadership and policy coordination

For the highest-level strategic responsibility for cybersecurity, there are two central bodies in charge of strategic leadership and policy coordination: the Cybersecurity Board and the Interministerial Coordination Committee for Cyber Prevention and Cybersecurity (*Comité Interministériel de Coordination en matière de cyberprévention et de Cybersécurité*). The High Commission for National Protection or HCPN plays an important part in national strategic leadership and ensures coordination tasks in both of the aforementioned bodies (CSB and CIC-CPCS).

The Cybersecurity Board (CSB) was created after the Government Council's (*Conseil de gouvernement*) decision of 2011.[46] According to the *Grand-Ducal Decree of 28 May 2019 on the constitution of ministries,* the Board is under the authority of the Ministry of State.[47] According to the first National Cybersecurity Strategy, the CSB was created to implement and monitor the strategy's execution.[48] The third iteration explains that the CSB has a strategic role.

The Interministerial Coordination Committee for Cyber Prevention and Cybersecurity was established in December 2017[49] to coordinate the more pragmatic initiatives alongside the CSB.[50] The High Commissioner for National Protection is the committee's chair and it consists of representatives from the Ministry of State, High Commission for National Protection, the Luxembourg Defence (Directorate of Defence and Luxembourg Armed Forces), the Ministry of Economy, SECURITYMADEIN.LU, the Government Information Technology Center (CTIE), the State Intelligence Service, the National Agency for the Security of Information Systems (ANSSI) and the governmental computer emergency response team, Government Computer Emergency Response Team (GovCERT). Five missions are assigned to the Committee: (1) ensuring the consistency of actions and initiatives; (2) coordination of initiative implementation originating from the EU or other international level; (3) monitoring the implementation of said initiatives; (4) playing an advisory role for the Government in cybersecurity matters; and (5) discussion of positions adopted by national representatives on cybersecurity.[51] Given the transversality of cybersecurity, the CIC-CPCS ensures national coordination and addresses matters that fall within the competence of the entities involved.

---

[44] Code Penal: Section VII. - De certaines infractions en matière informatique (Art. 509-1 to Art. 509-7), http://data.legilux.public.lu/file/eli-etat-leg-code-penal-2020-03-20-fr-pdf.pdf.
[45] See links to the Treaty and Luxembourg's status at Details of Treaty No.185: Convention on Cybercrime. Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[46] Ministère d'État / SIP: Résumé des travaux du 5 juillet 2013, https://gouvernement.lu/fr/actualites/conseils_de_gouvernement/2013/07-juillet/05-conseil.html.
[47] Arrêté grand-ducal du 28 mai 2019 portant constitution des Ministères, http://data.legilux.public.lu/eli/etat/leg/agd/2019/05/28/a370/jo.
[48] Stratégie nationale en matière de cybersécurité, https://cybersecurite.public.lu/dam-assets/fr/scs-1-2011.pdf.
[49] Ministère d État / Haut-Commissariat à la Protection nationale, Engagement pour la Cybersécurité: le Luxembourg en 11e position au niveau mondial, https://digital.gouvernement.lu/fr/actualites.gouvernement%2Bfr%2Bactualites%2Btoutes_actualites%2Bcommuniques%2B2019%2B04-avril%2B02-cybersecurite-11-position.html.
[50] National Cybersecurity Strategy III, https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf.
[51] National Cybersecurity Strategy III, https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf.

The High Commission for National Protection (HCPN) is under the Ministry of State. Its origins go back to the Cold War. The *Grand-Ducal Decree of 31 December 1959 concerning the general organisation of national protection established* the Office of the Commissioner of National Protection (*Commissariat de la protection nationale*) as the secretariat for the National Protection Committee (*Comité de protection nationale*), an interministerial committee established by the same law to protect the country against the repercussions of an armed conflict. Its mission was to advise and assist the National Protection Committee in resource preparation, to protect the authorities and the population, to gather intelligence, to counter psychological operations and ensure public order and to communicate the National Protection Committee's decisions to ministerial departments.[52] It was renamed the HCPN in 1963, maintaining its original tasks,[53] and finally closed after the Cold War. However, the 9/11 terrorist attacks prompted a reactivation of the HCPN in December 2001,[54] and in 2016 it was turned into a government administration by law. Its new extended missions include the protection of critical infrastructure and it is the competent body for crisis prevention, anticipation and management.[55] As a result, it also bears responsibility for cyber crisis prevention and management and the cyber emergency response plan (see Section 3.3). The central role of the HCPN in the national cybersecurity landscape is also underpinned by the fact that both GovCERT and ANSSI are part of the HCPN.

Finally, cyber diplomacy is addressed by the Ministry of Foreign and European Affairs, covering EU and international working groups such as the Horizontal Working Party on Cyber Issues and the United Nations Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace in the context of international security.

3.2 Cybersecurity authority and cyber incident response

Governance of information security of classified and non-classified information

While Luxembourg does not have a central cybersecurity authority, the National Agency for the Security of Information Systems (*Agence nationale de la sécurité des systèmes d'information* - ANSSI) takes on a central role for systems installed and operated by the state. ANSSI was introduced by the nation's second cybersecurity strategy in 2015 and it is administratively situated under the HCPN. A Grand-Ducal decree adopted in February 2015 established three kinds of authorities in the organisation of information security of classified and non-classified data: the regulatory authority and incident management; the operational authority; and the homologating authority.[56]

ANSSI was originally considered the regulatory authority and incident management body under the HCPN and was to define policies and guidelines for the security of classified and unclassified information, ensure that protective measures concerning the security of information systems were implemented, certify the means of processing unclassified information and act as the national and governmental CERT. ANSSI was also established to be the TEMPEST authority and the cryptographic approval authority ensuring that cryptographic products comply with security policies.[57] Since its establishment, ANSSI has covered the CERT's function unifying many responsibilities and was

[52] Arrêté grand-ducal du 31 décembre 1959 concernant l´organisation générale de la protection nationale, http://data.legilux.public.lu/eli/etat/leg/agd/1959/12/31/n1/jo.
[53] Règlement grand-ducal du 25 octobre 1963 concernant l'organisation générale de la protection nationale, http://data.legilux.public.lu/eli/etat/leg/rgd/1963/10/25/n2/jo.
[54] Projet de loi relative à la Protection nationale Projet No 44/2012-1, https://www.csl.lu/fr/telechargements/avis/a8a46508ca.
[55] Loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, http://legilux.public.lu/eli/etat/leg/loi/2016/07/23/n1/jo.
[56] Grand-Ducal Decree of February 10, 2015 1. establishing governance in the area of information security management 2. amending the Grand Ducal Decree of July 30, 2013 determining the organisation and attributions of the Governmental Computer Emergency Response Team, also known as the 'Computer Emergency Response Team Governmental' (no longer in force).
[57] Arrêté grand-ducal du 10 février 2015 1. portant fixation de la gouvernance en matière de gestion de la sécurité de l'information 2. modifiant l'arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé «Computer Emergency Response Team Gouvernemental», http://legilux.public.lu/eli/etat/leg/agd/2015/02/10/n1/jo.

hierarchically situated under the HCPN. A 2018 legal amendment removed the incident management function from ANSSI and transferred the function of the cryptographic approval authority (*autorité d'agrément cryptographique*) to CTIE, leaving the ANSSI with its function as TEMPEST authority. ANSSI's mission regarding policy coordination and creation for state systems in cooperation with other national stakeholders and authorities is unchanged. Finally, the National Security Authority (*Autorité nationale de Sécurité* - ANS) is the homologating authority.[58]

The Government IT Center (*Centre des technologies de l'information de l'Etat* - CTIE), founded in 2009, acts as the central IT body for many administrations and ministries in Luxembourg.[59] It also counts as part of its missions the operation, planning and management and the assurance of classified communication and information systems for policy consultation and information exchange for the government and the management of cryptographic material in its function as the National Distribution Authority.[60] CTIE is the independent cryptographic accreditation authority of the state.[61]

Governance of information security of classified and non-classified information		
Regulatory Authority (*autorité régulatrice*)	**Operational Authorities (*autorité opérationnelle*)**	**Homologating Authority (*autorité homologative*)**
ANSSI (*Agence nationale de la sécurité des systèmes d'information*)	Affected administrations and services	ANS (Autorité nationale de Sécurité)

Figure 2. Governance of information security of classified and non-classified information for IT systems installed and operated by the state

The ILR is responsible for network and information systems security for the energy, transport, health, drinking water and digital infrastructure sectors. However, the CSSF is the competent authority for network and information systems security covering credit institutions' sectors and financial market infrastructures.[62]

Computer Security Incident Response Teams

The GovCERT was founded by a Grand-Ducal decree in 2013 to handle, among other things, all major security incidents affecting the government's networks and communication and information processing systems.[63] In 2015, GovCERT became the responsibility of the ANSSI after its creation and set to act as the national and governmental CERT. This structure and responsibilities were then amended in 2018 when it was placed under the HCPN and started covering three functions: national CERT (NCERT), governmental CERT (GovCERT) and military CERT (MilCERT).

In its function as the national CERT, it operates as the official national point of contact for foreign government CERTs and relays information to sectoral CERTs. In its function as the MilCERT, it operates as the official national point of contact for foreign military CERTs and monitors, detects, alerts and responds to computer attacks on armed forces' networks and communications and information processing systems. Other missions of MilCERT are to maintain a centralised inventory of incidents

[58] Arrêté grand-ducal du 9 mai 2018 portant fixation de la gouvernance en matière de gestion de la sécurité de l'information. http://legilux.public.lu/eli/etat/leg/agd/2018/05/09/a423/jo.
[59] Loi du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat. http://legilux.public.lu/eli/etat/leg/loi/2009/04/20/n2/jo.
[60] Loi du 24 novembre 2015 modifiant la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat. http://legilux.public.lu/eli/etat/leg/loi/2015/11/24/n1/jo.
[61] Arrêté grand-ducal du 9 mai 2018 portant fixation de la gouvernance en matière de gestion de la sécurité de l'information. http://legilux.public.lu/eli/etat/leg/agd/2018/05/09/a423/jo.
[62] Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 (NIS Directive) du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'Information de l'État et la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, http://data.legilux.public.lu/eli/etat/leg/loi/2019/05/28/a372/jo.
[63] Arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé «Computer Emergency Response Team Gouvernemental», http://legilux.public.lu/eli/etat/leg/agd/2013/07/30/n2/jo.

affecting the security of communication and information systems to allow the Chief of the Defence Staff (Chef d'État-Major) to have a complete strategic view on the subject and to operate nationally with specialised intervention teams responding to security incidents.[64]

The Computer Incident Response Center Luxembourg (CIRCL) is operated by the state-funded economic interest group *Security Made in Lëtzebuerg* (also referred to as SECURITYMADEIN.LU) and is responsible for the private sector, municipalities and non-government entities.[65] In 2015, SECURITYMADEIN.LU was mandated by the Minister of the Economy to operate CIRCL and performing research at the international level, establishing collaboration, sharing threat information and implementing an early warning sensor network to increase Luxembourg's trustworthiness and hence attractiveness as an e-economy hub.[66]

HealthNet-CSIRT is responsible for computer incidents in the healthcare field and is operated by the Agence eSanté (see Section 1.2).[67]

The non-profit RESTENA Foundation (see Section 1.2) also has a CERT named RESTENA-CSIRT responding to security incidents in Luxembourg's research and education field.[68]

There are also several private CERTs in Luxembourg and many are connected to the public CERTs via the CERT.LU community, which enables information sharing and further cooperation through several projects.[69]

Cybersecurity certification

The national cybersecurity certification authority is ILNAS (the Luxembourg Institute of Standardisation, Accreditation, Safety and Quality of Products and Services) (see Section 1.2). It is in the framework of *EU Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, among other things responsible for participation in the European Cybersecurity Certification Group, application and supervision of the rules concerning the different European cybersecurity certifications, collaboration with the national accreditation body *Office Luxembourgeois d'Accréditation et de Surveillance* (OLAS) and collaboration with the European Commission and other national cybersecurity certification authorities.[70]

3.3 Cyber crisis management

Luxembourg's government provides its population with a website called inforcrise.lu containing a plethora of information on potential crises and reaction and mitigation plans. The emergency response plan concerning cyber, or *Plan d'intervention d'urgence en cas d'attaque contre les systèmes d'information ou de faille technique des systèmes d'information* (PIU Cyber) was developed by HCPN and is under the responsibility of the Prime Minister. It has four main objectives: the adoption of protective and preventive measures; the definition and role of crisis management entities; the definition of emergency measures, actions and actors; and alerting and disseminating information to the public.

The plan foresees four kind of units during a crisis: the Crisis Unit (cellule de crise - CC), Operational Unit (cellule opérationnelle – CO), Cyber Risk Assessment Unit (Cellule d'évaluation du risque cyber -

[64] Arrêté grand-ducal du 9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental », http://legilux.public.lu/eli/etat/leg/agd/2018/05/09/a424/jo.
[65] Computer Incident Response Center Luxembourg (CIRCL): RFC 2350 CIRCL - the CERT for the private sector, communes and non-governmental entities in Luxembourg, https://www.circl.lu/mission/rfc2350/index.html.
[66] Ministère de l'Économie MANDATE for the 'security made in Lëtzebuerg' (SECURITYMADEIN.LU) g.i.e, https://securitymadein.lu/assets/media/convention-MECO-2021-2025.pdf .
[67] Portail de la cybersécurité: HealthNet-CSIRT, https://cybersecurite.public.lu/fr/acteur/csirts/restena-csirt1.html.
[68] Restena: Computer Security Incident Response Team (CSIRT), https://www.restena.lu/en/csirt.
[69] Cyber emergency Response Community Luxembourg: About cert.lu, https://cert.lu/
[70] Portail-Qualite.lu: L'ILNAS désigné comme autorité nationale de certification de cybersécurité au Luxembourg https://portail-qualite.public.lu/fr/actualites/confiance-numerique/2020/l-ilnas-designe-comme-autorite-nationale-de-certification-de-cybersecurite-au-luxembourg.html

CERC) and Communication/Information Unit (Cellule communication/information - CCI). In a crisis or anticipation of a crisis, the Prime Minister can activate a CC composed of the HCPN, Director General of the Grand-Ducal Police, Director of the State Intelligence Service, Chief of the Defence Staff, Director of the CTIE, Executive Officer of the Department of Media Telecommunications and Digital Policy, Director of GovCERT, Director of CIRCL and Director of the Crisis Communication Department. The CC initiates, coordinates and ensures the execution of all measures designed to deal with the crisis and its effects while preparing decisions for government approval. It remains in place until the end of the crisis. The CC may in turn activate the CO to execute, implement and control measures.

The CERC is led by the Director of GovCERT and is composed of experts that monitor the crisis and inform the crisis unit. The CERC also monitors the overall situation before a crisis and before the CC's activation. The CCI relays communication to the population and media.

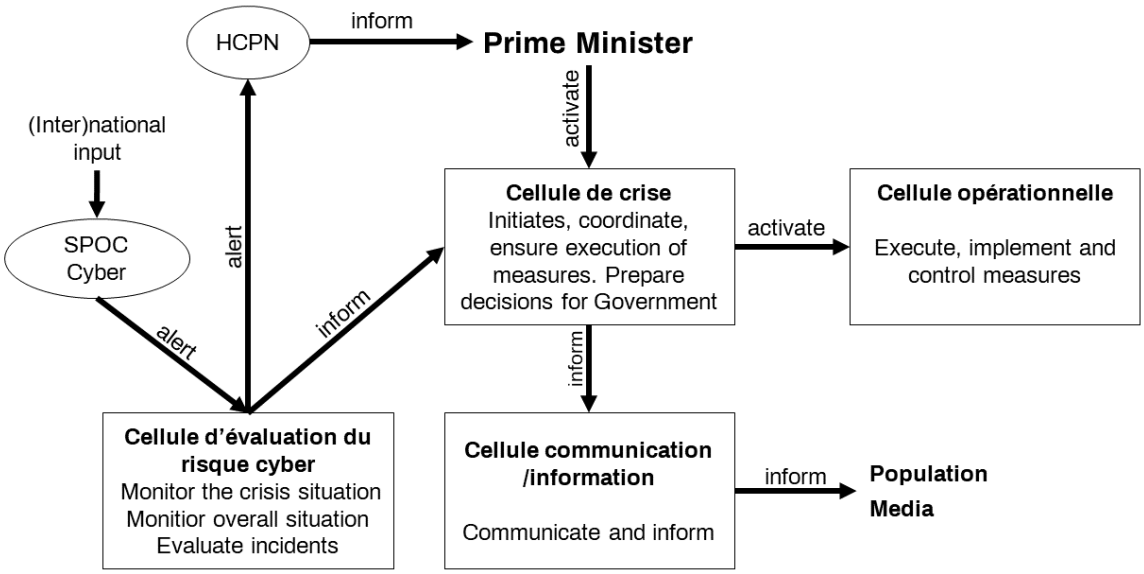

Figure 3: Simplified representation of processes described in the cyber emergency response plan

Information and analysis coming through national and international ways can be reported to the SPOC Cyber (Single Point of Contact Cyber) which is permanently staffed for this purpose. The CERC is alerted in case of a cyber incident and can alert the HCPN after assessing the threat. If the threat level requires, the Prime Minister is then informed by the High Commissioner for National Protection and can decide to activate the crisis unit.

There are several tools and measures available to support decision-makers. These encompass evaluation as a first step to assess the urgency and impact and increased surveillance including situation reports on affected networks, state of infection and efficiency of measures taken and the evaluation of available statistics. Technical analysis of the factors leading to the incident can be undertaken. Isolation (*Cloisonnement*) is a measure to counter denial-of-service attacks and to isolate the threatened systems. System upgrades and protection foresees contacting potential targets to verify vulnerabilities. After assessing the situation, the CERC can propose to the CC preventive and protective measures or partial and full disconnection of the potential target. The activation of the national cyber reserve is a measure intended to call on experts from the public administration in IT security and would only be triggered in case of a crisis of significant impact. Restoration of services describes the actions necessary to ensure activities' resumption and return to normality.[71]

[71] Plan d'intervention d'urgence en cas d'attaque contre les systèmes d'information ou de faille technique des systèmes d'information « PIU Cyber » (version publique), https://infocrise.public.lu/fr/publications/cyber/plan-intervention-cyber.html

3.4 Military cyber defence

The role of the military CERT is covered by the GovCERT in one of its three functions. Luxembourg Defence (Directorate of Defence of the Ministry of Foreign Affairs and Luxembourg Armed Forces) is represented at the Interministerial Coordination Committee for Cyber Prevention and Cybersecurity. The Chief of Defence (Chef d'État-Major) is part of the crisis cell in the cyber emergency response plan framework (PIU Cyber).

The Armed Forces Communication and Information Systems (CIS) Department houses the Cyber and CIS Security Bureau tasked with the army's cybersecurity and CIS security. Reconnaissance being the Armed Forces' core business, the Bureau's main task is to enable mission assurance by ensuring cybersecurity. Luxembourg is a member of NATO and the EU, meaning that the armed forces partake in many initiatives and efforts of the EU and Alliance in cyber-related matters. The bureau also covers a broad spectrum of cyber exchanges within bodies and expert groups of NATO and the EU such as CAP4, CD CaT, (PT) Cyber Defence and C3 Board and bilateral cyber initiatives. The nation is in the process of joining the NATO Collaborative Cyber Defense Centre of Excellence (CCDCOE) and contributes experts to support the Centre. The armed forces also take part in the two main NATO cyber exercises, Locked Shields and Cyber Coalition. In education and training, the armed forces work with SECURITYMADEIN.LU's Cyber Competence Center (see Section 3.5) to train and instruct its personnel. Luxembourg Defence also supports the development of the open-source threat intelligence platform, MISP (Malware Information Sharing Platform), in cooperation with CIRCL.

The Directorate of Defence Cyber Team works in close collaboration with the armed forces and contributes to the implementation of the Cyber Defence Strategy and develops Cyber Defence capabilities. The Cyber Team ensures that Luxembourg Defence meets national requirements and EU and NATO obligations. Preparation and representation at national and international cyber defence-related meetings also fall under its main tasks.

Cyber Defence Strategy

Luxembourg Defence published its Cyber Defence Strategy[72] at the beginning of 2021 with the ambition to have one of NATO and the EU's most cyber-secure defences by 2030 through maximisation of its cyber defence capabilities. Luxembourg also plans to share its progress and the results of its investments in people, technology, research and development with national and international partners and with national and international organisations. The Luxembourg Cyber Defence Strategy is structured to allow direct mapping of reporting structures (e.g. NATO's Cyber Defence Pledge and NDPP). The strategy spans four strategic goals covering workforce, cooperation, integration of cyber defence and preparedness for the future, with corresponding capabilities to achieve these goals.

(I) A skilled and motivated workforce

The first strategic goal consists of upskilling existing personnel and attracting new talent, next to contributing to the country's overall cyber competence and enhancing national cyber resilience. The strategy states four capabilities. The first, 'knowledgeable and experienced defence personnel' describes the integration of cyber aspects into military exercises and operations, participation in national and international exercises and the promotion of internal cybersecurity training. 'Increased positive public perception of Luxembourg Cyber Defence, including as an employer', targets the defence sector's attractiveness as an employer. 'Established and strengthened key cyber defence bodies' addresses the national cyber reserve support, dedicated MilCERT capabilities and enhanced need for building human resource capacities. 'Enhanced national non-military/non-defence cyber expertise' states that cyber defence is considered a fundamental part of defence and will provide training and exercises using, for example, the newly established Luxembourg Cyber Range.

[72] Luxembourg Cyber Defence Strategy, https://defense.gouvernement.lu/dam-assets/la-defense/Luxembourg-Cyber-Defence-Strategy.pdf

(II) Strong national and international cyber cooperation

Acknowledging that geographical borders do not apply to cyberspace, the strategy emphasises the importance of upholding international rules-based order and commitments. Capabilities under this strategic goal encompass 'Mutual needs and capacities and enabling factors identified', where through fact-finding missions, research and benchmarking, future needs will be identified. 'Continuous exchange of expertise and resources' outlines the exchange of best practice and the promotion of expertise and participation in multinational exercises and threat sharing initiatives. 'Strengthened cooperation with national actors' sets a commitment to continue cooperation and collaborating within national entities and initiatives.

(III) Cyber Defence integrated in all Luxembourg Defence activities, assets and culture

The third strategic goal focuses on resilience and defence in cyberspace domestically and in operations abroad, while mentioning the increased risk stemming from digitalisation. The first capability, 'Cybersecurity anchored in organisational culture', describes guiding principles and mainstreaming organisational culture, whereas the second capability 'Governance, implementation and execution' mentions mechanisms to mainstream cybersecurity through an information security management system framework, initiatives such as the Cyber Range and continued efforts to improve resilience.

(IV) 'CyberFutures' Landscape mapped, priorities identified and research programmes underway

The fourth strategic goal focuses on mapping future challenges and emerging developments and their effect on the armed forces' operational role, distinguishing between short- and medium-term capabilities. Thus, 'Continuous mapping of future challenges and opportunities, defined research, development and technology priorities (medium-term)' focuses on regular horizon scanning to use the results to identify relevant CyberFutures. 'Cyber defence assets and capabilities alignment (short term)' uses the results to align assets and capabilities to upcoming challenges while undertaking regular reviews to determine if the developments are still aligned. The last capability, 'Cyber integrated into Luxembourg Defence R&D' states that relevant results of the horizon scanning process are used to direct national research.

3.5 Engagement with the private sector

As is apparent through the third national cybersecurity strategy, the Ministry of Economy plays a central role in engagement with the private sector undertaking many initiatives related to IT and cyber. Supporting the Luxembourg economy, the Ministry is a driving force behind initiatives under the R*esearch and Innovation Smart Specialisation Strategy (RIS3)* and others laid out in Section 1.3. As described in Chapter 2, SECURITYMADEIN.LU under the third guideline (Promotion of the Economy) of the third National Cybersecurity Strategy manages the Cybersecurity Competence Center (C3) which provides observatory services, training and testing.[73]

SECURITYMADEIN.LU (or *Security Made In Lëtzebuerg*) was founded in 2010 and is supervised by the Ministry of Economy. Its board consists of the Ministry of Family, Integration and the Greater Region (*Ministère de la Famille, de l'Intégration et à la Grande Région*), Ministry of Education, Childhood and Youth (*Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse*) and SIGI (see Section 1.2) and SYVICOL (*Syndicat des Villes et Communes du Luxembourg*). SECURITYMADEIN.LU consists of three entities:[74] CIRCL, CASES and C3.

The CIRCL (see Section 3.2) is the CERT for the private sector, communes and non-governmental entities in Luxembourg. Initiatives such as the CERT.LU (see Section 3.2) where private sector and governmental CERT cooperation is nurtured.

Cyberworld Awareness and Security Enhancement Services Luxembourg (Cases) offers many services related to Cybersecurity from publications, educational material and best practices to tools like the risk analysis method MONARC (see Chapter 2).[75]

[73] National Cybersecurity Strategy III, https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf
[74] SECURITYMADEIN.LU: ABOUT SECURITYMADEIN.LU, https://securitymadein.lu/contact/about/
[75] Cyberworld Awareness and Security Enhancement Services Luxembourg (CASES), https://www.cases.lu/

The Cybersecurity Competence Center (C3) has three primary missions: to increase Luxembourg's attractiveness and its reputation through cybersecurity, to offer government to business to business (G-to-B-to-B) services and to promote long-term wealth and competence building. The C3 defines its three competence areas in observation, training and testing. It offers a catalogue of training and events and interacts with the private sector. One of the most prominent training pieces is Luxembourg made flagship cyber-attack simulation *Room#42* focusing on crisis management and awareness-raising.[76]

[76] Cybersecurity Competence Center (C3): About C3, https://c3.lu/#about

References

Policy

5G strategy for Luxembourg, Roadmap for the 5th generation of mobile communication in Luxembourg, https://digital-luxembourg.public.lu/sites/default/files/2018-11/Digital-Luxembourg_Strategy5G_V1_WEB.pdf

Artificial Intelligence: a strategic vision for Luxembourg, https://digital-luxembourg.public.lu/sites/default/files/2019-05/AI_EN.pdf

Digital Luxembourg, Progress Report spring 2018, https://digital-luxembourg.public.lu/sites/default/files/2018-06/DL_201804022_PROGRESS%20REPORT_08%20BAT.pdf

Les partis de la coalition DP, LSAP et déi gréng: Koalitionsvertrag 2018-2023, https://gouvernement.lu/de/publications/accord-coalition/2018-2023.html

Luxembourg Cyber Defence Strategy, https://defense.gouvernement.lu/dam-assets/la-defense/Luxembourg-Cyber-Defence-Strategy.pdf

Luxembourg Ministry of the Economy: Research and Innovation Smart Specialisation Strategy (RIS3), http://www.fonds-europeens.public.lu/fr/publications/s/smart_spec_strategy_2017/ris3_2017.pdf

Luxembourg: Ministry of the Economy: The Data-Driven Innovation Strategy for the Development of a Trusted and Sustainable Economy in Luxembourg, https://gouvernement.lu/en/publications/rapport-etude-analyse/minist-economie/intelligence-artificielle/data-driven-innovation.html

National Cybersecurity Strategy II, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf

National Cybersecurity Strategy III, https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf

Plan d'intervention d'urgence en cas d'attaque contre les systèmes d'information ou de faille technique des systèmes d'information « PIU Cyber » (version publique), https://infocrise.public.lu/fr/publications/cyber/plan-intervention-cyber.html

Stratégie nationale en matière de cybersécurité, https://cybersecurite.public.lu/dam-assets/fr/scs-1-2011.pdf

Law

Arrêté grand-ducal du 10 février 2015 1. portant fixation de la gouvernance en matière de gestion de la sécurité de l'information 2. modifiant l'arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé «Computer Emergency Response Team Gouvernemental», http://legilux.public.lu/eli/etat/leg/agd/2015/02/10/n1/jo

Arrêté grand-ducal du 28 mai 2019 portant constitution des Ministères, http://data.legilux.public.lu/eli/etat/leg/agd/2019/05/28/a370/jo

Arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé «Computer Emergency Response Team Gouvernemental», http://legilux.public.lu/eli/etat/leg/agd/2013/07/30/n2/jo

Arrêté grand-ducal du 31 mars 1982 autorisant la création d'un syndicat de communes pour l'organisation et la gestion d'un centre informatique intercommunal (S.I.G.I.), http://data.legilux.public.lu/file/eli-etat-leg-recueil-identification_numerique-20161227-fr-pdf.pdf

Arrêté grand-ducal du 5 décembre 2018 portant constitution des Ministères, http://data.legilux.public.lu/eli/etat/leg/agd/2018/12/05/a1099/jo

Arrêté grand-ducal du 9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental », http://legilux.public.lu/eli/etat/leg/agd/2018/05/09/a424/jo

Arrêté grand-ducal du 9 mai 2018 portant fixation de la gouvernance en matière de gestion de la sécurité de l'information. http://legilux.public.lu/eli/etat/leg/agd/2018/05/09/a423/jo

Arrêté grand-ducal du 9 mai 2018 portant fixation de la gouvernance en matière de gestion de la sécurité de l'information. http://legilux.public.lu/eli/etat/leg/agd/2018/05/09/a423/jo

Institut Luxembourgeois de Régulation - Règlement ILR/N19/1 du 5 novembre 2019 portant sur la fixation des services essentiels - Service NISS, http://legilux.public.lu/eli/etat/leg/rilr/2019/11/05/a768/jo

Loi du 14 août 2000 relative au commerce électronique, http://data.legilux.public.lu/eli/etat/leg/loi/2000/08/14/n8/jo

Loi du 15 juillet 1993 tendant à renforcer la lutte contre la criminalité économique et la fraude informatique, http://data.legilux.public.lu/file/eli-etat-leg-memorial-1993-63-fr-pdf.pdf

Loi du 17 décembre 2010 portant réforme du système de soins de santé et modifiant: 1. le Code de la sécurité sociale; 2. la loi modifiée du 28 août 1998 sur les établissements hospitaliers, http://legilux.public.lu/eli/etat/leg/loi/2010/12/17/n12/jo

Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, http://data.legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo

Loi du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat. http://legilux.public.lu/eli/etat/leg/loi/2009/04/20/n2/jo

Loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, http://legilux.public.lu/eli/etat/leg/loi/2016/07/23/n1/jo

Loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, http://legilux.public.lu/eli/etat/leg/loi/2016/07/23/n1/jo

Loi du 23 mai 2016 modifiant la loi du 4 décembre 2007 sur la réutilisation des informations du secteur public, http://data.legilux.public.lu/eli/etat/leg/loi/2016/05/23/n1/jo

Loi du 24 novembre 2015 modifiant la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat. http://legilux.public.lu/eli/etat/leg/loi/2015/11/24/n1/jo

Loi du 27 février 2011 modifiant la loi du 30 mai 2005 portant organisation de la gestion des ondes radioélectriques. http://data.legilux.public.lu/eli/etat/leg/loi/2011/02/27/n2/jo

Loi du 27 février 2011 sur les réseaux et les services de communications électroniques, http://data.legilux.public.lu/file/eli-etat-leg-memorial-2011-43-fr-pdf.pdf

Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 (NIS Directive) du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'Information de l'État et la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, http://data.legilux.public.lu/eli/etat/leg/loi/2019/05/28/a372/jo

Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 (NIS Directive) du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'Information de l'État et la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, http://data.legilux.public.lu/eli/etat/leg/loi/2019/05/28/a372/jo

Loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, http://data.legilux.public.lu/eli/etat/leg/loi/2005/05/30/n4/jo

Loi du 30 mai 2005 portant organisation de la gestion des ondes radioélectriques., http://data.legilux.public.lu/eli/etat/leg/loi/2005/05/30/n2/jo

Projet de loi relative à la Protection nationale Projet No 44/2012-1, https://www.csl.lu/fr/telechargements/avis/a8a46508ca

Règlement grand-ducal du 21 février 2018 déterminant les modalités du recensement et de la désignation des infrastructures critiques, http://legilux.public.lu/eli/etat/leg/rgd/2018/02/21/a152/jo

Règlement ILR/N19/1 of 5 November 2019, http://legilux.public.lu/eli/etat/leg/rilr/2019/11/05/a768/jo

Other

Agence eSanté, https://www.esante.lu/portal/de/ich-informiere-mich/die-agence-esante-259-323.html

CERTIFICATE OF CONFORMITY for LUXTRUST by LSTI (Certificate LSTI 11085-124-V1.0), https://www.luxtrust.lu/upload/data/repository/certificate_lsti_ndeg_11085-1082_v4.0_luxtrust_1.pdf

Computer Incident Response Center Luxembourg (CIRCL): Operational Statistics, https://www.circl.lu/opendata/statistics/

Computer Incident Response Center Luxembourg (CIRCL): RFC 2350 CIRCL - the CERT for the private sector, communes and non-governmental entities in Luxembourg, https://www.circl.lu/mission/rfc2350/index.html

Cyber Emergency Response Community Luxembourg: About cert.lu, https://cert.lu/

Cybersecurity Competence Center (C3): About C3, https://c3.lu/#about

Cyberworld Awareness and Security Enhancement Services Luxembourg (CASES), https://www.cases.lu/

Digital Economy and Society Index, Country Profile: Luxembourg (DESI 2020 Report), https://ec.europa.eu/digital-single-market/en/scoreboard/luxembourg

Digital Transformation Scoreboard 2018–EU Businesses Go Digital: Opportunities, Outcomes and Uptake, https://op.europa.eu/en/publication-detail/-/publication/683fe365-408b-11e9-8d04-01aa75ed71a1

European Commission: Implementation of the NIS Directive in Luxembourg, https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-luxembourg

Grand Duchy of Luxembourg Statistics Portal, https://statistiques.public.lu/en/

Information and Press Service of the Luxembourg Government: The Government's Open Data policy (21.02.2018), https://gouvernement.lu/en/dossiers/2018/open-data.html#:~:text=According%20to%20the%20Luxembourg%20Government's,and%20data%20containing%20personal%20information

Institut Luxembourgeois de Régulation (ILR): A propos de l'Institut, https://web.ilr.lu/FR/ILR/A-propos-de-lInstitut

Ministère d État / Haut-Commissariat à la Protection nationale, Engagement pour la Cybersécurité: le Luxembourg en 11e position au niveau mondial, https://digital.gouvernement.lu/fr/actualites.gouvernement%2Bfr%2Bactualites%2Btoutes_actualites%2Bcommuniques%2B2019%2B04-avril%2B02-cybersecurite-11-position.html

Ministère d'État / SIP: Résumé des travaux du 5 juillet 2013, https://gouvernement.lu/fr/actualites/conseils_de_gouvernement/2013/07-juillet/05-conseil.html

OECD country data profile for Luxembourg, https://data.oecd.org/luxembourg.htm

Portail de la cybersécurité: HealthNet-CSIRT, https://cybersecurite.public.lu/fr/acteur/csirts/restena-csirt1.html

Portail-Qualite.lu: L'ILNAS désigné comme autorité nationale de certification de cybersécurité au Luxembourg https://portail-qualite.public.lu/fr/actualites/confiance-numerique/2020/l-ilnas-designe-comme-autorite-nationale-de-certification-de-cybersecurite-au-luxembourg.html

Restena: Computer Security Incident Response Team (CSIRT), https://www.restena.lu/en/csirt

SECURITYMADEIN.LU: ABOUT SECURITYMADEIN.LU, https://securitymadein.lu/contact/about/

Service des médias , des communications et du numérique: Résultat des enchères en vue de l'octroi des fréquences destinées à la 5G, (Communiqué du 22.07.2020), https://smc.gouvernement.lu/fr/actualites.gouvernement%2Bfr%2Bactualites%2Btoutes_actualites%2Bcommuniques%2B2020%2B07-juillet%2B22-resultats-5g.html

Figures and Tables

Acronyms and Abbreviations

5G	5th generation (mobile network)
AI	Artificial Intelligence
ANS	National Security Authority/Autorité nationale de Sécurité
ANSSI	National Agency for the Security of Information Systems/Agence nationale de la sécurité des systèmes d'information
API	Application Programming Interface
C3 (Board)	Consultation, Command and Control (Board)
C3	Cybersecurity Competence Center
CASES	Cyberworld Awareness and Security Enhancement Services Luxembourg
CC	Crisis Unit/ Cellule de Crise
CCI	Communication/Information Unit/ Cellule communication/information
CERC	Cyber Risk Assessment Unit/ Cellule d'Évaluation du Risque Cyber
CERT	Computer Emergency Response Team
CGIE	Centre de gestion informatique de l'éducation
CIC-CPCS	Comité interministériel de coordination en matière de cyberprévention et de cybersécurité
CIRCL	Computer Incident Response Center Luxembourg
CIS	Communication and Information Systems
CNPD	Commission nationale pour la protection des données
CO	Operational Unit/ Cellule Opérationelle
CSB	Cybersecurity Board
CSIRT	Computer Security Incident Response Team CSIRT
CSSF	Commission de surveillance du secteur financier
CTIE	Government IT Center/ Centre des technologies de l'information de l'Eta
DDOS	Distributed Denial-of-Service
DESI	Digital Economy and Society Index
DP	Demokratesch Partei
eID	Electronic Identification
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUTF	European Cybercrime Task Force
FBI	Federal Bureau of Investigation
FTTP	Fibre to the premises
GDPR	General Data Protection Regulation
GovCERT	Computer Emergency Response Team Gouvernemental

HCPN	High Commission for National Protection/Haut-Commissariat à la Protection nationale
ICT	Information and Communications Technology
ID	Identification
ILNAS	Luxembourg Institute of Standardisation, Accreditation, Safety and Quality of Products and Services/Institut Luxembourgeois de la Normalisation, de l'accréditation, de la sécurité et qualité des produits et services
ILR	Luxembourg Regulatory Institute/Institut Luxembourgeois de Régulation
ILT	Institut Luxembourgeois des Télécommunications
ISO	International Organization for Standardization
IT	Information Technology
LSAP	Luxembourg Socialist Workers' Party/ Luxemburger Sozialistische Arbeiterpartei
MilCERT	Military Computer Emergency Response Team
MISP	Malware Information Sharing Platform
NATO	North Atlantic Treaty Organization
NCERT	National Computer Emergency Response Team
NIS(S)	Security of Network and Information (Systems)
NREN	National Research and Education Network
OECD	Organisation for Economic Cooperation and Development
OLAS	Office Luxembourgeois d'Accréditation et de Surveillance
OSCE	Organization for Security and Co-operation in Europe
PIU	Emergency Response Plan/ Plan d'intervention d'urgence
PPP	Public-Private Partnerships
R&D	Research and Development
RIS3	Research and Innovation Smart Specialisation Strategy
S.A.	Société Anonyme
SECURITYMADEIN.LU	Security Made In Lëtzebuerg
SIGI	Syndicat Intercommunal de Gestion Informatique
SMC	Service des Médias et des Communications
SME	Small and Medium Enterprises
SMS	Short Message Service
SNCI	Société Nationale de Crédit et d'Investissement
SPOC	Single Point of Contact Cyber
SYVICOL	Syndicat des Villes et Communes du Luxembourg
TEMPEST	Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions
UN	United Nations
UN GGE	United Nations Group of Governmental Experts

USB	Universal Serial Bus