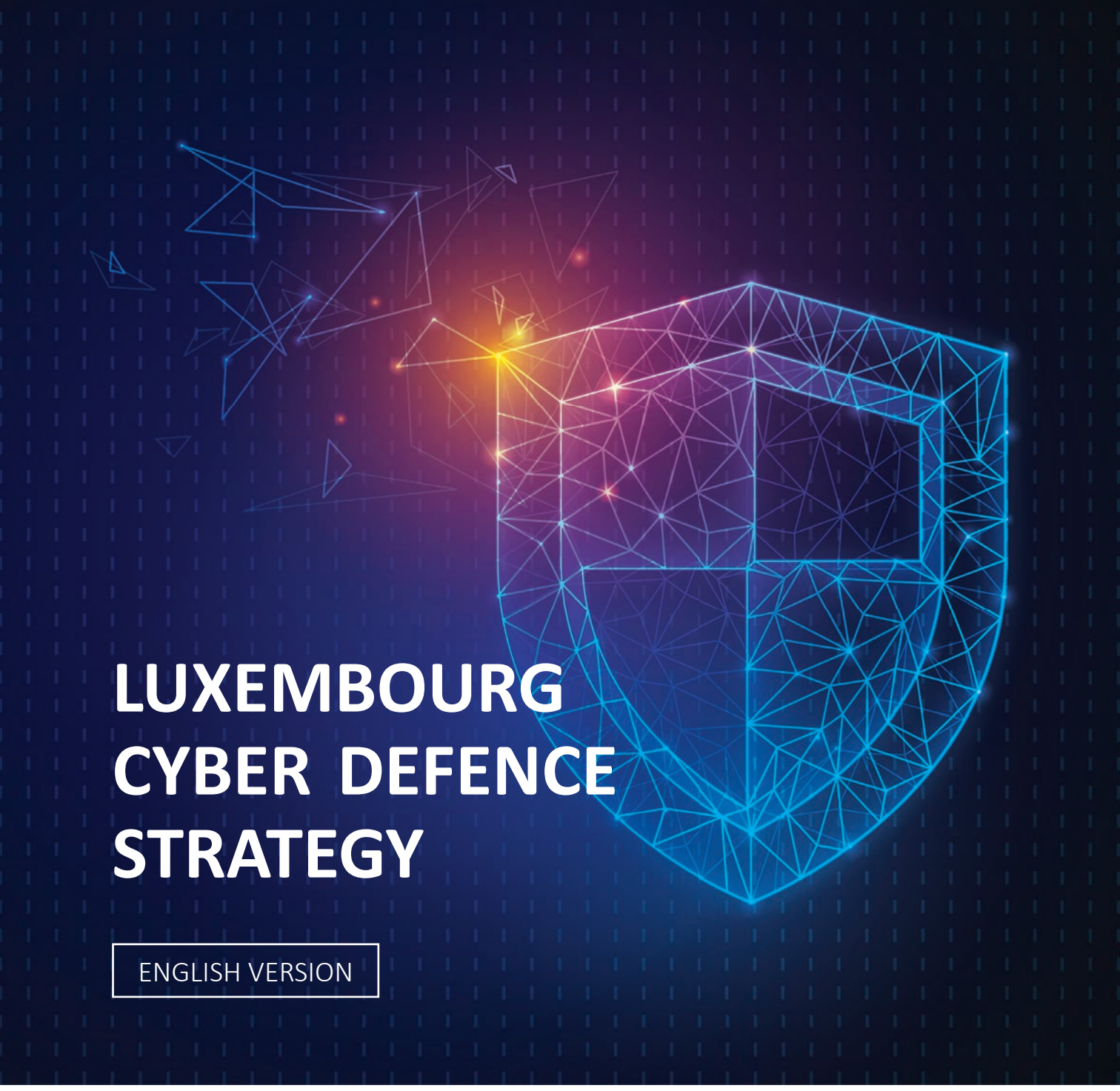


LUXEMBOURG CYBER DEFENCE STRATEGY

ENGLISH VERSION

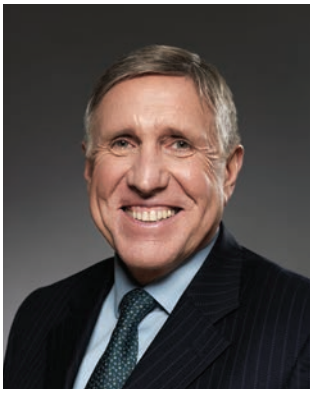
THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of Foreign and European Affairs

Directorate of Defense

Responsible publisher: Ministry of Foreign an European Affairs –
Directorate of Defence
6, rue de l'Ancien Athenée
L-1144 Luxembourg

Publication: Luxembourg | February 2021

MINISTERIAL FOREWORD



SIP / Yves Kortum

Luxembourg has enjoyed many years of peace, prosperity and progress as a result of stability of the global world order. Digitalisation and new technologies have given Luxembourg and the rest of the world great opportunity for development and progress but have also increased our exposure to factors undermining our democratic values, our way of life and the stability of the international rules-based order. We are facing new challenges through constant and pervasive activities below the threshold of conflict that require a broader view of security and defence policy, encompassing global environmental change and hybrid threats.

Therefore, it is with great pleasure that I present the inaugural Cyber Defence Strategy for Luxembourg. This 10-year long-term strategy is nested within the National Cybersecurity Strategy and aims to enhance the resilience of Luxembourg Defence by protecting its assets and capabilities from malicious cyber activities. The strategy lays the foundation for the development of cyber defence capabilities that can be used in a national and international context. A periodic review confers sufficient flexibility and adaptability to this long-term strategy in a domain that is in constant evolution.

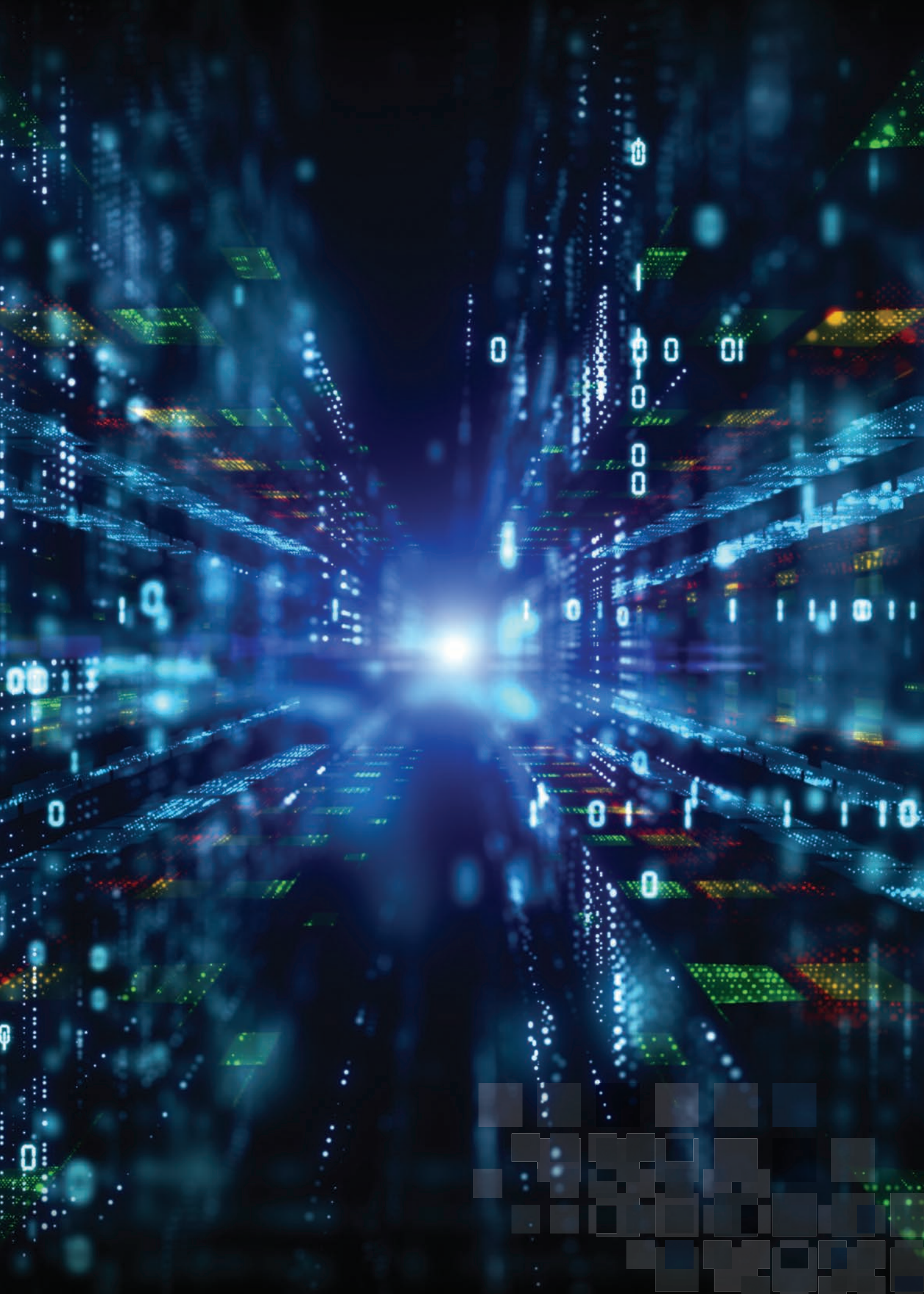
Luxembourg has made concrete commitments towards strengthening European defence, including cyber defence within both the European Union (EU) and the North Atlantic Treaty Organization (NATO). Luxembourg will honour these commitments and has defined its contribution to common defence in accordance with its own interests and objectives. Emphasis will be placed on upskilling our workforce, enhancing national resilience in cyberspace, supporting private sector capability and on strengthening our engagement with Allies and partners. This will ensure a sustainably resourced approach to integrating cyber defence across Luxembourg Defence and will set the conditions for Luxembourg to develop expertise and capabilities which can also be offered to Allies and partners.

As Minister of Defence, I am determined to see this strategy implemented in full. I will work closely with colleagues across Government, the wider public sector and academia to ensure we achieve this ambition.

François BAUSCH

Deputy Prime Minister and Minister
of Defence, Mobility and Public Works

CONTENTS



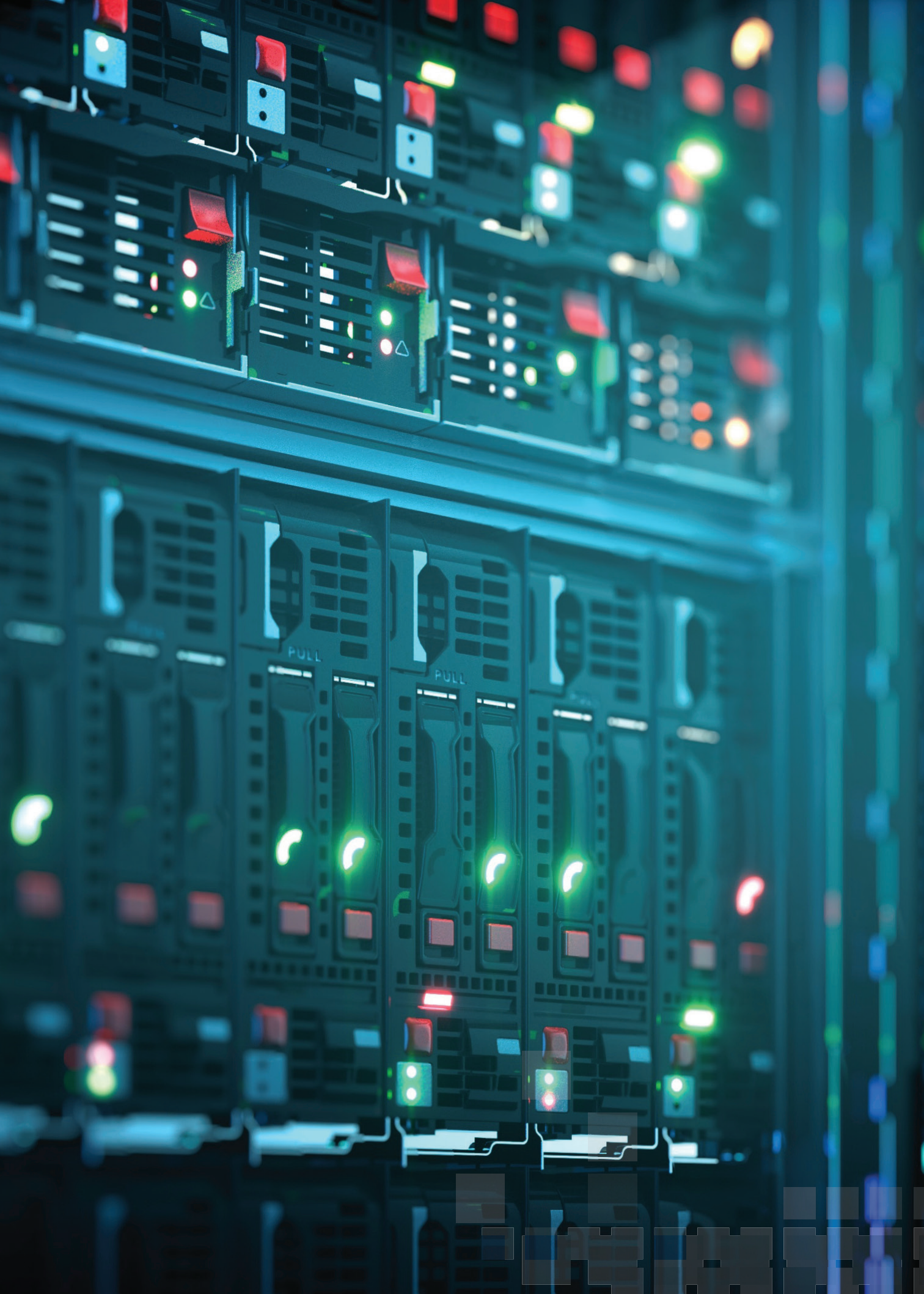
1 INTRODUCTION

The Luxembourg Defence Guidelines for 2025 and beyond highlight that threats to Luxembourg's vital interests do not stop at the physical border. Cyberspace is vital for Luxembourg's security and essential for the proper functioning and resilience of the country's dynamic and knowledge-based services economy that is open to the world. Resilience encompasses the full range of measures needed to ensure that institutions and public services continue to function in all circumstances and that populations and critical infrastructure are safeguarded. This broad concept of resilience naturally extends towards the cyberspace domain.

The Defence Guidelines outline the continued development of cyber defence expertise and capabilities in order to enhance cybersecurity of Luxembourg Defence and security of military personnel, particularly on deployments. A national strategy for cyber defence will underpin the "defence" component of the current and forthcoming national cybersecurity strategies. The long-term objective of this strategy is for Luxembourg to have one of NATO and EU's most cyber secure Defences, and to develop expertise and capabilities which can be offered to Allies and partners. The strategy focuses on four strategic goals which will be reviewed periodically in order to convey sufficient flexibility and adaptability in a fast-changing environment.

Luxembourg Defence is responsible for ensuring EU and NATO-defined cyber defence commitments and policies are upheld. On a national level, the Directorate of Defence is part of the Interministerial Coordination Committee for Cyber Prevention and Cybersecurity and thereby contributes to the National Cybersecurity Strategy as well as jointly ensuring that subsequent initiatives are coherent and coordinated. This inaugural Cyber Defence Strategy will allow Luxembourg Defence to mature its capabilities, to contribute further to national cybersecurity initiatives and to strengthen resilience of national infrastructure.

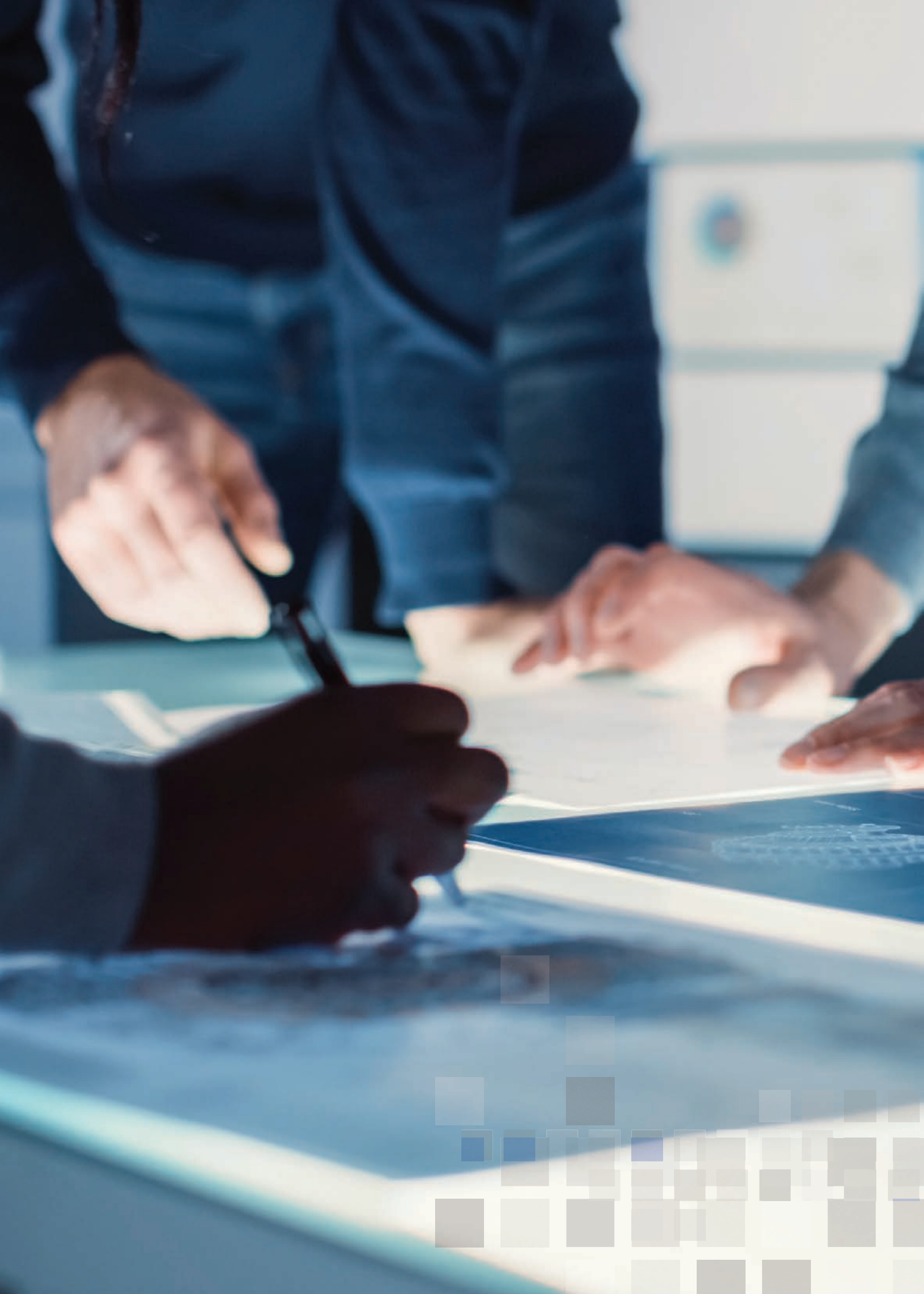
Cyber defence is not a new concept, with NATO having already released its first Cyber Defence Policy in 2008 and the EU's publication of their inaugural Cyber Defence Policy Framework in 2014. Neither is cyber defence new to Luxembourg where steps have already been taken to secure Luxembourg's assets. To continue asserting Luxembourg's interests, to have its voice heard and to enjoy the collective security assured in particular by NATO, this strategy incorporates Luxembourg's commitments towards international organisations, ensuring that Luxembourg bears its share of responsibility in efforts and risks inherent in collective and common defence, and be recognised as a partner making relevant contributions.


PULL
PULL

2 LUXEMBOURG CYBER DEFENCE LONG-TERM OBJECTIVE

By 2030, Luxembourg will have one of NATO/EU's most cyber secure Defences, through maximisation of its cyber defence capabilities.

By developing cyber defence capabilities and contributing to national cyberspace resilience, Luxembourg Defence aims to strengthen its reputation as a reliable partner for international organisations such as NATO and the EU, as well as a reference point for relevant national actors in the cyberspace domain. Through investment in people, technology, as well as in research and development, Luxembourg will develop expertise and capabilities which can also be offered to Allies and partners.



3 STRATEGIC GOALS

Luxembourg's cyber defence is young and needs to mature. It must establish its place in the Luxembourg Armed Forces and Luxembourgish cybersecurity landscape while at the same time building up core cyber defence capabilities. Hence, the Strategic Goals (SG) to implement this strategy cover a wide area of aspects:

- **SG1 A skilled and motivated workforce**
- **SG2 Strong national and international cyber cooperation**
- **SG3 Cyber defence integrated in all Luxembourg Defence activities, assets and culture**
- **SG4 "CyberFutures" landscape mapped, priorities identified and research programmes underway**

The aim is to **develop the right capabilities, govern and use them appropriately, embed cyber defence in Luxembourg Defence and establish Luxembourg Cyber Defence as a reputable partner both internationally and domestically.**

The achievement of the Strategic Goals depends on the implementation of different capabilities. The following sections define these Strategic Goals and the capabilities underlying them.

3.1 STRATEGIC GOAL 1 – A skilled and motivated workforce

The first prerequisite for the long-term objective is a cyber-literate, qualified and motivated workforce. Existing Luxembourg Defence workforce will be upskilled and new cyber talent will be attracted by raising the visibility of Luxembourg Cyber Defence. Furthermore, Luxembourg Defence will contribute to enhancing national cyber competence in order to increase national cyberspace resilience across private and public sectors.

CAPABILITY 1:

Knowledgeable and experienced defence personnel

Luxembourg Defence will establish and promote internal cybersecurity training and raise awareness of the importance of integrating cybersecurity in existing processes. Luxembourg Defence will send personnel to participate in national and international cyber exercises and courses. Cyber aspects will be integrated into military exercises and taken into account in operations.

CAPABILITY 2:

Increased positive public perception of Luxembourg Cyber Defence, including as an employer

Through presence at national cybersecurity conferences and job fairs, promotion of Luxembourg Cyber Defence initiatives via social media and public diplomacy and cooperation with the Luxembourg education sector, public perception of Luxembourg Defence as an employer will be improved.

CAPABILITY 3:

Established and strengthened key cyber defence bodies

Cyber defence is a growing area and requires capacity building of existing and new structures. Human resources will be increased, dedicated MilCERT capabilities will be put in place and Luxembourg Defence is in favour of the creation of a national cyber reserve, supporting its establishment.

CAPABILITY 4:

Enhanced national non-military/ non-defence cyber expertise

Cyber defence is an integral part of the posture of Luxembourg Defence which will provide training and exercises for relevant personnel, e.g. using the Luxembourg Cyber Range platform.

3.2 STRATEGIC GOAL 2 – Strong national and international cyber cooperation

Given that cyberspace has no borders, Luxembourg will work nationally and internationally in order to uphold the international rules-based order, to fulfil commitments made, *inter alia*, under the auspices of NATO and EU.

CAPABILITY 1:
Mutual needs and capacities and enabling factors identified

Luxembourg Defence will undertake fact-finding missions and commission regular bench marking, as well as a cataloguing of Luxembourg cyber defence industry capability in order to identify future needs. This work will also help Luxembourgish companies access the international cyber defence market.

CAPABILITY 2:
Continuous exchange of expertise and resources

Luxembourg Defence will promote Luxembourgish expertise and exchange of best practice by building national and international networks, becoming a member of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) and participation of other relevant activities, such as in international exercises. Luxembourg will also participate in international threat intelligence sharing to enhance situational awareness with and between NATO Allies and Partners, and EU Member States.

CAPABILITY 3:
Strengthened cooperation with national actors

Luxembourg Defence will continue to participate in the Interministerial Coordination Committee for Cyber Prevention and Cybersecurity, enhance collaboration with national actors and take part in cybersecurity-related national projects.

3.3 STRATEGIC GOAL 3 –

Cyber Defence integrated in all Luxembourg Defence activities, assets and culture

Digitalisation of modern societies has given great opportunity but also increased exposure to risk and Defence is no exception. Cyber awareness and literacy in Luxembourg Defence activities, assets and culture will be mainstreamed. Resilience of Defence and Luxembourg Armed Forces in cyberspace in particular will be increased, both domestically and in operations.

CAPABILITY 1:

Cybersecurity anchored in organisational culture

Luxembourg Defence will implement leading industry and international organisation best practice and guidelines to mainstream cybersecurity in organisational culture. Luxembourg Defence will also introduce a Cyber Defence visual identity.

CAPABILITY 2:

Governance, implementation and execution

Through a governance, implementation and evaluation framework, Luxembourg Defence will ensure mainstreaming of cybersecurity best practice through the implementation of a process-based Information Security Management System framework. Furthermore, Luxembourg Defence will implement projects such as the Cyber Range, training exercises and contribute to cyberspace operations. Luxembourg Armed Forces will continuously seek to improve cyberspace resilience of its personnel, infrastructures, capabilities and systems.

3.4 STRATEGIC GOAL 4 – "Cyberfutures" Landscape mapped, priorities identified and research programmes underway

Luxembourg Defence will map emerging and future challenges in order to identify threats and to make best use of technological developments for improving cyber defence. This should particularly benefit Luxembourg Armed Forces in their operational role.

CAPABILITY 1:
Continuous mapping of future challenges and opportunities, defined research, development and technology priorities (medium term)

Regular horizon scanning will be undertaken to identify challenges and opportunities, which will likely influence Luxembourg's cybersecurity and cyber defence posture in the years to come. Using the results of this recurring exercise, the "CyberFutures" most relevant to Luxembourg Defence will be identified.

CAPABILITY 2:
Cyber defence assets and capabilities alignment (short term)

Using these horizon scanning results ("CyberFutures"), Luxembourg Defence will align its assets and capabilities to future challenges. Given that most cutting-edge innovation takes place in the private sector, appropriate Luxembourg expertise and potential will be used to assist in the required development and procurement programmes.

Regular reviews will take place in order to ensure that previously identified "CyberFutures" are still relevant for Luxembourg Defence.

CAPABILITY 3:
Cyber integrated into Luxembourg Defence R&D

Relevant results of the cyber domain horizon scanning will be prioritised to direct nationally supported research.

MONITORING AND EVALUATION

4.1 Activities and programmes

The activities and programmes underpinning the Strategic Goals and capabilities will be subject to annual review against pre-agreed Key Performance Indicators (KPIs), after which there may be adjustment of KPIs, content or objectives.

4.2 Strategic Goals and capabilities

In light of review and adjustment of underlying activities and programmes, Strategic Goals and capabilities will be reviewed periodically.

GLOSSARY AND DEFINITIONS

CIS	Communications and Information Systems
CyberFutures	Emerging and future challenges and opportunities in cyber defence of potential relevance to Luxembourg Defence
EU	European Union
Luxembourg Defence	The Luxembourg Armed Forces and the Directorate of Defence of the Ministry of Foreign and European Affairs
Luxembourg Cyber Defence	The entities responsible for cyber defence in Luxembourg Armed Forces and the Directorate of Defence of the Ministry of Foreign and European Affairs
KPI	Key Performance Indicator
MilCERT	Military Computer Emergency Response Team (CERT)
NATO	North Atlantic Treaty Organization
R&D	Research and development
SG	Strategic Goal

Cyber defence[1]	The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems
Cybersecurity[1]	The application of security measures for the protection of communication, information and other electronic systems, as well as the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation. According to the NATO publications "Technical and Implementation Directive for CIS Security" (page 1-7) and "Allied Joint Doctrine for Cyberspace Operations" (page 4), an equivalency of terms CIS (Communication and Information System) security and cybersecurity has been established. Therefore, this strategy uses the term cybersecurity which also encompasses CIS security.
Cyberspace resilience[1]	The overall technical and procedural ability of systems, organizations and operations to withstand cyber incidents and, where harm is caused, recover from them with no or acceptable impact on mission assurance or continuity.
Cyber operation[2]	Actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve commanders' objectives.

1 NATO Definition according to AAP-06 (2019)

2 NATO Definition according to AJP 3.20

VERSION FRANCAISE ▶

https://gd.lu/6Bn6xL