STRATEGIC COUNTRY REPORT: BELGIUM

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

Chapter 1

Geopolitics

Executive Summary

Belgium's geopolitical standing in the digital domain is defined by a dual dynamic: deep integration into the European Union's collective security architecture and a marked technical reliance on non-European digital infrastructure. As the host of major EU institutions, Belgium leverages the "Brussels effect"—regulatory power exemplified by GDPR—to influence global digital standards and enhance national security [Source 1]. However, network analysis reveals a critical dependency on foreign upstream transit providers, specifically US-based entities, which introduces potential vulnerabilities regarding data sovereignty and extraterritorial legal reach, such as the US CLOUD Act [Source 1].

While Belgium is actively pursuing digital sovereignty through a €5 billion national investment plan and alignment with the EU's "Digital Decade" framework [Source 11], its current infrastructure shows high centralization. Technical intelligence indicates that a small number of Autonomous System Numbers (ASNs) hold significant leverage over Belgian connectivity, creating potential single points of failure [IYP-GRAPH]. Consequently, Belgium's geopolitical strategy is shifting toward bolstering "technological resilience" through EU-wide initiatives, such as the Global Gateway and cooperation with NATO on emerging disruptive technologies, to mitigate external dependencies and secure its position as a digital node in Western Europe [Source 2, Source 10].

1.1 Strategic Positioning and EU Integration

Belgium's digital geopolitics are inseparable from its role within the European Union. The nation actively participates in the EU's Strategic Compass, a framework designed to enhance the bloc's ability to act decisively in crises and secure strategic domains, including cyberspace [Source 2]. This integration allows Belgium to amplify its geopolitical weight, utilizing collective EU mechanisms to navigate the complexities of international data flows and regulatory divergences.

Despite this political integration, Belgium faces challenges related to the extraterritorial reach

of foreign jurisdictions. The influence of the US CLOUD Act, which allows US law enforcement to compel data disclosure from US-based tech companies regardless of where the data is stored, poses a sovereignty challenge for Belgian digital assets hosted or transited by American firms [Source 1]. To counter this, Belgium supports the European Network for Technological Resilience and Sovereignty (ETRS), aiming to develop a values-driven, resilient digital infrastructure that reduces reliance on non-EU technology stacks [Source 9].

1.2 Infrastructure Dependencies and Network Centrality

Technical analysis of Belgium's digital terrain highlights a significant reliance on a limited number of upstream transit providers. The network is heavily dependent on **COGENT-174**, a US-based operator, which exhibits the highest incoming dependency count (39,993) among identified providers [IYP-GRAPH]. Other critical dependencies include **COLT Technology Services** and **CLOUDFLARENET** [IYP-GRAPH].

The concentration of connectivity is further evidenced by "hegemony scores" (`d.hege`), where a score of 1.0 indicates total dependency. Analysis reveals that key operators such as **KPN B.V.**, **M247 Europe SRL**, and **Proximus NV** all possess a `d.hege` score of 1.0 [IYP-GRAPH]. This suggests a high degree of centralization, where specific networks act as unavoidable chokepoints for downstream traffic. While Belgium peers with diverse entities at Internet Exchange Points (IXPs)—including Akamai, Eurofiber, and Swisscom—the underlying transit architecture remains vulnerable to the operational or political decisions of a few dominant players [IYP-GRAPH].

1.3 Investment and Future Sovereignty

To mitigate these vulnerabilities, Belgium is executing a strategy focused on infrastructure hardening and economic digitization. The government has outlined a €5 billion investment aimed at expanding digital infrastructure and fostering a "Built in Europe, Powered by AI" ecosystem [Source 11]. This domestic spending is aligned with the EU's "State of the Digital Decade 2025" targets, which prioritize the deployment of foundational technologies like semiconductors and secure cloud services to reduce the digital trade deficit [Source 12].

Externally, Belgium is positioned to benefit from the EU-Africa Global Gateway Investment Package. This initiative focuses on strengthening secure digital connections, including submarine and terrestrial fiber-optic cables between Europe and Africa [Source 6]. While specific technical data on Belgium's current submarine cable ownership is opaque, the country's alignment with the Connecting Europe Facility (CEF) Digital Community ensures it remains a stakeholder in future cross-border backbone projects [Source 5]. Furthermore, as a NATO member, Belgium is integrated into alliance-wide strategies concerning Emerging and Disruptive Technologies (EDTs), ensuring its digital defense posture evolves in tandem with transatlantic security standards [Source 10].

References

- [Source 1] Geopolitical Aspects of Digital Trade - European Parliament (https://www.europarl.europa.eu/
- [Source 2] A Strategic Compass for Security and Defence - EEAS (https://www.eeas.europa.eu/eeas/strate compass-security-and-defence-1_en)
- [Source 3] Lobito Corridor: A Geopolitical Battleground for Critical Raw Materials (https://www.helvetas.org/en/switzerland/how-you-can-help/follow-us/blog/advocacy/Lobito-Corridor-A-Geopolitical-Battleground-for-Critical-Raw-Materials)
- [Source 4] Submarine communications cable - Wikipedia (https://en.wikipedia.org/wiki/Submarine_comm
- [Source 5] CEF Digital Community Conference | Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/events/cef-digital-community-conference)
- [Source 6] EU-Africa: Global Gateway Investment Package (https://international-partnerships.ec.europa.eu/policies/global-gateway/initiatives-sub-saharan-africa/eu-africa-global-gateway-investment-package_en)
- [Source 7] Belgium - Digital Economy - International Trade Administration (https://www.trade.gov/count commercial-guides/belgium-digital-economy)
- [Source 8] European DIGITAL SME Alliance (https://www.digitalsme.eu/)
- [Source 9] European Network for Technological Resilience and Sovereignty (https://www.bertelsmann-stiftung.de/en/topics/latest-news/2025/european-network-for-technological-resilience-and-sovereignty-etrs-to-strengthen-europes-digital-future)
- [Source 10] Emerging and disruptive technologies | NATO Topic (https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies)
- [Source 11] Meeting with Deputy Prime Minister David Clarinval on Belgium's Digital Infrastructure (https://www.linkedin.com/posts/marcus-jadotte-51534226_belgium-digitalinfrastructure-ai-activity-7402549011053780992-dsm1)
- [Source 12] State of the Digital Decade 2025 report (https://digital-strategy.ec.europa.eu/en/library/state digital-decade-2025-report)
- [IYP-GRAPH] Internal Knowledge Graph (Upstream Transit & Peering Analysis)

Chapter 2

Infrastructure

2.1 Executive Summary

Belgium's critical digital infrastructure is characterized by a dichotomy between rapid fixed-network modernization and a mobile sector recovering from regulatory delays. The nation has positioned itself as a "main mover" in fiber deployment, registering a 43% growth in homes passed, significantly outpacing many European peers in recent acceleration [1]. However, the mobile domain, particularly 5G, has historically suffered from chronic delays attributed to federal and regional disputes over spectrum and radiation standards [2]. Despite these hurdles, 5G outdoor population coverage has reached 95%, although indoor coverage lags at 76% [3].

The nation serves as a strategic node for data processing and interconnection. Belgium hosts major hyperscale facilities, notably Google's campus in Saint-Ghislain, with further developments underway in Farciennes [4]. The interconnection ecosystem is robust, anchored by the Belgian National Internet Exchange (BNIX), which connects over 660 Autonomous System Numbers (ASNs) [5]. Security posture is notably high, with 95.35% of ASNs enabling RPKI validation, signaling a mature approach to routing security [5]. Future infrastructure resilience faces challenges related to the escalating power demands of AI-ready data centers and the need to integrate a fourth mobile network operator, DIGI, into the existing physical landscape [6][7].

2.2 Fixed Network and Fiber Expansion

Belgium is currently undergoing a significant transformation in its fixed broadband infrastructure. The country has been identified as a high-growth market for Fiber to the Home (FTTH). Recent intelligence indicates that Belgium is a "main mover" in the European context, achieving a 43% annual growth rate in terms of homes passed [1]. This acceleration is critical for meeting the European Union's gigabit connectivity targets by 2025 and eliminating "white spots" where high-speed services are unavailable [8].

While the specific granular details of the National Broadband Plan regarding rural deployment remain opaque in open sources, the aggressive growth rate suggests a market-driven push sup-

ported by regulatory frameworks aimed at closing the digital divide. The focus remains on upgrading legacy copper and cable networks to full fiber to support increasing bandwidth demands [1].

2.3 Mobile Infrastructure and 5G Deployment

The Belgian mobile infrastructure sector is in a state of transition, driven by the rollout of 5G and the entry of a new market player.

5G Coverage and Spectrum After facing chronic delays due to complex federal structures and disagreements between regional governments regarding spectrum auctions and radiation limits—particularly in Brussels—deployment has accelerated [2]. Current intelligence places 5G outdoor population coverage at 95%, while indoor coverage stands at 76% [3]. Despite this progress, Belgium has historically lagged behind the EU average for 5G availability due to these regulatory bottlenecks [9].

Market Competition and Physical Assets The mobile landscape is shifting from a three-player to a four-player market with the entry of DIGI. This new operator has announced ambitious infrastructure goals, aiming to establish a network of 4,500 sites by 2030 [7]. To facilitate this entry and ensure immediate service continuity, DIGI has secured a national roaming agreement with Proximus. Concurrently, Proximus is decommissioning approximately 400 mobile sites and transferring them to InSky (associated with DIGI and Citymesh), optimizing the physical tower distribution across the country [7]. DIGI targets 30% 5G population coverage by the end of 2025 [7].

Service Availability Existing 4G infrastructure remains robust, with Telenet leading 4G availability at 93.74%, followed by Orange (86.02%) and Proximus (81.07%) [7]. However, user sentiment analysis indicates persistent frustration with cellular reception outside major urban centers, highlighting potential gaps in rural tower density [10].

2.4 Data Centers and Cloud Ecosystem

Belgium's central location in Europe makes it a key hub for data storage and processing, though it faces capacity and resource constraints.

Hyperscale and Colocation Facilities The country hosts significant hyperscale infrastructure. Google operates a major data center campus in Saint-Ghislain and has a new facility in development in Farciennes [4]. In the colocation market, "Digital Realty Brussels BRU1" is identified as a primary connectivity hub, hosting the highest concentration of ASNs (46) among data centers in the country [5]. Other key facilities include LCL Brussels (Diegem) and Level(3) Brussels [5].

Capacity and Power Challenges The projected growth of Artificial Intelligence (AI) and cloud computing presents physical infrastructure challenges. AI-ready server racks require 40-

60kW of power, significantly higher than the 10-14kW standard in legacy data centers [11]. This surge in power density places strain on the energy grid and necessitates the construction of new, environmentally sustainable facilities. The availability of data center capacity in major global markets is becoming critically low, a trend likely to impact Belgian expansion plans as demand for sovereign and local cloud processing increases [11].

2.5 Interconnection and Routing Security

Belgium's internet exchange ecosystem is highly centralized, providing efficient traffic exchange but also presenting potential single points of failure.

Internet Exchange Points (IXPs) The Belgian National Internet Exchange (BNIX) is the dominant exchange point, facilitating interconnection for 663 ASNs [5]. A secondary exchange, BelgiumIX, supports 118 ASNs, while smaller entities like NL-ix also operate within the territory [5][12]. This concentration around BNIX highlights its role as a critical national asset.

Routing Dependencies and Security Network analysis reveals high dependency ratios for major domestic providers. ASNs such as Proximus, Telenet, Orange Belgium, and Belnet exhibit high `d.hege` scores (1.0), indicating that they are critical upstream providers for a significant number of downstream networks [5]. Conversely, international connectivity relies heavily on transit providers like Cogent, Colt, and Cloudflare [5].

In terms of routing security, Belgium demonstrates exceptional hygiene. Approximately 95.35% of ASNs have enabled Resource Public Key Infrastructure (RPKI) validation on their prefixes, significantly reducing the risk of route hijacking and misconfiguration [5].

References

- [1] 2025 FTTH Market Panorama - Report by Country (https://www.ftthcouncil.eu/resources/all-publications-and-assets/2359/2025-ftth-market-panorama-report-by-country)
- [2] 5G Coverage in Europe: Progress Toward Goals Amid … - Ookla (https://www.ookla.com/articles/euro 5g-q2-2025)
- [3] 5G roll-out reaches 95% of Belgian households - BIPT (https://www.bipt.be/operators/publication/5g- roll-out-reaches-95-of-belgian-households)
- [4] Locations of Google Data Centers (https://datacenters.google/locations)
- [5] Internal Knowledge Graph [IYP-GRAPH]
- [6] Network sharing in the 5G era - Arthur D. Little (https://www.adlittle.com/sites/default/files/reports/
- [7] DIGI makes a splash as fourth MNO in Belgium, leans on convergence (https://www.ookla.com/articles belgium-launch)
- [8] Belgium - Digital Economy - International Trade Administration (https://www.trade.gov/country-commercial-guides/belgium-digital-economy)
- [9] Belgium 2024 Digital Decade Country Report (https://digital-strategy.ec.europa.eu/en/factpages/belg 2024-digital-decade-country-report)

- [10] Nmbs…Telecom providers… How and why, but please… fix it! - Reddit (https://www.reddit.com/r/belg
- [11] 2CRSi – Investors Presentation Feb 2024 (https://investors.2crsi.com/wp-content/uploads/2024/02/2CRSi-Presentation-Investisseurs-Fev-2024-v1.1-EN.pdf)
- [12] List of Internet exchange points by size - Wikipedia (https://en.wikipedia.org/wiki/List_of_Internet_

Chapter 3

Market

Executive Summary

The Belgian telecommunications market is currently undergoing a significant structural shift, transitioning from a stable oligopoly to a more contested environment characterized by aggressive price disruption. Historically, the market has been dominated by three primary incumbents—Proximus, Telenet, and Orange—resulting in a landscape often associated with premium pricing compared to neighboring markets [Source 1]. However, the recent entry of DIGI as the fourth Mobile Network Operator (MNO) has introduced immediate competitive pressure. DIGI has adopted a "disruptor strategy," leveraging convergence by offering cut-price tariffs for both mobile and fixed broadband services to rapidly acquire market share [Source 1].

While specific subscriber market share data for 2024 remains opaque, the market dynamics are clearly pivoting toward infrastructure competition, specifically in Fiber-to-the-Home (FTTH) deployment. The broader European context suggests a challenging environment for revenue growth, with Average Revenue Per User (ARPU) generally stagnating or declining in mature markets due to regulatory pressures and saturation [Source 2][Source 3]. Consequently, the Belgian market is expected to experience intensified competition focused on value-for-money offerings and the speed of fiber rollout over the medium term.

3.1 Competitive Landscape and Market Structure

The Belgian telecom sector has long been defined by a tripartite structure involving Proximus, Telenet, and Orange. Proximus remains the largest operator, holding significant sway in both mobile and fixed segments, while Telenet and Orange maintain strong competitive positions [Source 1]. This equilibrium is now being challenged by the operational launch of DIGI.

DIGI's entry marks a critical inflection point. As a new MNO, DIGI is deploying its own infrastructure but currently relies on a national roaming agreement with Proximus to provide 4G coverage while its network is built out [Source 1]. This hybrid approach allows DIGI to compete immediately on service availability while investing in long-term asset independence.

The market is also characterized by a race toward gigabit fiber, where incumbents are being forced to defend their market share against alternative operators and open-access fiber entrants [Source 4].

3.2 Pricing Dynamics and Disruption

The most immediate impact of the shifting market structure is visible in pricing strategies. Belgium has historically exhibited high pricing per gigabyte compared to markets like France [Source 1]. The entry of DIGI has shattered this pricing floor. The new entrant has launched with highly aggressive tariffs, notably offering mobile plans at approximately €5 per month for 15 GB of data and fixed fiber connections (500 Mbps) for as low as €10 per month [Source 1].

This pricing strategy is significantly lower than the historical norm for the region and is designed to disrupt the subscriber base of the incumbents. While specific Average Revenue Per User (ARPU) figures for Belgium are not publicly detailed in the current intelligence, broader industry trends indicate that ARPU for fixed broadband and mobile services in Europe is already under pressure, showing flat or negative growth (CAGR of -0.1% to -1.3%) [Source 2]. The introduction of such low-cost options by a fourth player is likely to exacerbate this trend, forcing incumbents to re-evaluate their pricing models or bundle value-added services to retain customers.

3.3 Regulatory and Regional Context

Belgium operates within the broader regulatory framework of the European Union, which significantly influences market behavior. The "Roam Like at Home" policy ensures that data usage is charged at domestic rates when traveling within the EU, a regulation that standardizes consumer expectations across the bloc [Source 5]. Furthermore, the EU has implemented wholesale data caps (currently €1.55/GB, decreasing to €1/GB by 2027), which limits the wholesale revenue potential for operators but lowers barriers for cross-border connectivity [Source 5].

The regulatory environment in Europe is described as "tough," often leading to artificially low prices compared to other global regions [Source 3]. This regulatory stance, combined with the capital-intensive nature of the required fiber and 5G rollouts, creates a high-pressure environment for Belgian operators. They must balance the need for heavy infrastructure investment with the reality of a price-sensitive, highly regulated consumer market.

References

- [Source 1] DIGI makes a splash as fourth MNO in Belgium, leans on convergence (https://www.ookla.com/articles/digi-belgium-launch)
- [Source 2] Perspectives from the Global Telecom Outlook 2024–2028 - PwC (https://www.pwc.com/gx/en/ outlook-perspectives.html)
- [Source 3] state of digital communications | 2023 - Connect Europe (https://connecteurope.org/sites/defau 09/downloads/reports/etno-state%2520of%2520digital%2520communications%25202023.pdf)

- [Source 4] The race to gigabit fiber | Arthur D. Little (https://www.adlittle.com/en/insights/report/race-gigabit-fiber)
- [Source 5] Roaming: Using a mobile phone in the EU - European Union (https://europa.eu/youreurope/cit telecoms/mobile-roaming-costs/index_en.htm)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 4

Localization

Executive Summary

Belgium's localization landscape is characterized by a tension between high reliance on non-European hyperscalers and a regulatory framework anchored in European Union standards. While Belgium does not currently enforce a strict, standalone data residency law for all data categories, it operates under the General Data Protection Regulation (GDPR), which imposes significant restrictions on cross-border data transfers [Source 1, Q6]. The market for cloud infrastructure is heavily dominated by US providers (AWS, Microsoft, Google), who hold approximately 72% of the European market share, compared to just 13% for European providers [Source 2, Q2]. This creates strategic vulnerabilities regarding data sovereignty, particularly in light of the US CLOUD Act, which allows US authorities to compel data disclosure from US companies regardless of server location [Source 1, Q8].

Despite these challenges, there are indicators of localization maturity. The national ccTLD, `.be`, retains high trust and preference among local consumers for e-commerce, supported by stricter identity verification measures to combat abuse [Source 1, Q11; Source 3, Q11]. Furthermore, the launch of local cloud regions, such as Microsoft's Azure Belgium Central, offers technical data residency capabilities, though the extent of public sector migration to these facilities remains unquantified [Source 1, Q10]. Belgium has also introduced investment screening mechanisms for vital infrastructure to mitigate national security risks [Source 2, Q5].

4.1 Regulatory Framework and Data Sovereignty

Belgium's approach to data sovereignty is primarily defined by its adherence to EU regulations rather than unilateral national mandates. There is no specific Belgian law explicitly mandating data residency within national borders for all health, financial, or personal data; instead, the GDPR governs the processing and transfer of such data [Source 1, Q6].

Extraterritorial Risks: A critical strategic concern for Belgian data localization is the applicability of the US CLOUD Act. This legislation permits US law enforcement to demand

data from US-based service providers (who dominate the Belgian market) even if that data is physically stored on servers located in Belgium. This creates a conflict of laws where US legal obligations may override Belgian and EU data protection principles, challenging the concept of effective data sovereignty [Source 1, Q8; Source 2, Q8].

National Security Measures: To address infrastructure security, Belgium implemented a national security-based investment screening law on July 1, 2023. This mechanism allows the government to review investments in "vital infrastructure" by non-EU beneficial owners, signaling a shift toward greater protective oversight of critical digital assets [Source 2, Q5]. Additionally, the European Court of Justice (ECJ) has intervened to ensure that national security mass surveillance activities within member states, including Belgium, operate within the bounds of EU privacy laws [Source 2, Q12].

4.2 Cloud Infrastructure and Hyperscaler Dominance

The Belgian cloud hosting market mirrors the broader European landscape, which is characterized by a heavy dependence on US hyperscalers.

Market Composition: US vendors (Amazon, Microsoft, Google) collectively control 72% of the European IaaS/PaaS market. In contrast, European providers hold only a 13% share, struggling to compete due to the vast capital resources of their American counterparts [Source 2, Q2]. While European providers like OVHcloud and Scaleway attempt to differentiate themselves through data sovereignty and compliance, their market share remains limited [Source 1, Q2].

Local Hosting Developments: There is a trend toward "technical localization" by foreign providers. Microsoft, for instance, launched its "Azure Belgium Central" region, enabling Belgian businesses and government entities to store data locally. This move aims to address latency and compliance concerns, allowing for innovation with "local data storage in Belgium" [Source 1, Q10]. However, definitive statistics regarding the percentage of Belgian government agencies that have migrated their primary citizen databases to this local infrastructure versus foreign-hosted infrastructure are not publicly available [Source 1, Q10].

Adoption Challenges: Belgian organizations face significant hurdles in cloud adoption, including skills deficits, difficulties in cost estimation, and concerns regarding vendor lock-in and data security [Source 3, Q2].

4.3 Domain Name Localization (.be)

The Belgian Country Code Top-Level Domain (ccTLD), `.be`, remains a critical asset for localization and digital identity within the country.

Trust and Usage: The `.be` domain is widely perceived as a strong indicator of local presence and is explicitly recommended for businesses targeting the Belgian market. It offers superior credibility and search engine visibility (SEO) on Google Belgium compared to generic TLDs like

`.com` or neighboring domains like `.nl` [Source 1, Q11; Source 2, Q11].

Security and Trends: To maintain the integrity of the namespace, administrators have introduced stricter registration policies, including identity verification, to combat phishing and malicious use. Intelligence indicates that 80% of phishing attacks in studied ccTLDs utilize compromised domains rather than newly registered ones, prompting these tighter security controls [Source 3, Q3; Source 3, Q11]. Broader market trends suggest a slowdown in the growth of European ccTLDs due to market saturation and rising deletion rates, alongside a shift where businesses must weigh the value of a `.be` domain against descriptive gTLDs (e.g., `.market`) [Source 2, Q3; Source 1, Q3].

4.4 Digital Infrastructure and Public Sector Maturity

Connectivity: Belgium utilizes the Belgian National Internet eXchange (BNIX) to facilitate local traffic exchange, aiming to keep local traffic within national borders. However, specific metrics regarding the percentage of traffic exchanged locally versus traffic routed internationally are not publicly detailed [Source 1, Q7].

Public Sector Digitalization: Belgium has historically pursued digital maturity through initiatives like the "National Action Plan for eInclusion," aimed at reducing the digital divide [Source 2, Q4]. While current E-Government Development Index (EGDI) scores were not explicitly retrieved in the immediate dataset, the strategic focus remains on the Sustainable Development Goals (SDGs) principle of "leaving no one behind" [Source 1, Q4]. The public sector has faced security challenges, with reports of data breaches in entities such as the National Belgian Railway Company, highlighting vulnerabilities in the management of citizen data [Source 3, Q5].

References

- [Source 1, Q6] Data protection under GDPR - Your Europe (https://europa.eu/youreurope/business/deali with-customers/data-protection/data-protection-gdpr/index_en.htm)
- [Source 2, Q2] EUROPEAN IAAS/PAAS MARKET - BDO (https://www.bdo.nl/getmedia/bf7e33fa-0447-42dd-a0e6-007259d6afe9/June_-2024_BDO_Market-research_IaaS_PaaS.pdf)
- [Source 1, Q8] The Purpose and Impact of the CLOUD Act - Justice.gov (https://www.justice.gov/crimina
- [Source 2, Q8] Clarifying Lawful Overseas Use of Data (CLOUD) Act - AWS (https://aws.amazon.com/compliance/cloud-act/)
- [Source 1, Q11] 10 Best Domain Extensions for EU Businesses - EuroDNS (https://www.eurodns.com/blog domain-extensions-for-eu-businesses-find-the-perfect-fit-for-your-brand)
- [Source 3, Q11] DNS Belgium: an added step for the registration of a .BE domain name (https://www.combell.com/en/blog/dns-belgium-introduced-an-additional-step-for-the-registration-of-a-be-domain-name/)
- [Source 1, Q10] Microsoft opens its first cloud region in Belgium accelerating… (https://pulse.microsoft.com/en/transform-2/na/fa2-microsoft-opens-its-first-cloud-region-in-belgium-accelerating-innovation-and-economic-growth/)

- [Source 2, Q5] Belgium - United States Department of State (https://www.state.gov/reports/2025-investment-climate-statements/belgium)
- [Source 2, Q12] Putting privacy limits on national security mass surveillance (https://www.atlanticcouncil.org/blogs/new-atlanticist/putting-privacy-limits-on-national-security-mass-surveillance-the-european-court-of-justice-intervenes/)
- [Source 1, Q2] Top Cloud Providers in 2024 - Hyperscalers and Alternative vendors (https://holori.com/top-cloud-providers-in-2024/)
- [Source 3, Q2] HYPERSCALERS CLOUD MONITOR IN BELGIUM - CIONET (https://www.cionet.com/hubfs/BE_CIONET-Belgium/2023%20events/BE2023118%20Cloud/Report%
- [Source 2, Q11] E-commerce in Belgium - KVK (https://www.kvk.nl/en/international/e-commerce-in-belgium/)
- [Source 3, Q3] Characterizing and Mitigating Phishing Attacks at ccTLD Scale (https://gsmaragd.github.io/publications/CCS2024/CCS2024.pdf)
- [Source 2, Q3] CENTRstats Global TLD Report: Edition 2_2024 - centr.org (https://www.centr.org/content_page/download/11253/8261/41.html?method=view)
- [Source 1, Q3] Your opinion about a descriptive TLD as a part of the business name (https://www.reddit.com/r/Domains/comments/1iheanh/your_opinion_about_a_descriptive_tld_as_
- [Source 1, Q7] Who are we? - Bnix (https://www.bnix.net/en/about/who-are-we)
- [Source 2, Q4] OECD e-Government Studies: Belgium 2008 (EN) (https://www.oecd.org/content/dam/oe e-government-studies-belgium-2008_g1gh949f/9789264055810-en.pdf)
- [Source 1, Q4] E-Government Survey 2022 (https://desapublications.un.org/sites/default/files/publication 09/Web%20version%20E-Government%202022.pdf)
- [Source 3, Q5] Privacy & Cybersecurity Law Blog - Hunton Andrews Kurth LLP (https://www.hunton.com/privacy-and-cybersecurity-law-blog/page288)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 5

Security

Executive Summary

Belgium exhibits a bifurcated security posture characterized by high-level governance maturity contrasted with specific vulnerabilities in network routing infrastructure. The nation ranks 6th globally on the National Cyber Security Index (NCSI) with a score of 94.17, indicating strong strategic cybersecurity frameworks [Source 14]. However, the technical implementation of routing security protocols remains inconsistent. While 72.39% of Belgium's announced IP prefixes have Resource Public Key Infrastructure (RPKI) Route Origin Authorizations (ROAs) configured, the validation rate among Autonomous Systems (ASNs) is mixed, and there are currently no Belgian ASNs listed as participants in the Mutually Agreed Norms for Routing Security (MANRS) initiative [Internal Graph].

The national network topology is heavily centralized around specific key players, creating potential single points of failure. Entities such as Belgacom International Carrier Services (BICS) and Proximus NV serve as critical chokepoints with significant upstream dependencies [Internal Graph]. The threat landscape is active, with historical precedents of large-scale Distributed Denial of Service (DDoS) attacks targeting government and parliamentary infrastructure [Source 5].

5.1 Global Cybersecurity Standing and Governance

Belgium maintains a leading position in global cybersecurity rankings. The country is currently ranked 6th on the National Cyber Security Index (NCSI), achieving a score of 94.17, which reflects a high degree of preparedness in cyber threat prevention and incident management [Source 14].

While the International Telecommunication Union (ITU) publishes a Global Cybersecurity Index (GCI), specific ranking data for Belgium in the most recent 2024 and 2017 reports was not explicitly detailed in the available intelligence [Source 11][Source 12]. Consequently, the NCSI remains the primary metric for assessing Belgium's comparative international standing in this

domain.

5.2 Network Infrastructure and Routing Security

Belgium's routing ecosystem shows a disparity between the adoption of address validation standards and the operational enforcement of routing security norms.

RPKI and MANRS Adoption Adoption of RPKI, a critical standard for preventing BGP route hijacking, is relatively high regarding configuration but inconsistent in validation. Approximately 72.39% of Belgium's announced IP prefixes have RPKI ROAs configured [Internal Graph]. However, when analyzing the security posture of individual ASNs, only 52.6% exhibit a "Valid" RPKI status. A concerning 36.8% are marked as "Invalid," and 10.5% have an "Unknown" status [Internal Graph]. Furthermore, despite the global push for collaborative routing security, zero ASNs in Belgium are currently listed as participants in the MANRS initiative, indicating a gap in voluntary adherence to global routing best practices [Internal Graph].

Critical Chokepoints and Dependencies The Belgian internet infrastructure relies heavily on a limited number of upstream providers, creating distinct chokepoints. Analysis of the network graph identifies the following critical ASNs: * **ASN-BICS (Belgacom International Carrier Services SA):** The most critical node, with 1,076 downstream dependencies. * **Servperso_Systems:** 471 dependencies. * **PROXIMUS-ISP-AS (Proximus NV):** 185 dependencies.

Other significant nodes include M247 Europe SRL and VERIXI SA. Notably, specific ASNs such as ASN 6848 and ASN 196755 (NET-3STARS-AS) exhibit 100% dependency hegemony over their downstream connections, highlighting acute vulnerability; if these upstream providers fail, the dependent networks lose connectivity entirely [Internal Graph].

BGP Incident Reports Despite the theoretical vulnerabilities exposed by the lack of MANRS adoption and mixed RPKI validation, there are no publicly available reports detailing specific BGP hijacking incidents targeting Belgium or its immediate neighbors in the recent period [Source 16][Source 17].

5.3 Threat Landscape and Encryption Standards

DDoS Activity Belgium remains a target for disruptive cyber activities. Intelligence from Q2 2021 indicates a surge in Distributed Denial of Service (DDoS) attacks, where over 200 organizations were targeted, including critical government and parliament websites [Source 5]. This historical data suggests a persistent threat vector aimed at political and administrative infrastructure.

Encryption and Data Security Intelligence regarding the specific percentage of encrypted internet traffic (HTTPS/TLS) in Belgium is limited, with no definitive adoption rate provided by Eurostat or other regional registries [Source 8]. However, security guidance emphasizes

that Belgian organizations—particularly those facilitating remote work or e-commerce—must implement encryption for data in transit to mitigate eavesdropping and tampering risks [Source 19].

Similarly, data regarding Domain Name System Security Extensions (DNSSEC) is opaque. While APNIC tracks these statistics globally, specific validation rates for Belgium are not explicitly reported in the available datasets [Source 1][Source 2].

References

- [Source 1] DNSSEC World Map - APNIC Labs Measurements (https://stats.labs.apnic.net/dnssec)
- [Source 2] A Guide to Using DNSSEC to Secure DNS - Catchpoint (https://www.catchpoint.com/dns-monitoring/dnssec-validation)
- [Source 3] RPKI I-ROV Filtering World Map - APNIC Labs Measurements (https://stats.labs.apnic.net/rp
- [Source 4] IPv6 and RPKI deployment in Vietnam - APNIC Conferences (https://conference.apnic.net/58/ipv6andrpkidep_1725494034.pdf)
- [Source 5] DDoS attack trends for 2021 Q2 - All About Security (https://www.all-about-security.de/ddos-attack-trends-for-2021-q2/)
- [Source 6] Significant Cyber Incidents | Strategic Technologies Program - CSIS (https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents)
- [Source 7] Identity Threat Protection Powered by Recaptured Dark Web Data (https://spycloud.com/)
- [Source 8] Home - Eurostat - European Commission (https://ec.europa.eu/eurostat)
- [Source 9] Cybersecurity Statistics 2025: Rising Threats and Industry Impact (https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics)
- [Source 10] 2024 APNIC Survey Report (https://www.apnic.net/wp-content/uploads/2024/09/APNIC-2024-Survey-Report-APNI-101-2401-V2.pdf)
- [Source 11] Global Cybersecurity Index 2024 - ITU (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf)
- [Source 12] Global Cybersecurity Index (GCI) 2017 - National Security Archive (https://nsarchive.gwu.edu/sites/default/files/documents/3897090/International-Telecommunication-Union-Global.pdf)
- [Source 13] GFCE Global Good Practices (https://thegfce.org/wp-content/uploads/GFCE-Triple-I-handbook-20230630.pdf)
- [Source 14] NCSI :: Ranking - National Cyber Security Index (https://ncsi.ega.ee/ncsi-index/)
- [Source 15] Report 2024 of the registry for the ccTLDs .ch and .li (https://www.nic.ch/export/shared/.cont
- [Source 16] 2024 in Review: DDoS Attacks Report by StormWall (https://stormwall.network/resources/blo attack-statistics-2024)
- [Source 17] Global DDoS Attack Statistics: Q1 2025 Report - StormWall (https://stormwall.network/resou report-q1-2025)

- [Source 18] SSL/TLS handshake errors & how to fix them - Sectigo (https://www.sectigo.com/blog/tls-ssl-handshake-errors-how-to-fix-them)
- [Source 19] Data Encryption - OFEP (https://www.ofep.be/data-encryption/)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 6

Governance

Executive Summary

Belgium maintains a robust digital governance framework characterized by strict adherence to European Union standards and a strong emphasis on fundamental rights. The nation's regulatory environment is defined by the "Brussels Model," prioritizing data protection, transparency, and the rule of law over state-centric control mechanisms [Source 9, Source 10]. A cornerstone of this governance structure is the independence of the telecommunications regulator, the Belgian Institute for Postal services and Telecommunications (BIPT), which was solidified following legislative reforms in 2015 to satisfy European Commission requirements [Source 4].

Key legislative developments include the transposition of the EU Network Information Security II (NIS II) directive into federal law in April 2024 and the implementation of a "Right to Disconnect" for the private sector in 2023, underscoring a policy focus on labor rights in the digital age [Source 2, Source 6]. Belgium has ratified the Budapest Convention on Cybercrime [Source 1] and maintains a clean record regarding internet shutdowns, with no documented instances of government-mandated connectivity disruptions [Source 7]. However, tensions remain regarding the balance of privacy and security, particularly concerning the country's undecided stance on the EU's proposed "Chat Control" legislation [Source 3].

6.1 Regulatory Independence and Telecommunications Framework

The governance of Belgium's telecommunications sector is overseen by the Belgian Institute for Postal services and Telecommunications (BIPT). The regulator's independence is a critical component of the national framework, established to comply with EU directives. Historically, the Belgian government held powers to suspend the regulator's decisions and approve its multi-annual strategy. These provisions triggered infringement proceedings by the European Commission in October 2014. In response, Belgium adopted a new law in March 2015 (published April 7, 2015) that abrogated these powers, effectively insulating the BIPT from direct political

interference and closing the infringement case [Source 4].

Currently, Belgium is aligning its domestic laws with the EU Digital Services Act (DSA) and the EU Digital Markets Act (DMA). Preliminary drafts have been approved, and amendments to the Belgian Code on Economic Law are in progress to facilitate this integration [Source 2].

6.2 Data Protection and Surveillance Architecture

Belgium's data protection regime is anchored in the EU General Data Protection Regulation (GDPR), implemented domestically via the Belgian Data Protection Act of 30 July 2018. This Act applies to both public and private entities, mirroring GDPR principles such as purpose limitation and data minimization [Source 8]. The territorial scope extends to entities established in Belgium and non-EU entities processing the data of individuals within Belgium [Source 8].

In the realm of cybercrime, Belgium ratified the Budapest Convention on Cybercrime, which took effect on December 1, 2012 [Source 1]. Regarding state surveillance, the country is currently navigating the transposition of the EU Network Information Security II (NIS II) directive, which became federal law in April 2024 [Source 2].

A point of ongoing strategic debate is the EU's "Chat Control" proposal, which would mandate the scanning of private messages and photos to combat illegal content. Intelligence indicates that Belgium's position on this proposal remains undecided, reflecting internal deliberation on the trade-offs between enhanced security measures and the preservation of digital privacy rights [Source 3].

6.3 Digital Rights and Labor Legislation

Belgium has distinguished itself through progressive digital labor laws. The "Right to Disconnect" came into force for the private sector on April 1, 2023. This legislation grants employees the legal right to disengage from professional digital tools outside of working hours, aiming to mitigate the "always-on" culture. Implementation is managed at the company level through collective labor agreements [Source 6].

In terms of information access, there are no documented instances of the Belgian government utilizing "kill switch" powers to restrict internet access or block social media platforms. Intelligence reviews of global internet shutdown data confirm that Belgium does not employ the connectivity restrictions seen in authoritarian regimes [Source 7]. This aligns with broader findings that contrast Belgium's regulatory environment with the global decline in internet freedom [Source 5].

6.4 Strategic Orientation: The Brussels Model

Belgium's digital policy trajectory is firmly oriented toward the "Brussels Model," a regulatory approach characterized by rights-respecting legislation and risk-based management of technology.

This stands in contrast to the "Beijing Model" of state control and digital repression [Source 10].

This orientation is evidenced by the country's support for the EU AI Act, which categorizes AI systems by risk level to prevent human rights abuses, and the rejection of mass surveillance tools often associated with authoritarian governance [Source 10]. The focus remains on safeguarding data privacy and ensuring responsible digital practices within the health and commercial sectors [Source 9].

References

- [Source 1] UNTC - Budapest Convention on Cybercrime (https://treaties.un.org/Pages/showDetails.aspx?
- [Source 2] Belgium - Digital Economy - International Trade Administration (https://www.trade.gov/count commercial-guides/belgium-digital-economy)
- [Source 3] EU 'Chat Control' would scan ALL your private messages and photos (https://www.reddit.com/r/belgium/comments/1mphxwh/eu_chat_control_would_scan_all_your_pri
- [Source 4] Commission closes Belgian telecom regulator's independence case (https://digital-strategy.ec.europa.eu/en/news/commission-closes-belgian-telecom-regulators-independence-case)
- [Source 5] FREEDOM ON THE NET 2024 (https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf)
- [Source 6] Belgium: The Right to Disconnect Q&A | Insights - Mayer Brown (https://www.mayerbrown.com/en/insights/publications/2025/03/belgium-the-right-to-disconnect-qa)
- [Source 7] Evading accountability through internet shutdowns: | Access Now (https://www.accessnow.org/wp-content/uploads/2023/03/Evading-accountability-through-internet-shutdowns.pdf)
- [Source 8] Belgium's data protection law: Everything you should know - Didomi (https://www.didomi.io/blog/belgium-data-protection-law)
- [Source 9] Vital Signs: Digital Health Law Update | Spring 2025 | Insights (https://www.jonesday.com/en/ signs-digital-health-law-update–spring-2025)
- [Source 10] Using AI as a weapon of repression and its impact on human rights (https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.p
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: The Office of the Prime Minister / President **From:** Chief Strategy Officer **Date:** October 26, 2025 **Subject:** STATE OF THE DIGITAL NATION – STRATEGIC DIAGNOSIS

8.1 1. Executive Summary: The "Big Picture" Diagnosis

8.1.1 The Narrative: The "Head Without a Body"

Belgium stands as the undisputed **regulatory capital of the digital world**. Through the "Brussels Effect," we draft the rules (GDPR, AI Act) that govern global technology. However, our technical reality contradicts our political stature. While we host the institutions that define digital sovereignty, our underlying infrastructure is heavily dependent on non-European actors and exhibits concerning hygiene gaps.

We are building a world-class regulatory fortress on top of rented, foreign-controlled physical foundations. We possess the governance of a superpower but the routing security of a developing nation.

8.1.2 The Paradox: "The Sovereignty Gap"

Strong Governance vs. Fragile Sovereignty. We rank 6th globally in cybersecurity governance (NCSI), yet **zero** Belgian operators participate in the MANRS global routing security initiative. We champion European data privacy, yet 72% of our cloud market—and the data of our citizens—resides on US-owned infrastructure subject to the extraterritorial reach of the CLOUD Act. We are politically sovereign, but technically dependent.

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

STRENGTHS (Internal Assets)	WEAKNESSES (Internal Flaws)
The "Brussels Node": Unrivaled geopolitical centrality; host to EU/NATO, making us a default connectivity hub. **Fiber Velocity:** "Main Mover" status with 43% growth in fiber deployment; fixed infrastructure is modernizing rapidly. **Regulatory Maturity:** Independent regulator (BIPT) and strong legal frameworks (Right to Disconnect).	**Routing Hygiene:** 0% MANRS participation and mixed RPKI validation create invisible security backdoors. **Network Centrality:** Dangerous reliance on single points of failure (BICS, Proximus) for upstream transit. **Energy Constraints:** Looming power shortages threaten the expansion of AI-ready data centers.

OPPORTUNITIES (External Leverage)	THREATS (External Dangers)
AI Hosting Hub: Leverage Google's Saint-Ghislain presence to become the "AI Engine Room" of Europe. **Market Disruption:** Entry of DIGI (4th operator) breaks the oligopoly, driving down costs and forcing innovation. **EU Funding:** Capitalize on the Global Gateway and CEF Digital to subsidize cross-border connectivity.	**The US CLOUD Act:** Legal vectors allowing foreign powers to access Belgian data regardless of GDPR. **Targeted Cyberwarfare:** As the seat of the EU, Belgium is a primary target for state-sponsored DDoS and espionage. **Hyperscaler Lock-in:** 72% market share by US tech giants stifles local innovation and sovereignty.

8.3 3. Strategic Roadmap: The Policy Agenda

8.3.1 Phase 1: Immediate - "The Security Shield" (Months 1-6)

Objective: *Close the gap between our high governance scores and low technical hygiene.*

- **Action 1 (Executive Decree):** Mandate **MANRS compliance and RPKI validation** for all ISPs and Cloud Providers servicing government contracts. If they want state money, they must secure the route.
- **Action 2 (Sovereignty Audit):** Conduct a classified "Dependency Stress Test" on BICS and Proximus. Simulate a disconnection of US upstream providers (Cogent/Lumen) to identify backup routing paths for critical state functions.
- **Action 3 (The "Brussels Bubble" Perimeter):** Establish a specific, hardened digital zone for the EU quarter, prioritizing encrypted, local-only routing to prevent foreign espionage via BGP hijacking.

8.3.2 Phase 2: Medium Term - "Infrastructure & Energy" (Months 6-24)

Objective: *Resolve the conflict between AI growth and energy constraints.*

- **Action 1 (Green Data Corridor):** Zone specific land in Wallonia for "AI Hyperscale Parks" paired directly with renewable energy projects (wind/solar) to bypass grid bottlenecks.
- **Action 2 (Market Liberalization):** actively support the rollout of DIGI and other alternative operators to reduce the "Hegemony Score" of incumbent providers. A decentralized network is a resilient network.
- **Action 3 (Data Residency Incentives):** Introduce tax credits for companies that utilize "Trusted European Cloud" providers or local regions (e.g., Azure Belgium Central) to keep data physically within borders.

8.3.3 Phase 3: Long Term - "Digital Federalism" (Years 2-5)

Objective: *Transform Belgium from a regulator to a technical leader.*

- **Action 1 (The "Digital Switzerland"):** Position Belgium as the neutral, secure data vault of Europe. Leverage our strong privacy laws to attract sensitive data hosting (medical, financial) from across the EU.
- **Action 2 (Education Pipeline):** Realign university curricula to focus on **Network Engineering and Cybersecurity** to reduce reliance on foreign technical talent.
- **Action 3 (Sovereign AI Stack):** Invest in a national sovereign Large Language Model (LLM) infrastructure, ensuring the government does not rely on American AI for sensitive decision-making.

8.4 4. Final Verdict

8.4.1 Investability Score: HIGH

Explanation: Despite technical vulnerabilities, Belgium is a Tier-1 investment destination. The fundamentals—location, fiber growth, and legal stability—are rock solid. The entry of a fourth mobile operator signals a dynamic, competitive market. The risks identified (routing security) are technical configurations that can be fixed cheaply, not systemic failures of state.

8.4.2 Maturity Score: MATURE (With Technical Debt)

Explanation: Belgium is a mature digital economy with "First World" infrastructure but "Emerging Market" security habits. We have the fiber and the laws, but we lack the rigorous routing hygiene of our neighbors (like the Netherlands). We are a digital mansion with the front door locked (GDPR) but the back windows open (BGP/Routing).

Signed,

Chief Strategy Officer