Aalto-yliopisto

”Mobile is Global” project

Digital Networks Act (DNA)
Summary of results from wind tunneling workshops

Aalto University

School of Business

Centre for Knowledge and Innovation Research (CKIR)

Scenario-specific summaries from workshops

New Threat Awaits

This 2030 scenario depicts a situation in which Europe's technological sovereignty has strengthened, but the global political situation has become increasingly tense, to the point of war. The US is partially withdrawing from Europe, the Russian threat continues, China is increasing its pressure on Taiwan, and the EU is responding by increasing its investments in defence, artificial intelligence, semiconductors, satellites, and 5G/6G. In this world, large European technology and dual-use players will thrive, while small EU countries, mediocre technology companies and players with weak digital resilience will be more vulnerable. In this scenario, Europe's success will depend on its ability to combine technological capability, security, investment and political unity.

Against this backdrop, **the basic logic of DNA is right but unbalanced**. It strengthens the EU's internal market and harmonises regulation through, for example, the Single Passport model, spectrum coordination, centralisation of satellite licences, copper decommissioning, a new ODN governance structure and preparedness and resilience requirements. In this way, it can support the growth of European players, the European satellite and 6G ecosystem and the continuity of critical infrastructure. This is important precisely in this scenario, where own technological capacity, network redundancy and defence-supporting 5G/6G development are key success factors.

The key conclusion, however, is that DNA is more of an **internal market and governance reform** than a true industrial instrument for building sovereignty. It recognises the needs for security, resilience and strategic autonomy, but does not bring together sufficient investment or industrial policy instruments. In this scenario, Europe will not succeed with coordination alone, but will simultaneously need investments, piloting, standardization capabilities, its own production capacity and security-driven innovation. DNA therefore adds more guidance and control than investment conditions.

Another key observation is that the **benefits and risks of DNA are unevenly distributed**. It can benefit large European actors and strengthen the EU's position in competition between blocs, but at the same time it weakens the flexibility of peripheral Member States, like Finland. Too much harmonisation can slow down decision-making, reduce national security flexibility, weaken piloting, and concentrate investments in large markets. This is critical, because the security environment is not symmetrical across the EU: the needs of Finland, the Baltics and the rest of Eastern Europe differ substantially from the starting points of Southern and Western Europe.

Therefore, the most relevant parts of DNA in this scenario are not consumer or contractual rules, but those **elements that strengthen resilience, convergence of satellite and terrestrial networks, flexible use of spectrum, prioritisation of critical services and the European scale**. DNA is useful when it supports the transition from the old telecom market logic to a dual-use infrastructure policy. If, on the other hand, centralisation slows down

decisions, weakens piloting, reduces national responsiveness and reduces investment, it will erode the very resilience it was intended to build.

Recommendations:

- DNA should include a clear and operational national security and preparedness **deviation mechanism**, so that Member States retain a concrete possibility to deviate from the EU policies when the security environment requires it.
- **A two-tier model** should be built for satellite licensing and frequency management: the EU would be responsible for interoperability, scale and pan-European resources, but the national level would retain rapid competence for security, piloting and small-scale needs.
- An **implementation package** should be prepared alongside DNA, including investment, piloting and testing mechanisms for 6G, satellite networks, dual-use solutions, standardisation testing and security services.
- The implementation of DNA and the effectiveness of the measures should be assessed using **new metrics**, such as the amount of investment, service level in peripheral areas, speed of piloting, strengthening of European ownership and the development of 6G, satellite and resilience capabilities.

Overall, DNA can support Europe in the **New Threat Awaits** scenario, but only if it is not seen as a mere harmonisation project. In this world, DNA combines the European scale, rapid security response, strong investment incentives and national preparedness. Finland's strategic goal should therefore not be to defend or oppose DNA per se, but to transform it into a security and sovereignty-sustainable framework.

Europe's Prometheus

In this scenario, Europe is in a good position in 2030. Its technological position is strong, international trade is functioning well and the EU's internal market has become more integrated than before. The 6G market is growing rapidly and the EU is investing heavily in telecommunications, artificial intelligence, data, semiconductors, quantum computing, space and defence technologies. The geopolitical situation has calmed down, international cooperation is trusted and invested in. The absence of an external threat gives the EU opportunities to build a stronger Europe and the internal market.

In this situation, **DNA mainly acts as an instrument supporting Europe's strengths**. It unifies markets, strengthens consumer rights, increases investment predictability, supports the development of 6G and satellite services and improves security of supply of digital infrastructure. However, the impact of regulation is twofold: it can strengthen the EU's technological sovereignty, but at the same time it increases market concentration, administrative burden and regional inequalities.

The main impact of DNA is that it **moves Europe towards a truly unified digital single market**. The Single Passport model will transform the European telecommunications market from national markets to an EU-wide operator market, where scale, capital, service platforms, spectrum and data capabilities, and the ability to operate in multiple countries are more important than before. This will make it easier for operators and new service providers to scale across borders.

The Single Passport will accelerate market concentration. Large operators will be best placed to exploit a converging market, which could lead to small and national players losing their position. For sparsely populated areas, the impact is twofold: the model can bring in new service providers, satellite and hybrid connections, but it can also direct large operators' investments to the most profitable urban and corporate markets. Consumer rights will not be implemented equally across Europe.

Permanent licences will improve the willingness of operators to invest. The uncertainty associated with fixed-term licences will be eliminated, which will support long-term investments, especially in 5G and 6G networks. This is complemented by the "use it or share it" principle, which prevents spectrum hoarding and can open capacity for other operators. Together, they can create new business models, for example in private 5G/6G industrial networks, campus networks, ports, energy networks, agricultural sensor networks, research networks and rural access cooperatives.

Centralising the management of satellite communications at EU level will fundamentally strengthen the position of European satellite operators. It will create a larger and more unified domestic market, reduce national fragmentation, improve investment predictability and strengthen the EU's strategic autonomy. At the same time, it will improve Europe's bargaining power vis-à-vis the large satellite operators in the US and China. However, the benefits will not be automatic: authorisation processes need to be fast, competition must be ensured and satellites must be integrated to the 6G and terrestrial networks.

The replacement of copper networks with fibre networks is also largely a good thing in this scenario. It modernises the EU's digital infrastructure and supports competitiveness in the 6G era. However, the requirement could become problematic if it becomes too expensive and rigid, undermining regional equality or diverting capital from other future investments.

Recommendations:

- **The competition must be preserved**. Regulation must strengthen competition and must not lock the market to just a few large players. The EU needs strong competition supervision, reasonable authorisation conditions and open models where multiple service providers can use the same infrastructure.
- **The "use it or share it" principle must also work in practice**. The EU must clearly define how spectrum usage is measured, when a spectrum is considered unused and under what conditions it is made available to others.
- It is particularly important for Finland that **"use it or share it" enables genuinely local experiments, research networks and solutions for sparsely populated areas**. Without them, the EU's infrastructure is technically strong, but its market structure is vulnerable.
- **The special needs of sparsely populated areas must be taken into account**. At EU level, it must be ensured that basic connections also work in remote areas, on key transport routes and at critical sites. Countries like Finland should have the right to impose additional obligations to secure security of supply, services in border areas and official networks. Centralising satellite administration can improve backup connections, coverage and official and defence communications in the Northern regions.
- **Avoiding excessive bureaucracy**. Centralisation and harmonisation will only strengthen the EU's position if authorisation processes are fast and predictable. If EU processes slow down, small players are denied access to the market or the specific needs of member states are ignored, regulation can backfire.

DNA is a largely positive and strategically justified instrument in the **Europe's Prometheus** scenario to strengthen the EU's digital competitiveness. It supports 6G investments, unifies the internal market, improves the operating conditions for satellite services and makes the digital infrastructure more crisis-proof. The biggest risks are related to market concentration, regulatory burden and the fact that sparsely populated areas and small players are overshadowed by large operators. DNA will be most successful if it combines investment certainty, competition, local flexibility, security of supply and regional equality.

Frog in a Pot

In this scenario, Europe operates in 2030 in a formally peaceful but geopolitically tense environment, with little EU technological sovereignty. However, the Russian threat has not completely disappeared in Eastern Europe, the situation with China and Taiwan remains tense, and instability in the Middle East continues. Europe's traditional main ally, the US, has turned inward and focused on repairing the consequences of the deep divisions that emerged during President Trump's disastrous second term.

Europe remains prosperous and institutionally strong, but it is cautious in its investments, its decision-making is slow, and its ability to influence global politics has weakened. The EU has sought to harmonise its rules and strengthen its internal market, but the added value of new technologies, such as platforms, cloud services, artificial intelligence and quantum computing, remains largely with American and Chinese tech giants. The standardisation of 6G technology has been delayed and there is a risk of regional versions. The public debate on the break-up of the EU has intensified.

In such an environment, it is difficult for Europe to succeed. It is more a question of **whether Europe can survive** and maintain its strategic space for manoeuvre when the ownership, know-how, skills and innovations of critical technologies are flowing outside the EU. Can EU's technology diplomacy translate value-based regulation into international partnerships? In this situation, telecommunications networks are critical infrastructure: their operational capacity directly affects the security, economy, security of supply and resilience of society.

In this scenario, the objectives of the DNA package would be in the right direction, if the EU were a strong actor, but its **impact will be limited in the context of weak European technological sovereignty**. DNA has increased harmonisation and predictability and facilitated the scaling of networks and services, but at the same time it has opened up wider access to non-EU actors and accelerated consolidation. Investments have increased, with funding mainly coming from outside the EU, while value creation, data management and ownership are being shifted out, deepening dependence on US and Chinese technology stacks and solutions. Frequencies, licences, satellite services and security of supply have been brought to EU level, but fragmentation, national exemptions and slow implementation are weakening the impact. Replacing copper with fibre improves capacity, energy efficiency and 6G readiness, but the benefits are largely channelled to non-European actors.

The risk is that **regulation will increase bureaucracy and slow down decision-making** in a situation where Europe is already too slow compared to its competitors. In such a situation, regulation may accelerate the erosion of Europe's technological sovereignty and the transfer of added value outside Europe. A burdensome pre-approval process may slow down 6G trials, the development of satellite services and industrial networks, and the modernisation of government networks. The aim of the regulation is to support European technology suppliers, but in this scenario, there are hardly any left and the rest are moving out.

The Single Passport model can make the European telecom market truly European, but it can also lead to the concentration of the market in favor of strong global players who can drive smaller local competitors out of the market with their economies of scale. This can lead to a decrease in network investments, as small local players cannot afford and global players have

no interest in developing networks outside large cities. Value creation will shift from networks to the upper layers, and there too global players will dominate the market. These systemic risks must be balanced with competition, safety and security of supply requirements.

Overall, the impact of DNA in this scenario is to weaken Europe's technological sovereignty and push the EU further into the role of a subcontractor and a customer and marketplace for large global players.

Recommendations:

- **The Commission's power to intervene must be subject to clear grounds and conditions**. The Commission should only intervene in national decisions when they harm the internal market, cause cross-border disruptions, jeopardise security of supply or allow a risky actor to access critical infrastructure.
- **Deadlines must be set for approval processes**. If the Commission does not react in time, the decision should be able to proceed on the principle of silent approval.
- **Member States must be left with local flexibility**. The use of frequencies is affected by factors such as geography, population density, border neighbours, military needs and existing infrastructure. The EU should harmonise objectives but not force everyone to adopt the same implementation model.
- **Services in sparsely populated areas must be secured through separate coverage, financing and sharing mechanisms**. The Single Passport alone will not guarantee better services for remote areas.
- **Security of supply and redundancy requirements must be implemented on a risk basis** and financed realistically. A higher level of requirements must be set for critical functions, such as official communications, energy networks, border regions and satellite backup connections.
- **The focus of RDI activities must be shifted from infrastructure to higher application and service layers:** regulatory sandboxes for SMEs, easing the reporting and compliance burden on companies, directing long-term funding at EU level to scalable technology-neutral service and platform solutions.

The proposed regulation is strategically justified in the **Frog in a Pot** scenario, because Europe needs a more unified and stronger European digital infrastructure. However, its success depends on implementation: regulation must be fast, risk-based, investment-supportive and security-policy coherent. Otherwise, there is a risk that well-intended regulation will increase the very slowness and fragmentation it is intended to correct. A reform that strengthens the internal market will only create an even better and more attractive market for non-European operators in a situation where Europe lacks technological capability and leading companies.

From Bad to Worse

In 2030, a technologically weak Europe will have to respond alone to concrete threats from Russia. After the war in Ukraine, Russia has continued its aggression against Eastern European countries and is trying to drive a wedge between the Eastern and Western regions of Europe. China has continued its heavy armament even after the occupation of Taiwan, warfare continues in the Middle East between groups supporting Israel and the Palestinians, and the politically divided United States has focused on spreading the MAGA ideology and solving internal problems.

In this scenario, the most important element of the regulation presented in the DNA is **multi-layered redundancy** and the **cooperation of networks** implemented with different technologies. Multi-layered redundancy supports crisis management and different technologies complement each other's shortcomings and weaknesses. Creating a situational picture, cooperation between authorities, managing exceptional situations, and information distributed to the civilian population are especially important for Member States along EU's Eastern border.

Member States facing a specific threat must have decision-making power: the right to prioritise traffic, direct capacity and backup connections, restrict access to networks for high-risk actors, make rapid exceptions and keep some of the critical information under national control. The EU can set a common framework and coordinate activities, but decision-making must take place at national level when the need for response and security requires. Since Europe's technological sovereignty is weak, those actors that still have capabilities must be given more room to operate.

In spectrum policy, the application of the "use it or share it" principle enables the flexible use of unused spectrum, for example in various experiments, testbeds and private networks. In this scenario, a **flexible culture of experimentation** may be more important than strict regulation when it comes to creating own capabilities and encouraging European technology companies to fill the vacuum left by companies that have moved away. At the same time, however, it must be recognized that the frequency licenses valid until further notice can also lock the market: the position of large operators is strengthened, the negotiating power of the regulator is weakened and the entry of new players into the market becomes more difficult.

In this scenario, the risks of implementation are related to **financing, expertise, bureaucracy and market structure**. Developing and maintaining network infrastructure redundancy is costly and if the obligations are financed only from the balance sheets of operators, there is a risk that other investments will slow down, prices will rise and sparsely populated areas will suffer, which may accelerate market consolidation. Centralizing decision-making may increase bureaucracy. Long processing times, more onerous safety assessments and unclear division of labor may slow down the entry of new players and innovations into the market. A weak technological base drives away experts who move to seek opportunities outside Europe.

The Single Passport model **enables large players from outside the EU to expand their operations into telecommunications services**. The risk is that European telecoms companies will remain subcontractors and the EU's technological sovereignty will be further weakened. Medium-sized and small national operators are also likely targets as consolidation accelerates. The progress of the Single Passport model will revolutionise the operator landscape and

introduce new, specialised players to the market. However, without binding coverage, investment and security of supply obligations, it may weaken the level of service in sparsely populated areas as new players focus on the most profitable markets.

Recommendations:

- **DNA must be linked with resilience development funding and verified training**. Funding can be implemented through funds, PPP models, co-financing of critical industries, tax incentives and EU-level joint procurement. Resilience must also be tested regularly (simulations, backup connections, audits, energy production, joint exercises, etc.).
- **National decision-making authority in crisis situations** must be ensured through specific procedures recorded in DNA, which enable traffic prioritization, capacity allocation, restriction of risk actors and rapid information management.
- **The implementation of DNA regulation must be risk-based and multi-layered**. Connections to critical sites are secured first and with a network-like solution that includes several alternative technologies.
- **The "use it or share it" principle in frequency regulation must be implemented with clear, measurable criteria and effective supervision**. Unused frequencies should be released to private networks, RDI pilot areas and authorities without undue delay.
- **Over-emphasis on bureaucracy must be avoided in EU-level governance**. Authorisation processes must be phased, transparent and fast, so that they do not become an obstacle to innovation and new players. Coverage, investment and security of supply obligations must be emphasised in Single Passport solutions, so that sparsely populated areas are not left with only the bare minimum.

In the **From Bad to Worse** scenario, Europe must strengthen its resilience and digital infrastructure due to the tightened security environment. DNA aims to remove bottlenecks between the Member States and create a basis for long-term investments, but the benefits will only arise if the obligations are linked to funding, training and nationally managed and verified crisis management capabilities. In this situation, the functionality of telecommunications networks, the efficient use of frequencies and multi-layered preparedness are at the heart of the situation. The EU must ensure that its declining technological sovereignty does not completely erode and Europe withers into a mere subcontracting economy.