Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: TA Analysis

Europe is discovering the cost of technological dependence

On 29 September, Reuters published the contents of the new negotiating text of the European Union member states, dated 22 September, from which the fixed deadline of 36 months for replacing equipment from suppliers rated as high risk in key parts of mobile networks was removed.

The European Commission had proposed that deadline in January as part of the new version of the Cybersecurity Act.

Member governments now require that the timeframe for replacement be determined by the degree of risk, the lifetime of the existing equipment, the normal modernisation cycle, the ability to connect the new equipment to the rest of the network and the availability of suitable alternatives.

The negotiations are not over, and the final text will have to be agreed with the European Parliament.

This change is significant because, for the first time, it clearly shows the cost of the European policy of reducing technological dependencies.

In recent years, Brussels has gradually tightened its stance towards suppliers whose equipment it considers a security risk.

That assessment must now be applied to networks already in operation, where the equipment is installed, forms part of the existing infrastructure and is connected to other systems on which the network depends.

The political decision therefore feeds into the investment plans of telecoms operators, and the security goal acquires a clearly defined financial cost.

Three years is a short period in which costs can rise sharply

In 2023, the Commission supported member states' decisions to restrict Huawei and ZTE, judging that these companies pose a significantly higher risk than other 5G suppliers.

Huawei rejects this assessment and maintains that its origin is not, in itself, evidence of a security risk.

The proposal for a new Cybersecurity Act, published in January, aims to make the existing European approach more uniform and legally robust.

It introduces a common framework for risk assessment of suppliers from third countries and allows their equipment to be restricted in the most critical parts of information and communication systems.

For mobile networks, the Commission has stipulated that the period for removing equipment from high-risk suppliers should not exceed 36 months from the publication of the corresponding European list.

> The three-year deadline has faced strong resistance from the industry

Such a deadline has a clear security rationale. If equipment is installed in a part of the network that is important for the functioning of the state and is assessed as a serious risk, a long waiting period undermines the assessment itself.

Telecommunications networks, however, are built over many years. Antennas, radio equipment, traffic management systems and software are not installed or replaced simultaneously.

Replacing a single component often requires additional testing, adjustments to other network elements and work at a large number of locations, while ensuring that customer service continues uninterrupted.

That is precisely why the three-year deadline has faced strong resistance from the industry.

In a joint letter to the European authorities, the directors of Deutsche Telekom and 16

other companies estimated that accelerated replacement could cost up to €40 billion.

Because that estimate comes from the operators themselves, it clearly reflects their interests in negotiations with regulators.

Nevertheless, the figure still illustrates how expensive it could be to remove existing equipment from European networks at short notice. In practice, operators would have to replace equipment before the end of its working life and divert money intended for network development to replace systems that are still functioning.

The same capital is needed for both security and the next network

European operators are already financing the completion of 5G networks, the expansion of fibre optics, capacity growth driven by increasing data transmission and preparations for the next generation of mobile communications.

In this environment, prematurely replacing equipment that is still functioning immediately disrupts the investment sequence.

The company can take on additional debt, postpone another project or try to pass on part of the cost to users.

> At the heart of the debate are speed, cost, and how the security goal can be implemented without seriously damaging network modernisation

The state can help with subsidies or other forms of support, but cybersecurity then also becomes a matter of public finances.

In this context, two policies that Brussels considers important collide. The European Union wants to reduce reliance on suppliers it does not wish to entrust with the most sensitive parts of its infrastructure, while at the same time trying to accelerate investment in digital networks in which it already lags behind the most advanced markets.

Both policies draw funding from the same companies, and for roughly the same period.

At the heart of the debate, therefore, are speed, cost, and how the security goal can be implemented without seriously damaging network modernisation.

The existing dependency is the most expensive to remove

The cheapest time to change suppliers is usually at the next scheduled purchase.

At that point, the company will in any case buy new equipment and can make a different choice.

It is much more expensive when the regulator requires the existing system to be replaced several years before the end of its planned service life.

Part of the previous investment is then written off early, and the new one must begin earlier than envisaged in the business plan.

Telecommunications is the first major test of this approach, but the same questions may soon arise in other areas.

The Cybersecurity Act proposal introduces a European framework for risk assessment in supply chains that may include electrical systems, connected vehicles, cloud computing services, drones, surveillance equipment, space services and semiconductors.

> Limiting new purchases can be relatively quick, whereas replacing existing equipment takes time

In each of these sectors, limiting new purchases can be relatively quick, whereas replacing existing equipment takes time, alternative suppliers and substantial capital.

Future European decisions on technological security will therefore increasingly have to include an economic calculation.

A risk assessment shows how problematic a dependency is. The decision on the deadline determines how quickly the problem should be eliminated and how much of the cost is due to acceleration.

With infrastructure worth billions and planned for ten or more years, the security decision therefore simultaneously becomes a decision about time and money.

Flexibility reduces costs but makes a common policy difficult

The member states' proposal aims to adapt the deadline to specific circumstances.

Equipment in the most sensitive parts of the network may require faster replacement, while in less critical sections it may be possible to wait for a regular modernisation cycle.

This approach reduces pressure on investment budgets and gives operators more time to find alternatives that can be integrated into the existing network.

The price of that flexibility may be new inequality within the Union. One country may interpret the same risk more strictly and complete the replacement within a few years, while another may accept a much longer transition period.

The European Commission has been pushing for a common approach because the previous 5G security framework was implemented at different speeds among member states.

The most likely compromise points to more detailed rules rather than a single deadline for the entire network

If the final law leaves too much room for national discretion, some of the old differences could return through varying deadlines and differing interpretations of what constitutes an acceptable risk.

The most likely compromise points to more detailed rules rather than a single deadline for the entire network.

The most sensitive systems may face shorter deadlines, while other parts of the infrastructure would go through a longer replacement period linked to their working life and the availability of alternatives.

The European Parliament can again press for tighter deadlines during the negotiations, but the space that governments have now opened will hardly disappear completely, because behind it lies the very concrete problem of cost and technical feasibility.

The bill for technological independence has yet to arrive

The final form of the Cybersecurity Act will show how the European Union intends to conduct the next phase of its technology policy.

Until now, much of the political energy has been focused on identifying risky dependencies and preventing them from deepening further.

The final form of the Cybersecurity Act will show how the European Union intends to conduct the next phase of its technology policy

The far more demanding work begins when an existing dependency must be physically removed from already functioning infrastructure.

In the coming years, similar disputes are likely to arise whenever a security assessment calls into question a supplier whose equipment is already widely installed.

Governments will have to decide early whether the cost remains with the companies, whether part of it is taken on by the state and how much time the market is given to find a replacement.

Such questions will become an integral part of technological security policy, because the speed at which dependence is reduced will determine the price the economy pays.

The next contract will have to account for exit as well

In their next major purchases of telecommunications equipment, European operators will scarcely be able to focus only on price, quality, technical capabilities and maintenance costs.

They will also have to estimate how much it would cost to change suppliers in five or ten years if the security assessment or political relations were to change.

This may also affect how future networks are designed. Systems in which equipment from different manufacturers can be connected and replaced more easily, without reconstructing a large part of the network, will be more valuable.

Such a solution may be more expensive and more complex at the outset, but it gives operators more options to change suppliers without incurring huge additional costs.

> More important than the final deadline in the Cybersecurity Act will be how European operators choose the technology and companies with which they enter into long-term contracts

More important than the final deadline in the Cybersecurity Act will be how European operators choose the technology and companies with which they enter into long-term contracts.

In addition to the price, quality and reliability of the equipment, they will have to assess how difficult and expensive it would be to change suppliers in future.

For networks that remain in use for many years, this becomes a very tangible question.

A company that chooses a supplier today is not only choosing the equipment it will use in the years ahead; at the same time, it is deciding how much freedom it will have if, one day, it has to replace that supplier.

In a world where political relations change faster than infrastructure, the ability to break free from technological dependence may become as important as the technology a company purchases today.