Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

The UK is changing the course of European cyber security

The UK government, following several serious security incidents, has decided to change its current approach. Instead of relying on the market and private suppliers, the state is taking greater control over systems critical to the operation of hospitals, energy networks, water supply, and other public services.

For years, it was believed that digital security would develop spontaneously and that competition would encourage companies to protect themselves.

Recent events have demonstrated the ineffectiveness of this approach. Therefore, the government is now introducing clearer rules and assuming a role it has avoided for a decade.

This change followed two serious incidents that affected systems relied upon by state institutions, large companies, and public services within a short period.

The first incident involved an intrusion into F5, one of the world's leading manufacturers of network equipment and software.

Banks, telecommunications companies, government agencies, and the healthcare sector use their products to manage network traffic and protect their systems.

The company confirmed it had discovered unauthorised access to internal systems and parts of its source code—an event that does not in itself constitute an immediate disaster but clearly demonstrates the vulnerability of a key supplier.

A security breach in a particular part of the chain

In practice, this means that those behind the intrusion – according to experts, most likely a group linked to China – had access to information about the functioning of F5 products.

This does not mean these products have been immediately compromised or altered, but it does mean there is a real possibility that the stolen information could be used for future attacks on users of F5 equipment, including many British public institutions.

The National Cyber Security Centre (NCSC) promptly advised all organisations in Britain to verify configurations, implement patches, and enhance access controls.

Another problem emerged at the same time, but from an entirely different direction. Salesforce, one of the most widely used cloud services for managing customer data, has faced a series of claims by hacker groups that they have stolen large volumes of data from various environments.

> Salesforce had to revoke access tokens for certain applications and remove them from use to prevent the problem from spreading further

Salesforce did not confirm the extent of the damage but did confirm that they are investigating and that the problem originated with applications developed by external suppliers.

Gainsight's software, which is used in many organisations alongside the Salesforce platform, attracted the most attention. A security breach occurred in this particular part of the chain.

In the most recent phase of this incident, Salesforce had to revoke access tokens for certain applications and remove them from use to prevent the problem from spreading further.

As a result, many organisations, including UK public services and private companies, have temporarily lost access to parts of their own data – not because their systems were attacked, but because a supplier in another layer of the software chain had a vulnerability.

The state sets the minimum protection

Events like these explain why the British government has decided to change its approach. The new legal framework, presented as the "Cyber Security and Resilience Bill", marks a shift from a system that relies on recommendations and voluntary standards to one in which the state sets the minimum protection required in every part of the critical digital infrastructure.

Critical infrastructure does not refer only to hospitals, water supply, energy networks, and transport, although these are the focus of public attention. For the first time, the new law includes companies that operate in the background of state systems.

> The government is now ending the practice of monitoring only what is visible to the public

These are not only hospitals, water networks, or energy networks; they are also data centres, cloud service providers, and companies that develop or maintain key IT systems.

This layer of infrastructure has so far been largely outside serious oversight, even though it forms the foundation of the entire state's operations.

The government is now ending the practice of monitoring only what is visible to the public, while the greatest risks remain in the chain of private suppliers that hold the most sensitive parts of the system.

Digital security – a core state function

This law grants regulators significantly greater powers. In practice, the British authorities will be able to order organisations to take emergency measures, conduct detailed checks, and impose much harsher penalties than before.

There is also public debate about banning the payment of ransoms in ransomware attacks, which would cut off one of the main sources of funding for criminal groups.

The government does not yet have a final position on banning ransom payments, but the fact that it is considering this option indicates a desire to change its current approach. Instead of merely dealing with the consequences of attacks, it aims to influence the very model from which criminal groups profit and survive.

> Recent attacks have demonstrated how vulnerable digital infrastructure is when the state does not play a key role in its protection

The most important aspect of this change is not in the technical wording of the regulations but in the message sent by the entire state apparatus: digital security is becoming a core state function, not a peripheral issue for external suppliers.

For a long time, the prevailing idea was that the market could be regulated by itself and that companies would solve the security problem through innovation.

Recent incidents in the United States, Europe, and Asia have demonstrated the unsustainable nature of relying solely on the market and voluntary standards.

The attack on Colonial Pipeline (the largest US oil pipeline supplying the East Coast), SolarWinds (an American company whose software is used to manage networks in government institutions and large corporations), and frequent attacks on hospital systems in several countries have demonstrated how vulnerable digital infrastructure is when the state does not play a key role in its protection.

A laboratory for a new European digital security policy

The UK is now taking a different approach. Instead of expecting each local agency to handle government hacking groups independently, the government is taking the lead and setting binding rules.

It is effectively introducing a system in which digital security receives treatment similar to that already given to financial regulation, public health, or the protection of energy networks.

This approach could have significant consequences for the rest of Europe. The European Union is introducing the NIS2 directive (Network and Information Security Directive 2), but the British model goes further by centralising responsibility and requiring key suppliers to bear direct accountability.

The UK is now acting as a laboratory for a new European digital security policy - Keir Starmer with Ursula Von der Leyen

If this model proves effective, other European countries will be pressured to follow the British example, as digital infrastructure has no borders.

If one country maintains high standards while another has lower criteria, the weaker system automatically becomes the entry point for all actors seeking to bypass the stronger one.

In this respect, the UK is now acting as a laboratory for a new European digital security policy. The question is not only whether the new law will be effective, but also whether the political will to maintain such a demanding model will endure.

Costs for companies will be higher, and the resilience of the system depends on whether the state can keep pace with the rapid development of technology and increasingly aggressive attacks.

A path that places the state back at the centre

Britain is choosing a path that places the state back at the centre of the digital order, at a time when global security is declining and the capabilities of criminal groups and state actors are increasing.

This shift concerns not only experts but every citizen who expects hospitals to have access to data, the water supply to function without interruption, and the electricity grid to remain stable.

> The British move raises an issue that Europe will have to address much more quickly than planned

The British move raises an issue that Europe will have to address much more quickly than planned. Digital infrastructure can no longer operate on the assumption that systems will protect themselves and that the private sector will always stay ahead of attackers.

If this change in London demonstrates that it is possible to establish clearer control and greater responsibility among suppliers, it will indicate that other European systems can also be stabilised.

If there are no results, Europe will have to accept that it lacks the basic mechanisms to defend itself in an environment where attacks are becoming daily and the consequences increasingly severe.