

Modern warfare is undergoing a profound transformation. While conventional military strategy has historically focused on territorial control, industrial capacity and military installations, the expanding dependence of governments and economies on digital infrastructure is introducing an entirely different category of strategic vulnerability. Data centres, semiconductor supply chains, cloud computing networks and communication platforms are increasingly becoming critical components of national security.

Reported Ukrainian drone strikes against Russian data infrastructure, including facilities associated with technology companies Sberbank and Yandex, illustrate this emerging dimension of conflict. Accounts of the attacks have suggested substantial disruption to digital services, while claims of a corresponding decline in Russian disinformation activity remain contested.

Irrespective of the precise operational consequences, these developments raise a fundamental geopolitical question: *Can a nation achieve genuine digital sovereignty by concentrating technological control within its territorial boundaries, or does such concentration create vulnerabilities that adversaries can exploit?*

The answer has significant implications not merely for Russia and Ukraine, but for every country seeking to reconcile technological independence with national security.

The Physical Geography of Digital Warfare

The internet is frequently perceived as a decentralised, almost intangible environment. Yet its functionality depends on an extensive physical architecture comprising data centres, submarine cables, telecommunications exchanges, energy infrastructure and semiconductor manufacturing facilities.

How Data Centres are Becoming Strategic Targets in the Battle for Digital Sovereignty

Data centres occupy a particularly important position within this architecture. They host the computing systems that enable financial transactions, government databases, cloud applications, artificial intelligence, communication networks and essential public services.

Consequently, their strategic significance extends considerably beyond their immediate commercial value.

Disrupting a major data centre can generate cascading consequences across multiple sectors. Banking transactions may be delayed, logistics networks interrupted, digital marketplaces rendered inaccessible and communication services temporarily disabled.

Where civilian and military systems share infrastructure, disruption may also affect defence-related communications, intelligence processing and logistical coordination.

The strategic attraction of such facilities is therefore understandable. Unlike dispersed military formations, major computing installations are geographically fixed, energy-intensive and dependent on specialised equipment that cannot always be replaced quickly.

However, their growing importance as potential targets introduces serious humanitarian and legal concerns. Data centres are ordinarily civilian objects under international humanitarian law. Their use for certain military purposes does not automatically make every facility a lawful target; assessments must consider military necessity, distinction, proportionality and feasible precautions.

The digital battlefield cannot be separated from its civilian consequences.

Russia's Digital Sovereignty Paradox

Over the past decade, Russia has pursued an increasingly centralised approach to digital governance, framed around the concept of technological sovereignty.

Legislation introduced in 2015 established requirements for storing certain categories of Russian citizens' personal data domestically. Subsequent regulatory measures expanded state influence over internet infrastructure, information distribution and digital platforms.

The stated objectives included national security, data protection and reducing dependence on foreign technological systems.

Nevertheless, Russia's approach also facilitated tighter information control and the restriction of international digital services.

Following the full-scale invasion of Ukraine in 2022, international sanctions and the withdrawal of numerous Western technology companies further accelerated the separation of Russia's digital ecosystem from global markets.

This created a strategic contradiction.

By seeking greater domestic control over its information infrastructure, Russia potentially increased its dependence on a narrower set of locally concentrated facilities, technology providers and equipment supply chains.

Geographic concentration is not inherently incompatible with resilience. Well-designed domestic networks can incorporate redundancy, geographically separated backups and robust disaster-recovery systems. The vulnerability arises when concentration is combined

with limited international alternatives, restricted procurement channels and inadequate operational resilience.

In such circumstances, the loss of a relatively small number of facilities can produce disproportionately large consequences.

Digital sovereignty, pursued primarily through territorial isolation, may therefore undermine the very security it is intended to guarantee.

Disinformation and the Infrastructure of Influence

The potential relationship between attacks on digital infrastructure and disruptions to information operations introduces another important strategic consideration.

Russian influence campaigns have long been associated with coordinated online activity, including automated accounts, manipulated narratives, information laundering and attempts to exacerbate political divisions in foreign societies.

Yet disinformation should not be understood exclusively as the circulation of demonstrably false statements.

Contemporary influence operations frequently exploit genuine grievances, selective facts, emotionally charged interpretations and existing social divisions.

Their objectives may include undermining institutional legitimacy, reducing public confidence in electoral processes, amplifying social hostility or creating uncertainty about the credibility of established information sources.

Examples from democratic societies illustrate the complexity of this phenomenon. Australia's 2023 Indigenous Voice referendum demonstrated how competing narratives and contested claims can circulate within highly polarised political environments. In New Zealand, researchers have documented online harassment and gendered abuse directed at public figures and participants in political debate.

Such phenomena should not automatically be attributed to foreign interference. Rather, they demonstrate the broader informational conditions that organised influence operations can exploit.

Traditional counter-disinformation strategies have concentrated on identifying misleading content, fact-checking claims, improving media literacy and moderating coordinated inauthentic behaviour.

These interventions remain essential, but they primarily address the visible outputs of influence operations.

The underlying infrastructure receives comparatively less public attention.

Automated campaigns depend on computing resources, hosting providers, network connectivity, account infrastructure and financial arrangements. Interrupting these enabling systems may, under appropriate legal authority, constrain the scale or continuity of malicious operations.

Nevertheless, a reduction in platform traffic does not establish a corresponding reduction in disinformation. Influence networks may migrate between services, operate through foreign infrastructure or rapidly restore disrupted capabilities.

Claims linking particular infrastructure strikes to measurable declines in coordinate