KCS Group International

We look at the world differently...

Preparing for the day that systems go down

August 2026

For several decades, technological progress has been treated almost soley as improvement. Faster computers, permanent connectivity, satellite navigation, cloud storage, artificial intelligence and increasingly sophisticated communications, have transformed civilian life, government and business. Yet, a counter-trend is becoming increasingly difficult to ignore. In some environments, particularly those involving security, intelligence and critical infrastructure, older and simpler technologies are returning because the newest technology has created far greater vulnerabilities of its own.

This trend is not as a result of technological nostalgia. It is as a direct response to hacking, electronic surveillance, jamming, spoofing and an equally serious problem that is often overlooked, human complacency. As organisations become accustomed to technology doing their thinking for them, traditional skills disappear. The result can be greater capability under normal conditions but present a much greater vulnerability when those conditions change.

When convenience becomes dependency

Although the famous story that NASA spent millions developing a pen that could work in space, while Soviet cosmonauts simply used pencils is largely mythical (The Fisher Space Pen was privately developed, while pencils themselves presented hazards from floating graphite and combustible materials), the story survives because the underlying point remains relevant. The most sophisticated solution is not necessarily the most appropriate one.

Satellite navigation demonstrates this particularly well. GPS transformed military and civilian navigation, but it has simultaneously created dependence on satellites and electronic signals.

GPS can be jammed, preventing a receiver from determining its position, or spoofed so that it confidently displays the wrong position. The problem is therefore no longer simply whether technology works, it is whether the operator knows when it has stopped working correctly. This is why militaries still train personnel to navigate using maps and compasses. Finland, among others, has continued emphasising traditional navigation skills precisely because satellite navigation cannot be assumed to remain available during conflict. Paper does not require a satellite. A compass cannot be remotely given a software update. Both remain useful precisely because they are technologically limited.

Smartphones and the surveillance problem

The smartphone represents perhaps the greatest example of technological convenience becoming a security liability. It combines communications, GPS, Wi-Fi, Bluetooth, cameras, microphones, applications, cloud storage and personal information, all in one device. For civilian life, this is extraordinarily convenient. For military personnel, intelligence officers, government employees or corporate executives dealing with sensitive information, it becomes an electronic beacon. Indeed, Western government officials and company executives travelling to China use 'burner phones' that contain no personal or valuable data at all.

The Strava controversy demonstrated the danger. Fitness tracking information published through its global heat map revealed activity patterns around military facilities. Nothing had been hacked. The technology was working exactly as intended. That is perhaps the more disturbing lesson. A technological system does not need to malfunction to create vulnerability. It can compromise security simply by doing what its designers intended. Increasing awareness of these risks is encouraging a return to deliberately disconnected technology: basic telephones, non-networked computers, standalone watches and physical documentation for information that does not need to exist online.

The return of the typewriter

Russia provided an unusually visible example in 2013 when reports emerged that the Federal Protective Service (FSB) had purchased electric typewriters amid concerns about electronic surveillance and information leakage. The story had been exaggerated into claims that the Kremlin was abandoning all computers. It was not. The Kremlin had just decided to use typewriters for the more sensitive work. A typed document cannot be remotely stolen from a network because there is no network. This does not make typewriters completely secure. Documents can still be photographed, stolen or copied.

Indeed, during the Cold War, American IBM Selectric typewriters in Moscow were themselves covertly modified so that keystrokes could be monitored electronically. However, the point is not that old technology is invulnerable. It is that its vulnerabilities are different and, crucially, often require physical access rather than remote penetration from thousands of kilometres away.

Government, infrastructure and deliberate isolation

The same reasoning explains why apparently antiquated equipment has survived within nuclear command systems and critical infrastructure. Power generation, nuclear facilities, pipelines and transportation networks frequently continue operating equipment far older than ordinary consumer electronics. Such systems may appear obsolete, but they are predictable, extensively tested and isolated from external networks. Replacing them with permanently connected equipment may improve efficiency, while simultaneously expanding the number of routes through which an attacker can gain access. Air-gapping therefore remains one of cybersecurity's simplest but strongest principles. If a sensitive computer does not need access to the outside world, physically disconnecting it can eliminate entire categories of remote attack. Sometimes the safest network is no network at all.

HUMINT versus the seduction of SIGINT

The same lesson increasingly applies to intelligence gathering. Governments and corporations have become fascinated with signals intelligence, data harvesting, cyber monitoring, artificial intelligence and vast electronic databases. These systems can process quantities of information that human analysts could never examine manually. But information volume is not the same as understanding.

Corporate intelligence increasingly risks becoming dependent on databases, online searches, social media monitoring and electronically gathered material. Much of this tells the analyst what has already been recorded. It does not necessarily explain motivation, relationships, private intentions or what people are deliberately concealing. This is where traditional HUMINT again becomes important. A knowledgeable person sitting across a table from another human being can detect hesitation, contradiction, personality, relationships and intent, in ways that digital collection cannot. Local contacts may understand informal power structures that never appear in corporate databases. A conversation may identify information that nobody has ever put online. SIGINT can tell an organisation an enormous amount about communications. HUMINT can explain what those communications actually mean. The future of effective intelligence therefore may involve rediscovering methods that existed before the digital revolution, rather than assuming that increasingly powerful software can replace them.

Automation and the loss of human ability

Aviation illustrates the wider danger. Automation has made aircraft dramatically safer, but excessive reliance on automated systems can reduce pilots' familiarity with manual flying. When automation behaves unexpectedly, the person supposedly supervising the system may suddenly have to perform a task they rarely practice. The same problem now appears throughout society. People who continuously use GPS gradually lose their sense of direction. Organisations dependent on cloud systems lose familiarity with paper procedures. Employees trusting computer-generated information can become less inclined to question whether it is correct. Artificial intelligence will magnify this problem considerably if human judgement is gradually replaced by automatic acceptance of machine-generated conclusions.

Conclusion

The emerging return to older technology should not be misunderstood as resistance to progress. It represents recognition that technological sophistication without redundancy creates fragility. Organisations will almost certainly continue adopting artificial intelligence, advanced communications, satellite navigation and digital intelligence systems. But the most resilient will also preserve paper maps, physical documents, isolated computers, basic communications and human intelligence networks.

The important question will increasingly be not how advanced an organisation's technology is when everything works, but how effectively that organisation continues functioning when systems are hacked, communications disappear or electronic information can no longer be trusted. The irony therefore may be that the genuinely technologically sophisticated organisation of the future is the one that knows when not to use technology.