DEFENCE HOLDINGS

DEFENCE HOLDINGS PLC

Information Warfare: Sovereignty in the Cognitive Domain

This white paper charts the evolution of information warfare, analyses its forms and tactics, presents case studies from recent operations, and examines the UK's current posture. It sets out a statement of intent from Defence Holdings: sovereignty in information warfare must be substance, not slogan, and the UK must act now.

defenceplc.com

White Paper | Published 15 September 2025

72 Charlotte Street, London, England, W1T 4QQ.
Company number 12187837.

Executive Summary

— To secure resilience, the UK requires sovereign capabilities.

> In the wars of the twentieth century, sovereignty was a visible commodity. It was displayed in the steel of warships, the roar of fighter jets, and the underground silos of nuclear missiles. A sovereign nation was one that could design, manufacture, and command its own tools of war.

Today, sovereignty is contested in terrain that cannot be photographed from a satellite. It is measured in code, in algorithms, and in the invisible currents of information that shape what societies believe to be true. In this new domain, information is infrastructure, and it is under attack.

Information warfare has become the defining feature of modern conflict. It goes far beyond propaganda. It is an orchestrated effort to destabilise societies, fracture alliances, and erode trust in institutions by manipulating the very fabric of perception. It is waged through disinformation, deepfakes, cyber operations, censorship, and narrative control.

The UK has recognised this shift. **The National Security Act 2023** updated espionage and foreign interference laws for the digital era. **The Strategic Defence Review 2025 (SDR25)** placed cyber and information warfare at the heart of force design. New structures, such as the **Cyber & Electromagnetic Command**, are being created to consolidate capabilities across cyber, signals, and information operations.

But recognition alone is not enough. To secure resilience, the UK requires sovereign capabilities in this space. Sovereignty cannot be measured in jobs or data-centre postcodes. It must mean ownership of intellectual property, control over development direction, and freedom from foreign restriction.

This white paper sets out the scale of the challenge. It charts the evolution of information warfare, analyses its forms and tactics, presents case studies from recent operations, and examines the UK's current posture. It concludes with a statement of intent from Defence Holdings: sovereignty in information warfare must be substance, not slogan, and the UK must act now.

Information Warefare

— The New Battleground

For centuries, war has been defined by its material. Rome projected its power through legions and roads. Britain's empire was sustained by its navy. The Cold War was measured in tanks, missiles, and megatons.

These were assets that could be counted, photographed, and paraded. They gave citizens a visible assurance of national strength.

But in the information age, much of this assurance has evaporated. The most consequential operations often leave no trace on the ground. They unfold in social feeds, encrypted chats, or manipulated news stories. The aim is not to destroy a bridge or occupy a city, but to erode a society's ability to function by corroding its information environment.

This is not an abstract concept. Russia's invasion of Ukraine was preceded by years of disinformation campaigns that cast doubt on Kyiv's legitimacy. China's strategy in the South China Sea relies not only on building islands but on shaping narratives of historic entitlement. Western democracies have felt the tremors through election interference, conspiracy movements, and viral falsehoods that polarise debate.

In this new battlespace, information is both weapon and target. The infrastructure once built to connect people, fibre-optic cables, cloud platforms, mobile networks, now doubles as the terrain of warfare. Control it, and an adversary can destabilise a nation without firing a shot.

Sovereignty, therefore, must be redefined.

It is no longer enough to own the shipyards. A sovereign nation must also own the code, the algorithms, and the systems that safeguard its information environment

Information Warefare

— The Arsenal of Information Warfare

Information warfare is not a single tactic.
It is a spectrum of operations, each reinforcing the other, designed to exploit vulnerabilities in perception, trust, and truth.

- **Psychological Operations** remain one of the most enduring tools. They target populations with messages designed to fracture morale or sow confusion. In Ukraine, Russia's repeated circulation of messages predicting collapse, encirclement, or betrayal sought to instil fear before battles had even begun.

- **Disinformation and Misinformation** represent the industrialisation of falsehood. Disinformation is intentional deception; misinformation is its unknowing transmission. The viral dynamics of modern platforms ensure both travel faster than truth. Troll farms and bot networks amplify divisive stories, while generative AI now allows deepfakes to erode confidence in political leaders with fabricated audio or video.

- **Cyber Operations** add another dimension. Breaches and leaks are not only intelligence-gathering exercises; they are timed for narrative effect. The SolarWinds hack compromised thousands of systems, but its strategic impact lay in the erosion of trust in digital infrastructure. Similarly, GRU hacks of political organisations were released at moments calculated to influence democratic outcomes.

- **Narrative Warfare** plays a longer game. It is less about shock and more about shaping the lens through which reality is interpreted. By repeatedly framing invasions as "liberations" or adversaries as "terrorists," states create storylines that legitimise their actions and delegitimise their opponents.

- **Media Manipulation** ensures these narratives circulate. State broadcasters provide overt platforms; covertly funded websites mimic independence; influencers and astroturf movements carry messages into subcultures. The result is a saturation effect, where hostile narratives are always available, no matter where citizens turn.

- **Censorship and Denial** provide the other half of the equation. Authoritarian regimes ensure their own populations remain within curated information bubbles by blocking foreign platforms, restricting access, or shutting down the internet entirely during moments of unrest.

- Finally, **memetic warfare** has become the most agile weapon of all. Memes and short-form content can encapsulate complex narratives in a single image or joke. Their irony and self-awareness make them harder to regulate, while their virality ensures rapid spread. ISIS pioneered this for recruitment; Russia has weaponised it for ridicule and destabilisation.

Case Study

Operation Doppelgänger

In the summer of 2023, readers across Europe clicked on what they believed were the websites of leading newspapers.

The logos were familiar: Le Monde, Der Spiegel, The Guardian. The layouts were indistinguishable from the originals. Yet the stories they carried were fabrications.

These articles claimed Ukrainian refugees were draining European economies. They argued sanctions were destroying Western livelihoods while leaving Russia untouched. They alleged Kyiv's soldiers were neo-Nazis. All were designed to weaken public support for Ukraine and fracture European solidarity.

This was Operation Doppelgänger, a Russian disinformation campaign of remarkable scale. Hundreds of spoof websites were created, each mimicking established outlets down to the smallest typographical detail. Thousands of fake articles were generated. The campaign spread across France, Germany, Italy, the UK, and the US.

When French authorities publicly denounced the operation in 2023, many assumed it would cease. Yet by 2025, the campaign was still active, adapting, shifting domains, and re-emerging under new guises. Meta removed accounts; OpenAI disrupted bot networks. Still, the sites returned.

The objective was not total persuasion. It was pollution. By flooding the information environment with credible-looking falsehoods, Russia sought to ensure that citizens hesitated before believing any source. Doubt was the weapon. If every story could be fake, then no story could be trusted.

> Operation Doppelgänger demonstrates the strategic potency of information warfare. It shows how adversaries exploit the openness of democratic media environments. And it underlines why the UK requires sovereign tools to detect, disrupt, and defend against such campaigns.

— State Strategies

The potency of information warfare lies not only in the tactics themselves but in the way states institutionalise them. Adversaries have elevated information operations to the level of military doctrine.

Russia has pioneered what is often called hybrid warfare. In Georgia in 2008, in Crimea in 2014, and in Ukraine in 2022, Moscow combined conventional forces with cyberattacks and information operations. It blurred the line between peace and war, state and proxy. The GRU, Russia's military intelligence agency, orchestrated hacks of political servers and timed their release to coincide with key elections. Its Internet Research Agency — the infamous St. Petersburg "troll farm" — created thousands of fake personas to infiltrate Western debates. In each case, the aim was not simply to deceive, but to divide, to exhaust, to destabilise.

China approaches information warfare with a different lexicon but similar ambition. Its "Three Warfares" doctrine — psychological, legal, and public opinion warfare — was formally adopted by the People's Liberation Army in 2003. It is visible in Beijing's extensive censorship apparatus at home, in its use of TikTok to curate content abroad, and in its global media investments designed to shape perceptions of Chinese power. In the South China Sea, China has combined land reclamation with narrative reclamation, insisting on "historic rights" through constant repetition until they become part of the discourse.

Western democracies have not stood idle. The US and UK have both developed counter-disinformation units and digital influence operations. NATO has created a Strategic Communications Centre of Excellence in Riga to coordinate narrative defence. Yet the West is constrained by liberal values — by commitments to freedom of speech, independent media, and privacy. While this distinction is a source of strength, it also creates vulnerabilities. Adversaries exploit the openness of democratic societies, knowing that responses will be slower, more cautious, and more contested.

The lesson is clear. Information warfare is not a passing tactic. It is doctrine, embedded in the strategic outlook of hostile states. If the UK is to respond effectively, it too must institutionalise sovereignty in this domain.

Information Warefare

— Platform Exploitation and Policy Gaps

The digital platforms that dominate the modern information environment were not designed for war. They were built to maximise engagement, virality, and growth.

Their moderation systems are reactive, their algorithms optimised for attention rather than accuracy. Hostile states have learned to exploit these weaknesses with precision.

Coordinated inauthentic behaviour is perhaps the most common tactic. Networks of bots and sockpuppet accounts create the illusion of consensus or outrage. They flood comment sections, hijack hashtags, and brigade trending topics. To the casual user, it appears as spontaneous public sentiment. In reality, it is orchestration.

Grey-zone satire takes advantage of the ambiguity between humour and harm. Memes and "ironic" jokes spread conspiracy theories under the cover of jest. A claim that vaccines contain microchips, framed as a meme, can reach millions while evading moderation. Platforms struggle to distinguish between parody and propaganda.

Incitement disguised as analysis pushes the boundary further. Posts framed as neutral commentary can in fact encourage unrest or violence. During protests in Iran and Belarus, messages highlighting "injustice" often carried cryptic instructions designed to spark confrontation.

Geo-spoofing and language fragmentation exploit the fact that moderation systems are uneven across languages. Russian and Chinese operatives often use obscure dialects, coded emojis, or deliberate misspellings to evade detection. In Africa, Chinese state media pushes anti-Western narratives in Swahili, knowing that moderation resources are minimal.

Leaks, doxing, and hacks weaponise stolen data. The publication of soldiers' personal details, or the timed release of hacked emails, can shift narratives instantly. In 2016, GRU hacks of the US Democratic Party were released at carefully chosen moments to maximise political damage.

Manipulated media and deepfakes represent the newest frontier. Videos of Ukrainian President Zelenskyy urging surrender, or AI-generated robocalls impersonating US President Biden, show how synthetic media can erode trust in leaders. Once such tools proliferate, even authentic material is doubted — a phenomenon known as the "liar's dividend."

Amplification of fringe content closes the loop. Radical influencers are boosted into the mainstream under the guise of "exposure." In reality, the amplification gives their narratives reach they would never achieve alone. Russian and Chinese actors have promoted both pro- and anti-vaccine rhetoric simultaneously, not to persuade but to polarise.

Each of these tactics thrives on the structural incentives of digital platforms. Engagement algorithms reward outrage. Moderation systems lag. Business models prioritise reach. This environment gives adversaries constant loopholes to exploit.

Closing them requires sovereign capabilities — not only to detect manipulation but to defend national narratives in real time.

Case Study

Telegram Sabotage Networks

In early 2024, a British court convicted three men of arson at a warehouse storing aid for Ukraine. On the surface, it appeared a criminal act with limited political significance.

Yet the details revealed a far darker pattern.

The men had been recruited via Telegram channels linked to Russian networks. Promised small payments and ideological validation, they were instructed to carry out attacks designed to disrupt logistics and create psychological impact. Similar incidents occurred across Germany, Poland, and Lithuania: fires at supply depots, symbolic acts of intimidation such as placing coffins near landmarks, even parcel bombs disguised as cosmetics or consumer goods.

Western intelligence agencies identified these as part of a broader GRU-aligned strategy: decentralised sabotage conducted by disposable assets. By recruiting from vulnerable or criminal backgrounds, handlers created a network of operatives who were both expendable and deniable.

The strategy was effective. Each incident was minor in isolation but cumulative in effect. It sowed fear, tied up security resources, and generated headlines that undermined public confidence. Because the recruits had no direct link to Moscow, attribution was difficult.

For the UK, this case underlined the fusion of information and physical domains. Telegram was not simply a communications platform; it was an operational pipeline. Sabotage was not random crime; it was state-linked information warfare with physical consequences.

The implication is stark. Defending against information warfare cannot be confined to digital spaces. It requires integrated monitoring of online networks, physical infrastructure, and law enforcement intelligence. Only sovereign capabilities, embedded across agencies, can provide the resilience to disrupt such hybrid campaigns before they manifest.

— The UK Policy Context

The UK has not been blind to these threats. Over the past five years, it has undertaken significant reforms to update its legal, strategic, and institutional frameworks.

The National Security Act 2023 replaced the ageing Official Secrets Acts and created new offences for espionage, sabotage, and foreign interference. It gave law enforcement greater powers to arrest, detain, and prosecute individuals acting on behalf of hostile states. For the first time, foreign information operations could be explicitly targeted under UK law.

The Strategic Defence Review 2025 marked a decisive shift. It placed cyber, electromagnetic, and information operations alongside land, sea, and air as core domains of warfare. It called for modernisation of ISR (intelligence, surveillance, reconnaissance), autonomy, and digital command systems — with an emphasis on software-led solutions. Importantly, it emphasised sovereignty, stating that critical capabilities must be UK-controlled.

Institutional reform has followed. **The National Cyber Force (NCF)** now provides offensive cyber capability, blending GCHQ expertise with MOD command. The forthcoming Cyber & Electromagnetic Command will consolidate cyber, signals intelligence, and information warfare into a single coherent structure. This reflects an understanding that hybrid threats cannot be addressed in silos.

The government has also invested in counter-disinformation capacity. The National Security and Online Information Team (NSOIT), formerly the Counter-Disinformation Unit, monitors hostile narratives and works with platforms to downrank or remove harmful content. Departments are trained with the RESIST 2 Toolkit — a structured process to anticipate, identify, and counter disinformation.

Legislation has kept pace. **The Cyber Resilience Bill**, announced in 2024, mandates incident reporting across critical infrastructure and extends regulatory oversight. It empowers auditors and regulators to hold organisations accountable for vulnerabilities exploited by hostile actors.

Finally, the MOD has embraced the concept of grey-zone warfare. Parliamentary reports now explicitly recognise that hostile states operate below the threshold of open war through influence, cyber, and sabotage. This conceptual clarity is vital: it legitimises proactive defence rather than reactive crisis management.

These moves are significant. But they are fragmented. What remains lacking is a sovereign industrial base capable of delivering the software platforms that operationalise these policies. Without UK-owned tools, the frameworks risk being dependent on foreign providers whose priorities may diverge.

Information Warefare

— The UK Sovereign Defence Ecosystem

Britain does not start from scratch.
It possesses world-class research institutions, innovative SMEs, and established defence primes.

The challenge is integration and scale.

The Defence Science and Technology Laboratory (Dstl) leads government research in cyber and influence operations. The National Cyber Security Centre (NCSC) provides authoritative guidance across public and private sectors. The UK National Authority for Counter-Eavesdropping (UK NACE) protects against technical espionage.

Among SMEs, firms such as Oxford Dynamics have delivered sovereign AI tools to support SDR25 itself. Mind Foundry, spun out of Oxford University, develops explainable AI for radar, sonar, and cyber-signal processing. Roke Manor Research provides mission analytics and operational cyber capabilities.

Larger players include Nexor, trusted for secure information exchange at the highest assurance levels; QinetiQ, with deep expertise in sensors and robotics; Darktrace, a pioneer of AI-driven anomaly detection; and Raytheon UK, which develops national security cyber solutions.

The open-source intelligence (OSINT) ecosystem is equally vital. The Cabinet Office and techUK have launched INDEX, a platform to standardise OSINT across government. Startups such as OSINT Industries and tools like ShadowDragon and Fivecast ONYX support law enforcement and counter-terrorism with AI-enabled analytics.

The ecosystem exists. **The gap is sovereign integration.** Defence Holdings' role is to consolidate, scale, and deliver sovereign platforms that translate innovation into operational capability.

Conclusion

— A Call to Action

Information warfare is not hypothetical. It is active, organised, and escalating. Operation Doppelgänger continues to pollute European media environments. Telegram sabotage networks have already reached Britain's shores. Deepfakes, memes, and leaks erode trust daily.

The UK has recognised the threat through SDR25, new legislation, and institutional reform. But recognition must be matched by sovereign capability.

> **Without it, Britain risks outsourcing the defence of its cognitive domain to actors whose control lies elsewhere.**

The choice is stark. Either sovereignty is reduced to jobs and postcodes, or it is reclaimed through ownership, direction, and freedom of action.

Defence Holdings exists to ensure the latter. Our commitment is to build sovereign software platforms that secure the UK's information infrastructure. Our first AI product, dedicated to information warfare, marks the beginning of that journey.

Sovereignty must be substance, not slogan. And when the UK speaks of defending itself in the cognitive domain, it must mean what it says.

defenceplc.com