

Warfare by any other name?

February 2026

For years, European officials have spoken about “hybrid warfare” as though it were a future threat. It is not. It is already embedded in the political and economic landscape of the continent, and has been raging for years.



Hybrid warfare does not begin with tanks crossing borders. It begins with ambiguity. It operates in the space between peace and war, exploiting legal systems, open media environments, financial markets and digital infrastructure. Its purpose is not necessarily to defeat an adversary outright, but to weaken cohesion, distort perception and erode confidence over time.

Russia has been refining this method over the past 20 years. Cyber intrusions, disinformation campaigns, political influence efforts, weaponisation of social media, energy leverage and other clandestine activities, have all been documented across Europe and North America. The objective is rarely to fabricate instability from nothing. Rather, it is to identify existing social or political fractures and widen them. A narrative that blends fact with distortion is often more effective than an outright falsehood. When public trust is already fragile, small manipulations can have disproportionate effects.

Moscow increasingly frames the conflict with Ukraine as a broader confrontation with the West, and its actions reflect a willingness to pressure NATO and EU member states below the threshold of conventional war. Hybrid activity allows the Kremlin to challenge Western cohesion without triggering collective military response.

Cyber operations targeting infrastructure, efforts to interfere in electoral processes and co-ordinated online amplification of polarising content have all formed part of this approach. These activities do not replace conventional military operations, they complement them.

While Russian forces continue their war in Ukraine, political and informational pressure is applied elsewhere to complicate Western unity.

Yet, it would be analytically careless to reduce Europe's strategic challenge to Russia alone, or to cast it in ideological terms reminiscent of the twentieth century. Modern Russia is not a communist state. It is an authoritarian system with strong nationalist and security-service characteristics. Its competition with the West is geopolitical, not ideological in the Cold War mould.

China presents a different kind of challenge. Beijing's engagement in Europe is rarely disruptive in the Russian sense. It is incremental, economic and institutional. Chinese financial institutions have expanded their presence in European centres such as Luxembourg, as part of broader efforts to internationalise the renminbi and deepen financial linkages. For China, relationships are pursued methodically.

If Russia's approach can appear blunt, China's is patient. One seeks leverage through disruption and political friction, the other often seeks influence through integration and long-term economic positioning. Neither approach fits neatly into old ideological binaries. Both operate within the realities of global interdependence.



The real vulnerability for Europe lies not in dramatic acts of sabotage alone, but in complacency. Open societies derive strength from transparency, pluralism and economic openness. These same qualities can be exploited if resilience is weak. Disinformation is effective only where trust is already eroded. Economic leverage matters most where dependencies are poorly managed.

Conclusion

The challenge, therefore, is less about alarmist declarations of “war” and more about disciplined resilience. Clear public communication, diversified energy and trade relationships, cyber defence investment and institutional cohesion reduce the effectiveness of hybrid tactics, but fragmentation magnifies them.

It is tempting to view today’s strategic environment through the language of creeping ideologies or existential confrontation. Such framing may mobilise attention, but it obscures more than it clarifies. The competition unfolding across Europe is subtle, persistent and adaptive. It does not require dramatic rhetoric to be serious.

Warfare by any other name is still conflict. But understanding its character accurately is the first defence against it. Exaggeration weakens credibility. Precision strengthens it.

KCS Group International – Strategic Intelligence & Corporate Security

KCS Group International is a leading provider of security and intelligence services, operating in some of the world’s most difficult environments on complex cases of fraud, theft, corruption or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients identify and deal with any risks, weaknesses and threats which could impact on their business, financially or reputationally.

Our key areas of expertise include: Corporate Intelligence Services – New market or sector entry research – Know your customer screening.

In addition, we offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits – providing unparalleled analysis, contingency planning and implementation.

To find out more or to arrange a meeting to discuss your business needs, please email the team at info@kcsgroup.com or call (00 44) 20 7245 1191 – www.kcsgroup.com