Neutrality Under Fire: Evolving Geostrategic Realities for Neutral EU Member States and the European System of Financial Supervision (ESFS) as of October 2025

Dr Michael Huertas*

Armed conflict; Austria; Banking supervision; Contingency planning; Cyprus; EU law; Financial institutions; Financial regulation; Ireland; Malta; Neutrality; Sanctions

Abstract

This article critically examines the implications of neutrality for EU Member States and the European System of Financial Supervision (ESFS) in the context of armed conflict, as of October 2025, with a particular focus on Austria, Ireland, Malta and Cyprus. It explores how neutrality, while shaping defence and foreign policy, does not exempt these states from obligations under EU financial law, sanctions, or crisis management frameworks. The analysis addresses the operational and legal challenges faced by neutral states in a rapidly evolving geostrategic environment, including intensified hybrid threats (cyberattacks, disinformation, economic coercion), the implications of recent NATO enlargement (e.g., Sweden and Finland) and advanced EU defence integration initiatives. It highlights the need for robust supervisory coordination, resilient financial infrastructure capable of withstanding quantum-enabled cyberattacks and credible, adaptive enforcement of sanctions against increasingly sophisticated evasion techniques. Drawing on historical lessons and contemporary EU legal gateways, the article proposes practical measures to ensure continuity of core financial services, harmonised crisis response and the safeguarding of Single Market integrity, considering the potential operationalisation of the digital euro. Ultimately, it argues that neutrality in defence posture can be reconciled with uncompromising financial stability and market stewardship, if preparedness, proportionality and transparent coordination are prioritised.

Focusing on neutrality

This article critically assesses the implications of neutrality for EU Member States and the European System of Financial Supervision (ESFS) in the context of potential armed conflict. As previously explored in this Journal in "The Evolution of the ESFS if Faced with Conflict"[1] the EU generally as well as the ESFS specifically is likely to undergo significant centralisation with irreversible changes should the European Union face actual armed conflict, including in a NATO (North Atlantic Treaty Organisation) context. While such a scenario remains a theoretical exercise, it underscores the imperative for robust preparedness, particularly within financial services and highlights the specific considerations applicable to militarily non-aligned EU Member States.

That previous article focused on supervisory override of business-as-usual (SOBAU) measures, the EU legal bases for emergency action (including arts 122, 347 and 352 TFEU (Treaty on the Functioning of the European Union)), the need to expand and adapt the Digital Operational Resilience Act (DORA) plus the architecture and enforcement mechanics of sanctions to wartime realities along with questions around Notgeld and a wartime role for the (still proposed) Digital Euro. Building on that foundation without repetition, this article focuses on what this might mean for the financial sectors of neutral or militarily non-aligned EU Member States, considering the operational status of the digital euro by October 2025 and whether and how they could keep core services functioning if the EU and/or NATO were at war with Russia, or in an armed conflict directly affecting European markets. The emphasis is on practical operating mechanics, supervisory and infrastructural levers, lessons from recent crises (e.g., COVID-19, Ukraine war) and historically grounded lessons from World War II that remain salient but in need of adaptation in a digitally-integrated Single Market facing intensified hybrid threats and advanced sanctions evasion techniques.

This article, like the previous article relies on EU Treaty level gateways, directly applicable regulations and recent directives, supervisory soft law and crisis practice and it distinguishes settled law from forward-looking proposals. It operates on a central premise that bears underlining at the outset: Neutrality may not be a shield against kinetic attack, coercion, or occupation in modern warfare, nor against sophisticated hybrid operations. In a future Russia–NATO and/or EU conflict, neutral EU Member States may not be spared and neutrality may be violated de facto or de jure. Financial centres could face

* Dr Michael Huertas, LLM, MBA, is a Partner and the Global Financial Services Legal Leader for PwC Legal. He is a Solicitor-Advocate (England & Wales), Solicitor (Ireland) and a German Rechtsanwalt. His professional practice focuses on emerging regulatory issues in the Banking Union and Capital Markets Union. The usual disclaimer applies. The views expressed here are purely personal and need not reflect those of PwC nor PwC Legal. The author would welcome dialogue on any of the issues raised herein or in relation to his research interests. Michael can be reached via: *https://www.linkedin.com/in/michael-huertas-157a788*.

[1] See (2025) 40 Journal of International Banking Law & Regulation 10.

kinetic and hybrid operations (including quantum-enabled cyberattacks and disinformation campaigns), legal compulsion under EU emergency acts and abrupt supervisory direction aimed at preserving stability and supporting the broader war economy. While neutrality limits military participation, foreign basing and alliance obligations, it does not confer exemptions from EU law or relieve financial firms of their duties under prudential, conduct, or market-stability frameworks. In practice, neutral/non-aligned EU Member States (currently Austria, Cyprus, Ireland and Malta) who are also not members of NATO will nevertheless continue to be expected to implement measures that support the EU's efforts during wartime at pace, visibly and credibly, notwithstanding constraints in alliance integration and intelligence flows.

Scope, core premises and operational logic

The points of legal principle underpinning the EU's emergency gateways and the centralisation tendencies of the ESFS under severe stress—together with SOBAU as an operative doctrine—form the baseline. As explored previously, these mechanisms, notably arts 122, 347 and 352 TFEU, provide the legal authority for the EU to take exceptional measures during crises. Their scope, however, is not open-ended: Article 122 is confined to exceptional occurrences and severe supply difficulties and cannot serve as a general wartime-economy clause; Article 347 operates as a Member State derogation subject to notification/consultation and proportionality review rather than a Union-level enabling power; and art.352 (flexibility) requires unanimity and Parliament's consent and cannot be used to circumvent explicit Treaty allocations or proportionality/subsidiarity constraints.[2] The present discussion pivots to execution: the practical steps regulators, financial market infrastructures and firms must take to keep core functions running and the peacetime preparations that render those steps lawful, proportionate and operable on short notice.

Three premises guide the analysis. First, neutrality may fail to protect market actors against direct targeting, occupation or sophisticated hybrid threats (including quantum-enabled cyberattacks) and will not relieve them of obligations under EU sanctions and financial law, which demand continuous adaptation against evasion. Second, in a unionised legal order, crisis management will skew toward centralised, uniform measures to minimise fragmentation and arbitrage and neutral states will be expected to implement at speed and with transparency. Third, modern operational dependencies—digital infrastructure, cloud, cross-border data and real-time settlement—multiply the attack surface and demand pre-authorised fallback modes (including resilient offline digital value transfer) tested end-to-end well before contingency. These premises apply across neutral jurisdictions notwithstanding their differing constitutional and policy foundations.

Layered onto this is the ESFS's crisis fitness under geopolitical stress. The European Supervisory Authorities' (ESAs) (comprised of the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA)) rulemaking, convergence and emergency powers,[3] together with breach of Union law investigations and peer reviews, provide a spine for uniform implementation. The European Systemic Risk Board's (ESRB) macroprudential warnings and recommendations can be oriented to Central Counterparty (CCP) exposures, FX funding and fund liquidity risks. Emerging EU level Anti-Money Laundering (AML) supervision, reflecting the finalised AML package by October 2025, will narrow arbitrage in sanctions-adjacent controls. In particular, the new EU Anti-Money Laundering Authority (AMLA) is expected to coordinate Financial Intelligence Units (FIUs), harmonise supervisory expectations and, where warranted, directly supervise selected high-risk cross-border institutions under a hub and spoke model—materially raising baseline expectations in funds, payments and correspondent banking, with a focus on advanced analytics and AI-driven monitoring to counter sanctions evasion. The ESAs' emergency powers—engageable only upon a Council declaration of an emergency—also provide for decisions addressed to national competent authorities (NCAs) and in last resort to institutions, where necessary to safeguard stability and market integrity. The convergence imperative is not cosmetic. It will be the difference between supervised continuity and disorderly fragmentation for all EU Member States regardless of their neutrality.

Constitutional neutrality and NATO posture—country analyses and EU/NATO implications

Neutrality in EU Member States is a constitutional or policy stance on military alignment. It is not a derogation from EU law. It shapes defence and foreign policy, basing and overflight rights and participation in collective defence structures, but does not displace obligations under the acquis, including directly applicable sanctions,

[2] Article 122 TFEU permits Council measures in the face of severe difficulties in the supply of certain products or in exceptional occurrences, but it does not confer a general "war economy" competence; any market-intervention measure must be justified under the principles of necessity and proportionality and remain within the provision's material scope. Article 347 TFEU operates as a Member State derogation—allowing national measures in time of war or serious internal disturbances, subject to notification to and consultation with the Commission—and is not a Union-level enabling clause; emphasis should be placed on the notification and coordination mechanics and on proportionality review to minimise fragmentation. Article 352 TFEU (the flexibility clause) requires unanimity in the Council and the consent of the European Parliament and cannot be used to circumvent explicit Treaty allocations of competence or the principles of subsidiarity and proportionality; it should not be portrayed as a general fallback for systemic redesign of the financial sector. Finally, arts 42(7) TEU (mutual assistance) and 222 TFEU (solidarity) do not themselves expand financial-services supervisory competences; they may trigger coordination but must be operationalised through existing sectoral legislation.

[3] ESAs' art.18 emergency powers engage only upon a Council emergency declaration; otherwise, coordinated Q&As, Opinions, Guidelines and breach-of-Union-law procedures are the practical tools for convergence.

prudential requirements and financial stability measures. arts 42(7) in the Treaty on European Union (TEU) and 222 TFEU preserve the "specific character" of neutral states' defence policies—ensuring mutual assistance does not compel combat deployments—but this safeguard has no bearing on the application of EU financial law. The above also co-exists with a number of EU and international commitments to ensure security. Notably in respect of EU measures The EU's Permanent Structured Cooperation (PESCO) framework, established under art.42(6) and Protocol 10 of the Treaty on European Union (TEU) (introduced by the Treaty of Lisbon in 2009 and initiated in 2017), is a key component of the EU's Common Security and Defence Policy (CSDP). PESCO enables 26 of the 27 national armed forces to pursue structural integration through collaborative projects launched in 2018, with Malta as the sole EU Member State not participating. Together with the Coordinated Annual Review on Defence (CARD), the European Defence Fund and the Military Planning and Conduct Capability (MPCC), PESCO forms a comprehensive defence package for the EU. Participation in PESCO is similar to enhanced cooperation in other policy areas, as integration does not require all EU Member States to participate. This should also be assessed in the context of linkages to NATO outside of formal membership.

Austria

Austria maintains permanent neutrality anchored in its 1955 constitutional law linked to the State Treaty. Austria is not a NATO member but participates in NATO's Partnership for Peace (PfP) and in EU CSDP missions and it is fully within the euro area and Banking Union. Practically, Austria's neutrality constrains foreign basing and formal alliance commitments, but it does not inhibit implementation of EU sanctions, ESFS measures or European Central Bank (ECB)/Single Supervisory Mechanism (SSM) directions. For NATO, Austria's PfP status enables interoperability and limited host-nation support short of alliance obligations. For the EU, Austria's euro area integration makes Vienna structurally central to monetary, supervisory and resolution actions and its neutrality does not qualify those financial obligations. Operationally, EU and Austrian institutions should assume full supervisory oversight in wartime, with pre-cleared contingency protocols for liquidity, settlement and cyber-resilience, mindful that intelligence asymmetries may require reinforced bilateral and EU channels for threat sharing.

Ireland

Ireland pursues a longstanding policy of military neutrality and is not a NATO member. It participates in PfP and in CSDP operations and has domestic "triple lock" constraints on overseas deployments, noting the ongoing political debate about reform. Ireland's position within the Single Market and its preeminent role as a hub for funds means that neutrality has no bearing on sanctions, anti-money laundering and countering the financing of terrorism (AML/CFT) or market-stability execution. For NATO, Ireland is a close partner for intelligence, cyber and maritime domain awareness but not an ally and for the EU.

Ireland hosts major banking, fund management, insurance/reinsurance, payments and aircraft leasing activities, as well as the Euronext Dublin debt listing venue. Post-Brexit, Dublin is a primary English-speaking EU platform for U.S. and UK-headquartered firms serving EU clients. Consequently, its dominant role in aviation finance, capital markets, funds, data centres and market infrastructure impose a duty to align swiftly with ESMA/EBA/EIOPA emergency measures, with the Central Bank of Ireland having a likely coordination role (notably on funds and liquidity management tools (LMTs) and the EU's DORA incident reporting) notwithstanding its neutrality. In a conflict, the legal tension is not with EU law but with operational exposure: Irish digital and financial nodes would be high-value targets despite neutrality, particularly from hybrid and quantum-enabled cyberattacks. Firms should pre-arrange independent crisis communications, robust cyber redundancies and offline-capable fallbacks and prepare for near-real-time supervisory reporting on liquidity, collateral and sanctions exposure, ensuring enhanced cooperation with non-EU jurisdictions in sanctions enforcement.

Malta

Malta's 1987 Constitution declares neutrality and non-alignment, restricting foreign military presence absent international mandate. Malta is not a NATO member, but it participates in PfP and in limited CSDP activity. As an EU and euro area Member State, Malta is bound by sanctions and ESFS measures and neutrality does not create carve-outs for enforcement in shipping services, payments or corporate services. For NATO, Malta's geography and maritime services sector are operationally relevant for logistics and sanctions enforcement and for the EU, Malta's small but open financial centre must avoid becoming a sanctions-evasion vector, especially given increasingly sophisticated evasion techniques. Neutrality will not shield it from hybrid pressure against maritime and financial nodes. Credibility depends on transparent, risk-based supervision of maritime registries, including explicit references to classification, P&I cover and ship-to-ship transfers, insurers and corporate-service providers, with clear licensing criteria, enforcement metrics, stress on FIU liaison cadence and beneficial ownership transparency mechanics and rapid liaison with EU authorities and global partners (US, UK, G7) for enhanced sanctions coordination.

Cyprus

Cyprus is not a NATO member and is not in PfP, reflecting the island's unresolved security situation and the presence of non-EU forces, alongside UK sovereign base areas. Cyprus participates actively in EU CSDP and PESCO and is in the euro area. Its non-alignment vis-à-vis NATO complicates formal alliance coordination and intelligence flows, particularly given deconfliction sensitivities with a NATO ally in the region. For the EU, Cyprus's shipping cluster and financial services footprint make it pivotal for sanctions delivery in the Eastern Mediterranean. Neutrality offers no derogation from EU financial law and may in practice increase exposure to coercion targeting shipping registries, classification and insurance, especially from hybrid threats and sophisticated sanctions evasion attempts. Institutions must heighten monitoring, information-sharing protocols and cyber-resilience, coordinated through EU channels (EBA/ESMA/EIOPA/AMLA/Commission) and global partners for typologies and inspections, given the sensitivity of Eastern Mediterranean corridors and the growing role of strategic actors like China.

Overall EU and NATO implications are clear. First, neutrality within the EU is compatible with full participation in Union legal measures and it does not excuse non-compliance with sanctions, prudential or market-stability acts. EU harmonisation of criminal offences and penalties for sanctions violations supports credible enforcement, dovetailing with confiscation and asset-recovery instruments to deter evasion, including against novel techniques such as digital assets and alternative payment systems. Second, the absence of NATO membership in these Member States limits alliance planning for host-nation support, basing, overflight and classified intelligence sharing, which can slow NATO's military logistics and hybrid-threat response, necessitating robust EU Hybrid Fusion Cell integration.[4] Third, for the EU's economic warfare toolkit, these jurisdictions are critical enforcement and resilience nodes—funds domicile and data (Ireland), shipping and corporate services (Cyprus, Malta) and Banking Union transmission (Austria). Their neutrality places a premium on legal clarity, visible enforcement and infrastructure hardening to avoid becoming weak links, especially against quantum-enabled cyberattacks. Finally, in extremis, neutrality may not be respected, and contingency plans must assume kinetic or hybrid targeting and prepare for EU-directed emergency measures that supersede ordinary peacetime discretion, requiring strengthened coordination with partners like the US, UK and G7 along with careful consideration of China's growing role.

For financial markets, the salient question is how each state's neutrality and NATO relationship condition its legal latitude, operational dependencies and contribution to EU-level crisis governance.

EU-level actions to reflect neutrality within a wartime economy

The Commission's 2023 Economic Security Strategy, together with the revised Foreign Direct Investment Screening Regulation (the revisions also referred to as the Critical Technologies Screening Regulation), introduced a parallel layer of scrutiny over cross-border capital flows, mergers and portfolio investments in dual-use and strategic sectors. This impacts the financial sector across all EU Member States. These frameworks extend beyond prudential supervision to encompass national-security and foreign-policy alignment. Moreover, for neutral Member States, participation in the EU's High-Level Group on Economic Security and outbound-investment screening mechanisms constitutes a de facto qualification of neutrality: cooperation in these measures is mandatory under Union law, notwithstanding differing defence postures. Future crisis coordination must therefore reconcile ESFS powers with the economic-security competences now embedded in the Single Market acquis.

If the EU were to pivot to a wartime economic footing, several EU-wide actions would be required to both respect neutral Members' defence posture and secure the Single Market functions in which those states are systemically important. The following measures are legally and operationally achievable within existing Treaties and crisis gateways and should be pre-drafted for activation:

- Clarified mutual-assistance guidance: The European Council and EEAS should issue guidance reconciling art.42(7) TEU's neutrality safeguard with economic-warfare execution. This guidance should confirm that neutral states' obligations concentrate on sanctions delivery, civil protection, cyber-defence cooperation and financial-stability measures, explicitly excluding combat tasks.
- Single Market continuity package: The Commission, ESMA, EBA, EIOPA and the ESRB should adopt a coordinated package that: (i) harmonises emergency trading protocols and disclosure relief under Markets in Financial Instruments Regulation (MiFIR), Market Abuse Regulation (MAR) and Short Selling Regulation (SSR) and (ii) pre-authorises use of liquidity management tools in funds, drawing on ESMA's work on LMTs and recent Alternative Investment Fund Managers Directive (AIFMD)/Undertakings for Collective Investment in Transferable Securities (UCITS) reforms endorsing LMTs and facilitating national toolkits and supervisory coordination for

[4] See, "The Diplomatic Service of the European Union", *A Europe that Protects: Countering Hybrid Threats*, *https://www.eeas.europa.eu/node/46393_en* and "Realising the EU Hybrid Toolbox: opportunities and pitfalls" (December 2022), *https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf*

gates/suspensions, subject to SOBAU as provided for in sectoral legislation (e.g., art.47 MiFIR, art.28 SSR, art.46 European Market Infrastructure Regulation (EMIR), art.16 Central Securities Depositories Regulation (CSDR), art.69 UCITS, art.21 AIFMD) and in accordance with the crisis-management gateways in the Treaties and relevant secondary law; and (iii) sets anti-procyclicality floors for Central Counterparties (CCPs) margin under EMIR, with specific calibrations for jurisdictions hosting key infrastructures (Ireland, noting the ongoing political debate about its "triple lock" constitutional constraints) or Banking Union transmission channels (Austria).

- ESFS crisis compacts with neutral states: The ESAs and ECB/SSM should agree memoranda that formalise rapid direction, data-sharing and joint supervision during SOBAU, while tailoring implementation pathways for neutral jurisdictions with constrained access to NATO intelligence. This includes EU-run threat-intelligence pipelines to compensate for alliance asymmetries and DORA-integrated incident-sharing with national Computer Security Incident Response Teams (CSIRTs).
- Trans-European Automated Real-time Gross settlement Express Transfer system (TARGET) services and Real-Time Gross Settlement (RTGS) resilience: The Eurosystem should pre-arrange TARGET/RTGS operating extensions, cross-border intraday credit lines and collateral-mobility opinions to keep payment rails open if nodes in neutral states are targeted. Where necessary, ECB guidance should enable temporary settlement-cycle adjustments and collateral eligibility expansions.
- Digital euro offline capability as contingency: Recognising the forward-looking nature of a digital euro, the ECB and Commission should, contingent on legal adoption by co-legislators and Eurosystem design choices, ensure an operable, time-bound offline functionality. This offline capability would be crucial for retail continuity if cash logistics or networks are degraded by hybrid threats or quantum-enabled cyberattacks. This effectively complements strengthened cash-cycle continuity and enables degraded-mode operations playbooks derived from Payment Services Directive 2 (PSD2), Network and Information Systems Security Directive 2 (NIS2) and DORA. National central banks in neutral states could be designated as priority distribution hubs for this contingency, highlighting its cross-border interoperability and resilience.
- Shipping, aviation and insurance backstops: Working with EIOPA and Member States, the Commission should pre-design pooled war-risk capacity or state guarantees for shipping and aviation critical to sanctions enforcement and supply continuity. Such mechanisms must consider Solvency II review outcomes, comply with EIOPA guidance on war exclusions and establish conditions for state-backed war-risk pools to avoid state aid pitfalls and ensure Solvency II compliance, with governance that leverages Malta's and Cyprus's maritime clusters but ring-fences compliance risk.
- War-risk pools and liquidity guarantees must satisfy state-aid constraints: with risk-based pricing, targeted eligibility, hard sunsets, clawbacks and transparency commitments to mitigate distortion.
- Capital-flow management coordination: To avoid fragmentation and ensure legal robustness, the Commission and ESRB should publish a template for temporary, necessary and proportionate capital-flow measures as reflecting the specifics to the neutral Member States. This template should specifically address the invocation of art.65(1)(b) TFEU exceptions (public policy/public security) and adhere to the Commission and CJEU (Court of Justice of the European Union) proportionality jurisprudence. Measures must be targeted, time-bound, reviewable and transparent to prevent arbitrage and legal challenge. The template should also detail robust notification mechanics to the Commission, including ex ante metrics, clear sunset clauses and structured reporting requirements, complementing existing provisions under arts 63–66 TFEU and art.347 TFEU, to enable neutral states to act quickly and effectively without creating arbitrage. Where capital flows to or from third countries, particularly those of geostrategic concern like China or non-EU G7 members, raise systemic concerns, the Council safeguard route under art.66 TFEU provides a high-threshold instrument distinct from art.65 exceptions, with strict necessity, notification and proportionality controls.

- Procurement and industrial prioritisation guidance: If defence-industrial prioritisation is triggered, the Commission should clarify how neutral states participate in non-lethal supply chains and critical infrastructure protection consistent with their constitutional constraints, while ensuring access to EU support instruments.

These actions recognise neutrality in defence posture while safeguarding the Single Market roles of Austria (Banking Union and monetary transmission), Ireland (funds, data and ICT (Information and Communications Technology) infrastructure), Malta (maritime, registries, corporate services) and Cyprus (shipping, insurance and Eastern Mediterranean corridors). They minimise divergence, preserve enforcement credibility and close coordination gaps created by non-NATO status.

Scenario analysis: neutrality translated into operational responses

Conflict with Russia could have differing degrees of impact on the EU and its response generally as well as what that means for individual Member States, notably the non-aligned neutral Member States. Accordingly, Austria, Ireland, Malta and Cyprus may have to assess on how they behave as conflict intensity escalates and what that means for financial-sector operations and EU coordination, especially in light of increased hybrid threats and sophisticated sanctions evasion. This could also entail neutral Member States receiving additional functions (and potentially personnel) as firms re-route risk, operations, or clients within the EU to comparably neutral safe havens from more exposed financial centres. The table below sets out hypothetical conflict scenarios and possible response scenarios. In summary thought, while neutrality constrains military participation and basing/access decisions, financial institutions, even headquartered or otherwise operating in neutral Member States remain fully bound by EU financial law, ESFS/ECB directions and sanctions—which may need to address the shift of the Single Market to a wartime footing.

Conflict Scenario	Austria	Ireland	Malta	Cyprus	Financial-sector policy-maker considerations
Limited border incident / low-level skirmish	• Constitutional permanent neutrality • No belligerency • Deny offensive use of territory • Provide humanitarian/civil support	• Policy neutrality with Triple Lock—Political rebellion on reform of Triple Lock? Continues[5] • No combat deployments absent UN mandate Provide limited logistical cooperation if approved	• Constitutional non-NATO and neutrality • No combat role and offensive use of ports/airspace • Provide humanitarian support	• Non-NATO, CSDP participant; sensitive to declination • No combat role • Provide humanitarian/diplomatic support	• Continue/step-up full EU sanctions implementation • Focus on continuity under constraint • Ensure early activation of enhanced reporting, cyber posture and liquidity monitoring • Initial assessment of operational routing for select functions/clients by firms into neutral safe havens
Limited NATO engagement (defensive ops)	• Neutrality controlling; possible tightly circumscribed overflight/logistics • No bases/combat	• Triple Lock constraints deployments • Political alignment strong	• Constitution allows non-alignment and no basing • Humanitarian transit possible	• Non-alignment complicates intel/logistics • Provide civilian support only	• Tighter venue controls and FX documentation • CCP anti-procyclicality • Follow ESAs guidance; Enhance cyber posture and sanctions enforcement with advanced analytics • Facilitate increased reliance on MiFID, payments and EMI platforms based in neutral Member States to serve EU clients • Immediate SOBAU and managed-market regime

[5] See, "What is Ireland's 'Triple Lock' and why is it in the news again?" *https://www.rte.ie/brainstorm/2025/0522/1514313-ireland-triple-lock-explainer-legislation-defence-forces-peacekeeping/*

					• Support settlement-cycle adjustments • Extend collateral and central bank facilities
Major NATO–Russia hostilities (general war footing)	• Maintain non-belligerency absent constitutional change • Provide expanded civil protection	• No combat deployments absent UN mandate/legal reform • Provide increased non-military support	• No combat; strict territorial neutrality • Provide civil protection	• No combat; heightened regional risks • Provide civilian support	• Support surge in sanctions inspections (shipping, funds and CASPs). CASPs (Crypto-Asset Service Providers) must implement the crypto 'travel rule' for originator and beneficiary information, with calibrated thresholds, enhanced due diligence for high-risk flows and demonstrable chain-analytics capabilities, leveraging AI-driven monitoring for evasion techniques. DORA-aligned ICT resilience obligations apply, alongside MiCAR authorisation, asset-reference token regimes and white-paper/market abuse frameworks, specifically addressing threats from quantum-enabled cyberattacks. Significant re-routing of operations, including back-office and cyber/tech functions, to neutral safe haven Member States, alongside shifts in fund governance to ManCos
Article 42(7) TEU invoked (Member State requests aid)	• Provide aid "by all means in their power" consistent with neutrality (non-military) • Provide strong economic/civil support	• Same as above non-military assistance; Support • Evacuation, cyber/medical/logistics	• Same as above provide humanitarian and diplomatic support	• Same as above provide rapid EU coordination in Eastern Mediterranean corridors	• Financial duties intensify: emergency disclosure • Targeted capital-flow measures and cross-border contingency bridges • EU crisis compacts operationalised • Enhanced sanctions enforcement leveraging advanced analytics and coordination with global partners (e.g., G7, US, UK). Heightened supervisory scrutiny of re-routed operations, particularly delegation and outsourcing chains

Given the above, in a climate of heightened geopolitical risk, particularly following the escalation of armed conflict or intensified hybrid threats, neutral Member States like Austria, Ireland, Malta and Cyprus are poised to become critical conduits for re-routed financial activities within the EU. Firms, particularly those operating in more exposed financial centres, are likely to re-evaluate their operational footprints and shift risk, core operations and client servicing functions to entities located in these comparably neutral safe havens. This strategic recalibration aims to bolster resilience and ensure continuity of services amidst potential disruption, leading to a significant evolution in the functional landscape of these jurisdictions.

This anticipated re-routing may likely manifest in several key areas:

- Booking-model adjustments for banks and brokers. Financial institutions may adjust their booking models to centralise certain activities in neutral Member States,

leveraging existing infrastructure and legal frameworks to serve EU clients from a less exposed periphery. This could involve greater reliance on MiFID platforms, as well as payments and Electronic Money Institution (EMI) platforms (regulated entities authorised to issue electronic money and provide payment services) to continue serving EU clients remotely.

- Fund governance and administration shifts. There will likely be a noticeable shift in fund governance and administration functions towards Management Companies (ManCos) (entities responsible for the management of investment funds) and other service providers located in these neutral Member States. This relocation will inevitably lead to increased supervisory scrutiny of delegation and outsourcing chains, requiring robust oversight frameworks to ensure compliance and investor protection.
- Relocation of back-office and cyber/tech resilience functions. Certain critical back-office operations and cyber/tech resilience functions may also be relocated to leverage existing clusters and expertise in neutral Member States. This strategic move aims to diversify operational risk and ensure that essential support functions remain secure and operational even in scenarios affecting more prominent financial hubs. Supervisors will need to ensure that such relocations do not create new points of systemic vulnerability but rather enhance overall resilience.

Locating offsite recovery in "neutral" EU Member States can enhance business continuity optics and regulatory predictability, but neutrality alone is not a resilience strategy. Under DORA, NIS2 and the CER Directive, supervisors expect demonstrable diversity across energy, telecoms, cloud aand providers segregated control planes; immutable, offline backups; and realistic live failovers. Because neutral states still fully implement EU sanctions and face the same cyber and infrastructure threats, firms should engineer for threat-vector diversity rather than lean on political labels.

A single centralised hub in a neutral jurisdiction is cheaper and easier to govern and test, yet it concentrates risk in one grid, cable system, cloud region, legal regime and management plane. If that hub is impaired—by energy curtailment, telecom disruption, emergency legal measures, or a cyber incident—continuity can collapse. Centralisation can be defensible for less time-critical workloads where latency and RTO[6]/RPO[7] tolerances are wider, provided firms maintain genuinely independent, offline backups and rehearse full loss-of-hub scenarios.

For critical services, a decentralised, multi-site design—spanning at least one neutral Member State alongside other EU locations—materially improves resilience and aligns with supervisory expectations. Active architectures, multi-cloud/colo[8] strategies, diverse subsea routes and IXPs[9], on-site energy contingencies and tested exit/portability rights reduce correlated failures and vendor concentration. In practice, Austria and Ireland can serve as strong (primary or co-primary) recovery nodes[10] within a distributed mesh, while Malta and Cyprus are better suited as niche secondary sites rather than single points of recovery.[11] The governing principle is to diversify infrastructure and providers, then prove it works through regular, regulator-observable failovers.

These scenarios map directly onto the supervisory and operational levers discussed in the remainder of this article and frame the EU-level actions outlined above, including the operational implications for firms re-routing business, risk and personnel to neutral Member States as safe havens.

Continuity under constraint: day-to-day market operations

In a European war environment, neutral Member States should, like their militarily active peers, nevertheless plan to preserve essential functions—payments, custody, settlement, retail and wholesale banking, market making

[6] RTO (Recovery Time Objective): The maximum acceptable time to restore a service or system after a disruption. Example: If the RTO for payments processing is 2 hours, the firm must be able to recover that service within 2 hours of an outage.

[7] RPO (Recovery Point Objective): The maximum acceptable data loss measured in time—the point in the past to which data must be recoverable. Example: An RPO of 15 minutes means backups or replication must ensure no more than 15 minutes of data is lost.

[8] A "colo strategy" refers to how a firm uses third-party colocation data centres—facilities that provide secure space, power, cooling and physical connectivity for the firm's own servers and network equipment—to meet performance, resilience and compliance goals. Instead of building and operating private data centres, firms place their hardware in neutral, carrier-dense sites, gaining access to multiple telecom carriers, Internet Exchange Points (IXPs), cloud on-ramps and interconnection ecosystems. A well-designed colo strategy defines which workloads run where, how capacity is split across primary and recovery sites, the diversity of power feeds and network routes and the contractual terms that enable rapid scale, portability and audited controls. In practice, a colo strategy often complements cloud ("hybrid" or "multi-cloud/colo") to reduce vendor concentration and improve latency, with active-active or active-standby designs across multiple facilities and regions. Under DORA and related EU regimes, it should evidence geographic and provider diversity, segregated control planes, immutable offline backups, tested failovers, clear exit/portability rights and resilience to correlated risks (grid, telecom and provider).

[9] IXP (Internet Exchange Point): A physical network facility where internet service providers, content networks and other operators interconnect to exchange traffic directly. Using multiple IXPs (in different locations/providers) reduces latency and dependency on any single network route.

[10] Ireland offers unparalleled cloud adjacency and carrier density in the EU, extensive colocation options with multiple cable landings, mature cyber talent pools and sophisticated financial-sector supervision. Residual risks relate to data-centre energy curtailment and subsea concentration, which can be mitigated by selecting facilities with diverse landing points and on-site energy contingencies and by pairing Ireland with a continental node. Austria provides robust power and telecom infrastructure, high legal predictability and proximity to CESEE networks, making it an excellent continental counterpart. Its main constraints are regional energy interdependencies and the need to engineer diverse cross-border fiber routes and multi-provider architectures to avoid correlated failures.

[11] Malta and Cyprus can play valuable roles as secondary or workload-specific recovery sites, but they are not optimal as sole or centralised hubs. Both jurisdictions bring advantages in regulatory clarity and sector expertise (notably payments and maritime), yet their island geographies imply reliance on limited subsea cable corridors and imported energy. While these risks can be reduced through carefully chosen carrier-diverse facilities, satellite/microwave fallbacks for command-and-control and staged (warm/cold) recovery profiles, they remain less suitable for active-active, low-latency critical services.

in critical instruments and hedging in core derivatives—while operating within an intrusive, real-time supervisory envelope. Payments systems and retail access would be treated as essential services. Domestic high-value payment rails, card networks and ATM cash cycles would be kept running with extended intraday liquidity, contingency provisioning and prioritisation of critical sectors (e.g., energy, food, healthcare, public utilities). Branch networks could operate on reduced hours with targeted geographic coverage and security support. If logistics or communications impair physical cash distribution, resilient offline functionality in a future Digital Euro, reflecting its operational realities including cross-border interoperability, would provide a lawful fallback for retail payments and where strictly necessary and proportionate, temporary derogations could support localised emergency scrip, subject to central bank oversight and rapid withdrawal once conditions normalise.

Trading venues would aim to remain open but might shorten hours or deploy harmonised, tighter volatility controls. Circuit breakers and volatility interruptions would be calibrated to preserve orderly pricing rather than suppress discovery. Sector-specific halts or temporary suspensions could be applied where sanctions changes or supervisory directions render trading disorderly or noncompliant. Foreign-exchange markets would continue to function, with priority for genuine hedging and real-economy trade. Supervisors may tighten documentation requirements for specific corridors, impose enhanced reporting and, in extremis, reintroduce authorised-dealer-style licensing in practice for high-risk flows, particularly those suspected of sanctions evasion via digital assets, alternative payment systems, or third-country intermediaries. Price interventions would be used sparingly, if at all and only within transparent, time-bound frameworks. Ultimately, emergency trading-day adjustments and disclosure relief should be harmonised with the MiFIR review architecture, ensuring time-bound, uniform measures to avoid venue arbitrage.

Custody, settlement and clearing would pivot to stability mode. Central counterparties (CCPs) would deploy anti-procyclicality tools, collateral schedules would be adapted to volatility and, where settlement fails mount, cycles could be temporarily lengthened to ease operational stress. Contingency accounts and interoperability bridges would be pre-cleared to reroute flows if specific custodians or infrastructures are compromised. At a firm level, the operating model would be recognisably "managed market": private actors continue to transact, but under immediate override powers, granular reporting and activity constraints designed to preserve liquidity where most needed and to prevent hostile exploitation of market structure.

Operating constraints: capital, FX, disclosure and liquidity support

Neutral states should anticipate time-bound constraints to counter disorderly dynamics and evasion risk, coordinated closely with EU institutions and global partners (e.g., G7, US, UK) to minimise fragmentation. Capital-flow measures, implemented under the exceptions of art.65(1)(b) TFEU (public policy/public security) where applicable, would be targeted, necessity-based, proportionate, time-limited, reviewable and transparent. Administered reporting thresholds, pre-approval for specific outbound flows and temporary frictions for categories of non-essential capital could dampen flight dynamics. To prevent arbitrage and legal challenge, any such measures must be supported by Commission/CJEU proportionality jurisprudence, including a model notification structure to the Commission detailing ex ante metrics, sunset clauses and reporting. Current-account transactions, trade finance and humanitarian flows would remain prioritised.

Foreign-exchange administration would tighten for high-risk corridors. Supervisors could require enhanced documentation for specific counterparty types or jurisdictions, insist on transparent intermediaries and beneficial ownership, deploy rapid licensing or no-objection processes for sensitive transactions and implement advanced analytics for detecting evasion techniques including digital assets and alternative payment systems. Hedging for real-economy exposures would be protected and leveraged speculative flow may be curtailed.

Issuer and market disclosure would pivot to emergency protocols. Issuers would be expected to maintain periodic reporting while providing ad hoc updates on sanctions effects, supply-chain disruption, cyber incidents, operational outages and material changes to liquidity or covenant compliance. Timetable relief could be granted in calibrated fashion, but selectivity and transparency are essential to avoid information vacuums.

Central bank liquidity and collateral mobilisation would expand. Bank crisis management will follow the re-calibrated CMDI framework, enabling earlier transfer strategies for failing smaller banks, accelerated DGS payouts and SRB-led resolution playbooks aligned with liquidity-in-resolution tools. Neutral/non-aligned status does not alter these obligations. Instead, this heightens the need to pre-clear data pipelines and bridge-bank operational readiness. In addition, intraday liquidity extensions, collateral eligibility adjustments and temporary valuation haircuts would be applied to stabilise payment rails and core repo markets. Where necessary, discretionary support could be conditioned on de-risking plans and governance remediation.

Cross-border payments, settlement and ICT (Information and Communications Technology) resilience

A war environment heightens the probability of hybrid attacks on financial market infrastructures (FMI) and their critical dependencies. Neutral Member States should therefore preauthorise and rehearse measures that can be executed at speed without legal ambiguity. First, standardised incident reporting and isolation playbooks, harmonised with national cyber authorities and compliant with PSD2, NIS2 and DORA requirements, must be operational at the FMI and participant level. Drills should include degraded-mode operations, extended power outages and communications failures, with telecom and energy providers integrated into exercises. Financial entities that are simultaneously in scope of DORA, NIS2 and the CER Directive should align incident taxonomy and reporting cadences, while supervisors coordinate joint inspections. Priority restoration orders for energy and telecom support to FMIs should be pre-authorised, with tested fallbacks for degraded modes. Second, settlement cycles, margining and collateral eligibility should be adaptable, with pre-agreed parameters that can be invoked on supervisory direction. This reduces the need for ad hoc exemptions under pressure and helps avoid hidden procyclicality. Third, contingency accounts and interoperability bridges should be mapped and tested to reroute flows across custodians or Central Securities Depositories (CSDs) if a node is compromised. Legal opinions should be maintained on emergency reuse and cross-border mobility of high-quality collateral to avoid disruption of payment and settlement chains. Fourth, central bank intraday liquidity windows should be extended for longer operating days and aligned across relevant RTGS systems. Where cross-border liquidity corridors are affected, coordinated action among euro area and non-euro area central banks will be needed to keep the rails open.

The EU's pivot towards sovereign cloud solutions—operationalised through the EU Cybersecurity Certification Scheme for Cloud Services (EUCS) and the Data Act—has direct wartime implications. Neutral Member States hosting hyperscale data-centre infrastructure (notably Ireland and Malta), particularly those receiving re-routed cyber/tech resilience functions, must ensure compliance with EUCS-certified, region-based data storage and portability guarantees. Crisis protocols should explicitly address cloud-switching rights, escrow of critical data and lawful access by EU authorities under DORA and the Data Act, while respecting constitutional neutrality vis-à-vis allied intelligence-sharing frameworks.

Neutrality complicates aspects of coordination. Institutions in non-NATO jurisdictions may not benefit from real-time alliance threat intelligence and must therefore rely on robust EU-level pipelines (e.g., EBA/ESMA/EIOPA/AMLA/Commission channels) and trusted bilateral channels for cyber indicators, sanctions typologies and operational warnings. Those pipelines should be formalised, audited and exercised to ensure timely flow despite the absence of alliance integration and to avoid implying NATO intelligence-sharing lines. This includes DORA-integrated incident-sharing with national CSIRTs.

Contracts and legal friction-proofing

Crisis execution falters if contracts cannot be performed or terminated lawfully when circumstances change abruptly. Neutral Member States' firms should ensure their key arrangements expressly accommodate wartime realities. Force majeure clauses should explicitly encompass war, armed conflict, emergency supervisory override (e.g., SOBAU directives), government orders, sanctions updates, cyber incidents and prolonged outages. They should provide for suspension and termination pathways, notification mechanics, mitigation obligations and cost allocation rules tied to objective events. Drafting should respect due-process and fundamental-rights constraints (rights of defence, property and freedom to conduct a business), ensuring triggers and remedies are objectively defined and proportionate in line with EU law. Material adverse change provisions should include triggers for emergency legislation, capital controls, sanctions designations, market closures or dramatic liquidity impairment, with structured renegotiation frameworks. Firms should consider including a specific trigger for SOBAU to preserve the ability to pivot quickly when supervisory directions arrive.

Sanctions clauses should explicitly require compliance with all applicable EU sanctions measures and defined trusted-partner regimes, with immediate freeze, reporting and exit mechanics. They should allocate risk for changes in sanctions regimes and provide clear representations and warranties on beneficial ownership and control. Business-continuity and outsourcing covenants should include step-in rights, dual-running and termination for national-security concerns, with increased supervisory scrutiny of delegation and outsourcing chains, especially for ManCos and other service providers in neutral safe haven Member States. These rights must be drafted to be operable in practice (including escrow of IP and data, access to premises and personnel and handover obligations). Harmonisation of these terms across group entities and key counterparties reduces fragmentation and litigation risk at the moment flexibility is most needed.

Moreover, contracts should anticipate the impact of the Data Act, ensuring provisions for data portability and cloud-switching duties are aligned with DORA's exit and step-in strategies. This integration is critical for maintaining operational continuity and should consider the practicalities of escrow arrangements for critical data and software.

Sector-specific considerations

Banks and investment firms should plan for dynamic recalibration of capital and liquidity settings. For banks, this flexibility sits within CRR/CRD and ECB/SSM powers. For investment firms, IFR/IFD applies with proportional crisis expectations. Countercyclical buffers may be released or reimposed and sectoral risk weights may rise in energy, transportation and defence supply chains and restrictions on distributions may be tightened. Supervisors may instruct de-risking from designated sectors or counterparties, restrict proprietary accumulation in certain derivatives absent demonstrable hedging purpose and intensify fit-and-proper scrutiny with national security lenses. Near-real-time reporting of liquidity ladders, collateral positions and exposures to sanctioned or high-risk sectors can be compelled under SOBAU. This also includes the need for booking-model adjustments for banks and brokers and a greater reliance on MiFID, payments and EMI platforms to serve EU clients from beyond the frontline, particularly from neutral Member States.

Capital markets authorities may adopt temporary short-selling prohibitions in sectors critical to wartime resilience, strengthen position limits in energy and agricultural derivatives and harmonise circuit breakers. Issuer disclosure guidance should be issued rapidly on war-related risks, impairments and forward-looking statements, with consistent application across venues to avoid arbitrage.

Funds and asset management will need to use liquidity management tools (LMTs) decisively. Building on ESMA's work on LMTs and the recent AIFMD/UCITS reforms, national toolkits and supervisory coordination for gates/suspensions, swing pricing, anti-dilution levies, redemption gates, notice periods and, in extremis, suspensions should be activated under clear governance and supervisory consultation. Valuation for hard-to-price assets must be reinforced by independent committees, fair value policies and robust external data. Transfer agent and distributor networks should be tightened for sanctions screening and evasion typologies. Additionally, fund governance and administration may increasingly shift to Management Companies (ManCos) and service providers within neutral Member States, leading to increased supervisory scrutiny of delegation and outsourcing chains. For Alternative Investment Funds (AIFs) with concentrated exposures to energy, commodities, transport and defence, concentration limits, leverage caps and enhanced reporting may be directed.

Insurers and reinsurers must clarify war-adjacent cover and test solvency resilience. War exclusions in property, political violence and cyber must be transparent and consistently applied, drawing on EIOPA guidance on war exclusions. Solvency II ratios, informed by review outcomes, should be stressed for severe asset shocks and correlated underwriting and investment hits. Authorities should prepare pooled capacity or state backstops for shipping, aviation and energy war risks, ensuring conditions avoid state aid pitfalls and ensure Solvency II compliance and verify claims-handling continuity under degraded conditions.

FMIs and critical ICT providers, including those serving CASPs, should expect DORA obligations to harden and reflect the latest requirements under crisis conditions. Exit and substitution plans must be executable, incident reporting must integrate with national cyber authorities and red-team testing should extend to offline and manual fallbacks, including scenarios involving quantum-enabled cyberattacks. Neutral Member States may also see a relocation of certain back-office and cyber/tech resilience functions, leveraging existing clusters to serve as comparably neutral safe havens. Supervisory direction to disconnect compromised providers or segments must be grounded in pre-cleared legal authority and operationally feasible.

Sanctions architecture: credible enforcement in neutral states

As explored in the previous article, EU sanctions regulations are directly applicable and binding across all Member States, including neutral ones. The challenge for neutral jurisdictions is credibility in enforcement, especially given the evolution of sophisticated evasion techniques, including the use of digital assets, alternative payment systems and third-country intermediaries. A single national sanctions authority should be designated with clear primacy in interpretation, licensing and coordination with the FIU and prosecutorial bodies, able to issue near-real-time guidance and compel information. Statutory powers should support freezes on reasonable suspicion and administrative and criminal sanctions for noncompliance. EU harmonisation of criminal offences and penalties for sanctions violations supports credible enforcement, dovetailing with confiscation and asset-recovery instruments that are adapted to new methodologies that facilitate stronger means to deter evasion.

Sector specific supervisory programmes must be risk-based and visible. Banks should undergo targeted reviews on correspondent networks and nested accounts and anticipate booking-model adjustments as firms re-route risk and operations to neutral safe havens. Funds and administrators should be assessed for investor eligibility and portfolio screening and Trust and Corporate Service Providers (TCSPs) and corporate services providers should face inspections on beneficial ownership verification. Maritime clusters should ideally be further and more intensively scrutinised for flagging, insurance, classification and ship-to-ship transfer risks, specifically addressing sophisticated obfuscation techniques. CASPs operating under MiCAR authorisation, asset-referencing token regimes and white-paper/market abuse frameworks should be monitored for obfuscation techniques, high-risk flows (including those enabled by digital assets or alternative payment systems) and compliance with DORA overlays for ICT resilience and the travel rule under the

latest AML package. The increased reliance on MiFID, payments and Electronic Money Institution (EMI) platforms to serve EU clients from neutral Member States will also require heightened supervisory attention. Transparency builds credibility. Publishing licensing criteria, summary statistics on approvals and rejections and aggregate enforcement metrics deters arbitrage and supports cross-border cooperation. Embedded liaison with AMLA and relevant Commission services—and structured engagement with trusted third-country partners (e.g., US and UK)-strengthens evidence-gathering and concurrent enforcement, leveraging advanced analytics and AI-driven monitoring.

Jurisdictional nuances matter both in terms of domestic law as well as domestic market specifics. Austria's significant role as a regional banking hub, with deep ties to Central and Eastern Europe, means that its sanctions authority must also address correspondent banking relationships, cross-border lending and the use of Vienna-based trusts and holding companies for asset structuring. Enhanced scrutiny of private banking, wealth management and real estate transactions is warranted, given their potential as channels for sanctions evasion. Specific SSM/SRB interfaces for Austrian LSIs/Significant Institutions and the SRB's crisis playbooks should be integrated into national contingency planning.

In Ireland, the funds ecosystem, administrators and depositaries require DORA-aligned screening and resilience protocols that integrate sanctions typologies into operational playbooks. Ireland's position as a global centre for fund administration and domiciliation, with a high concentration of UCITS and alternative investment funds, necessitates robust investor eligibility checks, ongoing portfolio screening and close monitoring of fund flows for exposure to sanctioned entities or jurisdictions. The Central Bank of Ireland should coordinate with the national sanctions authority, leveraging its likely coordination role for funds LMTs and DORA incident reporting, to ensure that fund managers, administrators and custodians implement real-time transaction monitoring and report suspicious activity promptly. Additionally, while the 'triple lock' is accurately described as a constraint, the ongoing political debate about its reform should be noted without asserting changes as settled. The presence of major international payment processors and fintech firms in Ireland calls for sector-specific guidance and regular audits to detect and deter sanctions circumvention through digital channels.

In Malta, maritime registries, classification, P&I cover, ship-to-ship transfers and corporate-service hubs warrant targeted inspections, with clear corrective timelines and public aggregate reporting. Malta's status as a leading flag state and its extensive network of ship management, insurance and corporate service providers create vulnerabilities to sanctions evasion, particularly in the context of ship-to-ship transfers, reflagging and the use of shell companies. Supervisory authorities should implement risk-based inspections of maritime operators, require enhanced due diligence on beneficial ownership verification, stress FIU liaison cadence and beneficial ownership transparency mechanics and publish aggregate enforcement statistics to deter non-compliance. The gaming and virtual asset sectors, which are significant in Malta, also require tailored sanctions screening protocols and close cooperation with the Financial Intelligence Analysis Unit (FIAU).

In Cyprus, shipping insurers and banks serving the Eastern Mediterranean should be subject to heightened monitoring and rapid information-sharing with EU bodies, reflecting the region's strategic sensitivity. Cyprus's large shipping registry, concentration of ship management companies and its role as a financial services centre for Eastern Mediterranean and Russian clients increase the risk of sanctions evasion through complex ownership structures and layered transactions. The national sanctions authority should prioritise inspections of shipping insurers, banks and fiduciary service providers, with a focus on high-risk clients and transactions involving sanctioned jurisdictions. Enhanced cooperation with EU channels (EBA, ESMA, EIOPA, AMLA and the Commission) is essential to ensure timely intelligence sharing and coordinated enforcement actions, carefully avoiding any implication of NATO intelligence-sharing lines. Public reporting of enforcement outcomes and corrective measures will further strengthen deterrence and support cross-border compliance.

Historical analogues: World War II lessons for a digital Single Market

A nuanced examination of World War II-era financial and regulatory responses across neutral and non-belligerent European states reveals significant jurisdictional differences and market segment adaptations-parallels that are instructive for today's EU Single Market. Switzerland, for example, leveraged its unique legal framework and central bank autonomy to maintain open banking and capital markets, but imposed comprehensive exchange controls, gold and foreign exchange (FX) licensing and rigorous oversight of correspondent banking. Swiss private banking, commodity trading and insurance sectors each faced tailored restrictions: private banks operated under strict client due diligence and reporting, while commodity traders were subject to export licensing and end-use verification. The insurance sector, vital for cross-border trade, was required to ring-fence reserves and report exposures to sanctioned or belligerent parties. These measures reflected Switzerland's dual imperative to preserve neutrality and prevent its financial system from becoming a conduit for circumvention.

Sweden's approach during World War II was similarly sector-specific but reflected its industrial structure and export orientation. Swedish banks and export credit agencies were directed to prioritise financing for essential industries-steel, timber and shipping-while rationing credit to non-essential sectors. The central bank imposed strict

FX administration and the government established sectoral quotas for trade finance, ensuring that critical supply chains remained functional. Insurance and shipping companies were required to report cargoes and routes, with state oversight to prevent indirect support to belligerents. Sweden's experience underscores the importance of aligning financial controls with the real economy's sectoral composition and trade dependencies. Sweden is now a member of NATO.

Portugal and Spain, as peripheral but strategically located states during World War II, operated under pervasive FX administration and export controls, but with distinct market segment impacts. Lisbon's emergence as a controlled safe-haven hub was facilitated by disciplined surveillance and licensing, allowing the city's financial sector-particularly private banks and gold dealers-to serve as intermediaries for neutral and belligerent clients alike, provided compliance with state-imposed controls. Spanish banks, meanwhile, were tightly integrated with state agencies and the insurance sector was mobilised to support export industries under government direction. Both countries' experiences highlight the role of legal and regulatory discipline in enabling financial centres to remain open without becoming vectors for sanctions evasion. Both Portugal and Spain are NATO members.

During World War II, Ireland remained neutral and executed its "Emergency" regime even though it was functionally pegged to sterling, sustained banking and payments through a combination of exchange control, rationing and emergency trade-finance legislation due to its links to the UK. Ireland's modern funds and payments ecosystem-comprising clearing banks, building societies and trade finance providers-was subject to sector-specific licensing and reporting, with the central bank empowered to direct liquidity to essential sectors. The insurance and shipping segments were similarly regulated, with state oversight of reinsurance and cargo underwriting to prevent indirect support for belligerent trade. Ireland's experience demonstrates how a small, open economy can maintain financial continuity under constraint by leveraging sectoral regulation and close coordination with external partners.

World War II experience across neutral and non-belligerent economies offers enduring lessons for continuity under constraint. Switzerland, during World War II, remained neutral and non-aligned (as it is now) and kept banks and markets open under comprehensive exchange controls, licensing of gold and FX trades and close central bank management of external balances. Cross-border correspondent networks functioned, yet within tight routing and censorship regimes. The lesson is not isolation, but rule-bound control: maintain liquidity for essential trade while tightly policing evasion.

The common thread of these case studies is supervised continuity. Financial sectors became extensions of state capacity for distributing sovereign debt, administering rationed FX and sustaining essential trade finance. Continuity was not laissez-faire and it was continuity under constraint, delivered through transparent, uniform rules, directed liquidity and centralised coordination. The modern EU corollary is the operation of euro-area payment rails and capital markets with enhanced sanctions screening, FX licensing for sensitive flows and legally pre-cleared supervisory directives. However, the Single Market's harmonised legal framework and supranational supervision (via ESMA, EBA and the ECB/SSM) offer a level of coordination and uniformity that was absent in the fragmented wartime environment. Today, jurisdictional nuances persist-such as differences in AML/CFT enforcement, sectoral risk appetites and the prominence of specific market segments (e.g., funds in Ireland, shipping in Cyprus, gaming and virtual assets in Malta)-but are mediated by EU-level directives and crisis management protocols. The challenge for neutral EU states is to transpose the lessons of supervised continuity and sectoral discipline, as well as those gleaned from recent crises such as the COVID-19 pandemic and the Ukraine war (e.g., speed of regulatory response, effectiveness of sanctions, resilience of cross-border financial flows), into a digital, unionised infrastructure. This ensures that market segments most exposed to sanctions risk are subject to tailored controls, while leveraging the Single Market's capacity for coordinated enforcement and intelligence sharing.

Governance for crisis execution

Execution falters where governance is unclear. Neutral states should constitute a wartime financial stability council on a statutory footing linking the central bank, national competent authority, finance ministry, FIU, market infrastructures, cyber and energy regulators, defence and foreign ministries and the debt management office. The council should be empowered to issue joint directions and guidance, convene industry as needed and operate as the single front door for crisis communications. As explored in the previous article, SOBAU requires legal anchoring and procedural credibility. Templates for urgent supervisory decisions, compressed hearing and review procedures and expedited judicial oversight should be drafted and tested. Where national emergency derogations are invoked, notification to the Commission with clear necessity and proportionality statements is essential to avoid later legal challenges. Templates for expedited judicial oversight, proportionality statements and confidentiality handling for sensitive material should be readied to withstand rights-of-defence scrutiny.

At the EU level, neutral states should be prepared for enhanced direction from ESMA, EBA, EIOPA, the ESRB and, for euro area members, the ECB/SSM and the Single Resolution Board. Formal pipelines to EU crisis bodies and trusted third-country authorities (notably for sanctions and cyber) should be established and joint tabletop exercises conducted to rehearse cross-border dependencies. Neutrality's practical asymmetry—reduced access to NATO intelligence and logistics—should be offset by reinforced EU channels and tested arrangements with trusted partners.

Risk themes and countermeasures

Several cross-cutting risks warrant explicit countermeasures that are relevant to all Member States alike—whether neutral or not. Flight-to-quality and fragmentation pressures require transparent deployment of countercyclical tools and liquidity backstops, coordinated at EU level to avoid arbitrage. Derivatives margin spirals—especially in energy futures and financial CDS—should be addressed through pre-agreed procyclicality dampeners, margin floors and member liquidity arrangements at CCPs. The cyber-physical nexus demands integrated drills that link digital incident response with physical site and energy contingency planning. Legal uncertainty must be minimised by avoiding idiosyncratic national measures absent necessity, harmonising contract clauses and ensuring supervisory guidance is uniform and promptly disseminated. Opaque exemptions and discretionary licensing fuel black markets and corrode compliance and publishing objective licensing criteria, summary logs of approved and denied applications and aggregate sanctions metrics helps sustain credibility and deter evasion. In parallel, EU work to shield financial market infrastructures from extraterritorial interference and to reduce structurally significant exposures to third-country CCPs should be accelerated to harden the Single Market's autonomy under stress.

Conclusions

Neutrality in defence posture neither dilutes obligations under EU financial law nor obviates the duty to act decisively in support of financial stability and sanctions integrity. In a wartime environment, supervisory centralisation will accelerate and the operational burden on small, open financial economies will intensify. Neutral Member States might likely receive additional functions and personnel as firms re-route risk, operations, or clients within the EU to entities located in these comparably neutral safe havens from more exposed financial centres. For Austria, Ireland, Malta and Cyprus, the task is to align national legal gateways and supervisory capabilities with that reality while sustaining market confidence and the continuity of core functions. The legal keys are preparedness and proportionality: pre-drafted emergency instruments that are legally anchored, procedurally credible SOBAU with sanctions enforcement woven into prudential and conduct supervision. The operational keys are resilience and redundancy: secure payments, settlement and data with offline-capable value transfer along with reliable liquidity and collateral lifelines. This includes ensuring a future 'offline digital euro' is developed as a forward-looking contingency, clarifying its legislative status and the division between ECB scheme design and co-legislators' framework and pairing its function with strengthened cash-cycle continuity and PSD2/NIS2/DORA playbooks for degraded-mode operations. The strategic key is trust: transparent communication, demonstrable enforcement and close coordination with EU institutions and trusted third-country partners.

Experience suggests that emergency centralisation, once enacted, rarely fully unwinds. The likely legacy of a conflict of this magnitude would be a more integrated supervisory environment, a stronger role for EU-level bodies in crisis-time financial governance and a financial sector more explicitly entwined with security policy. Neutral Member States should aim to shape that settlement not as exceptions, but as exemplars of disciplined legality, operational excellence and market stewardship under extreme strain.

From the EU's side, credibility, whether in deterrence or neutrality, will hinge on implementing the targeted wartime-economy measures outlined above—(i) clarified art.42(7) TEU practice, (ii) ESFS crisis compacts, (iii) harmonised Single Market continuity tools, (iv) strengthened sanctions operations and Eurosystem liquidity and settlement backstops—tailored to the neutral states' systemic roles. Respect for neutrality in defence posture can be fully reconciled with uncompromising Single Market integrity if these measures are prepared and deployed with speed, transparency and proportionality. That reconciliation depends on remaining within clear legal bases, applying necessity and proportionality rigorously and ensuring due-process safeguards in crisis-time supervision and sanctions enforcement.