# **This House would authorise a small democracy to conduct limited covert influence and cyber operations for defensive purposes.**

## **0-1 minute motion framing and definitions**

Chair and colleagues good morning. If an adversary shapes our public discourse and our networks while we wait for certainty it is not moral to stand idle. I rise to propose the motion that this House would authorise a small democracy to conduct limited covert influence and cyber operations for defensive purposes.

First I define the terms in plain operational and legal language. Limited means narrow in scope time bound and proportionate. These acts are capped at low intensity and have no kinetic effects. They sit within defence law and require clearance through the Attorney General. Covert means not publicly attributed during execution yet fully lawful and auditable with disclosure to the Oireachtas after the fact when it is safe to do so. Influence means truthful efforts to expose or blunt foreign disinformation abroad. It excludes deception and it excludes any messaging at our own public. Defensive means responses below the threshold of armed conflict that deny harm and restore the status quo. These are triggered by threats that meet an agreed attribution standard. My thesis is direct. Ireland needs these bounded tools to defend neutrality and democracy in the grey zone.

## **1-3 minutes threat and concept frame**

The grey zone is the space below war where actors blur peace crisis and conflict. Sari and Regan describe it as a wider band where peaceful and warlike features can coexist and they separate the place from the means. The grey zone marks location on the spectrum of competition while hybrid threats describe the integrated means used in that space. That lens helps law strategy and operations work to one map while avoiding exaggerated claims of novelty. Hoffman warns that future contests blend conventional irregular and criminal modes and are likely to unfold in and around cities. For Ireland this translates to risks for our open economy our infrastructure and our information environment. Picture one simple vignette. Foreign actors spread false claims about public health through botnets and coordinated pages. Trust erodes hour by hour. That is the blend of informational and cyber pressure that the literature identifies. Our national Strategy Statement for the years from two thousand and twenty five to two thousand and twenty eight puts resilience and whole of government crisis response at the centre. The White Paper on Defence and its update uphold neutrality international engagement and periodic capability review. These anchors let us handle the blurred boundary that Sari and Regan set out.

## **3-5 minutes positive case part one necessity**

Adversaries seek to change the status quo below red lines. Azad and colleagues describe a repertoire that includes proxy pressure faits accomplis and salami tactics. Cases from Crimea to the South China Sea and from Iran to South Asia show how ambiguity is used to avoid open war while shifting reality on the ground. Starling and colleagues stress the first mover edge. Early denial and rapid attribution beat slow reaction in grey zone contests. Ireland needs that posture to signal with partners through European mechanisms and to steady our own public. Necessity also fits our doctrine and practice. The Strategy Statement emphasises risk management and the connection between civil and military instruments. The White Paper supports coordination through national security structures when handling hybrid threats. Authorisation for limited covert action allows counter disinformation with allies and narrow cyber disruption against hostile foreign botnets while the triple lock for kinetic force remains intact.

## **5-7 minutes positive case part two feasibility and safeguards**

This is feasible inside Irish frameworks if we build strong guardrails. The Strategy Statement commits to capability building and inter agency action. We can leverage existing cyber investigative and intelligence assets and we can connect them to legal and diplomatic tools. Safeguards ensure ethics and legality. We set a statutory basis under defence law with oversight by a board that includes the national security community. The legal gate runs through the Attorney General. Warrants are time bound. Every act passes tests of necessity and proportionality. Domestic targeting and deception are banned. Post action audits are routine. The Oireachtas is informed after the fact when disclosure does not risk sources or ongoing operations. Feasibility aligns with the hallmarks in the White Paper. Neutrality is respected. Governance cycles are observed. International ties are used to amplify evidence rather than to outsource judgment. The ethical core is truth bound action. The practical burden is modest and shaped by effect per euro. Alliance politics are served through the European Union rather than through offensive military commitments. Hoffman and colleagues argue that coalitions and lawfare blunt multi vector coercion. That is the space where a small state can add weight. Ireland can plug into European attribution and joint messaging without losing control of our own decisions.

## **7-8 minutes address principled objections**

Some critics call hybrid a fashion and warn that policy hype drives scholarship. Others argue that hybrid war is not a distinct form and that success in Crimea was situational while Donbas proved costlier and less clear. The lesson is not to discard the tools. The lesson is to scope them tightly and to measure what they achieve. Our motion does exactly that. It is not hype chasing. It protects sovereignty and trust through clear effects that can be counted. For example we can track time to detection and time to attribution and time to takedown. We can track partner amplification and public trust trends and the rate at which adversaries attempt to repeat a tactic. After action disclosure and coordination with partners reduce the risk of propaganda creep.

## **8-9 minutes adversary lens and deterrence logic**

The risks of misattribution and escalation are real and we address them openly. We mitigate them through allied evidence coalitions red team vetting legal thresholds and pre planned responses. This aligns with our tradition of ethical neutrality. We act to deny harm not to punish. We keep actions reversible. We work below armed conflict thresholds and we maintain diplomatic space. An adversary lens strengthens the case. Senior Russian writings argue that non military means can exceed military force in effect at the political level and that states should integrate these means to shape outcomes before open fighting. The right response is not to copy the methods in a reckless manner. The right response is to contest the grey space with discipline. Defensive options that are calibrated and reversible raise the cost of hostile acts without breaching neutrality or the triple lock. They also fit European frameworks for joint attribution and lawful counter measures. Authorisation signals resolve and buys time for diplomacy and law to work.

## **9-10 minutes close**

I close with three concrete steps for Ireland. First enact a narrow statute that authorises limited covert defensive influence and cyber operations. State the purpose the scope the red lines and the oversight. Ban domestic targeting and ban kinetic effects. Hold to necessity proportionality and reversibility. Require judicial warranting and regular review by an Oireachtas committee. Second build national triggers and playbooks. Define the indicators for below threshold action and tie them to pre authorised steps for attribution takedown and counter narrative. Pre clear legal and communication templates with partners. Exercise them and report the metrics each quarter. Third form a European attribution coalition for shared releases that protect sources and raise credibility. This scales the effect of a small state spreads risk and strengthens law.

Ireland is a small island with open systems and a strong reputation. We are an attractive target for low cost meddling. Public trust is a centre of gravity. It falls quickly and it is slow to rebuild. The correct response is not loud. It is quiet work done early and done under law. It is a truthful nudge placed where it blunts a hostile push. It is a narrow disruption of a harmful node abroad. It is a joint release that drains the sting from a lie. It is a review that keeps us honest. The grey zone is not theory. It is where we live. If we refuse bounded tools in that space we will react late and pay more for less effect. For these reasons this House should vote yes.

## **3-Line Summary for the Chair**

Proposing as Irish Defence Forces officer, I advocate authorising limited covert defensive operations against grey zone threats.

Speech defines terms, demonstrates necessity and feasibility, counters objections, provides recommendations.

Urges Yes vote for pragmatic sovereignty protection.

# **This House would not authorise a small democracy to conduct limited covert influence and cyber operations for defensive purposes**

## **0-1 minute motion framing and burden**

Chair and colleagues, I oppose the motion. Limited covert influence and cyber operations are not necessary, not safe, and not wise for a small democracy like Ireland. The burden on the proposition is heavy. They must prove necessity, legality, effectiveness, proportionality, and alliance fit. If any one of these pillars fails, the motion falls. We cannot gamble our national integrity on shadow tactics that risk eroding the very foundations of our society. As a state committed to transparency and the rule of law, we must ask whether these tools align with our values or merely invite avoidable risks. Our strength has always been openness rather than opacity, credibility rather than cleverness. In the grey zone we defend best by steady law and clear truth, not by stepping into the shadows.

## **One to three minutes definitions and the test**

Let us be precise. Limited means narrow in scope and time-bound in application. Covert means hidden at the time of execution, with attribution withheld. Influence means shaping perceptions and choices among foreign audiences. Defensive means action below the threshold of armed conflict, aimed at denying harm and restoring the status quo. On paper this sounds tidy. In practice these words creep. Who decides what narrow means when pressure rises. How do we prevent mission drift from defensive measures to offensive habits. Our test should be simple and strict. If open and transparent tools can deliver the same or better effects at lower risk, covert tools are not justified. That test reflects our history as a peacekeeper and a neutral democracy. It keeps the focus on outcomes, law, and trust rather than on the allure of secrecy.

## **3-4 minutes concept cautions and measurement gaps**

Concepts matter because they guide powers. The grey zone is described as a band between peace and war. That is a map, not a compass. Sari and Regan offer useful language but not the metrics to police boundaries or to trigger powers. Hybrid has often behaved like a fashion term. Libiseller warns that usage tracks policy cycles more than scientific progress. Tuck cautions that outcomes in Crimea and Donbas turned on local context rather than a magic doctrine. Hoffman adds that blended threats are real but resists over-generalisation. The lesson is clear. Do not build secret authorities on unsettled ideas. Without shared measures and thresholds, elastic concepts become excuses for overreach. A small state should move only on firm ground with clear rules that can be tested and reviewed.

## **4-5 minutes risk one trust and democratic legitimacy**

Public trust is our centre of gravity. It takes years to build and can be lost in a week. Covert state speech and covert cyber operations cut at that root. One exposure, one leak, can damage credibility far longer than any short tactical gain. Citizens will ask what else is being done, to whom, and on whose authority. Partners will question our word. In a digital age leaks are normal not rare. Small states win by law, reputation, and open truth. Shadow speech invites suspicion at home and friction abroad. Our democratic legitimacy depends on accountability that can be seen and tested. Better to build trust through transparency than to risk it on covert gambits that we may not be able to defend in public.

## **5-6 minutes risk two legality and governance**

Irish and European law demand necessity, proportionality, and the protection of rights. Those standards are not obstacles; they are our shield. Secrecy blunts scrutiny and bends red lines under crisis pace. Misattribution is a real danger in noisy information space. Strike the wrong node and we risk unlawful interference abroad and rights breaches at home, from data protection to free expression. Paper safeguards cannot repair trust once secrecy fails. An audit after the fact does not erase the harm. The Defence Acts and European frameworks require clear justification. Covert operations invite legal challenge and public doubt. The Attorney General may gate a file and judges may sign warrants, but oversight cannot fully test facts it cannot see in time. Good governance works best in daylight.

## **6-7 minutes risk three escalation, reciprocity, and offence drift**

Covert acts invite covert reply. A larger power can squeeze a small state quietly through pressure on diaspora, media, finance, or energy. Even more dangerous is drift inside our own system. Measures sold as defensive can slide toward offence in practice. The quickest way to deny harm is often to strike first. First-action bias grows once the tool exists. Operators will argue that pre-emption is the safest defence. Defensive tooling becomes an offensive capability in all but name. That is at odds with our liberal norms and with military neutrality. It would pull Ireland toward a posture we neither need nor can sustain. Azad and colleagues show how ambiguity fuels escalation spirals. The safest way to avoid offence drift is not to start it.

## **7-8 minutes effectiveness challenge transparency beats secrecy**

Proponents claim a first-mover edge. Speed without proof backfires. Move fast in the dark and you hand the adversary a narrative gift. Early public disclosure, anchored by allied evidence, can blunt hostile acts without the trust cost of covert action. Starling and colleagues stress early denial and rapid attribution. We can do that in the open, with proof standards that guide first-hour statements and day-one updates. Estonia’s experience points the same way. Resilience through openness and swift attribution beats hidden operations in sustaining public trust. If transparency and law can deter and deny, covert fails the necessity test. The right counter to propaganda is credible fact delivered quickly by trusted voices, not a mirror image of the tactic we oppose.

## **8-9 minutes alliance and neutrality fit**

Our strength is multilateral and lawful. The Strategy Statement for the years ahead sets resilience and whole-of-government action. The White Paper and its update uphold neutrality and international engagement. These point to open coordination, lawfare, and attribution coalitions, not to covert influence or covert cyber strikes. An offensive cyber arm would sit against our liberal norms and against neutrality. It would complicate cooperation with partners who value our clean reputation. European initiatives, including cooperative defence projects, focus on collective resilience and lawful countermeasures. Our comparative advantage is predictability and honesty. Partners trust us when our tools match our values. Covert authority would erode that trust and pull us into contests we cannot shape or sustain.

## **9-10 minutes the alternative plan and close**

There is a better way that serves security and values together. Adopt a transparency-first doctrine for grey-zone events. Set clear proof standards, first-hour lines, and day-one evidence updates. Stand up a national attribution cell that fuses technical, legal, and diplomatic work so that speed and credibility align. Use European coalitions for joint public releases and for lawful economic counters that impose costs without secrecy. Fund resilience rather than covert arms. Invest in detection, forensics, crisis communication, cyber defence, public education, and information readiness, while keeping a credible conventional and civil support core. Measure what matters: detection latency, attribution confidence, false positives, public trust trends, and partner amplification. Enact a statutory bar on offensive cyber and on covert state influence operations, so that offence drift does not take root. Anchor every response in open law, strong oversight, and partner coordination.

Covert tools promise speed, yet they put trust, law, and stability at risk. A small democracy wins with sunlight, law, and alliances, not with shadow speech. If open means can deliver the effect with less risk, covert means fail the necessity test. Our people deserve safety and honesty. Our partners expect reliability and legality. Our laws require both. Prudence points in the same direction. Vote no on the motion.

## 3-Line Summary for the Chair

Ireland should not authorise limited covert influence or cyber operations: they are unnecessary, unsafe, and unwise for a small democracy.  
They erode public trust, strain legality and neutrality, and risk escalation or drift into offensive practice.  
Choose transparency first: open attribution with EU partners, lawful counters, and investment in resilience and public communication.