**Syndicate Room Discussion SRD Briefing**

**The Grey Zone: Competition Below Armed Conflict**

Defence and Strategic Studies Module | SRD 07  
Prepared by: [Rank Name], Syndicate 1 | Date: [Insert Date]

## Executive summary

This brief uses eight readings to show how the grey zone affects Irish defence. The primary text sets the terms. Sari and Regan treat the grey zone as a wide band between war and peace and treat hybrid threats as the tools used inside that band (Sari and Regan, 2024, pp.10 to 12).

Hoffman turns this into posture advice. Small forces should prepare for mixed and urban fights where opponents combine regular and irregular and criminal and information methods (Hoffman, 2009, pp.5 to 7).

Azad and colleagues say the grey zone is a separate sub threshold space that aims to change the status quo through pressure and ambiguity (Azad et al., 2022, pp.5 to 6, 16 to 21).

Gerasimov signals a rival view. He says non military means can at times work better than force at the political level (Gerasimov, 2016, p.24).

Other authors warn against hype. Libiseller and Tuck say the term hybrid often renames old methods and can lead planning astray (Libiseller, 2023; Tuck, 2017).

Practitioner work stresses fast denial and clear attribution and partner messaging as key in the grey zone (Starling et al., 2022; Hoffmann and colleagues, 2024).

Bottom line for Ireland. Avoid buying into labels. Set clear triggers. Build inter agency playbooks. Use planned transparency to deter.

## 1 Conceptual foundation — Sari and Regan 2024

Sari and Regan give each term a job. The grey zone marks where on the competition spectrum events sit. Hybrid threats name the means used in that space. They replace a hard line with a broad band where peaceful and warlike features can co exist below armed conflict (Sari and Regan, 2024, pp.10 to 11).

This helps law and strategy and operations work to one map. It supports graded actions across diplomacy and information and law and economics and the military without assuming a single trigger.

Method. Conceptual synthesis that draws on NATO use and on the Mattis and Hoffman line of thought and on recent scholarship (Sari and Regan, 2024, pp.10 to 12).

Strength. Clear and usable limits on both terms.

Weakness. No metrics to mark shifts inside the band and no test to tell routine competition from hostile acts.

Test. If cross war data show a bright universal threshold or show no mixed behaviour across domains, then the band model fails (Sari and Regan, 2024, p.11).

What follows for Ireland. Keep analytic neutrality. Do not mirror image. Build escalation indicators and joint routes for attribution. Pre authorise below threshold options. Write a national lexicon that links terms to actions.

### Liberal universalism and the interference story — a risk to credibility

Regan notes a joint line from Russia and China that attacks Western interference under cover of democracy and human rights. The line also claims each state’s right to choose its own form of democracy (Regan, 2024). This speaks to a known risk. Liberal claims to universal values can look like meddling and can become illiberal in practice. What follows for Ireland. Lead with the law and process and consent. Use measured language. Show the same standards at home and abroad.

## 2 Debates and alternative lenses

Azad and colleagues map the grey zone as a distinct sub threshold (of war) space. It changes the status quo without crossing red lines. They list proxy war and faits accomplis and salami tactics (slowly-slowly piece-by-piece, each piece sub-threshold but making a cumulative change comparable to war) and information and cyber operations. Cases include Russia in 2014 and the South China Sea and Iran and India and Pakistan (Azad et al., 2022, pp.5 to 6, 16 to 21). So what? The cases are short and not measured. Pair this map with clear indicators and timelines for attribution and plans for rollback.

Libiseller says hybrid warfare acts like an academic ‘fashion’. Use spikes follow policy cycles more than theory. Broad labels blur measures and often re badge older methods from combined arms and political warfare (Libiseller, 2023). So What? Base one’s doctrine on mechanisms and effects. Demand definitions you can measure before you adopt them. Keep buying choices free from short term slogans.

Tuck makes a case based on contrast. Crimea moved fast under special local conditions. Donbas was slower and costlier and unclear in result. He concludes that hybrid war is not a separate form (Tuck, 2017, pp.2 to 3). Saif plainly, if we think the present is unique we call old things new and we spend in the wrong places. Use hybrid only as a training tag tied to clear conditions. Fund deterrence by denial and social cohesion.

Hoffman reframes force design under limits. Hybrid threats blend conventional and irregular and terrorist and criminal modes. He says these are the most likely and risky fights in the near term, above all in cities. He warns against false either or choices and suggests a balanced posture on the spectrum rather than at the extremes (Hoffman, 2009, pp.5 to 7). Irish take. The lens is US and not statistical, yet the risk logic travels. Build adaptable combined arms. Link with other services and civil actors. Train for urban complexity.

Gerasimov gives a view from the other side. Non military means can at times beat force in effect. Information action and political pressure and pre emption shape results before open conflict. He calls for one hand on all tools of state and for constant pressure (Gerasimov, 2016, pp.24 to 26). Caution. The essay is programmatic and light on proof. It still points to the need for strong information security and legal readiness and a joined civil military response below the threshold.

Starling and Iyer and Giesler focus on tempo. First movers do better. Early denial and fast attribution beat slow reaction. Free media and partners can be assets if you feed them facts fast and well (Starling et al., 2022, p.4). Guard rail. Speed needs a red team check to avoid error. Pre clear legal and communication templates with partners.

Hoffmann and colleagues scan what comes next. They point to more multi vector coercion. They stress social resilience and lawfare and coalitions for attribution as central tools (Hoffmann and colleagues, 2024, pp.1 to 4). Use: Treat this as a guide to needs, not as proof of effects. For Ireland it means regular inter agency drills and clear legal paths and EU aligned attribution.

### 2a Strategic communications and public trust — what matters for the grey zone

— Credibility is a centre of gravity. Trust falls fast and is slow to rebuild. Treat truth and speed as protection not public relations (Bennett and Livingston, 2018; Ireton and Posetti, 2018).

— Secrecy and disclosure must be in balance. Too much secrecy hurts trust. Raw openness can be abused. Use planned transparency with rules for who speaks and when and what evidence is shown. Estonia shows that fast attribution can deter by removing deniability (Gunneriusson, 2019; Ireton and Posetti, 2018).

— Watch for propaganda creep. Persuasion can slide into manipulation under stress. That burns the very credibility you need. Draw a hard line between inform and persuade and manipulate. Rehearse that line in peacetime (Lemmon, 2024; Bradshaw and Howard, 2019).

## 3 Application to a small state — Ireland versus Estonia

All sources point to resilience and attribution and measured response as decisive below the threshold. Estonia uses whole of society defence. It has pre authorised cyber actions and fast public attribution and routine civic readiness. This makes transparency a form of deterrence. Ireland leans on law and on EU routes and on careful public steps.

Five moves for Irish policy.

1. First set thresholds and indicators across cyber and law and economics and information tied to pre authorised options. This follows the band model from Sari and Regan and links it to action (Sari and Regan, 2024, pp.10 to 12).
2. Second build hybrid readiness in urban operations and in intelligence and surveillance and reconnaissance and in civil and agency links rather than counting platforms alone (Hoffman, 2009, pp.5 to 7).
3. Third use early denial with a red team gate. Pair speed with proof and partner backing (Starling et al., 2022, p.4).
4. Fourth harden the information space and public trust. Build clear routes for attribution and speak early and plainly to blunt hostile claims. This aligns with Hoffmann and colleagues on coalitions and lawfare (Hoffmann and colleagues, 2024, pp.1 to 4).
5. Fifth keep a credible kinetic core in case coercion rises. Note that non military tools can fail when stakes are high. This follows the warning in the rival view (Gerasimov, 2016, pp.24 to 26).

Reality check for Ireland. We lack metrics to tell when competition turns hostile inside the band. Set a national lexicon and a drill cycle and a metrics pack. Measure detection time and attribution confidence and decision time and the effect on public trust. Use the Estonian habit of fast and lawful openness, adapted to Irish law and culture.

## 3 Provocative SRD questions

1. **This House would authorise a small democracy to conduct limited covert influence and cyber operations for defensive purposes.**
2. **This House would reorganise the Irish Army entirely on Mattis and Hoffman hybrid war principles, prioritising unconventional over conventional capabilities.**
3. **This House would legislate national grey-zone triggers with pre-authorised state responses.**

## References

Azad, T. M., Haider, M. W. and Sadiq, M. 2022 Understanding Gray Zone Warfare from Multiple Perspectives.

Gerasimov, V. 2016 The Value of Science Is in the Foresight. Military Review, pp.23 to 29.

Hoffman, F. G. 2009 Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. Strategic Forum No. 240. Washington DC: National Defence University Press.

Hoffmann, F., Neumeyer, M. and Jensen, B. 2024 The Future of Hybrid Warfare. Panel brief.

Libiseller, C. 2023 Hybrid warfare as an academic fashion.

Sari, A. and Regan, M. 2024 Introduction. In Hybrid Threats and Grey Zone Conflict. Oxford: Oxford University Press, pp.10 to 12.

Starling, R., Iyer, C. and Giesler, M. 2022 Todays wars are fought in the gray zone.

Tuck, C. 2017 Hybrid War: The Perfect Enemy.

Additional references from Strategic Communications & Public Trust presentation

Bennett, W. L. and Livingston, S. 2018 The Disinformation Order.

Ireton, C. and Posetti, J. 2018 Journalism, Fake News and Disinformation. UNESCO handbook.

Bradshaw, S. and Howard, P. 2019 The Global Disinformation Order.

Gunneriusson, H. 2019 Strategic communication and trust (as cited in presentation).

Lemmon, E. 2024 Propaganda creep (as cited in presentation).

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

## zero to one 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.

## one to three 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.

## three to five 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.

## five to seven 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.

## seven to eight 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.

eight to nine 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.

## nine to ten 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

## Zero to one 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.

## Three to four 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.

## Four to five 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.

## Five to six 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.

## Six to seven 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.

## Seven to eight 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.

## Eight to nine 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.

## Nine to ten 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.