**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 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 space. It changes the status quo without crossing red lines. They list proxy war and faits accomplis and salami tactics 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). Action. Base 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). Plain meaning. 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).

— Institutional strength beats slogan wars. Weak processes make states easy to move. Close the say do gap. Speak in plain language. Fix the system as well as the story (Bennett and Livingston, 2018; Ireton and Posetti, 2018).

— What Ireland can do now. Create playbooks for first statements and evidence checks and hand offs. Stand up an attribution cell that joins technical and legal and diplomatic work. Give routine updates that admit uncertainty and show what will be checked next. Run a red team check before big campaigns. Exercise comms with cyber and legal drills.

## 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.

## 4 Provocative SRD questions

* Has Ireland already become a grey zone battleground and if so where is the proof in our own indicators and cases (Sari and Regan, 2024).
* Should a small democracy ever run covert influence to defend itself or does that burn the credibility it needs to win in crisis (Starling et al., 2022; Hoffmann and colleagues, 2024).
* Which works better for a small state under hybrid pressure, openness or secrecy, and how would an Irish version of the Estonian model work in practice.
* Are we preparing for the wrong war if hybrid readiness and not force size sends the clearest deterrent signal in our region today (Hoffman, 2009).
* A small democracy should run limited covert influence and cyber to defend itself.
* **Definitions & scope (frame this in 60s)**
* **Covert influence** = foreign-facing, effects-based activities that remain truthful and legal, never targeting Ireland’s domestic public.
* **Offensive cyber** = actions below armed conflict, authorised in law, aimed at disrupting hostile capabilities, not civil society.
* **Guardrails**: legality, necessity, proportionality, oversight, reversibility.

## 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.