The Hague Centre
for Strategic Studies

Guest Paper

Denying Strategic Gains

South Korea's conditional proactive response to North Korean grey-zone coercion

Jaechun Kim

November 2026





The Hague Centre
for Strategic Studies

Denying Strategic Gains

South Korea's conditional proactive response to North Korean grey-zone coercion
Guest Paper

Author:
Jaechun Kim (Sogang University)

Quality Assurance:
Davis Ellison and Hans Horan

The cover image was AI-generated.

November 2026

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, not should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defence.

This publication is **AI-supported***.

© *The Hague* Centre for Strategic Studies. All rights reserved. No part of this report may be reproduced and/or published in any form by print, photo print, microfilm or any other means without prior written permission from HCSS. All images are subject to the licenses of their respective owners.

* AI was used to assist with brainstorming, structuring ideas, reviewing arguments, identifying blind spots, and/or improving clarity. Core analytical tasks such as literature review, conceptual development, substantive judgement and final writing remain human led. The authors take full responsibility for the integrity of the work.

Introduction

Small and middle powers (SMPs) increasingly face security challenges below the threshold of conventional armed conflict. Often described as grey-zone tactics or sub-threshold coercion, these activities seek to achieve political objectives through measures that remain below the threshold of major conventional war while avoiding escalation that would trigger a decisive military response.[1]

SMPs often analyse case studies of grey-zone operations in similar geographic locations (e.g., Europe) to learn how best to minimise or mitigate such threats, with frontline countries such as Finland or Ukraine used as prime cases. However, the Korean Peninsula, an often-overlooked grey-zone frontline, offers a particularly valuable case for examining these challenges. For decades, North Korea has employed a wide range of coercive activities below the threshold of major war, including maritime confrontations around the Northern Limit Line (NLL), cyber operations, drone incursions, and periodic provocations along the Military Demarcation Line (MDL). Though they differ in form, these actions share a common objective: to pressure South Korea, test alliance cohesion, and secure strategic leverage without triggering general war.

At the same time, the Korean case differs from many other examples of grey-zone competition because it unfolds under the shadow of North Korea's nuclear capabilities, which draws direct parallels for European powers vis-à-vis Russia's latent nuclear threat. Therefore, the delicate balance South Korean decision-makers must maintain in deterrence and escalation management when responding to sub-threshold coercion is a particularly salient example for SMPs directly impacted by Russian grey-zone threats, such as those in Europe.

Given these parallels, this paper examines how South Korea has responded to North Korean grey-zone activities, how effective those responses have been, and what lessons may be relevant to other democratic SMPs. To analyse these responses, the paper employs **Conditional Proactive Response (CPR)** as an analytical framework. CPR refers to proportional, legally defensible, alliance-coordinated, and escalation-conscious actions taken in response to prior coercive activity.

The analysis focuses on four areas: borderland coercion along the NLL and MDL, cyber and information operations, drone incursions, and competition under the nuclear shadow. Collectively, these cases illustrate both the strengths and limitations of South Korea's responses and offer broader lessons for states confronting contemporary grey-zone challenges, helping strengthen SMPs' ability to proactively deter or respond to grey-zone threats.

---

1 Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: U.S. Army War College Press, 2015), 3–4. Mazarr defines grey-zone strategies as efforts that pursue political objectives while remaining below key escalatory thresholds and avoiding outright conventional conflict.

Conditional Proactive Response: An Analytical Framework

The principal argument of this paper is that many South Korean responses to North Korean grey-zone coercion reflect a common strategic logic, referred to here as **Conditional Proactive Response (CPR)**.

CPR seeks to balance deterrence and restraint through proportional, alliance-coordinated, and escalation-conscious responses to prior coercive actions. Unlike offensive grey-zone strategies, it does not seek to create ambiguity. Rather, it seeks to reduce ambiguity, deny an adversary's gains, and restore deterrence while remaining below the threshold of major military conflict.

South Korean responses to North Korean grey-zone coercion reflect a common strategic logic, referred to here as Conditional Proactive Response (CPR).

South Korea's experience suggests six conditions that influence the effectiveness of such responses. First, attribution is essential because ambiguity weakens deterrence and complicates coalition-building. Second, responses must be timely to deny adversaries the opportunity to consolidate gains. Third, actions must remain proportional to avoid unnecessary escalation. Fourth, alliance coordination strengthens both deterrence and crisis management. Fifth, information sharing and public exposure can reduce the effectiveness of coercive activities by undermining deniability. Finally, escalation management is particularly important on the Korean Peninsula given North Korea's nuclear capabilities.

CPR is used here as an analytical framework rather than a policy prescription. In this vein, the following sections apply this framework to four domains of North Korean grey-zone activity by examining three questions: how North Korea applied coercion, how South Korea responded, and what broader lessons can be drawn from the outcome.

Borderland Grey-Zone Coercion: Challenges to the Northern Limit Line and the Military Demarcation Line

Border regions have historically provided North Korea with some of its most attractive opportunities for grey-zone coercion. Both the Northern Limit Line (NLL) in the West Sea and the Military Demarcation Line (MDL) within the Demilitarised Zone are contested spaces where North Korea can challenge the status quo while avoiding large-scale military escalation. Although maritime and terrestrial environments differ operationally, they share similar strategic characteristics. Both involve questions of territorial control, military presence, legitimacy, attribution, and escalation management.

For decades, North Korea has used these border areas to test South Korean resolve, challenge existing security arrangements, and create political pressure on decision-makers in Seoul. The objective has rarely been territorial conquest. Instead, North Korean actions have typically sought to create uncertainty, undermine deterrence, and shift perceptions of the stability of existing boundaries.

The NLL and Maritime Grey-Zone Competition

The NLL remains the most enduring example of maritime grey-zone competition on the Korean Peninsula. Since the 1970s, North Korea has repeatedly challenged the legitimacy of the line through naval incursions, fishing disputes, maritime infiltration operations, and localised military confrontations. Incidents such as the First Battle of Yeonpyeong (1999), the Second Battle of Yeonpyeong (2002), the sinking of the *Cheonan* (2010), and the shelling of Yeonpyeong Island (2010) illustrate North Korea's long-standing effort to challenge the maritime status quo without provoking a general war. While all four incidents matter, the discussion below focuses primarily on the Cheonan sinking and the Yeonpyeong Island shelling, as they most clearly illustrate South Korea's responses to grey-zone coercion.[2]

South Korea's response to maritime coercion has generally rested on three pillars: maintaining a persistent military presence, establishing credible attribution, and coordinating closely with allies and international partners.

South Korea's response to maritime coercion has generally rested on three pillars: maintaining a persistent military presence, establishing credible attribution, and coordinating closely with allies and international partners.

The two Yeonpyeong naval battles demonstrated South Korea's willingness to defend the NLL through direct military action. In both cases, South Korean forces repelled North Korean incursions and preserved the existing maritime boundary. While the clashes were tactical engagements rather than comprehensive grey-zone campaigns, they reinforced the credibility of South Korea's commitment to defending the status quo.

The 2010 Cheonan incident revealed a different challenge. Although an international investigation ultimately concluded that the corvette had been sunk by a North Korean torpedo, attribution required nearly two months of forensic investigation involving South Korean and international experts.[3] North Korea denied responsibility throughout, and domestic political controversy emerged over the findings. As a result, Seoul struggled to impose immediate costs on Pyongyang. The case illustrates one of the central challenges of grey-zone coercion: ambiguity can delay decision-making and weaken deterrence even after responsibility is eventually established.[4]

Later that same year, the shelling of Yeonpyeong Island produced a markedly different response. Unlike the *Cheonan* incident, attribution was immediate and unambiguous. South Korea responded with artillery fire against North Korean positions and subsequently strengthened military readiness around the Northwest Islands. In CPR terms, the case shows how rapid attribution can enable timely, proportional cost imposition while reinforcing deterrence.[5]

Alliance coordination also played a critical role. After the Cheonan sinking, Seoul worked closely with the United States and other international partners to strengthen the investigation's credibility and mobilise diplomatic support. At the same time, alliance consultations helped manage escalation risks. Former U.S. Secretary of Defense Robert Gates later

2 For discussions of the First and Second Battles of Yeonpyeong, see Narushige Michishita, *North Korea's Military-Diplomatic Campaigns, 1966–2008* (London: Routledge, 2009), 143–70. For the sinking of the Cheonan, see Joint Civilian-Military Investigation Group, *Investigation Result on the Sinking of ROKS "Cheonan"* (May 20, 2010). For the shelling of Yeonpyeong Island, see Joseph S. Bermudez Jr., "The Yeonpyeong Island Incident, November 23, 2010," *38 North*, January 13, 2011.

3 Joint Civilian-Military Investigation Group, *Investigation Result on the Sinking of ROKS "Cheonan"*. The investigation involved South Korean and international experts from the United States, the United Kingdom, Australia, and Sweden and relied on extensive forensic, technical, intelligence, and explosive analysis before reaching its conclusion.

4 Republic of Korea Ministry of National Defense, *2024 Defense White Paper* (Seoul: MND, 2024); Bermudez, "Yeonpyeong Island Incident."

5 Joint Civilian-Military Investigation Group, *Investigation Result on the Sinking of ROKS "Cheonan"*.

recalled concerns in Washington that South Korea's anger following North Korean provocations could lead to excessive military retaliation and a broader confrontation. Close consultation between Seoul and Washington helped balance deterrence with escalation control, allowing the allies to maintain a united front while avoiding a wider conflict.

Overall, South Korea's maritime strategy has achieved mixed but generally positive results. North Korea has failed to alter the status quo; the NLL continues to function as the de facto maritime boundary, and South Korea retains control of the Northwest Islands. At the same time, periodic incursions and continuing North Korean challenges to the legitimacy of the NLL suggest that deterrence remains incomplete. The broader lesson is that successful grey-zone responses rarely eliminate coercion altogether. Rather, they prevent coercive actions from generating significant political or strategic gains.

Although Washington was concerned that Seoul might respond too forcefully and trigger a broader confrontation, close consultations helped align deterrence objectives with escalation management.

The 2015 and 2026 DMZ Landmine Incidents

If the NLL illustrates maritime grey-zone competition at sea, the 2015 and 2026 landmine incidents between North and South Korea demonstrate how similar dynamics operate along the MDL.

The August 2015 landmine incident involved the deliberate emplacement of North Korean wooden-box mines south of the MDL, resulting in severe injuries to two South Korean soldiers. Like many grey-zone operations, the attack relied on covert action and sought to impose costs while avoiding major escalation.

Former South Korean President Park Geun-hye and her administration (2013-2017) responded quickly by attributing the attack, imposing visible costs, and coordinating closely with allies. Soon after publicly attributing the attack to Pyongyang, Seoul resumed anti-North Korean loudspeaker broadcasts for the first time in more than a decade and heightened military readiness. The response generated a significant escalation cycle, including North Korean artillery fire and South Korean return fire. Yet the crisis also revealed North Korea's own sensitivity to escalation. As tensions mounted, Pyongyang requested high-level inter-Korean talks that ultimately produced the August 25 agreement and North Korea's expression of regret. According to senior South Korean officials involved at the time, North Korea's public rhetoric remained confrontational, but private discussions focused on preventing further escalation and ending the crisis.

Alliance coordination proved equally important. Although Washington was concerned that Seoul might respond too forcefully and trigger a broader confrontation, close consultations helped align deterrence objectives with escalation management. According to officials involved in the crisis, the United States ultimately supported South Korea's determination to impose costs while avoiding uncontrolled escalation.[6]

From a CPR perspective, the 2015 response performed relatively well across the core dimensions of attribution, timeliness, cost imposition, and alliance coordination. Its principal weakness was the heightened risk of escalation.

[6] Author's conversation with former senior South Korean officials directly involved in the 2015 inter-Korean crisis management and high-level negotiations.

In contrast, the September 2026 DMZ landmine incident presented a different challenge. Following a joint investigation, both the South Korean government and the United Nations Command concluded that the mines responsible for the explosion were North Korean in origin and had been emplaced south of the MDL, constituting a violation of the Armistice Agreement. Pyongyang nevertheless denied responsibility and characterised the incident as a fabrication.[7]

Unlike the *Cheonan* case, attribution was achieved relatively quickly. The central issue concerns what followed. While the Park administration moved quickly from attribution to punishment, the Lee Jae-myung administration has so far prioritised investigation, legitimacy, and managing escalation. The government has publicised the investigation's results, coordinated closely with the United Nations Command, and demanded accountability from North Korea. However, at the time of writing, Seoul has not yet articulated a clear cost-imposition strategy, raising questions about how it will restore deterrence after the incident.

The principal lesson is that attribution is necessary but not sufficient. Successful grey-zone responses require translating attribution into timely, proportionate action while maintaining alliance cohesion and escalation control.

The contrast between the two cases is therefore instructive. Both governments successfully attributed responsibility. The difference lies in how quickly and clearly attribution translated into action. The Park administration prioritised deterrence restoration, accepting greater escalation risks but ultimately securing negotiations and a North Korean expression of regret. The Lee administration has placed greater emphasis on legitimacy and escalation management, but has yet to show how it will translate attribution into credible punishment. It remains uncertain whether this approach will prove equally effective.

For other small and middle powers, the principal lesson is that attribution is necessary but not sufficient. Successful grey-zone responses require translating attribution into timely, proportionate action while maintaining alliance cohesion and escalation control.

Cyber and Information Operations

Cyber operations represent one of North Korea's most effective grey-zone instruments. Unlike maritime or border provocations, cyber activities let Pyongyang gather intelligence, evade sanctions, generate revenue, and impose costs while avoiding the risk of direct military confrontation. As a result, attribution is often more difficult, deterrence less immediate, and proportional responses harder to define.

North Korea's cyber activities have evolved significantly over the past decade. Early operations focused primarily on disruption and espionage targeting South Korean financial institutions, broadcasters, and government agencies. More recently, Pyongyang has increasingly relied on financially motivated operations, including the Bangladesh Bank heist (2016), the WannaCry ransomware campaign (2017), cryptocurrency theft, and the deployment of overseas IT workers operating under false identities. These activities demonstrate how grey-zone coercion can generate strategic and economic benefits without employing traditional military force.

7 "North and South Korea Trade Accusations over DMZ Landmine Incident," *Stars and Stripes*, September 2026; Republic of Korea Ministry of National Defense, official statements on the results of the joint ROK–UNC investigation.

South Korea's response has relied less on direct retaliation than on attribution, resilience, and international cooperation. Over time, Seoul has developed a cyber-defence architecture centred on the National Intelligence Service (NIS), the Ministry of National Defence, the National Police Agency, and the Korea Internet & Security Agency (KISA). Successive governments have invested heavily in cyber defence, information sharing, and cooperation with private-sector operators.[8]

The DPRK IT worker issue provides a particularly useful case for evaluating Seoul's approach. Since at least 2017, North Korean operatives have used false identities, forged resumes, accomplice networks, and, more recently, AI-generated profiles and deepfake technologies to obtain remote employment abroad. Initially, these activities appeared to involve legitimate software development, delaying recognition of the threat and enabling rapid international expansion.[9]

Alliance coordination has also become central to cyber defence, particularly in the DPRK IT worker case.

South Korea responded by combining attribution, public exposure, sanctions, and alliance coordination. In December 2022, the government issued its first advisory specifically addressing DPRK IT workers. Subsequent measures included sanctions against entities involved in North Korea's overseas revenue-generation activities, coordinated sanctions with the United States, and joint ROK-U.S. advisories designed to expose emerging DPRK IT worker tactics and warning indicators. Rather than pursuing offensive cyber retaliation, Seoul focused on exposing the networks, raising awareness, and restricting their access to international financial and employment systems.

Viewed through the CPR framework, the cyber domain reveals both strengths and weaknesses. Attribution has improved markedly as cooperation with the United States and other partners has expanded. Alliance coordination has also become central to cyber defence, particularly in the DPRK IT worker case, where joint advisories, sanctions, and investigations played an important role in constraining North Korea's room for manoeuvre.

However, cyber operations also expose a persistent limitation of CPR: cost imposition remains difficult. Unlike the 2015 landmine incident or the Yeonpyeong shelling, there is often no obvious way to impose immediate and proportional costs. Moreover, evidence suggests that DPRK IT worker networks operated internationally for years before large-scale international responses emerged, highlighting persistent challenges in attribution and timeliness.

The effectiveness of South Korea's approach is therefore mixed. DPRK cyber activities continue, suggesting that deterrence remains incomplete. Yet complete deterrence may be an unrealistic benchmark.

A more relevant measure is whether Seoul has reduced North Korea's ability to operate undetected. In recent years, coordinated attribution efforts and public exposure campaigns have revealed an increasingly detailed picture of DPRK cyber operations, including the use of false identities, intermediary networks, laptop farms, and AI-assisted deception techniques.[10] By making these methods more widely understood, South Korea and its partners

8 Republic of Korea Ministry of National Defense, *2024 Defense White Paper*; Republic of Korea National Intelligence Service, *National Cyber Security Strategy* (Seoul: National Intelligence Service, various editions).

9 Yena Kim and Donghee Kim, *Responding to the Evolution and Global Expansion of the DPRK IT Worker Threat* (Washington, DC: Center for Strategic and International Studies, March 2026), 1–3.

10 Kim and Kim, *Responding to the Evolution and Global Expansion of the DPRK IT Worker Threat*; DTEX Systems, *Exposing DPRK Cyber Syndicate and Hidden IT Workforce* (DTEX Systems, 2026).

have transformed what was once a largely hidden threat into an internationally recognised security concern.

Greater awareness has also encouraged practical defensive measures. Governments, technology firms, and private companies have strengthened identity-verification procedures, adopted more rigorous hiring and technical-screening processes, and become more attentive to suspicious remote-employment activities associated with DPRK operatives.[11] As a result, North Korean networks now face a more demanding operating environment than they did only a few years ago, even if they continue to adapt and remain active.

From a CPR perspective, this outcome is significant because it demonstrates that success in the cyber domain often depends less on punishment than on attribution, transparency, and coalition-building. While South Korea has not eliminated DPRK cyber activities, it has contributed to increasing the costs of operating covertly and reducing the effectiveness of deniability.[12]

Greater awareness has also encouraged practical defensive measures.

For other small and middle powers, the principal lesson is that cyber deterrence differs fundamentally from military deterrence. Attribution, public exposure, sanctions, and international cooperation may often prove more effective than attempts at direct retaliation. The DPRK IT worker case demonstrates that successful responses frequently depend on sustained cooperation and transparency rather than reciprocal action.

Drone Incursions and Tactical Ambiguity

Drone incursions represent a distinct form of grey-zone coercion because they occupy an ambiguous space between surveillance, provocation, and military intrusion. Unlike the 2015 landmine incident or the shelling of Yeonpyeong Island, drone operations in the Korean context have thus far rarely produced immediate casualties or significant physical destruction. Their principal value lies in intelligence collection, testing defensive systems, and exposing vulnerabilities in an opponent's security posture.

The most significant recent example occurred in December 2022, when multiple North Korean drones penetrated South Korean airspace, including areas near Seoul. The incident attracted considerable public attention because South Korean forces failed to intercept the drones despite deploying fighter aircraft, helicopters, and air-defence assets. From North Korea's perspective, the operation was successful not because it caused damage, but because it exposed weaknesses in South Korea's surveillance and response systems.[13]

Then South Korean President Yoon Suk-yeol and his administration (2022-2025) responded through a combination of military reform, technological investment, and deterrent signalling. Following the December 2022 incursion, Seoul accelerated counter-drone development, expanded low-altitude surveillance and detection capabilities, and established a specialised Drone Operations Command. Seoul placed particular emphasis on addressing

11 "How Companies Are Learning to Spot North Korean IT Workers," *Wall Street Journal*, video report; DTEX Systems, *Exposing DPRK Cyber Syndicate and Hidden IT Workforce*.

12 Kim and Kim, *Responding to the Evolution and Global Expansion of the DPRK IT Worker Threat*.

13 Republic of Korea Joint Chiefs of Staff, press briefing on North Korean drone incursions, December 26, 2022; Reuters, "South Korea Scrambles Jets as North Korea Sends Drones over Border," December 26, 2022.

weaknesses revealed during the 2022 incident, especially in detecting and tracking small, low-flying drones.[14]

The military also expanded training in drone detection, tracking, and interception while improving coordination among intelligence, air-defence, and ground units. Many of these efforts benefited from close cooperation with the United States, suggesting that effective counter-drone capabilities may require a combination of domestic investment and alliance support.[15]

In CPR terms, attribution was immediate and the response relatively timely. Rather than focusing primarily on punishment, Seoul sought to reduce future vulnerabilities through preparedness, institutional adaptation, and deterrence by denial. While the effectiveness of these measures is difficult to assess precisely, they appear to have strengthened South Korea's ability to detect and respond to future incursions.

Reciprocity does not necessarily generate effective deterrence. Actions that mirror an adversary's behaviour may create domestic political controversy regarding transparency and accountability.

However, the issue of cost imposition proved more complicated. Following the 2022 incident, allegations emerged that South Korea had conducted its own drone operations across the border. North Korea publicly accused Seoul of sending drones into Pyongyang, although the South Korean government neither fully confirmed nor fully denied such claims.[16] Whether such operations occurred is ultimately less important than the broader policy question they raise. Reciprocity does not necessarily generate effective deterrence. Actions that mirror an adversary's behaviour may create domestic political controversy regarding transparency and accountability while increasing escalation risks without necessarily changing the adversary's behaviour.

This distinction is important when evaluating effectiveness. Unlike the 2015 landmine case, where cost imposition was followed by negotiations and a North Korean expression of regret, the drone domain offers little evidence that reciprocal actions have altered Pyongyang's behaviour. North Korea continues to invest heavily in unmanned systems and has increasingly incorporated drones into broader strike exercises alongside missiles and long-range artillery.[17]

From a CPR perspective, the drone case therefore highlights both the strengths and limitations of retaliatory logic. Attribution was straightforward, but proportional punishment was far less clear. South Korea's most successful measures appear to have been those aimed at strengthening surveillance, detection, training, and alliance coordination rather than mirroring North Korean behaviour.

For other small and middle powers, the principal lesson is that effective responses to drone-based grey-zone coercion do not always require symmetrical retaliation. In the Korean case, the policies that most clearly reinforced deterrence without generating significant political or escalation costs were investments in surveillance, detection, training, and institutional adaptation. Strengthening resilience and denying future gains may ultimately prove more effective than attempting to replicate an adversary's tactics.

---

14 Republic of Korea Ministry of National Defense, *2024 Defense White Paper*; Il-Seok Oh and Yonghwan Choi, "Pyongyang's Showcase of UAVs During the Victory Day Military Parade and Its Implications," Institute for National Security Strategy, September 2023.

15 Republic of Korea Ministry of National Defense, *2024 Defense White Paper*.

16 Reuters and Yonhap News Agency, reporting on North Korean allegations of South Korean drone operations over Pyongyang and subsequent statements by the South Korean government.

17 "N. Korea Says Latest Missile Launches Were Joint Firepower Strike Drill," *The Korea Herald*, September 14, 2026.

Competition under the Nuclear Shadow: CPR under Conditions of Escalation Risk

Unlike the previous categories of grey-zone activity examined in this study, competition under the nuclear shadow reflects a condition that, while especially pronounced on the Korean Peninsula, increasingly confronts European states as well. South Korea faces a nuclear-armed North Korea, while many European small and middle powers must manage growing grey-zone pressures from a nuclear-armed Russia. In both cases, the central challenge is the same: how to respond to coercion without risking deterrence failure or uncontrolled escalation.

The Korean experience suggests that this dilemma is managed not by choosing between deterrence and restraint, but by calibrating responses carefully.

North Korea's nuclear capabilities complicate South Korea's response options in several respects. Actions that might otherwise be treated as limited tactical responses must also be assessed for their broader escalation implications. The result is a persistent dilemma. Excessive restraint may weaken deterrence, while excessive force risks escalation disproportionate to the original provocation. The United States has historically played an important role in managing this tension by emphasising both deterrence and crisis stability.

The Korean experience suggests that this dilemma is managed not by choosing between deterrence and restraint, but by calibrating responses carefully. South Korean reactions to the 2010 Yeonpyeong shelling and the 2015 DMZ landmine incident illustrate this approach. In both cases, Seoul imposed costs on North Korea while deliberately limiting the scope of retaliation. The objective was not simply to punish Pyongyang, but to restore deterrence credibility without creating a pathway to wider conflict.

The nuclear shadow influenced decision-making in both crises. South Korean policymakers were required to consider not only the immediate military value of retaliation but also the possibility that further escalation could disrupt alliance coordination, provoke additional North Korean actions, or generate broader regional instability. The result was a preference for responses that were visible and costly, yet clearly bounded in both scope and objectives.

Alliance support was equally important. Under nuclear conditions, successful deterrence depends not only on a state's willingness to respond but also on the confidence that allies will support that response if the crisis escalates. In the South Korean case, close consultation with Washington helped reassure decision-makers that firm responses could be undertaken without jeopardising alliance cohesion. At the same time, alliance coordination provided an important mechanism for escalation management by discouraging both passivity and overreaction.

These lessons have direct relevance for European small and middle powers. Countries such as the Netherlands, Finland, and the Baltic states face a challenge that differs geographically but follows a similar strategic logic. Russian grey-zone activities frequently occur below the threshold of conventional war, yet they unfold in the context of Russia's nuclear capabilities. As in the Korean case, the presence of nuclear weapons does not eliminate the need to respond. Instead, it raises the premium on attribution, alliance coordination, calibrated signalling, and escalation management.

Not all aspects of the Korean experience are directly transferable. South Korea confronts a geographically proximate adversary, a divided nation, and a decades-long pattern of military confrontation that few European states face. Nevertheless, the broader strategic lesson

is applicable. Under a nuclear shadow, effective responses should seek neither complete restraint nor unrestricted retaliation. Instead, they must impose meaningful costs while remaining limited, proportionate, and politically sustainable.

From a CPR perspective, the nuclear shadow matters less for preventing retaliation than for shaping its form. The Korean experience demonstrates that deterrence and escalation management are not competing objectives but complementary ones. The challenge is not whether to respond to grey-zone coercion, but how to do so in ways that preserve deterrence credibility while maintaining strategic stability. For European small and middle powers confronting Russian grey-zone pressure, that may be the most relevant lesson of all.

Lessons for Democratic Middle Powers: Implications for the Netherlands

South Korea's experience should not be treated as a template other states can directly replicate. The Korean Peninsula presents an unusually demanding security environment shaped by persistent military confrontation, geographical proximity to an adversary, and the constant possibility of nuclear escalation. Few democratic middle powers face comparable conditions.

South Korea's experience demonstrates that the central objective of grey-zone competition is often to deny strategic gains rather than to prevent every individual provocation.

Yet the Korean case remains valuable precisely because it demonstrates how a democratic state can respond to grey-zone coercion across multiple domains over an extended period of time. The principal lesson is not that South Korea successfully eliminated grey-zone threats. It did not. Maritime provocations, cyber operations, information campaigns, drone incursions, and other forms of coercion continue to occur. Rather, South Korea's experience demonstrates that the central objective of grey-zone competition is often to deny strategic gains rather than to prevent every individual provocation.

This finding has important implications for SMP countries such as the Netherlands. Much of the existing literature implicitly evaluates success in terms of deterrence failure or success.[18] The Korean experience suggests a different standard. Grey-zone competition rarely ends in decisive victories. Instead, success depends on a state's ability to attribute hostile actions, impose selective costs, strengthen institutional resilience, maintain public legitimacy, and coordinate with allies over time. The cumulative effect of these measures can significantly reduce an adversary's ability to convert tactical provocations into strategic advantages.

The Korean case also highlights the importance of flexibility. Different forms of grey-zone coercion require different combinations of coercion, restraint, signalling, attribution, and international coordination. In some cases, imposing visible costs may be necessary to restore deterrence. In others, careful investigation, diplomatic mobilisation, and alliance coordination may generate greater strategic benefits than immediate retaliation. The key lesson is not adherence to a fixed playbook but the ability to calibrate responses according to the nature of the provocation and the broader strategic environment.

Recent South Korean responses further illustrate this challenge. Critics have argued that the Lee Jae-myung administration's handling of the 2026 DMZ landmine incident placed greater

[18] Mazarr, *Mastering the Gray Zone*; Michael J. Mazarr et al., *What Deters and Why* (Santa Monica, CA: RAND, 2018); Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004).

emphasis on de-escalation, investigation, and international legitimacy than on visible cost imposition. Whether this approach ultimately proves successful remains unclear. Nevertheless, the episode underscores a broader point for democratic middle powers: excessive caution may reduce short-term escalation risks, but it can also raise questions about deterrence credibility if adversaries perceive limited consequences for coercive behaviour. Managing this trade-off remains a central challenge of grey-zone competition for all SMPs.

Excessive caution may reduce short-term escalation risks, but it can also raise questions about deterrence credibility if adversaries perceive limited consequences for coercive behaviour.

Finally, the Korean experience challenges the common assumption that authoritarian states possess a structural advantage in grey-zone conflict. Much of the literature emphasises ambiguity, deniability, and secrecy as strengths that favour authoritarian actors.[19] Yet South Korea's experience suggests that democratic states possess important advantages of their own, including transparency, political legitimacy, public accountability, international credibility, and durable alliance networks. When effectively integrated into national strategy, these characteristics can become significant sources of competitive advantage rather than constraints on action.

Not all aspects of the Korean experience are directly transferable to the Netherlands. The intensity of inter-Korean rivalry and the immediacy of the North Korean threat remain largely unique. Nevertheless, the nuclear dimension of the Korean case may be more relevant to Europe than is often assumed. While the Netherlands does not confront North Korea, it operates within NATO's strategic competition with a nuclear-armed Russia, where escalation risks similarly influence responses to grey-zone coercion. The Korean experience suggests that the presence of nuclear weapons does not remove the necessity of responding to coercion. Instead, it makes alliance cohesion, credible deterrence, and carefully calibrated signalling even more important in preventing tactical provocations from producing strategic gains.

Policy Recommendations for Democratic Small and Medium Powers

The Korean experience suggests that responding to grey-zone coercion does not necessarily mean preventing every provocation, but denying adversaries the ability to convert tactical actions into strategic gains. Based on the cases examined in this study, four policy recommendations emerge for democratic small and middle powers confronting contemporary grey-zone threats.

1. Maritime and Border Domains: Establish Clear Attribution and Response Mechanisms Before a Crisis Occurs

The South Korean experience demonstrates that attribution is a prerequisite for effective deterrence. The contrast between the *Cheonan* sinking and the Yeonpyeong shelling illustrates how uncertainty can delay responses and complicate coalition-building. Small and middle powers should therefore invest in surveillance, intelligence-sharing, and investigative capabilities before major incidents occur. Equally important, governments should develop pre-planned response options they can implement rapidly once responsibility is established. Deterrence is stronger when attribution can quickly translate into proportionate action.

[19] Mazarr, *Mastering the Gray Zone*, 4–8, 57–64; Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4 (2018): 30–47.

2. Cyber Operations: Prioritise Attribution, Exposure, and International Coordination

The DPRK IT worker case suggests that success in cyberspace often depends less on retaliation than on reducing an adversary's ability to operate undetected. Governments should expand cooperation with allies, private-sector firms, and cybersecurity organisations to improve attribution and information sharing. Public advisories, coordinated sanctions, and exposure campaigns can raise the operational costs of malicious cyber activities even when direct punishment is difficult. In many cases, transparency and disruption may prove more effective than retaliation, as greater awareness of the threat amongst private-sector partners lowers the effectiveness of the DPRK's IT worker tactics.

3. Drone Incursions: Emphasise Detection, Resilience, and Denial Rather than Reciprocity

The 2022 drone incursion demonstrated that vulnerabilities in detection and response systems may create greater risks than the intrusion itself. Small and middle powers should prioritise investments in surveillance, low-altitude air-defence networks, counter-drone training, and institutional adaptation. South Korea's experience suggests that resilience and denial often yield greater long-term benefits than mirroring an adversary's actions. The goal should be to reduce future vulnerabilities rather than simply respond symmetrically.

4. Competition under the Nuclear Shadow: Integrate Deterrence with Escalation Management

The Korean case highlights a lesson of increasing relevance for European states confronting Russian grey-zone pressure. Nuclear weapons do not eliminate the need to respond to coercion, but they increase the importance of calibration. Effective responses should impose meaningful costs while remaining limited, proportionate, and clearly connected to the original provocation. Close alliance coordination is particularly important because it strengthens deterrence credibility while helping manage escalation risks. Under nuclear conditions, strategic restraint and deterrence should be seen as complementary, not competing, objectives.

Conclusion

Across all four domains, the central lesson is that successful grey-zone responses rarely eliminate coercion altogether. Their purpose is to deny adversaries strategic gains while preserving political legitimacy, alliance cohesion, and escalation control. For democratic small and middle powers, effective grey-zone strategy therefore depends less on matching every provocation than on building the institutional, military, and political capacity to respond consistently, credibly, and sustainably over time.

Bibliography

Bermudez, Joseph S., Jr. "The Yeonpyeong Island Incident, November 23, 2010." 38 North, January 13, 2011.

Cha, Victor D. *Powerplay: The Origins of the American Alliance System in Asia*. Princeton, NJ: Princeton University Press, 2016.

DTEX Systems. "North Korean IT Workers: The Insider Threat." June 2024.

Freedman, Lawrence. *Deterrence*. Cambridge: Polity Press, 2004.

Gates, Robert M. *Duty: Memoirs of a Secretary at War*. New York: Alfred A. Knopf, 2014.

Ha, Choong Soo. "A Study on the Response Plan through the Analysis of North Korea's Drones Terrorism at Critical National Facilities." *Journal of the Society of Disaster Information* 19, no. 2 (2023): 395–410.

Hoffman, Frank G. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *PRISM* 7, no. 4 (2018): 30–47.

Joint Civilian-Military Investigation Group. *Investigation Result on the Sinking of ROKS "Cheonan."* May 20, 2010.

Kim, Yena, and Donghee Kim. *Responding to the Evolution and Global Expansion of the DPRK IT Worker Threat*. Washington, DC: Center for Strategic and International Studies, March 2026.

Mazarr, Michael J., et al. *What Deters and Why*. Santa Monica, CA: RAND, 2018.

Mazarr, Michael J. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Carlisle, PA: U.S. Army War College Press, 2015.

Michishita, Narushige. *North Korea's Military-Diplomatic Campaigns, 1966–2008*. London: Routledge, 2009.

Oh, Il-Seok, and Yonghwan Choi. "Pyongyang's Showcase of UAVs During the Victory Day Military Parade and Its Implications." Institute for National Security Strategy (INSS), September 2023.

Personal conversation with a former senior South Korean official involved in the 2015 inter-Korean crisis management and high-level negotiations. Anonymized.

Republic of Korea Joint Chiefs of Staff. Press briefing on North Korean drone incursions. December 26, 2022.

Republic of Korea Ministry of National Defense. *2024 Defense White Paper*. Seoul: MND, 2024.

Republic of Korea National Intelligence Service. *National Cyber Security Strategy*. Seoul, various editions.

Reuters. "South Korea Scrambles Jets as North Korea Sends Drones over Border." December 26, 2022.

Republic of Korea Ministry of National Defense. Official statement on the 2026 DMZ landmine investigation. 2026.

Stars and Stripes. Report on the 2026 DMZ landmine incident. 2026.

The Korea Herald. "N. Korea Says Latest Missile Launches Were Joint Firepower Strike Drill." September 14, 2026.

Wall Street Journal. Report on North Korean overseas IT workers.

Yonhap News Agency. "N. Korean Merchant Vessel Crosses Sea Border, Retreats after Warning Shots from South." September 26, 2025.



The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl