COUNCIL on FOREIGN RELATIONS

POLICY REPORT

Gray Zone Attacks Against U.S. Allies and Partners

Crisis Response Playbook no. 3

July 23, 2026

F. David Diaz, Principal, Geopolitical Risk Management and Executive Advisory, Signal Hill Advisers; Adjunct Assistant Professor, Georgetown University

Executive Summary

Gray zone attacks are deliberate but deniable acts of violence engineered to inflict strategic costs while stopping short of triggering a formal military or diplomatic response. Those attacks can take multiple forms: infrastructure destruction (undersea cable cuts, energy pipeline sabotage); industrial sabotage (arson, explosions, and defense supply-chain disruption); targeted violence (assassination plots and intimidation campaigns executed through criminal proxies); and drone harassment (over airports, military installations, and urban centers, an increasingly common target).

In all those attacks, the perpetrator's identity is difficult to discern, allowing the attacking state to deny involvement, at least initially. Unlike conventional military aggression, gray zone campaigns unfold without formal declarations, progress gradually, mimic crime or accident, and can be designed to appear coincidental or random. By the time a coordinated campaign is recognized for what it is, the attacker has already achieved significant strategic advantages: it may have weakened infrastructure, tested the victim's resilience or resolve, or positioned proxy networks and other capabilities to use in future attacks. The victim state may have already established a precedent of nonresponse, and its alliances may have been tested.

Although responses to gray zone attacks in the United States would be governed by domestic laws and regulations, one critical feature of these offensives abroad is that the primary targets are frequently not U.S. government assets but the commercial infrastructure, defense contractors, logistics networks, and private citizens of U.S. allies. Given the range of targets, responding effectively requires working from the outset with foreign governments, private businesses, and operators of critical infrastructure (power plants, rail networks, water utilities, etc.).

U.S. treaty commitments, alliance credibility, and commercial interests are all at stake, especially when attacks go unanswered. The U.S. intelligence community assesses that China, Iran, North Korea, and Russia are conducting or expanding gray zone campaigns against U.S. allies, a trend that the National Intelligence Council predicts will continue through at least 2030.

Four strategies are available before or during a crisis, each made viable by different prior decisions.

- **Monitor:** Wait and see, preserve flexibility, collect intelligence, and analyze patterns while the source of the gray zone attack remains uncertain.

- **Contain:** Harden targets, disrupt proxy networks, and share intelligence with allies without public attribution to reduce the attacker's operational success.
- **Deter and Respond:** Attribute the attack's source publicly, impose targeted costs (sanctions, expulsions, military or diplomatic moves), and reinforce the affected ally to re-establish deterrence.
- **Transform:** Pursue fundamental change: degrade the campaign's infrastructure, restructure alliance posture, and press for diplomatic agreements. This option will require sustained political will and allied coordination.

Although gray zone attacks produce physical effects that could provoke a military response, the most effective response could also be diplomatic, informational, or economic in nature. The options presented below deliberately incorporate all those tools, and the lessons that follow are designed to keep planners from defaulting to a false binary of military action or inaction.

Case studies across all four types of gray zone attacks yield a consistent set of findings:

- **A gray zone crisis requires a political decision, not just an intelligence assessment.** No single red line in international law or alliance policy exists that automatically converts a gray zone attack into a crisis. That determination is political, shaped by the scale and simultaneity of attacks, the significance of the target, the confidence of the attribution, the cumulative strategic effect, and the extent to which the attacked state may seek to invoke an allied response.
- **Pre-established protocols matter more than response capability.** Protocols and broad decision-making guidelines can streamline responses and improve outcomes. Without such guidelines, delays have opportunity costs. A Chinese-flagged vessel implicated in the 2023 Balticconnector incident, in which a dragging anchor severed a gas pipeline connecting Estonian and Finland, escaped into Russian waters before authorities could act; not for lack of ships, but for lack of an agreed-upon response.
- **Timely public attribution raises the cost of the next attack.** Each public attribution of the gray zone attack's origin increases the cost of future attacks and degrades the attacker's deniability, narrowing its diplomatic maneuvering room and reducing its ability to exploit ambiguity.

- **Bilateral and multilateral coordination multiplies deterrence.** Even without formal NATO or EU triggering mechanisms, U.S. allies can join in attributing the attack and imposing costs on the attacker. Multilateral efforts carry substantially greater deterrence value than unilateral action.
- **Policymakers should reach for civilian tools first.** Economic measures, law enforcement, and information operations are the primary instruments of gray zone response. Overreliance on military and intelligence tools constrains the use of nonmilitary response options.
- **Private-sector engagement is essential, not optional.** Direct engagement with private-sector infrastructure owners expands the range of available tools and helps mitigate risks.
- **Drone harassment is the fastest-growing gray-zone attack method.** Drone incidents over European airports, military installations, and urban centers—increasingly over those in the United States—have surged through 2025 and into 2026.

Two institutional gaps complicate every policy decision: no single U.S. government agency is responsible for integrating each of the warning indicators before a crisis, and no standing mechanism exists to orchestrate a rapid government-wide response during one. Which agency should lead the U.S. government's response—State, Defense, or Treasury—is best determined by attack type, and that determination should be made as a matter of policy before a crisis, not improvised under pressure.

1.0 Situational Assessment

1.1 What Is the Source of Concern?

Gray zone attacks are part of a deliberate strategy by states to weaken adversaries, in this case U.S. allies and partners, without crossing the threshold that would legally or politically compel a military response. The July 2024 National Intelligence Council assessment, "Conflict in the Gray Zone" [PDF], projects that China, Iran, North Korea, and Russia will conduct increasingly frequent, diverse, and damaging gray zone coercion through at least 2030.

The primary targets abroad are frequently not U.S. government assets, but the commercial infrastructure, defense contractors, energy companies, logistics networks, and private citizens of U.S. allies. As agencies coordinate internally, they should also work with those parties directly in crafting an effective response.

This playbook focuses on gray zone attacks abroad targeting those entities and individuals, though they are not the only provocations that fall short of military response. Excluded from its scope are cyberattacks and disinformation operations without physical consequences, whose response tool kit and legal authorities are sufficiently distinct; activities by openly state-linked actors where deniability is absent, such as Chinese Coast Guard provocations in the South China Sea or Wagner Group/Africa Corps deployments; and economic coercion and lawfare.

Types of Gray Zone Crises

The many different types of gray zone attacks addressed in this playbook all share a defining characteristic: they are designed to maintain plausible deniability.

- **Infrastructure Destruction:** This includes physical attacks on energy grids, undersea cables, pipelines, or transportation networks. Russia's Baltic Sea shadow-fleet campaign (2022 to present) has damaged Nord Stream pipelines, the Estlink 2 power cable, and at least eleven undersea telecom cables. China has severed cables connecting Taiwan's Matsu Islands on multiple occasions since 2023.

- **Industrial Sabotage:** This includes arson, explosives, and supply-chain disruption targeting defense-industrial facilities, logistics hubs, and commercial enterprises. The International Center for Counterterrorism and GLOBSEC document 151 confirmed Russian-directed industrial sabotage incidents in Europe between February 2022 and February 2026.

- **Targeted Violence:** This includes state-sponsored attacks on individuals, sometimes via criminal proxies using encrypted platforms. Russia deploys locally recruited criminals across Europe; Iran relies on drug trafficking networks and organized crime. Iranian-directed plots to assassinate U.S. officials have been documented on U.S. soil.

- **Drone Harassment:** This includes drone operations targeting airports, military installations, government facilities, and urban centers to probe defenses, erode public confidence, and impose financial costs. Russian-linked drones have forced repeated airport closures across Europe and even penetrated Estonian and Polish airspace in September 2025. China has used drones systematically against Taiwan's outlying islands since 2022, escalating to military-grade unmanned aerial vehicles (UAVs) in 2026. This is the fastest-growing gray zone modality and the one most likely to evolve into a low-level conventional attack.

1.2 Anticipating and Preparing for Potential Crises

The U.S. government and its allies should maintain a posture of awareness and deterrence before any specific attack or campaign has been launched or detected. Maintaining that posture, which can significantly expand the range of available options in a crisis, requires intelligence collection, infrastructure hardening, response-protocol development, and allied coordination.

Essential Information for Pre-Crisis Planning

Geographic scope and targeted infrastructure	Where is an attack likely to take place, and which targets are most at risk?
Attribution, proxies, and intermediaries	Which state will likely initiate a gray zone attack, and what is the degree of confidence in that assessment? Would they act directly, or through proxies or criminal intermediaries?
Attack vector and modality	What form would an attack take? Are there diplomatic events or military exercises that could prompt a gray zone attack?
Threatened interests	Would U.S. military installations, embassies, commercial assets, or treaty allies be threatened? Are any particularly vulnerable?
Warning indicators	Are there indications that a gray zone attack is likely? Have unusual vessels been active near undersea infrastructure, or drones near military sites or airports? Have criminal networks changed their recruitment patterns? Have there been upticks in hostile intelligence officers near NATO facilities?

Key Concept: The Campaign Recognition Problem

The ambiguity that defines gray zone attacks creates two distinct analytical problems that planners need to work through sequentially—and quickly.

Problem 1: Recognizing the campaign. Individual gray zone incidents are varied in method and timing and calibrated to fall below any single response threshold. Each incident, viewed in isolation, may appear to be crime, accident, or coincidence; the pattern that reveals a coordinated campaign only becomes visible in retrospect. Per Lindsey Sheppard and Matthew Conklin, two specific challenges compound this problem:

- **Frequency of attacks:** Attacks unfold over months or years, preventing any single incident from crossing the formal response threshold. No one incident looks like a campaign.
- **Intent:** Even when a pattern is noticed, determining whether it reflects deliberate state direction versus opportunistic or criminal activity requires analysis that goes well beyond what any single incident can support.

Problem 2: Attributing the campaign to a state actor. Once a campaign is recognized, a separate and equally difficult problem begins: identifying which state is responsible. Gray zone attacks are specifically engineered to obfuscate provenance, for example by routing through criminal proxies, civilian vessels, unregistered drones, and encrypted platforms. Attribution requires sustained, collaborative analysis and often yields only probabilistic conclusions.

The practical consequences: These problems need to be dealt with sequentially, with compounding time costs. Recognition typically arrives late, and attribution still later. By the time a campaign is both recognized and attributed with sufficient confidence, the attacker has often already achieved significant strategic effect.

That carries practical implications for planners: the goal of intelligence-collecting should not just be "what happened?" but "does this pattern match known gray zone campaign signatures?" And separately, "what additional collection is needed to attribute this to a specific state actor?" Pre-crisis monitoring needs to be active, not passive, and interagency coordination to recognize patterns needs to be a standing task, not an ad hoc response.

1.3 Assessing Crisis Situations

When Does a Gray Zone Attack Become a Crisis for the United States?

No red line automatically determines when a gray zone attack becomes a crisis. NATO policy holds that a hybrid attack can reach the level of an armed attack triggering Article 5, but that it is a political decision

every time, first on the part of a nation and then its NATO allies. The ODNI IC Gray Zone Lexicon (July 2024) identifies campaign-level factors of gray zone attacks, but no single incident threshold.

This can be understood through the concept of the uncertain-onset problem. Crisis onset in gray zone attacks is rarely a discrete, identifiable moment. Because recognition and attribution are sequential problems, no single actor is positioned to declare that an attack has taken place or by whom until well after the optimal window to respond has closed. Accordingly, a crisis is typically declared retrospectively rather than recognized in real time. Three implications follow for planners:

- Gray zone campaigns exploit the gap between detection and attribution.
- Attribution thresholds should be established in advance, defining when a high probability of deliberate state action is sufficient to trigger each response option, rather than awaiting legal-standard proof.
- Response options should be designed to be reversible where possible, enabling early action before certainty is achieved.

Once attributed, the gray zone campaign types in this playbook—infrastructure destruction, industrial sabotage, targeted violence, and drone harassment—are more likely to approach the legal threshold of "armed attack" under international law than cyber operations or disinformation campaigns. Under the Geneva Conventions and their Additional Protocols, which constitute the body of international humanitarian law, whether a situation amounts to armed conflict is determined by facts on the ground, not political labels. Physical destruction of critical infrastructure, targeted assassinations, and drone violations of national airspace each engage those criteria more directly than non-physical operations, though none automatically crosses the threshold for response without a political determination by the affected state and, where applicable, its allies.

Whether a gray zone campaign should be considered a background concern or a political crisis requiring a U.S. response hinges on the answers to certain critical questions.

Essential Information for Crisis Response Determination and Planning

Scale and simultaneity	Have multiple allied states been attacked simultaneously? Has a single attack crossed a state's declared threshold? (Norway, for example, has stated publicly that an attack on its critical

	infrastructure can be considered an armed attack, triggering Article 4 or 5 consultation.)
Target significance and U.S. equities	Have attacks targeted infrastructure with direct consequences for the U.S. military (bases, logistics chains, undersea command and communications); U.S. embassy compounds or diplomatic facilities; treaty allies' defense infrastructure; or U.S.-affiliated commercial entities?
Attribution confidence	What is the United States' level of confidence in its determination of the perpetrator? Attribution is itself a political crisis trigger: once attributed to a state with high confidence, the political calculus shifts from law enforcement to strategic response.
Cumulative effect	Have repeated sub-threshold actions eroded infrastructure, degraded deterrence credibility, and/or shifted the strategic balance in ways that collectively constitute a crisis?
Allied invocation	Has a U.S. ally invoked Article 4 or signaled Article 5 consideration? If so, the United States faces a political decision regardless of the technical threshold. Allied disagreement over how to respond is itself a gray zone success for the attacker.

2.0 Assessment of U.S. Interests

U.S. policy planners should weigh the strategic interests threatened and proximate challenges posed by gray zone attacks abroad to guide policy design and resource allocation. The following immediate concerns, broader strategic stakes, and timing factors should inform the U.S. response.

2.1 Proximate U.S. Concerns

- Ensuring the safety and security of U.S. diplomatic personnel, military forces, and private citizens abroad. Arson and targeted violence can directly endanger Americans; drone operations have targeted facilities near U.S. military installations.

- Protecting U.S. military installations, embassy compounds, and equipment located on allied facilities.
- Upholding U.S. treaty commitments (Article 5, bilateral defense treaties) and the broader credibility of U.S. security guarantees.
- Securing U.S. commercial interests that rely on the targeted ally's infrastructure, financial networks, or logistics chains. Gray zone attacks increasingly target private-sector U.S. defense production supply chains.
- Preventing spillover onto U.S. territory: the 2024 parcel bomb plot routed through U.S. cargo channels; Iranian-directed assassination plots have used criminal proxies recruited on U.S. soil.

2.2 Strategic Interests at Risk

- **Alliance cohesion and credibility:** The September 2025 Russian incursions into NATO airspace, in which frontline states shot down Russian drones while the United States signaled ambiguity about Russian intent, illustrate the fracture risk. The attacker's goals advance with every unanswered incident and every allied disagreement.
- **Critical infrastructure interdependence:** Damage to undersea cables, energy pipelines, and logistics networks cascades for both governments and the private sector. The private sector owns most of the at-risk critical infrastructure and should be integrated into resilience planning.
- **Norms, escalation dynamics, and trade-offs:** A lack of response can erode norms; over-response risks unintended escalation. CFR's Liana Fix assesses that Russia may step beyond the gray zone toward low-level conventional provocations, using drones against civilian targets to demonstrate the U.S. security guarantee is hollow.
- **Intelligence equities and trade-offs:** Publicly attributing attacks may protect allies but compromise intelligence sources. Establishing tier-based declassification protocols, in which more sensitive sources can be protected, resolves this trade-off in advance.

2.3 Decision Timeline: Essential Tasks

Once a gray zone attack or campaign is suspected, the following timeline structures the essential response tasks. It is designed as a decision checklist, not a rigid sequence—some tasks will overlap, and the pace will

be driven by the nature and scale of the attack. The intent is to ensure that no essential step is skipped under pressure.

- **0 to 24 Hours:** The National Security Council staff should establish an interagency crisis task force and designate the lead U.S. government agency based on the nature of the attack (for example, the FBI would take point on targeted violence against U.S. interests abroad from criminal proxies). This interagency task force should compile confirmed facts about the attack or campaign and identify what essential information is unknown and required by decision-makers. The interagency task force should then coordinate internal guidance on public communications before the source of the attack is attributed. The lead agency should notify relevant congressional committees depending on the target and nature of the attack and any statutory requirements that might apply. Similarly, the U.S. embassy or mission in the affected country should be alerted.

- **24 to 72 Hours:** The interagency task force should begin pattern analysis, identifying all incidents in the preceding twelve to twenty-four months that could be linked by target type, geography, or adversary signature. Meanwhile, the lead agency, State Department, and intelligence community should coordinate with counterparts in the targeted country and relevant allies to share preliminary assessments. The lead agency should contact the relevant private-sector parties if the attack affects U.S. commercial assets.

- **72 Hours to 30 Days:** The interagency task force should develop a package of information establishing at the appropriate confidence level the attack's attribution, while the State Department should work with allies on a coordinated attribution posture. Intelligence that supports the attribution should then be released per the established declassification protocols. The NSC staff and lead agency should then assess policy options based upon the available attribution, political will, and available tools. Congressional leadership should be kept abreast of those developments.

- **30+ Days:** The lead agency should execute the selected policy option and establish mechanisms to monitor and adjust it as needed. At the same time, the State Department should convene U.S. allies to coordinate complementary action and establish longer-term mechanisms, if needed. That may entail engaging multilateral frameworks (e.g., NATO Article 4, EU hybrid threat mechanisms, and the UN

Security Council) as warranted. Finally, the NSC should review and update gray zone attack protocols based on lessons from the onset phase.

Special Considerations

Gray zone attacks present distinctive timeline challenges: individual attacks may remain ambiguous for weeks or months, yet the deterrent signaling window can close rapidly if the attacker interprets U.S. silence as acquiescence.

- **Campaign recognition lag:** Gray zone attacks are designed to look like unrelated incidents, and investigating the source of infrastructure damage can take weeks or months. The window to respond may close before attribution is complete: by the time a campaign is formally recognized and attributed, the attacker may have already achieved significant aims and established a pattern of nonresponse.
- **Partner stabilization timelines:** Allied governments and private sector infrastructure owners face immediate domestic pressure to act, often within days of a high-profile attack. The United States needs to be prepared to provide visible diplomatic support and public solidarity before attribution is complete, or risk the perception that Washington is disengaged, which can itself fracture allied cohesion.
- **Deterrence window:** The speed of the U.S. and allied response itself communicates the credibility of deterrence separate from the substance of that response. NATO's launch of Baltic Sentry in January 2025, which monitors ships in the Baltic Sea to protect undersea cables, was successful because it signaled that the alliance was watching and prepared to act. Visible deterrence can thus be effective, even without concrete attribution.
- **Congressional notification:** Security assistance mobilization, intelligence community tasking, and covert action findings all require notifying Congress, which needs to be factored into planning timelines. Planners should identify in advance which response actions will require notification, to which committees, and under what timeline, so that legal obligations do not delay the operational response.

3.0 Policy Formulation

3.1 Relevant Policy, Operational, and Legal Guidance

U.S. responses to gray zone attacks abroad need to be situated within existing legal authorities, treaty commitments, and current strategies and other policy guidance. These frameworks both enable and guide the range of available response options. Understanding which authorities apply, and where gaps exist, is essential to identifying what the U.S. government can do quickly, what requires advance preparation, and what may require new legislative or executive action. These are the key frameworks:

- **National Security Strategy (NSS) and National Defense Strategy (NDS):** Each administration's NSS indicates, implicitly and explicitly, its view of U.S. national security interests and the priority assigned to gray zone threats. Planners should assess each NSS/NDS upon publication for guidance gaps relevant to gray zone response, as these have historically been inconsistent from one administration to the next.
- **Agency Strategic Plans:** State, DOD, Treasury, and the Department of Homeland Security (DHS) all have strategic plans that provide the operating framework for each agency's operational considerations in gray zone response. Planners should identify gaps between current plans and the gray zone response requirements described in this playbook.
- **Statutory Authorities:** Six laws are particularly relevant for guiding gray zone responses: the War Powers Resolution (which requires a forty-eight-hour notification for armed forces in combat situations); Title 10 Section 127e (which directs special operations forces support to partner forces); Title 10 Section 333 (enabling capacity-building activities); PPD-21 (which guides critical infrastructure security); and the Leahy Law (22 USC Section 2378d governing security assistance). Gray zone response can span both Title 10 (covering military authorities) and Title 50 (governing intelligence and covert action), which can create interagency friction when the nature of the attack makes the lead agency unclear—an ambiguity adversaries may deliberately pursue.
- **Treaties and Guidance:** The following treaty frameworks and operational guidance documents are directly relevant to gray zone response planning:
    - **Europe and NATO:** NATO Article 5 (which provides for collective defense) and Article 4 (which provides for consultations with allies over security threats) provide the primary alliance framework.

NATO policy holds that a hybrid attack can trigger Article 5, a political determination by allies, not an automatic legal trigger.

- **Indo-Pacific:** The U.S.-Japan Treaty of Mutual Cooperation and Security (which contains Article 5 obligations regarding the Senkaku/Diaoyu Islands), the U.S.-Philippines Mutual Defense Treaty (invoked in discussions of Chinese Coast Guard harassment), and the AUKUS security partnership (formed between the United States, Australia, and the United Kingdom) each provide frameworks applicable to gray zone scenarios.
- **Current operational guidance:** The United States is engaged in several ongoing gray zone responses, which informs its policy. The NIC Gray Zone Assessment; NATO's operation Baltic Sentry; and the EU's Action Plans on Cable Security and Drone/Counter-Drone Security, to name a few. Planners should audit applicable National Security Memoranda for current administration revisions to critical infrastructure and counterintelligence directives.

3.2 Policy Framework and Parameters

Before selecting a response orientation, planners should resolve the following strategic decision points. Working through them in order will help avoid premature commitment to a course of action before the key variables are understood:

- Will this attack (or attack pattern) directly affect U.S. economic, military, diplomatic, or security interests? What is the confidence level in that assessment?
- Does sufficient attribution confidence exist for public or coordinated allied statements, or only quiet bilateral communication? Has a campaign-level assessment been made?
- Should the United States encourage and assist the affected ally to take the public lead, with the United States in a quieter supporting role, or should Washington lead public response?
- Are private-sector owners and operators of affected infrastructure engaged? What voluntary information-sharing mechanisms are available? Are any legally mandated?
- Should the United States seek to limit the external enablement of the campaign, such as by exposing shadow fleet operations or disrupting the recruitment of proxies?

- Should the United States request action by multilateral bodies, through NATO Article 4, EU hybrid threat mechanisms, or the UN Security Council?

3.3 Broad Strategic Options

Four strategic orientations are available both during a crisis and after. All four options should be considered against the full spectrum of diplomatic, informational, military, and economic instruments.

Policy Options: Strategic Orientations

Monitor	**Posture:** The United States actively collects intelligence and monitors developments, preserving flexibility and avoiding decisive action until the nature and source of the attacks are clearer. **Driving assumptions:** This orientation assumes that the stakes are relatively low for the United States, that attribution is uncertain, and that the gray zone attack's goals are also unknown. **Theory of change:** A cautious approach preserves flexibility and avoids premature overcommitment under high uncertainty; it positions the United States for more effective intervention when attribution becomes clear. **Trade-offs and risks:** Perceived hesitance on the United States' part could signal acquiescence; an inability to recognize the campaign in a timely fashion could limit U.S. options for effective deterrence. **Attribution required:** Low-to-medium (circumstantial indicators sufficient to begin collecting intelligence). **Primary tools:** Intelligence collection; interagency pattern analysis; quiet diplomatic signaling; private-sector threat briefings. **Lead agency:** NSC for policy oversight; ODNI for intelligence integration across the intelligence community; Cybersecurity and Infrastructure Security Agency (CISA) for private-sector engagement.

Contain	**Posture:** The United States hardens targets, disrupts proxy networks, shares intelligence with allies, and engages neighboring states—but does not publicly attribute the attack. **Driving assumptions:** This orientation assumes that the stakes are relatively low for the United States, that attribution is uncertain, and that allied and private-sector resilience need to be strengthened before adopting a more assertive posture. **Theory of change:** Containing the damage of the gray zone attack reduces the attacker's chances of success, raising costs without triggering escalation and buying time for a coordinated response. **Trade-offs and risks:** The attacker could adapt faster than defenses harden; a lack of public attribution will undermine the efficacy of deterrence. **Attribution required:** Medium (sufficient to identify infrastructure targets and proxy networks). **Primary tools:** Security assistance; intelligence sharing; target hardening; proxy network disruption; private-sector resilience programs. **Lead agency:** State for diplomatic efforts; DOD for security assistance; DOJ/FBI for proxy disruption; and DHS/CISA for infrastructure protection.

Deter and Respond	**Posture:** The United States attributes the attacks to a state and raises costs by coordinating that public attribution with allies, applying targeted sanctions, adjusting posture to appropriate levels, and providing security assistance. Ideally, those actions restore deterrence. **Driving assumptions:** This orientation assumes that the stakes are moderate or high for the United States; that there is sufficient confidence in attribution, and that effective tools are available and U.S. partners are willing. **Theory of change:** By raising the costs for the attacker, the United States re-establishes deterrence and reduces the probability of further escalation. **Trade-offs and risks:** Public attribution may accelerate escalation rather than deterring the attacker. The requisite coalition-building also takes time, potentially compromising an effective response. **Attribution required:** High-confidence intelligence community assessment of deliberate state action, but not a legal-standard proof. **Primary tools:** Coordinated attribution; sanctions on specially designated nationals (SDN); expulsions of the attacker's intelligence officials; military posture signaling; security assistance; DOJ prosecutions; public messaging campaign. **Lead agency:** State for diplomatic efforts; Treasury for sanctions; DOD for security assistance and posture; NSC for coordination.

Transform	**Posture:** The United States degrades the gray zone campaign's infrastructure, restructures alliance posture, and presses for diplomatic agreements. This orientation is the most resource-intensive and requires sustained political will. **Driving assumptions:** This orientation assumes that the stakes are high for the United States; that confidence in attribution is high; that political will is strong enough for a firm response; and that deterrence alone is insufficient. **Theory of change:** Comprehensively imposing high costs, combined with alliance restructuring, degrades the attacker's capacity and willingness to conduct gray zone campaigns. **Trade-offs and risks:** A transformative orientation carries a high risk of escalation; costs significant resources and political capital; and requires sustained commitment beyond the immediate political window. **Attribution required:** Very high; intelligence needs to support the attribution of a sustained gray zone campaign and/or proxy network. **Primary tools:** Comprehensive sanctions; disruption operations against proxy networks; alliance restructuring; diplomatic agreements; congressional engagement for sustained authorities. **Lead agency:** NSC for sustained oversight; State for diplomatic efforts; Treasury; DOD; intelligence community for covert actions.

3.4 Tools and Resources

An integrated gray zone response should employ civilian tools alongside security tools in a comprehensive response—including diplomacy and public messaging, intelligence and military options, economic incentives, law enforcement support, and congressional involvement.

Diplomatic

- **Public and private attribution statements:** Demarches to the initiating state; expulsion of its intelligence officers; coalition-building through NATO, the European Union (EU), and the Group of Seven (G7).

- **Multilateral forums:** UN Security Council, Organization for Security and Cooperation in Europe, and the International Maritime Organization for maritime incidents. Each public attribution contributes to a compounding record that makes future deniability harder to sustain.

- **Carrots alongside sticks:** Diplomatic engagement offering de-escalation incentives (such as a suspension of sanctions pressure, trade concessions, or security dialogue) may reduce the attacker's strategic incentive to continue the campaign. Quiet backchannel communication with aggressors about red lines has demonstrably deterred follow-on attacks in the past.

- **Public messaging and counternarrative:** Proactive allied communications, including declassified threat briefings to journalists and civil society and named intelligence community statements (as CIA and MI6 chiefs made in September 2024, in which they attributed a European sabotage campaign to Russia), erode the attacker's ability to deny the attribution. As presidential administrations reshape the organizations and resources available for this purpose, planners should identify the current lead for counternarrative programming in allied communications coordination.

Intelligence and Military

- **Intelligence, surveillance, and reconnaissance (ISR) and detection:** ISR deployment; Automatic Identification System (AIS) tracking of ships; commercial satellite imagery; artificial intelligence–assisted anomaly detection for drone and vessel activity. The complex network of assets in the Baltic Sea region designed to detect threats to undersea infrastructure, known as Baltic Sentry, is the current gold standard.

- **Intelligence sharing and declassification:** Pre-authorized tier-based declassification protocols, building on the Ukraine pre-invasion model, enable rapid intelligence sharing among allies without improvising under crisis pressure.

- **Security assistance:** Foreign military financing, foreign military sales, international military education and training, and excess defense articles (which transfer excess equipment to allies) can help harden the targeted ally's infrastructure; training allied law enforcement and deploying special operations advisors under applicable Title 10 authorities.

- **Military presence signaling:** Force posture adjustments have demonstrable deterrence value; for example, the naval deployment in Baltic Sentry has reduced subsequent cable incidents.
- **Counter-drone tools:** The provision of counter-drone systems to allied forces, such as the Multi-Mission Effects Remote Operations System (MEROPS) model for NATO's eastern flank or Danish jamming and tracking systems; support for allied Drone Wall architecture; and low-cost interceptor drone programs based on the Ukrainian first person view (FPV) model are all effective tools. Granting allies the legal authority to shoot down drones and using artificial intelligence–assisted detection and classification systems can further harden the targets of gray zone attacks.
- **Covert response options:** Title 50 covert action authorities provide options for disrupting proxy recruitment networks, interfering with gray zone campaign logistics, and imposing costs on the directing state without public attribution. Covert action findings require congressional notification for each applicable statute. These options should be developed in advance as part of pre-crisis planning.
- **AI-assisted detection and analysis:** AI tools applied to open-source data, including AIS vessel tracking, drone incident reporting, commercial satellite imagery, and social media recruitment pattern analysis, can dramatically accelerate campaign recognition, addressing the temporality and attribution detection problems identified in Section 1.2.

Economic

- **Targeted Specially Designated National (SDN) sanctions:** Economic tools against individuals, entities, and shadow-fleet vessels should be the first resort in the civilian tool kit, imposing costs without the escalatory signaling of military action. Sanctions can be calibrated to attribution confidence levels.
- **Secondary sanctions:** Pressure on third-party flag states and insurers complicit in shadow-fleet or drone supply operations can raise costs for the attacker. The Countering America's Adversaries Through Sanctions Act, Protecting Europe's Energy Security Act, and related legislation provide relevant legal authorities.
- **Financial intelligence sharing:** Treasury/Financial Crimes Enforcement Network coordination with allied financial intelligence units can track proxy network financing.
- **Economic incentives and carrots:** Export control waivers, trade facilitation, or economic assistance packages can all reward de-escalation. The Committee on Foreign Investment in the United States and allied investment-protection frameworks can be used as both sticks and carrots. Private-sector

engagement through CISA-led sector risk management frameworks enables coordinated resilience investments and threat-intelligence sharing.

Law Enforcement and Legal

- **FBI/DOJ prosecution of U.S. incidents:** Conspiracy, material support, and Foreign Agents Registration Act (FARA) violations can all be pursued. The United States can use Mutual Legal Assistance Treaty (MLAT) for evidence-sharing, INTERPOL red notices, and Europol/Eurojust coordination to disrupt cross-border proxy networks.

- **Designation authorities:** Foreign terrorist organization and SDN designations of proxy networks, as well as DOJ prosecution of material support violations, reduce the attacker's recruitment pool.

- **Legal ambiguity concerns around the targeting of undersea cables:** Although the UN Convention on the Law of the Sea only provides enforcement jurisdiction within a state's exclusive economic zone, Jennifer Counter and Amy Paik propose shared jurisdiction is an achievable reform. Interim workarounds include environmental enforcement, Safety of Life at Sea safety authorities, and port state control.

- **Counter-drone legal frameworks:** Domestic legal authority to shoot down or jam drones in noncombat environments remains unsettled in most NATO allies. U.S. assistance to allies in developing appropriate legal frameworks, including rules of engagement for counter-drone operations near civilian infrastructure, is a concrete near-term tool.

Congressional

- **Security assistance authorities:** Foreign military financing, foreign military sales, international military education and training, and excess defense articles all provide congressional authority for security assistance; sanctions legislation and special appropriations for gray zone response programs can also help.

- **Statutory notifications:** Gray zone responses will likely require war powers notifications; covert action findings to Gang of Eight; intelligence community oversight by the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence; diplomatic authorities from the Senate Foreign Relations Committee and House Foreign Affairs Committee; and security assistance from the Senate Armed Services Committee and House Armed Services Committee.

- **Legislative and oversight tools:** When carefully used, congressional oversight hearings on gray zone threats can amplify attribution, raise public salience, and signal bipartisan resolve to the initiating state.

On legislation, planners may need to consider the status of pending bills addressing specific gray zone vulnerabilities, such as those targeting undersea cable protection and counter-drone authorities. Where such legislation is enacted, it expands the available tool kit, and where it is pending, it may signal political will without yet providing legal authority.

3.5 Stakeholders and Partners

Gray zone response requires whole-of-government coordination. The following U.S. government stakeholders have distinct roles.

U.S. Government Stakeholders

Agency / Actor	Role and Equities in Gray Zone Crisis Response
NSC / Executive Office	Coordinates policy via Deputies and Principals Committees. Determines the lead agency based on the nature of the attack. Maintains pre-established declassification and response protocols.
Department of State	Leads on diplomatic tools and multilateral coordination through relevant bureaus (for example, the Bureau of European and Eurasian Affairs or the Bureau of Intelligence and Research). Serves as the lead agency for Deter, Respond, and Transform orientations.
Department of Defense / Joint Staff / Combatant Commands (COCOMs)	Directs military and security assistance through regional combatant commands (for example, the U.S. European Command); U.S. Special Operations Command; the Defense Intelligence Agency; and legal authorities provided by the undersecretary of defense for policy.
Intelligence Community (ODNI/CIA/NSA/DIA)	Leads on determining attribution, covert action authorities, and allied intelligence sharing. Intelligence community–wide integration of threat information to enable campaign recognition.

Department of the Treasury (OFAC/FinCEN)	Designs and implements sanctions and coordinates financial intelligence sharing with allied counterparts. The Office of Foreign Assets Control maintains the SDN list.
Department of Justice / FBI	Handles U.S.-nexus prosecutions, counterintelligence, Mutual Legal Assistance Treaty coordination, and FARA enforcement; and serves as liaison with allied law enforcement.
DHS (CISA / Coast Guard)	CISA protects critical infrastructure, manages sector risk, and engages with the private sector. The Coast Guard enforces maritime security and enacts shadow-fleet policy in U.S. waters.
Department of Energy (Office of Cybersecurity, Energy Security, and Emergency Response)	Oversees energy infrastructure protection, bilateral technical assistance to allied energy ministries, and forensic support for infrastructure attack analysis.
Department of Commerce / U.S. Trade Representative (USTR)	Bureau of Industry and Security enforces export controls. USTR uses trade leverage to impose economic costs or incentives.
Congressional Committees	Senate and House Armed Services Committees provide defense authorization; Senate Foreign Relations and House Foreign Affairs Committees manage foreign policy; Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence oversee the intelligence community; Senate Banking and House Financial Services Committees direct sanctions; and Appropriations Committees deploy supplemental funding.

Non-U.S. Stakeholders and Partners

- NATO: Collective defense consultations; Maritime Command; Baltic Sentry model; Article 4 consultation mechanism; and counter-drone architecture.
- European Union: Action Plans on Cable Security and Drone/Counter-Drone Security; Critical Entities Resilience Group; European External Action Service diplomatic coordination; and EU sanctions coordination.
- Indo-Pacific Partners: Quad members (United States, Australia, India, and Japan); bilateral partners (Philippines, South Korea, Taiwan counterparts via American Institute in Taiwan).
- Private-Sector and Critical Infrastructure Operators: Undersea cable operators; energy infrastructure owners; defense contractors; financial institutions; logistics companies.
- Five Eyes Partners: Primary intelligence-sharing mechanism for attribution coordination.

Illustrative Tasking Requests

- **Intelligence Community:** All-source assessment of the initiating state's gray zone doctrine, recent operational patterns, and proxy recruitment structures. Explicitly ask, "Does this incident match the pattern of known gray zone campaigns?"
- **DHS/CISA/DOT/DOE:** Assess the vulnerability and redundancy of U.S. and allied critical infrastructure, and identify existing bilateral information-sharing protocols and gaps. Engage relevant private-sector owners and operators.
- **Embassies/Missions:** Report on host-government threat assessments, domestic political tolerance for attribution, and allied law enforcement investigative capacity. Flag any targeting of embassy compounds or U.S.-affiliated commercial facilities.
- **Partners/Allies:** Share national threat assessments, vessel tracking data, drone incident reports, and forensic findings from prior incidents. The Nordic-Baltic model for pre-established intelligence-sharing is the benchmark.

4.0 Implementation and Operational Considerations

4.1 Operational Design

The following questions are organized as a decision checklist for practitioners operating under time pressure. The sequence reflects the rough order in which these decisions typically arise, though in practice several may need to be addressed simultaneously.

Answering Key Questions

Operational Question	Considerations and Immediate Actions
How is U.S. policy codified and communicated?	Determine whether an executive order, national security memorandum, or interagency policy directive is appropriate. The level of codification signals commitment to allies and sets the legal basis for resource mobilization.
Who leads and integrates implementation?	NSC retains close policy oversight; operational lead rotates to State, DOD, Treasury, or DHS depending on the type of attack.
What structures foster coordinated interagency implementation?	A rapidly activatable interagency task force may be appropriate for sustained campaigns. Pre-designate the structure; do not build it in crisis.
Will the U.S. military designate a named operation?	For security assistance–heavy responses or special forces advise-and-assist deployments, a named operation provides clarity of command and a structure for congressional notification.
What embassy and in-theater roles are needed?	The U.S. embassy is the primary in-country platform; the ambassador should coordinate with the host government. The relevant Combatant Command provides military operational oversight.

What steps are needed with Congress?	Security assistance mobilization, intelligence community tasking, and covert action findings trigger statutory notification requirements. Supplemental appropriations may be needed for sustained campaigns.

4.2 Coalitions and Partners

Gray zone response is inherently multilateral. The Center for Strategic and International Studies' brief "Partners, Not Proxies" identifies five structural considerations in coalition management that adversaries deliberately design campaigns to exploit:

- **Partners misidentified as proxies:** When the United States treats allies as implementers of U.S. strategy rather than as co-designers of a shared response, partners resist, act independently, or disengage. Effective coalition management requires treating allied governments as genuine partners with their own equities, capabilities, and domestic political constraints.
- **Civilian tools subordinated to military ones:** Gray zone campaigns operate across economic, legal, informational, and criminal domains. Defaulting to military signaling leaves the most effective civilian tools—sanctions, law enforcement coordination, and counternarrative programs—underutilized and nonmilitary attack and response vectors unaddressed.
- **Alliance coherence concerns:** The primary goal of some gray zone campaigns is to undermine alliance coherence by provoking divergent responses from different allied states. Adversaries calibrate attacks to expose differences in allied risk tolerance, legal standards, and political constraints. The September 2025 NATO split response on Russian airspace incursions illustrates how a single incident can fracture alliance solidarity without crossing any formal threshold.
- **Attribution consensus gaps:** Allied governments operate under different legal standards, evidentiary requirements, and domestic political constraints for public attribution. Without pre-negotiated attribution protocols, each incident triggers a new negotiation that delays coordinated response and allows the attacker extended diplomatic maneuvering room.
- **Burden-sharing asymmetry:** Frontline allies, particularly Baltic states, Poland, and Nordic NATO members, face disproportionate exposure to gray zone attacks but often have limited response

capacity. An effective coalition framework includes targeted security assistance and capacity-building to reduce this asymmetry and prevent smaller allies from becoming the weakest links.

Current operational models address those structural considerations directly. Baltic Sentry, a joint multinational patrol with pre-authorized rules of engagement, seabed-to-space sensors, and real-time allied intelligence-sharing is the benchmark. For drone harassment, the EU Drone Wall initiative and NATO Counter-UAS Week represent the emerging multilateral architecture. Private-sector partners, including undersea cable operators, energy companies, defense contractors, and financial institutions, need to be engaged in steady-state planning and resilience investments. For case studies illustrating these structural considerations in practice, see Appendix A; for the underlying research, see Appendix C.

4.3 Strategic Communications

Strategic communications are a critical and often underutilized component of effective gray zone response. Because gray zone attacks are designed to exploit ambiguity and erode public confidence, the United States and its allies need to treat communications as an instrument of deterrence in its own right. The following protocols establish the framework for doing so.

- **Pre-authorized declassification:** Developing standing tier-based declassification protocols is a pre-crisis task that requires sustained bureaucratic effort and senior-level commitment. Agencies are reluctant to pre-authorize the release of sensitive intelligence, and the interagency process for doing so can be slow. The Ukraine pre-invasion model in early 2022 demonstrates that such declassification is possible when there is political will, but planners should not assume this capacity exists without deliberate investment. Building these protocols before crisis onset is essential; attempting to negotiate them under pressure can be far less effective.

- **The Salisbury model:** When Sergei and Yulia Skripal were poisoned with the nerve agent Novichok in 2018, UK authorities took just nine days from the attack to publicly attribute Russia. More than twenty-five states conducted coordinated diplomatic expulsions within weeks. The successful "Salisbury model" entailed rapid forensic identification, UK-led attribution validated by allied intelligence services, and coordinated expulsions without a formal NATO or EU triggering mechanism. See Appendix A.

- **Proactive proxy exposure:** Publicly documenting criminal recruitment networks, naming shadow-fleet vessels, and providing journalists and civil society with declassified threat data help contain the

attacker's operation. Each disclosure contributes to the compounding record and makes future deniability progressively harder to sustain.

- **Counter-drone messaging:** Publicly naming the responsible actors, including their drone model, launch point, and mission profile, provides a deterrence signal distinct from other gray zone attribution. Japan's public announcement of shoot-down authority in June 2025 and Taiwan's immediate response to the 2022 Kinmen drone intrusion demonstrate that publicly setting response thresholds, when credible and enforced, has direct deterrence value.

Appendixes

Appendix A: Case Studies

Illustrative Case Studies

Baltic Sea Undersea Cable Campaign *Russia, 2022 to present; Infrastructure Destruction*	**What happened:** Shadow-fleet ships dragged anchors on the seabed to sever the Nord Stream pipeline (September 2022), the Balticconnector pipeline (October 2023), and multiple Baltic data cables and Estlink 2 (November to December 2024). *Eagle S,* a Russian shadow-fleet tanker that had been involved in such an incident, was seized by Finnish Coast Guard in December 2024. NATO Baltic Sentry launched in January 2025. **Key lesson:** Pre-established protocols matter more than response capability. Baltic Sentry demonstrably reduced subsequent incidents. **Source reading:** Braw, Atlantic Council (November 2025); Counter and Paik, Atlantic Council (January 2024)

Salisbury Novichok Poisonings *Russia/GRU, 2018; Targeted Violence*	**What happened:** Russian agents poisoned Sergei and Yulia Skripal with Novichok; one civilian died. The United Kingdom attributed publicly in nine days; more than twenty-five allied states coordinated the largest intelligence officer expulsion since the Cold War. **Key lesson:** Rapid attribution speed is strategically significant. Multilateral coordination without a formal treaty trigger is achievable. Structural follow-through is required for lasting deterrence. **Source reading:** UK House of Commons Defence Select Committee (July 2025)
Taiwan Drone Harassment, Kinmen Islands *China, 2022 to present; Drone Harassment*	**What happened:** Following U.S. Speaker of the House Nancy Pelosi's 2022 Taiwan visit, civilian drones appeared over Kinmen Island. Taiwan shot one down on September 1, and incidents largely ceased. China escalated to military-grade drones in 2026. Japan scrambled fighters twenty-three times in twelve months to intercept Chinese drones. **Key lesson:** Clear public threshold-setting and immediate enforcement has direct deterrence value. Counter-drone legal clarity must precede crisis onset. **Source reading:** 9dashline, "Grey-zone drones" (April 2026)

Iran, European Proxy Violence Networks *2022 to present; Targeted Violence / Industrial Sabotage*	**What happened:** Iranian Revolutionary Guards Corps (IRGC)–linked operators working through drug trafficking and organized crime conducted surveillance, intimidation, and violence across France, Germany, the Netherlands, Sweden, and the United Kingdom. The DOJ documented IRGC assassination plots against U.S. officials on U.S. soil. Following the 2026 Iran war, a new proxy group, HAYI, began operating in Europe, and teenagers were recruited via Snapchat for a bombing attempt in Paris. **Key lesson:** Proxy recruitment models are evolving faster than current frameworks track. Iranian and Russian templates are converging. **Source reading:** ICCT/GLOBSEC (February 2026); DOJ indictments 2022 to 2024
Russia, European Arson/Sabotage Network *GRU, 2022 to present; Industrial Sabotage*	**What happened:** 151 confirmed Russian-directed incidents took place in Europe from February 2022 through February 2026. Criminal proxies were recruited via Telegram for payments as low as 10,000 euros. The first Eurojust prosecutions took place in January 2026 with convictions in Romania and Czech Republic. **Key lesson:** Prosecution has some deterrent effect at the proxy level but is insufficient without network-level disruption. **Source reading:** Jones, CSIS (March 2025); ICCT/GLOBSEC (February 2026)

IRGC/Hezbollah Latin American Networks *Ongoing; Targeted Violence / Proxy Infrastructure*	**What happened:** IRGC-Quds Force and Hezbollah networks in Bolivia, Ecuador, and Venezuela provide logistics and safe passage for potential operations against U.S., Israeli, and Jewish diaspora targets in the Western Hemisphere. Their proximity to the U.S. southern border increases operational reach. **Key lesson:** Gray zone attack infrastructure is pre-positioned before operational activation. Proximity to U.S. territory elevates domestic risk. **Source reading:** DOJ indictments; CTC Sentinel; U.S. Southern Command reports

Appendix B: Lessons and Knowledge

The following lessons are drawn from the case studies in Appendix A and from the broader body of research reviewed in Appendix C. They are intended to inform both pre-crisis planning and crisis-phase decision-making and should be read alongside the policy options in Section 3.3 and the operational tools in Section 3.4.

- **Campaign recognition is the central diagnostic challenge.** Establishing explicit campaign-recognition protocols, including pre-defined signature indicators, interagency pattern-matching tasking, and artificial intelligence–assisted open-source analysis, is the highest-return pre-crisis investment available.
- **Pre-established protocols matter more than response capability.** A Chinese-flagged vessel escaped in 2023 after severing the Balticconnector pipeline not for lack of naval power, but for lack of agreed-upon response procedures. The Salisbury model generated a rapid twenty-five-nation coordinated response because pre-existing allied consultation channels existed.
- **Public attribution carries deterrence value that silence forfeits.** The Balticconnector cable incident showed that demanding legal-standard certainty allowed Russia to normalize shadow-fleet sabotage. A high probability of deliberate state action is sufficient. Timely attribution also narrows the attacker's diplomatic maneuvering room, reducing its ability to exploit ambiguity.

- **Multilateral coordination multiplies deterrence impact.** The twenty-five-nation Salisbury response, achieved without a formal NATO or EU triggering mechanism, is the benchmark. Pre-crisis attribution coordination frameworks with key allies are essential.

- **The civilian tool kit must lead.** Economic tools, law enforcement, and information operations are the primary instruments of gray zone response. Overreliance on military and intelligence tools leaves nonmilitary attack and response vectors unaddressed.

- **Private-sector engagement is essential, not optional.** Direct engagement of private sector infrastructure owners expands the range of available tools. Neglecting this coordination forfeits resilience benefits that cannot be replicated through government action alone.

- **Drone harassment requires distinct response protocols.** Distinct counter-drone legal frameworks, detection architecture, and deterrence signals are required. The cost asymmetry of a $400,000 AIM-9 air-to-air missile vs. $10,000 Russian Gerbera drone means that reactively shooting down drones is not a sustainable primary response.

- **Iranian and Russian proxy models are converging.** Response frameworks developed for one actor apply increasingly to the other. The 2026 Iran war has intensified the Iranian proxy threat, with the new proxy group HAYI and Snapchat recruitment representing evolution beyond current frameworks.

Institutional Recommendations

The following recommendations are drawn from the Center for Strategic and International Studies' report, "By Other Means Part II," and updated to reflect current institutional realities. Previously, higher-level versions of those recommendations went unimplemented; the formulations below are calibrated to be achievable through administrative action without new legislation or Senate confirmation.

- **NSC Director for Gray Zone Activity** (reporting to NSC Senior Director for Intelligence): Establish this role through administrative action without Senate confirmation; the director would serve as a day-to-day coordinator across State, DOD, Treasury, DOJ, and the intelligence community, maintaining pre-established protocols and lead-agency determinations.

- **Deputy National Intelligence Officer (NIO) for Gray Zone Threats** (reporting to existing NIO for military issues): No Senate confirmation required; produces intelligence community–wide monthly campaign assessments and coordinates with allied intelligence services.

Appendix C: Studies and Sources of Relevant Open-Source Information

The following open-source research, reports, and journalism were reviewed in the development of this playbook. Hyperlinks are provided where public URLs are available.

Foundational Gray Zone Research

- Kathleen J. Hicks et al., "By Other Means Part I and II," CSIS, 2019. Campaign plan framework and five institutional reform recommendations.
- Melissa Dalton and Hijab Shah, "Partners, Not Proxies," CSIS, May 2020. Five structural coalition considerations; civilian-tools-first argument.
- Lindsey R. Sheppard and Matthew Conklin, "Warning for the Gray Zone," CSIS, August 2019. Three-element detection framework.
- Michael J. Mazarr, *Mastering the Gray Zone*, U.S. Army War College Press, 2015.

Russia/Europe, Undersea Infrastructure, and Maritime Security

- Seth G. Jones, "Russia's Covert Campaign in Europe," CSIS, March 2025.
- ICCT/GLOBSEC, "Update of Russia's Crime-Terror Nexus," February 2026. 151 confirmed Russian-proxy incidents February 2022 through February 2026.
- Andrei Soldatov and Irina Borogan, *War Without End: Russia's Shadow Warfare*, Center for European Policy Analysis, 2025.
- Elisabeth Braw, "How the Baltic Sea Nations Tackled Suspicious Cable Cuts," Atlantic Council, November 2025.
- Jennifer A. Counter and Amy Paik, "International Law Doesn't Adequately Protect Undersea Cables," Atlantic Council, January 2024.
- Texas National Security Review, "Legal Deterrence by Denial," August 2025.

Drone Harassment, Counter-UAS, and Emerging Tools

- 9dashline, "Grey-Zone Drones: Lessons for Europe From the Indo-Pacific," April 2026. Taiwan/Japan drone case studies and European response framework.
- Liana Fix, "Defending Europe if Russia Steps Out of the Gray Zone," CFR, February 2026. Drones as the instrument most likely to bridge gray zone to conventional attack.

- European Union Institute for Strategic Studies, "Navigating the Grey Zone: Readiness, Solidarity and Resolve," October 2025. Three-pillar European drone response.
- European Commission, "Action Plan on Drone and Counter-Drone Security," January 2026. Primary EU-level policy document.
- Waterfall Security, "Threat Report 2026," March 2026. Cyber incidents with physical consequences.
- Cipher Brief / Booz Allen Hamilton, "Accelerating National Security Outcomes in the Gray Zone," 2024. AI-assisted detection.

CFR, Intelligence Community, and Parliamentary Sources

- Max Boot, James Appathurai, and Linda Lourie, "Navigating the Gray Zone," CFR Event Transcript, March 2025.
- National Intelligence Council, "Conflict in the Gray Zone," (NIE 2024-16734-A, July 2024). Intelligence community baseline assessment.
- ODNI/IC, "Updated IC Gray Zone Lexicon," July 2024. Official IC definitional baseline.
- International Committee of the Red Cross, "Hybrid Threats, Grey Zones, Competition, and Proxies: When is it Actually War?," January 2025. International human rights law criteria for armed conflict; cited in Section 1.3.
- UK House of Commons Defence Select Committee, "Defence in the Grey Zone," July 2025.
- International Institute for Strategic Studies, "Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure," August 2025.
- Irregular Warfare Initiative, "Sabotage as a New Normal," February 2026.
- Organized Crime and Corruption Reporting Project, "Make a Molotov Cocktail," September 2024. Primary source on Telegram recruitment tradecraft.