A Crisis Management Handbook

Responding to Hybrid Threats with Democratic Integrity

Author: Liam O´Shea
Editor: Filippa Almlund

Folke Bernadotte Academy
Swedish agency for peace and security

FBA

How to refer to this handbook

O'Shea, L. (2026).
A Crisis Management Handbook: Responding to Hybrid Threats with Democratic Integrity
Stockholm: Folke Bernadotte Academy.
DOI: https://doi.org/10.61880/KKTV7243

Author: Liam O'Shea
Editor: Filippa Almlund
Publisher: Folke Bernadotte Academy
Place of publication: Stockholm, Sweden
Year of publication: 2026
DOI: https://doi.org/10.61880/KKTV7243

Content

Acknowledgements

The author and editor would like to thank Prof Sir David Omand, Dr Olga Reznikova and members of the project's reference group for their valuable comments and input during the development of this handbook, namely Dominique Górska Rasangam, Emma Ingemansson, Fredrik Konnander, Ingrid Ioana Bicu, Jenny Lindqvist, Jonas Lövström, Kicki Westin and Lennart Nikolei. A special note of appreciation goes to Aina Boris, who oversaw all production details and ensured that the manuscript, layout, illustrations and final delivery came together smoothly.

Foreword

Shifting geopolitical landscapes and rapid technological advancement are changing the nature of conflicts. Threats to states and societies today go well beyond conventional military force. Instead, they manifest as hybrid threats, a calculated blend of cyberattacks, disinformation campaigns, economic coercion, and political interference. These tactics are deliberately designed to exploit the inherent openness of democratic societies, blurring the lines between peace and conflict, truth and deception, internal and external threats.

For government officials, particularly in democracies, navigating a hybrid crisis presents a paradox. The urgency to protect national security can create immense pressure to bypass standard protocols, centralize power, or curtail fundamental freedoms. Yet, when decision-makers sacrifice core democratic values in the pursuit of immediate security, they weaken the very fabric of the society they are sworn to defend.

True democratic resilience against hybrid threats does not lie in adopting the authoritarian tactics of the aggressor. It lies in fortifying democratic integrity.

The Folke Bernadotte Academy (FBA) is proud to present Responding to Hybrid Threats with Democratic Integrity: A Crisis Management Handbook. We hope that this practical guide will be a useful help to public servants as they navigate and respond to new threats and attacks.

At the heart of this handbook are seven core principles for democratic crisis management. The handbook translates these principles into reflective questions that officials can ask themselves both during peacetime preparation and in the heat of a crisis.

For democracies, building trusted, resilient institutions requires continuous effort and attention. It is our hope that this handbook serves as a steadfast companion for government officials, empowering them to plan and act decisively, effectively, and in line with democratic principles.

Protecting and promoting democracy is at the heart of Swedish foreign policy, by managing crises in ways that are fundamentally consistent with democratic principles, we do not just survive the threat; we actively protect and reinforce the institutional foundation upon which democracy is built.

Per Olsson Fridh
Director General, Folke Bernadotte Academy

Introduction

This handbook addresses how to act effectively in a crisis in ways consistent with democratic values. It is a practical guide to crisis management for government officials who may need to manage a crisis caused by hybrid threats, and it is designed for crises at the national level, where the response requires coordination across government and decisions at the most senior level of authority. Under a hybrid attack there is a risk that decision-makers sacrifice basic democratic principles in the pursuit of security, and in doing so weaken the values they are there to defend. But this handbook's approach is grounded in the argument that effective crisis management and democratic governance are complementary rather than competing. Security is a fundamental right, and the obligation of a democratic state to protect its population is a democratic obligation.

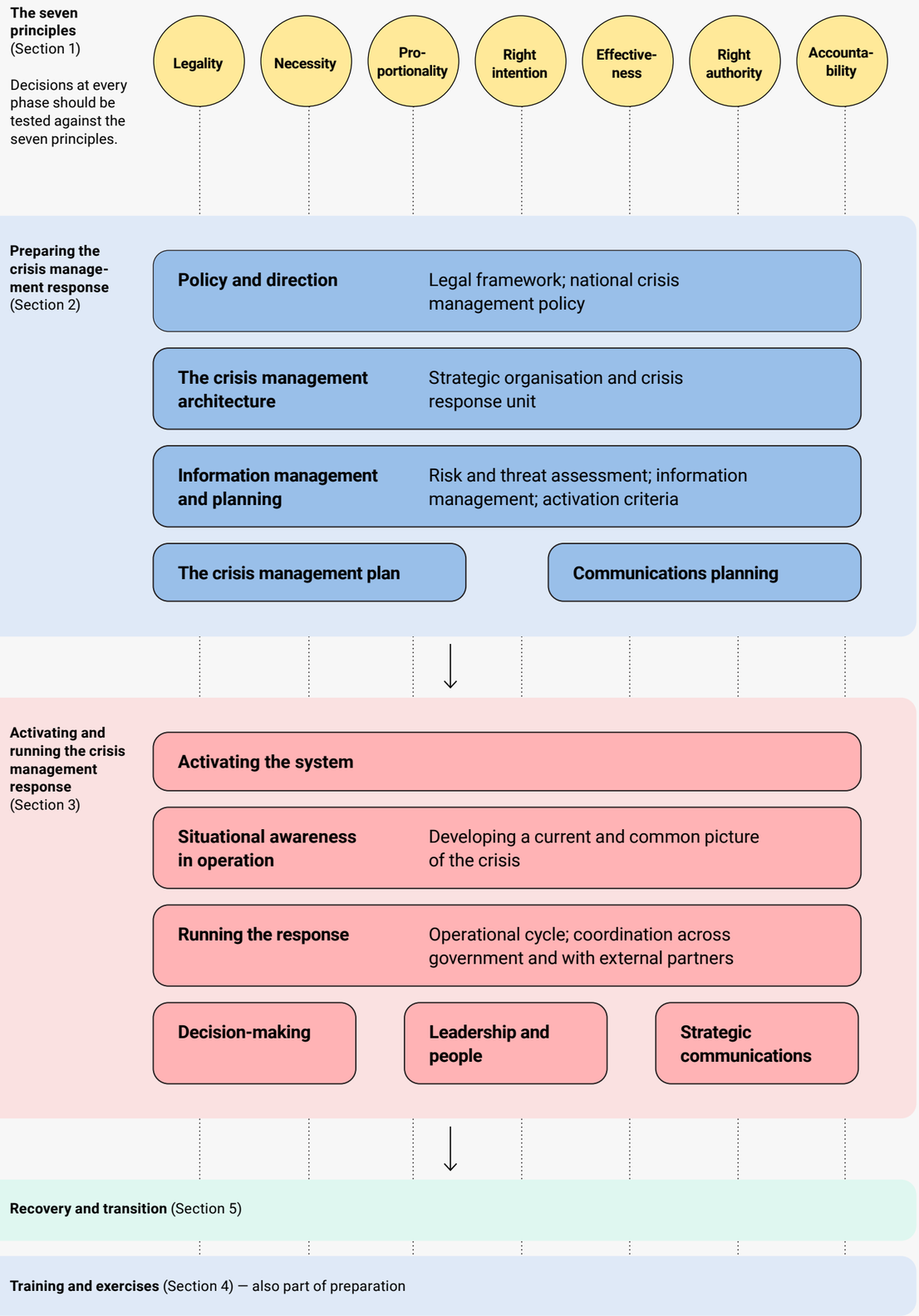
Crisis management is a strategic function. Crises are inherently abnormal, unstable and complex situations that represent a threat to a government's strategic objectives, reputation or survival.[1] Crises often exceed the capacity of pre-prepared responses and they come in two broad forms. Major shocks, which are sudden events, and slow-burns, which develop as warning signs are missed or misunderstood, often until the situation becomes unmanageable. Slow-burns are often more dangerous, because the case for action may not be compelling until the options for managing the situation have narrowed considerably. This distinction is particularly relevant to hybrid threats, as hybrid campaigns may present as slow-burns, with individually unremarkable activity accumulating in ways that may not be recognised as a crisis until the campaign is well advanced. A successful response to either form requires a crisis management system that can be activated and operated under pressure, with clear lines of authority, reliable information, and a structured basis for taking consequential decisions on incomplete evidence. Building, preparing, and operating that system is what this handbook covers.

The handbook is structured as follows. Section 1 sets out the analytical framework used to understand hybrid threats, the relationship between resilience and democratic governance, and seven principles for crisis decision-making that function as practical tests at the point of decision and run as a thread through the guidance that follows. Section 2 covers the preparations a government needs to have in place before a crisis occurs: the legal and policy foundations, the organisational architecture, the information management capability, and the communications arrangements on which an effective response depends. Section 3 covers the crisis response itself, from activation of the system through situational awareness, decision-making, leadership, and strategic communications under pressure. Section 4 addresses the training and exercises through which the system and the people who operate it are developed and tested. Section 5 covers recovery, transition, and the review process through which the experience of a crisis feeds back into the system's future capability.

1 For a comprehensive framework for crisis management as a discipline, including the distinction between crises, incidents, and emergencies, see: Cabinet Office (UK) and BSI Knowledge, "PAS 200:2011 - Crisis Management - Guidance and Good Practice," 2011, https://knowledge.bsigroup.com/products/crisis-management-guidance-and-good-practice; Arjen Boin et al., The Politics of Crisis Management: Public Leadership Under Pressure (Cambridge University Press, 2016).

This is a practical handbook. It draws on FBA's experience working in emerging democracies. It also draws on established crisis management frameworks, research on hybrid threats, international legal standards, and the wider literature, but references these only where they underpin the guidance or strengthen the reasoning behind it. It does not focus on wartime crisis management comprehensively, though some of the principles and frameworks it sets out will apply in wartime. A significant share of the guidance concerns preparation, as how a government organises itself before a crisis largely determines how effectively it can act during one. The handbook is designed for crisis management in response to hybrid threats in general, not for a specific country, government or a specific threat scenario. That has required a balance between offering guidance concrete enough to act on and avoiding prescriptions that assume a particular institutional structure or legal framework. The aim throughout is to equip those leading and managing a crisis caused by hybrid threats with the frameworks, principles, and practical tests they need to make good decisions, under pressure and consistent with democratic values.

Figure 1 Crisis Management: From preparation to recovery



01 *Hybrid threats, democratic resilience and crises*

This section sets out the foundations on which the operational guidance in the rest of the handbook rests: what hybrid threats are and how they work, why the resilience of democratic states depends on the strength of their democratic foundations, and the principles that should govern crisis decision-making when those foundations come under pressure.

1.1. Hybrid Threats

The crisis management system described in this handbook is designed to address hybrid threats, which are actions conducted by state or non-state actors whose goal is to undermine or harm a target by combining overt and covert, military and non-military means.[2] They can be defined by several characteristics. They are ambiguous: hybrid threat actors obscure their involvement and intent, so that whether an action is hostile at all, who is responsible for it, and whether apparently separate events are connected may all be deliberately unclear. They are directed at societal vulnerabilities rather than at military capacity, targeting political divisions, corruption, weak institutions, economic dependencies, fragile supply chains, susceptibility to disinformation, and inadequate infrastructure. Democratic societies are particularly exposed because their openness and pluralism create points of entry that hybrid threat actors can exploit. Hybrid threats are also typically calibrated to remain below the thresholds that would trigger a clear or unified government response. And they generally involve the coordinated use of multiple tools across several domains (see below).

Understanding and responding to hybrid threats requires a shared analytical framework. This handbook uses the CORE model, developed by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and the European Commission's Joint Research Centre, for that purpose.[3] The model describes how a hostile ***actor*** selects from a range of tools and applies them to specific domains within the affected society, through distinct phases of activity, to achieve its strategic ***targets***: undermining democratic governance, manipulating decision-making processes, and creating cascading effects. The tools available to a hybrid threat actor are wide-ranging, from cyber operations and disinformation to economic leverage, political subversion, and the use of proxies.[4] The model identifies thirteen domains spanning the full spectrum of societal functions. The phases describe how a campaign develops over time, from initial priming through destabilisation to potential coercion, though campaigns may oscillate between phases rather than escalating in a straight line. Figure 1 provides an overview of the model and its elements.

2 Hybrid CoE, "Hybrid Threats," Hybrid Threats, 2026, https://www.hybridcoe.fi/hybrid-threats/.
3 Hybrid CoE, The Landscape of Hybrid Threats: A Conceptual Model : Public Version. (Publications Office, 2021), https://doi.org/10.2760/44985.
4 For a detailed empirical analysis hybrid threats and the range of hostile activities conducted by state actors, see: Matthew R. Redhead, Old Wine, New Bottles? The Challenge of State Threats. (Serious Organised Crime & Anti-Corruption Evidence Research Programme, 2025), https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/67852e69ff4ff4079a9c3000/1736781420568/SOCACE-RP32-OldWineNewBottles_final.pdf.

Figure 2 Hybrid Centre of Excellence - Comprehensive Resilience Ecosystem Model*

* adapted from Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305

Domains are especially important to understand, as they are what hybrid threats are directed at and where hybrid threat activity is most likely to be detected. The CORE model organises the thirteen domains into three spaces: the governance space (political, public administration, legal, intelligence, diplomacy, military/defence), the civic space (social/societal, culture, political, information), and the services space (economy, infrastructure, cyber, space, information).[5]

5 The political domain sits across both the governance and civic spaces; the information domain sits across both the civic and services spaces.

These spaces are interconnected, and hybrid threat actors deliberately exploit those interconnections to create cascading effects, where disruption in one domain spreads into others. Recognising the full scope of a hybrid threat campaign requires understanding not only which domains are being targeted but how effects in one may cascade into the rest. Two challenges make hybrid threats particularly difficult to manage in practice. The first is detection. Hybrid threat activity is typically designed to fall below or outside conventional detection thresholds, and individual actions may appear unrelated to one another or register only within a single domain. A coordinated campaign may only become visible when information is drawn together across domains and over time, which requires analytical capacity and institutional arrangements that many governments do not have in place.[6] The second is attribution. Establishing who is responsible for hostile activity is a demanding analytical task, often made harder by the hostile actor's deliberate use of deniable means. The decision on whether and when to attribute publicly is also a strategic choice with significant operational and political consequences. Both challenges are addressed in Sections 2 and 3 in the context of crisis preparation and response.

Responding to a crisis caused by a hybrid campaign requires the crisis management system to manage the effects of the campaign on the state and society and, potentially, to direct measures at the threat actor. The former requires protecting the population, maintaining the functioning of institutions and services, and sustaining public confidence. The latter may involve imposing costs on the threat actor, disrupting its campaign, and where possible influencing the actor's decision to continue.

1.2. Resilience and democratic foundations

How a crisis is managed directly affects whether a society's resilience is maintained or degraded. Resilience refers to the ability of a state and its society to anticipate threats, withstand and absorb their effects, recover from disruption, and adapt so that future capacity is strengthened.[7] For democratic states, resilience against hybrid threats has an additional dimension. Because hybrid threats target the functioning of democratic institutions and the cohesion of democratic societies, resilience must also safeguard democratic processes. A society that restores its infrastructure and economic stability after a hybrid campaign but whose democratic institutions have been weakened, whose public trust in government has been eroded, or whose decision-making processes have been compromised has not demonstrated resilience in a democratic sense.

Democratic resilience is necessarily society-wide because the foundations on which resilience rests sit across society, not within the state apparatus alone. European and Nordic responses

6 For a detailed treatment of the detection and attribution challenges posed by hybrid warfare, see: Multinational Capability Development Campaign / Ministry of Defence (UK), Countering Hybrid Warfare Project: Countering Hybrid Warfare (2019), https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf.

7 For the resilience framework on which this section draws, including the functions of anticipation, resistance, recovery, and adaptation, see: Cabinet Office (UK) and BSI Knowledge, "PAS 200:2011 - Crisis Management - Guidance and Good Practice"; Hybrid CoE and European Commission, Hybrid Threats: A Comprehensive Resilience Ecosystem (Publications Office of the European Union, 2023), https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/.

to hybrid threats are therefore commonly framed around a whole-of-society approach, which holds that resilience against hybrid threats depends on the integration of government, the private sector, civil society organisations, and the public, recognising that the capabilities and trust on which resilience rests are distributed across society rather than held by the state alone. In relation to crisis management, the concept can help government understand the resilience context it is operating in, and how society as a whole is likely to respond to an attack. It also helps to frame the response as in service of protecting society as a whole rather than the state apparatus alone. Most practically, it directs the crisis management system to identify in advance, and engage during a response, those parts of society best placed to contribute, for example in the private sector or in civil society, recognising that these actors may have capabilities, information, and relationships the government does not. However, a crisis management response cannot incorporate all elements of a whole-of-society approach. Effective response requires concentrated authority and a decision-making body small enough to function under pressure, and the response should engage those parts of society best placed to contribute rather than an overly broad set of actors.

The CORE model can be used to understand hybrid threats and what aspects of resilience democratic states need to protect. It places seven foundations of democratic societies at its centre: the feeling of justice and equal treatment, civil rights and liberties, political responsibility and accountability, the rule of law, stability, reliability and availability of public services, and foresight capabilities.[8] These are the values, norms, and expectations on which the functioning of democratic societies depends. Trust between government and population is a central force that holds these foundations together, and it is trust that enables the connections and dependencies within the system to function as sources of strength rather than as vulnerabilities. Weakening these foundations degrades the resilience of the entire system. This does not mean that only democratic states can build resilience. Authoritarian systems can demonstrate considerable capacity to absorb shocks and maintain order, particularly in the short term. But that capacity typically depends on coercion, information control, and the suppression of dissent, which can make it brittle under sustained or adaptive pressure and vulnerable to sudden failure when those mechanisms are overwhelmed. For democratic states facing hybrid threats a key challenge is to ensure that the crisis response does not undermine the foundations, whether by eroding public trust, restricting rights without adequate justification, or weakening accountability, as doing so may achieve some of the goals of the hostile actor.

The degree to which a crisis management response aligns with these foundations, and is seen to align with them, can have a significant effect on crisis management outcomes. Trust between government and population is essential for sustaining voluntary public cooperation through a prolonged crisis. Open information flow within government generally produces better situational awareness, because people at all levels are more willing to report what they see, including information that senior leaders may not wish to hear.[9] Where blame is the institutional response to failure, this flow is compromised, and accountability mechanisms are the practical counter. Distributed authority within the response, where decisions that can and should be taken locally are not unnecessarily centralised, can allow faster and better-informed responses. None of this guarantees effective crisis management, but a crisis management process that is broadly aligned with these foundations is more likely to sustain the cooperation, information flow, and institutional legitimacy on which an effective response depends.

A crisis may also generate situations in which rights must be restricted, authority must be concentrated, and decisions must be taken at speed without the consultation that would normally be expected. International human rights law recognises this. Established legal frameworks provide that certain rights may be limited, or temporarily set aside under formal derogation,[10] in times of emergency, provided that such measures are strictly required by the situation, are proportionate, are non-discriminatory, and are subject to review.[11] These frameworks reflect the reality that democratic foundations and crisis management must coexist under pressure, and that managing the tensions between them is a practical task, not an abstract one. The seven principles set out in the next section provide a framework for doing so.

1.3. Principles for crisis decision-making

The democratic foundations described in the previous section establish what resilience depends on, but they are not specific enough to guide individual decisions under the pressure of a crisis. What is needed is a set of principles that can be applied at the point of decision, specific enough to shape the choices that those managing a crisis actually face and grounded in the ethical and legal reasoning that underpins the balancing of competing rights and obligations.

The seven principles set out below are drawn from established frameworks for ethical decision-making in security and crisis contexts, and are adapted here for crisis management responses to hybrid threats. They reflect general principles of decision-making in a democratic society, broadly applicable to the work of officials across government and the wider public service. The handbook applies them to the specific demands of preparing for and responding to a crisis caused by hybrid threats. Each is framed as a question. Together, they represent a structured set of tests that those taking significant crisis management decisions should be able to satisfy before a measure is authorised.[12]

8 The seven foundations and the role of trust within the model are set out in: Hybrid CoE and European Commission, Hybrid Threats.

9 For the role of trust, open information flow, and accountability in sustaining effective crisis management, see: Cabinet Office (UK) and BSI Knowledge, “PAS 200:2011 - Crisis Management - Guidance and Good Practice”; David Omand, How to Survive a Crisis: Lessons in Resilience and Avoiding Disaster (Viking, 2023).

10 The formal, temporary suspension of specific legal obligations by a state, subject to defined safeguards and oversight.

11 See in particular Article 15 of the European Convention on Human Rights, which permits derogation from certain Convention rights in time of war or public emergency threatening the life of the nation, subject to strict conditions; and the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (1985), which set out the conditions under which limitations on rights are permissible.

12 Drawing on the just war tradition, a framework of applying necessity, proportionality, right intention, and right authority as practical tests for security decisions is developed in: Omand, How to Survive a Crisis. Legality, necessity, and proportionality are also established principles in international human rights law, reflected in the conditions governing derogation under the European Convention on Human Rights (Article 15) and the Siracusa Principles. Accountability and recorded, reviewable decision-making draw on: Cabinet Office (UK) and BSI Knowledge, “PAS 200:2011 - Crisis Management - Guidance and Good Practice”; Boin et al., The Politics of Crisis Management.

Figure 3 The seven principles for crisis decision-making

Each of the seven principles is described in turn below. The purpose of using the principles around decision-making is not to constrain it or to slow it down. It is to give it structure. Under crisis pressure, decision-making tends to narrow. A process that works through each of these tests is more likely to produce sound decisions than one that does not, and provides a defensible record of why the decision was taken. During the preparatory phase (Section 2), the principles inform the institutional conditions that need to be in place before a crisis occurs, from legal authorities and accountability structures to the organisational culture that determines whether challenge and dissent are possible. During the response phase (Section 3), they function as tests at the point of decision.

Legality
Any significant crisis management measure should rest on a clear legal basis. Those taking the decision should understand the scope of their authority, the limits placed on it, and the legal framework within which they are operating. That framework includes the state's obligations under international human rights law, which continue to apply during a crisis. Where emergency powers are invoked, the legal conditions for their use should be understood and observed, including that any restrictions on rights are non-discriminatory, time-bound, and subject to independent review.

Necessity
A measure should be taken only where there is no other reasonable way to achieve the desired effect at lesser cost or risk. Necessity guards against the tendency, common under pressure, to reach for the most forceful option available rather than the most appropriate one. It requires decision-makers to consider whether less restrictive alternatives exist and whether they have been adequately assessed.

Proportionality
The ethical risks that flow from a decision should be kept in line with the harms that the measures being taken are intended to prevent. Proportionality requires an assessment not only of the intended effects of a measure but of its likely unintended consequences, including the risk of harm to those who are not the intended targets of the action. A disproportionate response may itself cause damage, provoke a wider reaction, or undermine the public trust on which the broader response depends.

Right intention
Those taking crisis management decisions should act with integrity and without hidden political or improper agendas affecting their analysis, assessment, or decisions. Right intention guards against the risk that the exceptional powers available during a crisis are used for purposes other than those for which they were granted. The distinction between measures that serve the interests of the population and measures that serve the interests of those in authority is not always self-evident, and this principle requires that the question is asked explicitly.

Effectiveness
There should be adequate justification for believing that a measure has a reasonable prospect of achieving what it is intended to achieve, based as far as possible on evidence and sound assessment rather than on assumption, political pressure, or the desire to be seen to act. A measure that satisfies the other principles but is unlikely to work does not meet this test.

Right authority
Decisions should be taken at a level appropriate to their significance and consequences. Decisions involving serious risks or far-reaching consequences should be taken by those with the seniority and mandate to authorise them. Equally, decisions that can and should be taken at a lower level should not be unnecessarily centralised. Effective crisis management depends on both strong strategic direction and the scope for those closest to a situation to make informed judgements in light of local circumstances.

Accountability
Those taking decisions during a crisis should be able to explain and defend the reasoning behind them. Decisions can only be justified on the basis of the information that was available or reasonably obtainable at the time they were taken, and not every decision must prove to have been correct. But accountability requires that decisions are recorded, that the basis on which they were taken is documented, and that there is provision for review after the event. Where crisis measures involve restrictions on rights or the exercise of emergency powers, accountability also depends on the functioning of independent oversight, including the judiciary and parliamentary scrutiny, to ensure that such measures do not extend beyond what the situation requires and that the rule of law is maintained throughout.

These seven principles will not resolve the dilemmas that arise in a crisis. They will not eliminate uncertainty, remove political pressure, or guarantee the right outcome. They also do not operate in isolation. A measure that is lawful and necessary but disproportionate fails the test, as does one that is proportionate and well-intentioned but has no reasonable prospect of being effective. What they provide is a disciplined basis for making and justifying hard choices when the stakes are high and the information is incomplete. A decision that has been tested against all seven principles may still prove to have been wrong, but it will have been taken on a defensible basis and can be honestly accounted for afterwards.

Case 1 Finland, 2023–2024: instrumentalised migration[13]

In the autumn of 2023, Finland faced a sudden increase in asylum seekers arriving at its eastern border with Russia, following years in which almost no arrivals had been recorded through those crossings. Finnish authorities assessed that Russian border guards were facilitating the movement. The arrivals were concentrated at remote crossing points in northern Finland, in conditions where the individuals concerned were at serious risk from the cold. The Finnish government assessed the situation as instrumentalised migration: a deliberate attempt to create pressure on Finland's border management and asylum systems, following Finland's accession to NATO in April 2023.

The government responded in stages. It first closed the four busiest southeastern border crossings, then extended closures to cover all crossings on the Russian border, effectively preventing asylum applications from being lodged at those border crossings. When the government determined that existing legislation did not provide a sufficient legal basis for a sustained response, it introduced emergency legislation: the Act on Temporary Measures to Combat Instrumentalised Migration, passed in July 2024 under a constitutional urgency procedure requiring a five-sixths parliamentary majority, followed by approval by a two-thirds majority. The Act grants border authorities powers, in narrowly defined circumstances, to refuse entry and return individuals arriving at the border during situations designated as instrumentalised migration, a measure that restricts the right to seek asylum in ways that generated significant domestic and international debate. UNHCR publicly urged Finland to ensure access to asylum. The Finnish government maintained that the legislation was a proportionate response to a security threat that exploited the asylum system, not a rejection of Finland's obligations under international law.

The Finnish government responded to a hybrid threat designed to create tension between security and rights, while attempting to balance security concerns with constitutional and international legal obligations. Finland's response was not legally or morally uncontested, and the measures remain controversial. But the government sought and obtained a constitutional mandate through democratic procedure, and the legislative process subjected the measures to substantial parliamentary and constitutional scrutiny.

13 Minna Ålander, "Death by a Thousand Paper Cuts: Lessons from the Nordic-Baltic Region on Countering Russian Gray Zone Aggression," Carnegie Endowment for International Peace, 2024; Finlex, "Act on Temporary Measures to Combat Instrumentalised Migration (Finland)," 2024; UNHCR, "UNHCR Urges Finland to Protect the Right to Seek Asylum." May 2024.

02 *Preparing the Crisis Management Response*

This section sets out the preparations a government needs to have in place before a crisis occurs, covering the legal and policy foundations, the organisational architecture, the information management capability, crisis management planning and the communications arrangements on which an effective response consistent with democratic values depends. These preparations are also where the principles for crisis decision-making established in Section 1.3 are given institutional form.

Figure 4 Preparing the crisis management response

2.1. Policy and direction

A crisis management response requires both legal authority, to establish what a government can do in a crisis, and a national crisis management policy, to direct how it will organise itself to do it.

Legal framework

Legality

A government needs established legal authority to act in a crisis, and those who exercise that authority need to know its scope and limits. At a minimum, the legal framework should establish what crisis management powers are available, including powers to restrict movement, control information, requisition resources, or direct the actions of public and private bodies. This includes provisions governing powers that may be needed if a hybrid threat scenario escalates towards or into armed conflict, including powers relating to martial law, partial or full mobilisation, the formal derogation of certain rights under international human rights law, and the transfer of specified authorities from civilian to military leadership. The framework should specify who can authorise such crisis measures, under what conditions, and for how long. It should set out the chain of authority through which crisis measures are approved. And it should define the rights and protections that remain in force during a crisis.

Right authority

It is especially important to assess whether the existing legal framework is adequate for the kinds of crises that hybrid threats may generate. Hybrid threats may not fit the categories on which emergency legislation is typically built. A coordinated campaign of cyber attacks, disinformation, and economic pressure may constitute a serious crisis without meeting the legal threshold for a "state of emergency" or triggering provisions designed for armed conflict or natural disaster. The legal framework should also encompass outward-facing measures, those directed at the threat actor itself, not only those governing the domestic response. Sanctions regimes, asset freezes, restrictions on diplomatic personnel, and authorities for cyber operations each rest on distinct legal bases, and those advising the crisis management system on legal questions need to understand the scope and constraints of both sets of authority. Where the framework contains gaps they should be identified and addressed before a crisis forces improvised workarounds. This assessment is a fundamental expression of the **principle of legality** as it ensures that crisis powers have a defined basis in law rather than being asserted or improvised under pressure, and it gives effect to the **principle of right authority** by establishing in advance who holds the power to authorise the most consequential measures.

Accounta-bility

The legal framework should also include oversight mechanisms that give effect to the **principle of accountability**. The key mechanisms are provisions for parliamentary scrutiny of emergency measures, including requirements to report to parliament when crisis powers are invoked and at regular intervals thereafter; judicial review, so that those affected by emergency measures have recourse to independent legal challenge; time limits and sunset clauses on emergency powers, requiring active renewal rather than allowing measures to persist indefinitely; and requirements to record decisions as they are taken, so that decisions and the reasoning behind them can be examined afterwards. These mechanisms serve a dual purpose. They constrain the misuse of emergency powers, and they protect those who exercise crisis management powers legitimately, by providing a framework within which decisions taken in good faith, on the basis of the information available at the time, can be defended.

National crisis management policy

Where the legal framework establishes what a government can do in a crisis, the national crisis management policy directs what it will build and maintain in order to be ready. Its function is to ensure that the system is authorised, resourced, and sustained. It should be a formal, written document, endorsed at the highest level of government, as a policy backed by the head of government or the national security council carries different weight from one issued by a single ministry.

The policy should state the objectives of the crisis management system in concrete terms: the ability to detect and assess a developing crisis, coordinate the response across government, take decisions at the appropriate level of authority, and review their effects. It should specify what types of situations the system applies to, what falls outside it, and how it relates to other national strategies and structures for security, defence, and resilience. For hybrid threats, the system will need to encompass agencies and functions that may not traditionally see themselves as part of crisis management, including those responsible for strategic communications, cyber defence, election security, and critical infrastructure protection. Its scope should also extend to the government's capacity to direct measures at the threat actor, bringing within the system the actors responsible for diplomatic, economic, and legal instruments and establishing that the crisis management system serves the coordination of both inward-facing and outward-facing responses. The policy should also establish the basis for cooperation with actors outside government on whom an effective response will depend, particularly private sector operators of critical infrastructure and, in some contexts, civil society organisations with roles in supporting affected communities or countering disinformation. These actors cannot be given obligations in the same way as government departments, but the policy should require that designated departments build and maintain the coordination arrangements, points of contact, and information-sharing agreements on which cooperation during a crisis will rely.

The policy should designate a senior official or body responsible for ensuring that the system is built, resourced, maintained, tested, and improved. Crisis management capacity degrades quickly if no one is responsible for sustaining it between crises. Departments and agencies brought within the system's scope should have defined obligations to contribute on a continuing basis, including through participation in exercises and the maintenance of their own preparedness. The policy should establish the resource commitments needed to sustain the system, including budget provision, staffing, and the facilities and systems on which it depends, with reporting arrangements that give senior leadership assurance that what the policy mandates is being delivered. Both the legal framework and the policy should be subject to periodic review, tested against exercises, real events, and changes in the threat environment.

2.2. The crisis management system

An effective crisis management response also requires that sufficient plans have been put in place to develop an organisational architecture through which a crisis response is directed and coordinated. This includes plans detailing the authority of the organisations leading the response, their functions, their logistical capabilities and the roles of the people who operate within them.

Right authority

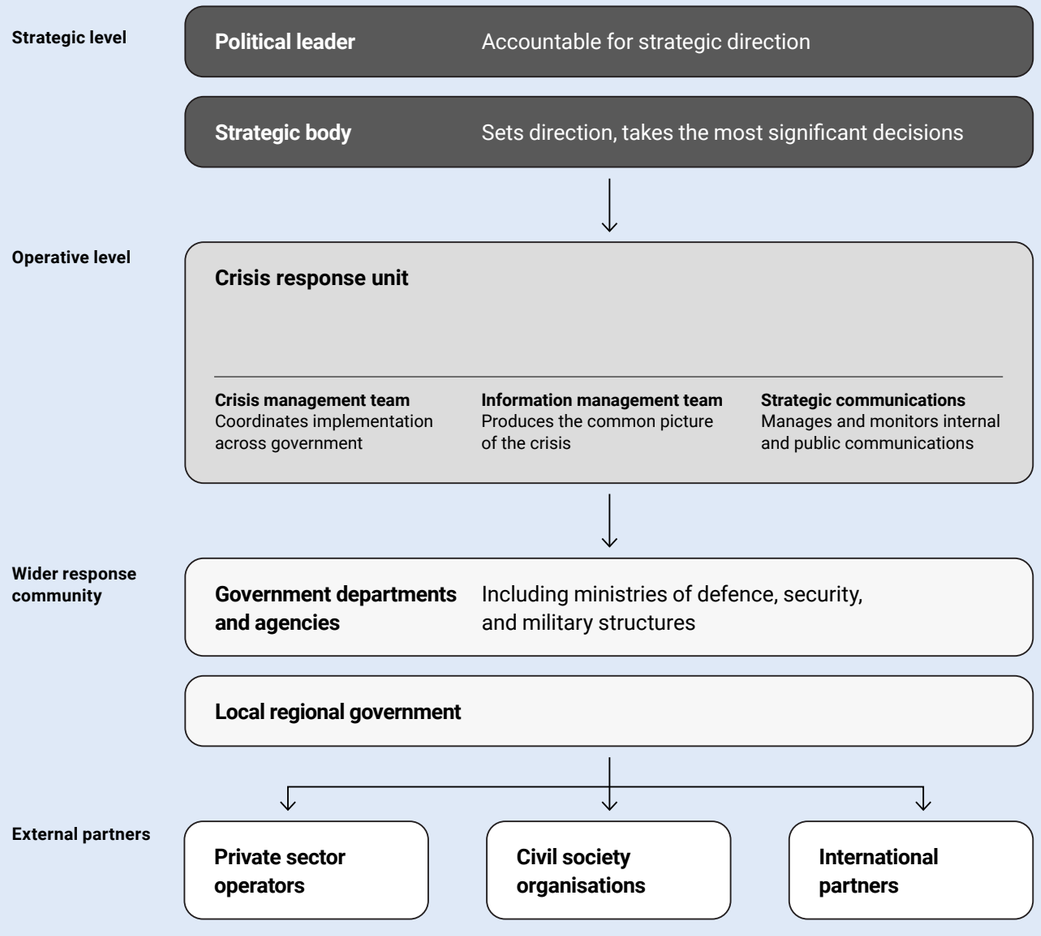
Effective government crisis management systems are required to operate on two levels: a strategic level that sets direction and takes the most significant decisions, and an operational level that coordinates the response on a continuous basis. Countries will adapt this to their own institutional arrangements. It is important that those responsible for setting the direction of the response and those responsible for coordinating its execution should be clearly distinguished, with defined reporting lines between them. This distinction gives structural effect to the **principle of right authority**, ensuring that the most consequential decisions are taken at a high level of seniority, and personnel at lower levels have sufficient authority to take operational decisions without seeking approval.

The designated political leader identified in the national crisis management policy, whether the head of government, a senior minister, or the chair of a national security body, must take accountability for the strategic direction of the response. The political leader should be supported by a strategic-level body, typically a committee or council, that provides the forum through which strategic decisions are taken, objectives are set and reviewed, and oversight of the response is maintained. This body should meet as events require but should not manage the response on a continuous basis. The critical discipline at this level is to set direction without directing operations. The risk, particularly in systems where political authority is highly centralised, is that political leaders are drawn into operational questions, which slows the response, overloads senior decision-makers, and leaves the strategic direction unattended.[14]

Below the strategic level, the crisis management system should have a crisis response unit with a dedicated crisis management team (CM team). The crisis response unit's core functions are to coordinate the implementation of decisions taken by the strategic body across departments and agencies, to maintain an up-to-date shared picture of the situation for decision-makers, to provide clearly presented analysis of the situation and the options available, to track whether decisions have been carried out, to record decisions and the reasoning behind them as they are made, and to identify issues that require escalation to the strategic level. These functions should be assigned, documented, and practised before a crisis occurs. Additional functions need to be allocated within the wider crisis management system, though not necessarily all housed within the crisis response unit itself. These include access to legal advice on the lawfulness of proposed measures, international liaison with relevant partners and multilateral mechanisms, monitoring the impact of the crisis and the response on the population, and strategic communications both within government and public facing.

14 For comparative research on how political leaders function most effectively during crises, including the discipline of setting direction without managing operations, seeL Boin et al., The Politics of Crisis Management; Omand, How to Survive a Crisis.

Figure 5 The crisis management response architecture



Note: countries will adapt this to their own institutional arrangements. The diagram shows generic functional roles.

Where the strategic body sets direction periodically, the crisis response unit translates that direction into coordinated action across government and maintains it between meetings of the strategic body. It should operate under a designated chair with the seniority and authority to direct its work and to represent the operational level to the strategic body. Reporting lines between the two should be clear, fast, and practised. The unit should sit above individual departmental interests, and may be housed in a dedicated body, in the national security apparatus, or in the centre of government. It should have the practical authority to convene the relevant departments and ensure decisions are implemented, operating alongside, rather than in place of, existing sectoral response mechanisms such as civil protection, military command, and cyber incident response.

In a hybrid crisis, the response may draw in departments and agencies across multiple domains, and assigning lead responsibility to a single ministry is unlikely to work. The response may also require measures directed at the threat actor, drawing on diplomatic, economic, legal, and intelligence instruments held by departments not traditionally involved in crisis response coordination. The crisis management system needs established arrangements that bring all of these actors into a single framework operating under common strategic direction.

The relationship between the civilian crisis management system and military and defence structures warrants particular attention. **A hybrid crisis** below the threshold of armed conflict is usually a civilian crisis, and the response should be directed by the civilian authorities described in this section, with military assets and capabilities operating in support. The military may contribute intelligence, surveillance, cyber defence, logistical support, and, through its posture, a signalling function that the civilian response alone cannot provide. These contributions should be coordinated through the crisis management system rather than running on a separate military track, and the arrangements for how military capabilities are requested, tasked, and reported should also be established in advance. Where a hybrid crisis escalates towards or beyond the threshold of armed conflict, the legal provisions described in Section 2.1 should govern how authority is transferred and under what conditions. The boundary between civilian-led crisis management and the transfer of specified authorities to military leadership should be defined clearly enough that the transition is a deliberate decision taken under established legal authority, not an incremental drift driven by ambiguity.

As well as having appropriate authority, the crisis response unit requires appropriate logistical capabilities. It should have a designated facility from which to operate, identified and equipped in advance with the communications systems, secure channels, and logistical support needed to sustain operations. Where the crisis may extend over days or weeks, this includes rest facilities, food, and basic amenities for personnel working extended shifts, since their absence compounds fatigue and degrades performance over time. It serves as the established seat of authority for the operational response, where the current picture is collated and where all concerned know that coordination is centred. The strategic body may also meet there, but the facility's primary function is to house the continuous operational work of the CM team. Backup arrangements should be in place in case the primary facility is compromised, and communications systems should be tested against disruption, including the kinds of cyber attack or infrastructure degradation that a hybrid threat campaign might involve. Those who will use the facility should be practised in doing so through exercises. A crisis is not the moment to introduce people to unfamiliar working arrangements, technology, or procedures.

Those who will fill crisis management roles should be identified and selected in advance on the basis of the specific competencies the work demands, including processing information under pressure, working across institutional boundaries, and making and communicating decisions clearly.[15] Designated alternates should be assigned in case primary personnel are unavailable. The team also needs to be developed as a team. The working relationships and shared procedures that allow a group to function effectively under crisis conditions can only be built through regular training and exercising together (see Section 4). Finally, the system should be planned for sustainment. Hybrid crises may last weeks or months, placing sustained demands on a relatively small number of people. The roster should be deep enough to allow rotation, and the ability to draw in additional trained personnel when the scale or duration of the crisis exceeds normal capacity should be established in advance.

The crisis management system also depends on cooperation from actors outside government, including private sector infrastructure operators and civil society organisations. This is the operational dimension of the **whole-of-society** approach described in Section 1.2. Coordination arrangements and designated points of contact should be identified in advance with those actors the response is most likely to depend on, particularly with private sector operators. Similarly, arrangements for information sharing, joint assessment, and access to the coordination facility should be agreed and, where possible, tested through exercises. Where civil society organisations are likely to play a role in supporting affected communities or in reaching populations that government channels do not effectively serve, the relationships through which that cooperation would work should also be established before they are needed.

15 For research on the competencies required for effective performance in crisis management roles, and on developing teams for critical incident management, see: Rhona Flin, Sitting in the Hot Seat: Leaders and Teams for Critical Incident Management (Wiley, 1996).

Case 2 Ukraine, 2015–2022: cyber defence and government-private sector coordination[16]

Between 2014 and 2022, Russia subjected Ukraine to a series of escalating cyber attacks on critical infrastructure, government systems, and the wider economy. In December 2015, attackers used BlackEnergy malware to shut down three regional electricity companies. In December 2016, a more sophisticated automated attack using Industroyer malware disabled electricity transmission in parts of Kyiv. In June 2017, the NotPetya attack spread through the update system of Ukraine's tax reporting software, and rapidly through Ukrainian institutions and then globally.

Each crisis drove institutional reform that the government had previously been slow to pursue. A cybersecurity law first developed after the 2015 attacks was only adopted in 2017, following repeated major cyber incidents including NotPetya. This helped consolidate Ukraine's national cyber-defence architecture: the State Service of Special Communications and Information Protection (SSSCIP) for policymaking, the National Police for cybercrime, the Security Service for counter-intelligence, and a National Cybersecurity Coordination Centre at the National Security and Defence Council. A revised strategy and 94-task implementation plan followed in 2021, albeit with delays. Five days before the full-scale invasion in February 2022, the Law on Cloud Services was adopted, enabling the transfer of government data to servers outside Ukraine. Ukraine also developed closer operational coordination with internet service providers, mobile operators, and international technology firms. When Russia launched a massive cyber offensive alongside the military invasion, these arrangements proved critical. Cloud migration allowed many government systems to continue functioning despite Russian attacks. The April 2022 Industroyer2 attack on the energy grid, using an updated version of the 2016 malware, was neutralised through real-time collaboration between SSSCIP, Microsoft, and a Slovak cybersecurity company, which had been tracking the Industroyer family since 2016.

There were limitations with Ukraine's approach. The government acted only under the pressure of major attacks. Civil society groups and independent researchers often played an important role in exposing vulnerabilities and pushing for reform. The centralisation of cyber defence powers raised legitimate accountability concerns, and Ukraine's defence depended heavily on international support. But the case illustrates the cumulative value of government-private sector collaboration, even if driven by successive crises and when the framework remains incomplete. When the full-scale invasion came, the legal and institutional groundwork proved sufficient to coordinate a defence that helped prevent Russian cyber operations from causing the level of strategic disruption many observers had anticipated.

16 Khrystyna Kvartsiana, Ukraine's Cyber Defense: Lessons in Resilience, German Marshall Fund of the United States, December 2023; Chris Bronk, Gabriel Collins, and Dan S. Wallach, "The Ukrainian Information and Cyber War," Cyber Defense Review 8, no. 3 (Fall 2023)

2.3. Information management and planning

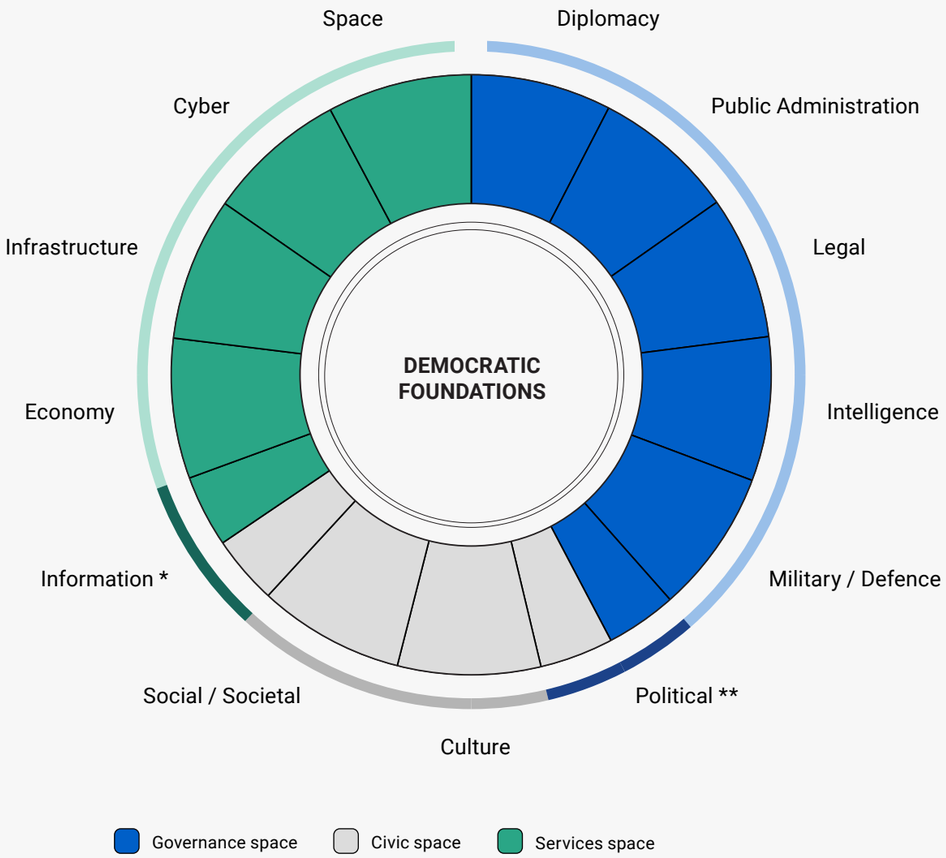
The crisis management system described above requires an information management capability through which the government assesses threats and produces the shared picture on which decisions are based. This should be developed and maintained on a standing basis, ready for activation.

Risk and threat assessment and situational awareness

The risk and threat assessment function provides the standing capability through which a government identifies threats early and prepares against them. It needs formalised processes to assess the threats the country faces and the vulnerabilities that could be exploited, across the various domains highlighted by the CORE model in Section 1.1. The assessment should also include an understanding of the principal actors that might target the country, their strategic objectives, and the means they have used or might use. Their own vulnerabilities and dependencies are also relevant, since this assessment provides the foundation for the development of response options directed at the threat actor. For hybrid threats, the process should be designed to connect information across domains rather than treating each in isolation. This is particularly important for pre-empting slow-burn crises, which often go undetected.

The CORE dartboard (Figure 6) provides a framework for organising the assessment across the thirteen domains grouped within their three spaces, making it possible to identify where threats are concentrated, where vulnerabilities exist, and where gaps in coverage remain. Alternative frameworks such as PEST analysis, which structures the assessment across political, economic, social, and technological dimensions, may also be useful depending on the country's circumstances and the nature of the threats it faces.

Figure 6 The Comprehensive Resilience Ecosystem*



* adapted from Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019

** Cross-cutting domains: Political spans the governance and civic spaces; Information spans the civic and services spaces

The assessment also needs a method for prioritising which threats to focus preparation on. Assessing each identified threat against the likelihood of it materialising and the severity of its potential impact provides a basis for this, and a simple matrix plotting likelihood against impact can help decision-makers see where the most serious risks lie and direct resources accordingly. A more comprehensive approach calculates risk as follows:

Level of risk = likelihood × vulnerability × initial impact × duration of disruption

Here, vulnerability refers to how exposed the state and its critical functions are to the specific threat if it materialises, and duration of disruption captures how long the effects are likely to persist before normal functioning can be restored. This captures more of the factors that determine how serious a threat is in practice but requires correspondingly greater analytical capacity to apply. The specific model for the risk and threat assessment function will need to be tailored to each country's situation, and for those facing resource constraints it is unrealistic to expect comprehensive coverage across every domain. But a basic preparatory step is to identify the priority threats the country faces, determine what information would indicate that those threats are developing, and establish a clear mechanism by which warnings can reach decision-makers with the authority to act. Whatever form the function takes, its findings should feed into the crisis management system both to inform the decision to activate a response and to support the development of response options, including options for measures directed at the threat actor.

Alongside the standing risk and threat assessment function, the government also needs an information management capability that can be activated when a crisis develops. This requires a dedicated information management team, established in advance and trained to seek out information, monitor reporting channels, and assess what is coming in. The team should draw on personnel from across government, reflecting the departments and agencies within the crisis management system, and should be led by a senior official with the standing to brief and advise effectively at the strategic level. Departments and agencies within the system should in turn be prepared to produce situation reports from their own areas of responsibility, feeding these into the information management function through pre-agreed reporting lines. **For hybrid threats, these reporting lines may need to draw on inputs from outside the national security apparatus**, from sectors that are likely early targets of a hybrid campaign, such as energy, media, and elections infrastructure. Where reporting lines from these sources into the crisis management system do not yet exist, establishing them is one of the most important preparatory actions a government can take. The team should work to consistent procedures and agreed formats, so that both those producing and those receiving information are familiar with the process before it is needed. These procedures should be established, documented, and tested through exercises. Arrangements should also be in place to activate the team quickly when the crisis management system is activated, with a standard operating procedure ready from the first hours.

The central product of the information management function is the common recognised information picture, or CRIP. This is a briefing document produced at regular intervals, setting out the team's assessed picture of the crisis situation as the agreed basis on which decisions are taken. It draws on the departmental situation reports described above and distils them into a single cross-government picture, distinguishing throughout between what is confirmed, what is uncertain or ambiguous, and what is being reported but not yet verified. Its purpose is to ensure that everyone involved in taking decisions starts from the same assessed picture, rather than arriving at the table with competing or partial accounts. The CRIP also serves the principle of accountability, providing a record of the assessed picture on which decisions were based and enabling subsequent review. The team should work to a consistent format so that the CRIP is immediately recognisable and usable, and the format, the procedures for producing it, and the reporting lines on which it depends should all be established and practised before a crisis occurs. How the CRIP is produced and used during a crisis is described in Section 3.2, but the format and the underlying processes must be in place before a crisis develops.

Procedures for activation

Right authority

The crisis management system requires clear procedures and criteria for its activation, both of which rely on the risk and threat assessment function. The national crisis management policy should designate who holds the authority to activate, so that this is settled before it is needed and not dependent on ad hoc negotiation at the moment a decision is required. Activation is a consequential decision and should be taken at a level appropriate to its significance, in line with the **principle of right authority**. Pre-agreed criteria should be established for determining when a situation has crossed the threshold. These will necessarily involve judgement rather than mechanical triggers but should be specific enough to support a timely decision. They might include the scale and severity of the threat, whether the situation exceeds the capacity of normal departmental responses, or whether it requires cross-government coordination at the strategic level. The risk and threat assessment function should monitor whether these criteria are being approached or met. There is a well-documented tendency for decision-makers to delay activation, particularly where the picture is uncertain or where the political costs of activating the system appear to outweigh the evidence of an emerging threat. The criteria and procedures should be designed to work against this tendency, enabling those responsible to act on assessed risk rather than waiting for certainty.

For hybrid threats, activation presents a particular additional challenge. Campaigns are often designed to fall below normal activation thresholds, and activity may be spread across multiple domains rather than concentrated in any one. Activation criteria should therefore be designed to capture patterns of coordinated activity across multiple domains. Provision should also be made for graduated activation, so that the government is not faced with an all-or-nothing choice between full mobilisation and no response. A lower level of activation, such as enhanced monitoring and partial assembly of the crisis response unit, allows the response to be strengthened as the situation develops and the picture becomes clearer.

2.4. The crisis management plan

Once a crisis has been declared, a dedicated and pre-planned crisis management plan should then be activated. This plan is the document prepared in advance to translate the decision to activate the system into a functioning operation. It should set out how the system is stood up: notification and assembly of personnel, access to the crisis coordination facility, the procedures for getting systems working from the first hours, how the information management function begins producing the initial picture for decision-makers, and how the crisis management system integrates with other national response mechanisms that may already be active, such as civil protection, military, or cyber incident response arrangements. The plan should also establish the standing operating procedures by which the response runs once activated: the meeting and reporting rhythm, the procedures for recording decisions and tracking their implementation, and the arrangements for escalation and handover.

The plan cannot be a script for specific scenarios; rather it is a framework for organised adaptation, providing a common basis from which those managing the response can work whatever situation they face. Its value lies in providing a discipline that those within the system can rely on without needing to negotiate arrangements under pressure. For hybrid threats, the plan takes on particular importance. The nature of the crisis may be unclear at the point of activation, several national response mechanisms may need to operate simultaneously, and the response may shift across domains as the campaign develops. The plan should therefore include, or reference, pre-assessed response options that the strategic body can draw on when setting the direction of the response. These are not prescriptions for specific scenarios but a prepared range of measures, covering both the domestic response and measures that may be directed at the threat actor across diplomatic, economic, legal, and other domains, with the legal authorities required, the coordination arrangements involved, and the likely effects and risks assessed in advance. Their value is that the strategic body can consider and adapt options that have already been thought through rather than developing them under crisis pressure. The activation arrangements and standing procedures need to be robust enough to function under these conditions, which places a premium on flexibility in the plan and discipline in its execution.

Continuity of government operations during a crisis requires deliberate planning. Crisis management and the maintenance of normal government functions are distinct activities that draw on the same personnel, resources, and senior leadership attention, and without advance arrangements for how these are shared, both will suffer. A typical failure is that the crisis response absorbs capacity needed to sustain essential public services, or that continuing demands from normal operations starve the crisis response. The plan should therefore identify which government functions are essential and must be maintained during a crisis, which can be reduced or suspended to free capacity, and who holds the authority to direct these allocation decisions across departments.

Much of the value of the crisis management plan lies in the process of producing it. Working through the arrangements across departments and agencies builds familiarity with the system, surfaces problems in the design before they are encountered under pressure, and develops the working relationships on which effective coordination depends. A plan written by one office and distributed without wider engagement will not achieve this. Once produced, the plan should be tested through regular exercises, which are addressed in Section 5, and reviewed as the threat environment changes, as lessons are learned, and as personnel and structures evolve. A plan that is not actively maintained will degrade.

2.5. Communications planning

The crisis management system also requires advance preparation for how the government communicates during a crisis, with the public, with the media, within government itself, and with international partners. A government that has not prepared its communications arrangements will be slow to inform the public and reactive in its engagement with the media. In a hybrid crisis, the problem is more acute. The information domain may be the primary domain of attack, with hostile actors working to shape public perception, undermine confidence in government, and exploit uncertainty well before the government has recognised that a crisis is underway. A government that enters this environment without prepared arrangements for public communication, coordinated messaging, and monitoring of the information space will find itself competing for the narrative from a position of disadvantage.

A dedicated strategic communications function should thus be allocated within the wider crisis management system described in Section 2.2. This is responsible for managing the government's public communication during a crisis, for coordinating internal communications so that government personnel are informed through official channels, for monitoring public discourse and media reporting as the basis for adapting the communications approach, and for advising decision-makers on the communications implications of response options. In the context of hybrid threats, this last responsibility is particularly important as response decisions may need to be assessed not only for their operational effect but for what they communicate to the public, to the hybrid threat actor, and to international partners. Strategic communication should not be an additional duty assigned to officials whose primary responsibilities lie elsewhere. Instead, it requires a designated lead with the standing to advise the CM team and the strategic body on communications matters, and with the authority to coordinate messaging across the departments and agencies involved in the response. The government should also designate in advance the senior officials who will act as public spokespersons during a crisis, at a level appropriate to the severity of the situation.

The communications function needs its plans, procedures, and preparatory materials in place before a crisis occurs. Pre-prepared holding statements and templates should be ready for rapid adaptation, structured around a clear content hierarchy: what has happened, what is being done, and what the government's position is. Background information on the government's crisis management arrangements and on areas of likely public concern should also be prepared, so that it can be issued quickly in the first hours of a crisis to fill the information void that will otherwise be filled by speculation or, **in the case of hybrid threats,** by hostile actors. These materials cannot anticipate every scenario, but they reduce the time between the onset of a crisis and the government's first substantive public communication. Procedures for media engagement should be established in advance, including the arrangements for briefings, the coordination of public statements with other agencies involved in the response, and the circumstances under which different levels of spokesperson are deployed. Those designated as spokespersons should be trained and practised in the role before a crisis occurs. The audiences the government will need to communicate with should be identified in advance, including the general population, specific groups likely to be affected, government personnel, the media, and international partners. For each, the government should understand how they receive and process information, and should have established the channels through which it will reach them. Crises also generate new audiences that were not anticipated, and the communications plan should be designed to adapt as the situation and its effects become clearer.

The communications function also requires resilient infrastructure. Primary communications channels may be disrupted during a crisis, whether through technical failure, overload, or deliberate attack, and alternative systems should be identified and tested in advance. Arrangements should be in place to expand the government's capacity to handle public and media contact rapidly, since the volume of enquiries in the first hours of a serious crisis will exceed what normal staffing can manage. The function should also maintain a standing capability to monitor public discourse, media reporting, and social media activity, as a communications-specific responsibility distinct from the information management team described in Section 2.3. At a minimum, this requires designated personnel with responsibility for tracking relevant media outlets and online platforms, pre-identified sources and channels to watch based on the country's information environment, and established reporting lines so that significant developments reach the communications lead and the CM team quickly. Where resources are limited, the priority is to ensure that someone is systematically watching the information space rather than to build a comprehensive monitoring operation. Relationships with civil society organisations, fact-checking bodies, or media partners can supplement government capacity. For hybrid threats, the monitoring capability should be designed on the assumption that the information environment will be actively contested and that hostile information operations may be underway before the crisis is formally recognised.

Right intention

An overarching narrative framework, prepared in advance, can help a government provide coherence to its public communication during a crisis. The framework sets out the government's core position on the security challenges facing the country: the values and interests it is defending, the approach it is taking, and the basis on which it is acting. Grounding that position in the protection of the population and the democratic values described above gives practical expression to the **principle of right intention,** committing the government in advance to a communications posture oriented towards the public interest. In practice, this can take the form of a short guidance document, ideally concise enough to function as a single reference, setting out the government's core narrative and the key themes that all public communication should reflect. It provides the reference point from which departments and agencies develop their own communications, so that the public hears a consistent account even when different parts of government are addressing different aspects of the crisis. In a hybrid crisis, the narrative is received not only by the domestic public but by the hostile actor and by international partners, and what the government says and does will signal resolve, intent, and the basis on which it is acting to all three audiences. A narrative grounded in the protection of the population is harder for the hostile actor to undermine than one framed around the authority or interests of the state, and gives international partners a basis for alignment and support. The framework should be endorsed at the strategic level and understood across the departments and agencies involved in the response, so that public communication is consistent without requiring every statement to be centrally cleared.

The communications preparations described in this section also contribute to building and maintaining the trust between government and population but they cannot compensate for a broader failure to align government conduct with democratic foundations. Credible crisis communication ultimately depends on consistency between what the government says and what it does. Honest communication is not a guarantee against the effects of disinformation, particularly where pre-existing societal divisions or low media literacy create vulnerabilities that hybrid threat actors can exploit regardless of what the government says, but it remains the most defensible basis on which to sustain public confidence. What the government states publicly during a crisis also becomes part of the record on which its conduct will be judged afterwards, and any gap between its statements and its actions will be identified and exploited.

Case 3 France, 2017: the “Macron Leaks” operation[17]

During the 2017 French presidential election, a coordinated operation sought to undermine the candidacy of Emmanuel Macron and the liberal, pro-European agenda he represented. Kremlin-aligned media and online networks fabricated claims that Macron held secret offshore accounts and served foreign financial interests, amplified further by alt-right and far-right networks. In parallel, hackers infiltrated campaign staff email accounts. On 5 May, two days before the second-round vote and timed to coincide with the legally mandated election silence, 15 gigabytes of stolen data were released online, with forged documents mixed into authentic material.

The French government’s response drew on an interministerial coordination structure under the Secretariat-General for National Defence and Security (SGDSN), with the Defence and National Security Council providing the strategic framework within which ministries and security authorities exchanged information and coordinated action. Preparation had begun months earlier, after the SGDSN tasked the national cybersecurity agency (ANSSI) with monitoring the electoral campaign and raising awareness across political parties. ANSSI convened parties for a cybersecurity workshop in October 2016, and visited the Macron campaign headquarters directly in early 2017 to warn of the threat. When the leak came, the response operated through pre-established channels: the electoral commission urged media outlets to exercise restraint in reporting unverified material during the election silence period; the media regulatory authority reinforced this to broadcasters. According to later reporting, the campaign had inserted some decoy documents into its systems, and it issued a rapid statement noting the presence of forgeries in the leak. Major media outlets, led by Le Monde, declined to publish the material before verification.

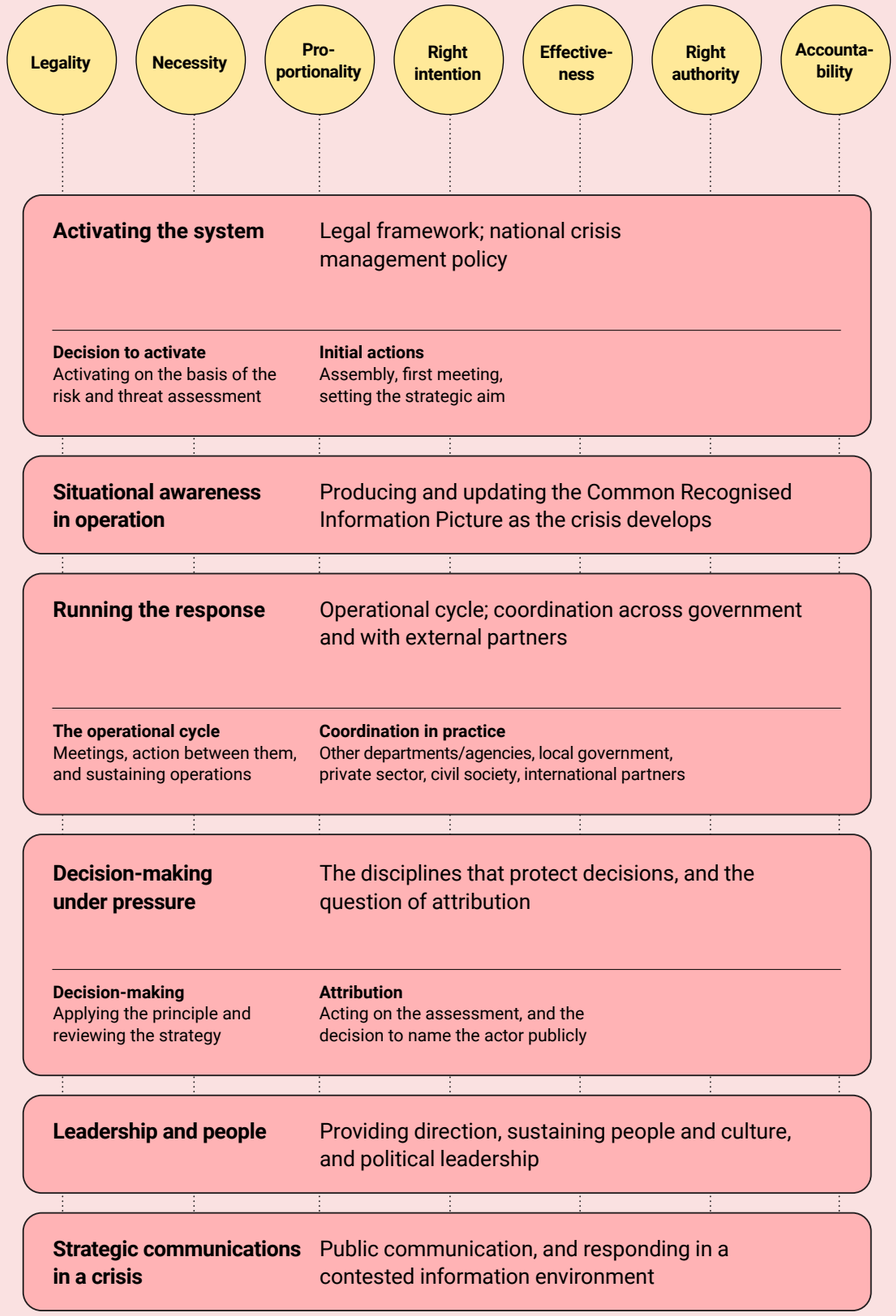
The case illustrates the value of preparation coordinated across government before a crisis materialises. The SGDSN’s coordination framework, ANSSI’s direct engagement with political parties, and the pre-existing regulatory mechanism of the election silence period provided the channels through which the response operated. In 2025, France formally attributed the operation to Russia’s GRU military intelligence.

17 Jean-Baptiste Jeangène Vilmer, The “Macron Leaks” Operation: A Post-Mortem, Atlantic Council / IRSEM, 2019; Boris Toucas, “The Macron Leaks: The Defeat of Informational Warfare,” CSIS, 2017; Erik Brattberg and Tim Maurer, Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks, Carnegie Endowment for International Peace, 2018.

03 *Running the Crisis Management Response*

This section covers activating and running the crisis management system under the pressure of a hybrid attack. It addresses the activation of the system, situational awareness and the assessed picture, the operational cycle and coordination, decision-making under pressure, leadership, and strategic communications during the response. Throughout, the response must be conducted on the assumption that a hybrid threat actor is actively working to undermine it. By applying the principles for crisis decision-making established in Section 1.3 those managing the response can ensure that the decisions they take under pressure remain consistent with the democratic values the response exists to protect.

Figure 7 Running the crisis management response



3.1. Activating the system

The first action in responding to a crisis is to activate the crisis management system, on the basis of the criteria and arrangements described in Section 2.3. The individual designated to activate the system should do so where the risk and threat assessment function indicates that the criteria for activation are being approached or met but they should also be alert to the risk of a slow-burn crisis developing. A hybrid campaign may approach the activation threshold gradually rather than cross it suddenly, generating coordinated pressure across several domains while no single element, taken in isolation, appears to warrant an extraordinary response. Decision-makers should therefore engage with the risk and threat assessment on a continuing basis and be prepared to act on imperfect information rather than waiting for decisive evidence that a campaign is running. A precautionary activation that is later stood down carries far less risk than a delayed response to a threat that has been allowed to develop. Where the picture is particularly uncertain, activating at a lower level, for example enhanced monitoring and partial assembly of the crisis management team, is preferable to waiting. The individuals responsible must be reachable at short notice, and if unavailable, it must be clear who acts in their place. The decision to activate, and the assessment on which it was based, should be recorded from the outset.

Once activated, the core crisis management team should assemble at the designated facility as quickly as possible. The information management team should begin work immediately, producing an initial assessment of the situation from whatever information is available. The communications lead should prepare to issue an initial public statement, drawing on the preparations described in Section 2.5. Where other national response mechanisms are already active, such as civil protection, military, or cyber incident response arrangements, the crisis response unit should establish contact and confirm how these will be coordinated within the overall response. In the first hours, available information will be sparse and much of it unverified. The priority is to get the system functioning and to establish a shared, if provisional, understanding of the situation, not to commit to detailed response decisions before the team is assembled and the information picture has begun to form.

The first meeting, chaired by an individual of sufficient seniority to match the seriousness of the situation, should bring together the strategic body and the CM team, and should open with a briefing on the initial CRIP. On that basis, the strategic body should confirm the strategic aim of the response: a clear statement of what the government is trying to achieve, broad enough to guide action while the situation is still developing but specific enough to give direction. In a crisis caused by a hybrid attack, the aim should encompass both what the government is seeking to protect, directed at the welfare of the population, and what it is trying to achieve in relation to the hostile actor, so that the response is directed against the campaign as a whole rather than only at its immediate effects. The strategic body should set the initial priorities and issue direction to the departments and agencies involved, so that all parts of the response understand the scope of the crisis, their role within it, and what they are expected to do first. The legal adviser should brief the meeting on what powers are available, any constraints on their use, and whether the available authorities are adequate to the situation as it is developing. Where the crisis does not fit neatly within the categories on which existing legal powers are built, which may occur in hybrid campaigns, this should be identified at the outset so that any expansion of authority is sought through proper legal channels rather than improvised under pressure. The chair should establish the operating rhythm by which the response will be conducted, including the schedule for meetings, CRIP updates, and reporting. Where the crisis has an international dimension, the international liaison function should initiate contact with relevant counterparts early. All decisions should be recorded as they are agreed, with each action allocated to a named individual and a clear deadline. The strategic aim will need to be reviewed as the picture develops, but establishing one from the outset gives the response coherence and provides the framework within which the CM team and departments can act.

3.2. Situational awareness and the CRIP in operation

The CRIP is the principal tool for providing decision-makers with situational awareness during a crisis. The exact structure should be adapted to each government's processes, but each update should set out, in a consistent format, what has happened (or what might have been expected but has not occurred), what the current effects are, the scale and severity of the situation, how it is developing, and what might happen next under different assumptions about how events could unfold. The team should go beyond compiling reported facts and assess what the information means for the government's response. Where the situation presents a choice, the team should frame the options and trade-offs clearly enough for decision-makers to act on them. The team should also state the assumptions on which the assessment depends, particularly where significant decisions rest on them, so that decision-makers can revisit them as new information comes in. In the early hours, the first CRIP will necessarily be brief and contain significant gaps. It should be issued nonetheless. As the crisis develops, the team should expand the scope and depth of the assessment, but what it covers at any point should be driven by what decision-makers need at that stage, not by the team's ambition to produce a comprehensive document.

Through the crisis, the information management team should maintain the CRIP as a continuous, standing product, updated at regular intervals, so that each meeting of the crisis management team opens with a current assessed picture. The team draws primarily on departmental situation reports, supplemented by intelligence assessments and open-source reporting, synthesising these into the cross-government picture and identifying where the gaps are. It should direct departments to report on specific questions or areas where the picture is incomplete, rather than relying on whatever individual departments choose to provide. If a significant development occurs between scheduled updates, the team should alert decision-makers immediately rather than waiting for the next meeting. During a prolonged crisis, the CRIP also serves as the basis for handovers between shifts. Producing the CRIP should never slow the decision-making process, however. If the team is spending disproportionate effort on refining the document, the balance between the product and the response it exists to support is wrong.

For hybrid threats, the CORE model introduced in Section 1.1 provides a framework for structuring the CRIP so that the cross-domain picture is visible in a single document. It may be advantageous for the information management team to organise the assessment around the CORE domains, to track not only where hostile activity is occurring but also where its effects are spreading. A cyber attack on energy infrastructure, for example, may simultaneously be producing economic disruption, undermining public confidence, and creating political pressure, and these connections will not be apparent if each is reported by a different department in isolation. To produce a cross-domain picture, the team should extend its reporting as far as its capacity allows, focusing on the domains most relevant to the threats the country faces. This will primarily draw on government departments and agencies, but may also require reaching into sectors outside the traditional security apparatus. Most governments will not be able to maintain comprehensive coverage across every domain, and they do not need to. Even a basic structure for connecting reporting across domains will add significantly more value than detailed coverage within individual domains that is never drawn together. The team should also look beyond the domains where hybrid threat activity has already been identified. Even if only covered in broad terms, a working assessment of what the hostile actor's objectives appear to be and where the campaign may move next helps decision-makers anticipate developments rather than responding only to what has already occurred.

The information management team should also encourage departments to report activity that does not fit expected patterns, even where its significance is unclear. Asking departments to flag unusual activity and looking for connections between seemingly unrelated developments may not require additional analytical capacity. It requires the team to think systematically about what it is not seeing as well as what it is. In a hybrid crisis, the information environment itself may also be contested, and some of what reaches the team through open sources and media reporting may have been placed or shaped by the hostile actor's information operations. The team should question the reliability of its sources and flag where the picture may be being deliberately distorted, so that decision-makers understand not only what the information says but how confident the team is in it.

3.3. Running the response

The operational cycle

Once the crisis management system has been activated and the initial meeting has taken place, the response operates through a continuing operational cycle. The cycle runs at both levels of the architecture: the strategic body meets periodically to review direction and take the most consequential decisions, and the crisis response unit works continuously between those meetings to maintain the response. The cycle gives the response its structure and continuity and provides a common rhythm that all parts can work to. **In a crisis caused by a hybrid attack**, where the response may draw in departments and agencies that do not normally operate together under crisis conditions, this common rhythm helps hold the cross-domain response together.

Accounta-bility

The meetings are where the cycle is formalised: where the assessed picture is reviewed, decisions are taken, and direction is issued. They should be structured around the decisions that need to be taken, not around standing agenda items or departmental reporting, with the most urgent decisions addressed first. Each meeting should open with the current CRIP briefing, so that all participants begin from the same assessed picture and do not spend the meeting trying to establish one. On that basis, the team should confirm whether the current strategic aim and priorities remain valid, take the decisions required, and issue clear direction to those responsible for carrying them out. Decisions should be recorded as they are taken, with the reasoning behind them, and direction issued immediately rather than held until a formal record is compiled afterwards. This avoids delay, preserves the reasoning where decisions are taken in rapid succession, and creates the record on which decisions can be reviewed and their basis explained afterwards. Each decision should be expressed clearly enough to act on, allocated to a named individual with a realistic deadline, and accompanied by a clear line of reporting so that the team can track its implementation. The chair should bring meetings to a prompt end, so that the team and those it directs have time to carry out what has been decided and prepare for the next cycle. Where a matter requires further analysis or consultation before a decision can be taken, the team should commission that work and set a deadline for its completion, rather than extending the meeting into open-ended discussion.

Between meetings, the crisis response unit should track whether the direction issued at the last meeting has been carried out and what effect it has had. Where an action has stalled, been overtaken by events, or produced consequences that were not anticipated, this should be identified early rather than discovered at the next meeting. In a crisis caused by a hybrid attack, the hostile actor may be actively working to disrupt the implementation of decisions, and the crisis response unit should be alert to the possibility that implementation failures are not simply operational problems but effects of the campaign itself.

The unit should also prepare the basis for the next round of decisions, identifying the issues that will need to be addressed, assembling the information the team will need, and structuring the agenda so that the meeting can focus on the decisions that matter most at that point in the crisis. Where a significant development occurs between scheduled meetings, or where an operational matter turns out to carry political, legal, or resource consequences that exceed the unit's delegated authority, it should be escalated to the strategic body immediately rather than held for the next scheduled meeting at that level. Where the situation is moving quickly and the interval between formal meetings is too long for effective coordination, shorter and less formal mechanisms can be used to bridge the gap, such as brief standing meetings at which participants compare notes and confirm their immediate next steps without the full structure of a formal CM team meeting.

A crisis caused by hybrid threats may last weeks or months, and the operational cycle must be maintained without degradation over that period. The preparations for sustainment described in Section 2.2, including arrangements for rotation, rest, and surge capacity, should already be in place. When the crisis extends beyond the first day, the crisis response unit should operate on a structured shift system, with a formal handover between outgoing and incoming personnel at each changeover. The handover should cover the current assessed

picture, the outstanding actions and their status, the decisions pending and the deadlines attached to them, and the current strategic direction. It should be treated as a defined procedure rather than an informal conversation, thorough enough that incoming personnel can maintain the response without loss of continuity. There is a natural tendency for those on duty to remain beyond the end of their shift to see how events develop. This should be resisted. Fatigued personnel make worse decisions, and allowing the boundary between shifts to blur will undermine the rotation arrangements on which sustained operations depend.

As the crisis develops, the pace and frequency of the cycle should be reviewed. The rhythm established in the acute phase of the crisis, when decisions may be needed several times a day, will not necessarily remain appropriate as the situation stabilises or as the character of the response shifts from immediate containment to longer-term management. Where the crisis enters a slower phase, the meeting frequency can be reduced and the intervals between CRIP updates lengthened, provided the ability to reconvene at short notice is maintained. Where a hybrid threat actor renews or redirects pressure across a different domain, the cycle may need to accelerate again. The logistical arrangements that support the cycle, including the crisis coordination facility, communications systems, and administrative support, should also be reviewed periodically. Arrangements that are adequate for a response lasting days may prove insufficient over weeks.

Coordination in practice

Effective coordination across departments, agencies, and other key actors requires active management during a live crisis. The coordination structures described in earlier sections should be prepared in advance, but having them in place does not produce effective coordination on its own.

The crisis response unit maintains regular contact with departments throughout the response, confirming that direction is being acted on and identifying early where the response is fragmented or where gaps have opened between areas of responsibility. Where a department is not acting on the current direction, the reason may be a failure of communication, a capacity constraint, or a substantive disagreement about priorities, and each requires a different response. The crisis response unit needs the authority and the situational awareness to distinguish between these and to address them. Coordination is also strengthened by the presence of departmental representatives in the CM team. Representatives with sufficient seniority and authority to commit their departments to action allow coordination problems to be resolved in the meeting rather than through slower exchanges between the centre and individual departments, and they bring operational knowledge of what their departments can and cannot deliver, which improves the quality of decisions and reduces the gap between what is decided centrally and what is implemented. Where pre-established arrangements do not fit the situation, the crisis response unit needs to adapt them: bringing in departments or agencies that were not part of the original plan, creating new arrangements for problems that were not anticipated, or adjusting the division of responsibilities. Effective crisis coordination typically involves a degree of improvisation within the established framework, and those managing the response need to be prepared and empowered to do this rather than persist with arrangements that are not working.

Measures directed at the threat actor should be developed and decided within the same strategic framework as the rest of the response, and reported into the same assessed picture, so that the strategic body is directing a single coherent effort rather than overseeing two that may be working at cross-purposes. The risk is that the two are not coordinated, as a result of classification constraints on intelligence, the political sensitivity of action directed at another state, and the direct reporting lines some departments hold to political leaders. The result can be that outward-facing measures are disconnected from the domestic response and from what the government is communicating publicly, creating incoherence that the hostile actor can exploit.

Pro-portionality

Regional and local authorities and operational agencies are closest to the effects of the crisis and the response. The crisis response unit should require regular situation reports from them covering conditions within their areas of responsibility, the impact of the crisis on the population and on the systems and services they manage, and the practical effects of measures taken at the national level. This reporting is essential for decisions about resource allocation, public protection, and whether national-level measures are achieving what they are intended to achieve. It should also identify where measures are having unintended or disproportionate effects on specific communities or regions, since in a hybrid crisis a hostile actor may be looking for precisely these effects to exploit and amplify. In return, regional and local authorities and agencies need to understand the government's strategic direction and current priorities, and to see how their reporting is being used, if they are to align their own response effectively.

Necessity

Coordination may also be required with private sector operators of critical infrastructure. Where energy, telecommunications, transport, or financial services infrastructure is being targeted or disrupted, the crisis response unit should share operational information on the nature and extent of the threat, conduct joint assessment of the risks to specific systems, and agree the government's role in protecting, prioritising, or restoring services. Where the crisis directly involves infrastructure or supply chains on which the government's own response depends, bringing sector representatives into the coordination facility with access to their own operational data and communications can create a shared information capability significantly more effective than exchanges conducted at arm's length. Modern supply chains are deeply interconnected, and the dependencies between sectors may not be immediately obvious; coordination with the private sector should therefore extend to identifying and monitoring these dependencies as the crisis develops. Civil society organisations may also have a significant role during the response, particularly where they provide support to affected communities, play trusted intermediary roles with populations that do not engage readily with government, and have ground-level knowledge of how the crisis and the response are being experienced that official reporting channels may not capture. The nature of that role will vary and cannot be prescribed in advance, but the crisis response unit should know which organisations are active in relevant areas and should have the means to communicate with them.

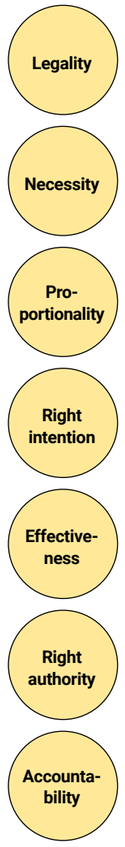
Effective-ness

For all of these non-government actors, coordination works through practical reciprocity. The government provides information, assessment, and where possible direct support, and in return draws on operational capacity, local knowledge, and specialist expertise that it cannot generate from the centre. Not all governments will have the established relationships or the institutional capacity to coordinate across all of these actors in depth during a crisis, and where capacity is limited, the priority should be those whose cooperation is most critical to the effectiveness of the response.

Where the crisis has an international dimension, coordination with allies, partners, and multilateral mechanisms brings information, analytical capacity, and joint action that the national government cannot generate on its own. The crisis response unit should maintain this coordination throughout the response: sharing assessments with counterparts so that there is a common understanding of what is happening and how it is developing, coordinating response measures where the actions of one government have implications for others, and aligning public communications so that the government's narrative is not contradicted by what allies are saying. For hybrid threats, international coordination is particularly important. The same threat actor may be targeting several countries simultaneously or sequentially, and international partners may hold information or assessments that the national government does not have access to on its own. Attribution decisions, discussed further in Section 3.4, may carry greater weight when taken or announced jointly with partners. Achieving a coordinated multinational response requires more time and effort than a purely national one, and the crisis response unit will need to manage this alongside the demands of the domestic response. Those responsible for international liaison need the authority to share information and coordinate positions on behalf of the government, within the parameters set by the strategic body.

3.4. Decision-making under pressure

The way decision-makers process and act on information under crisis conditions is subject to predictable pressures. The initial reading of the crisis, formed rapidly and often on limited evidence, tends to shape every subsequent assessment, and a flawed initial frame can persist long after the evidence should have corrected it. Teams under pressure converge on a shared view too quickly, and individuals become reluctant to challenge it. Departments feeding information into the process may filter it, presenting what senior leaders are expected to want to hear. In a hybrid crisis, a hostile actor may be working to amplify several of these pressures simultaneously. These are standard features of crisis decision-making rather than failures of those experiencing them, and the response is to build awareness of them, and discipline against them, into the way the team operates.



All seven of the principles set out in Section 1.3 apply to significant decisions taken during the response. For the most consequential decisions, particularly those involving restrictions on rights, the use of exceptional powers, or measures that carry significant risk of unintended harm, those chairing should ensure that the principles are worked through before the decision is confirmed. The questions are designed to be applied under pressure and need not be a lengthy exercise. Building them into the meeting discipline ensures they are addressed as part of the decision rather than as an additional step.

Several of the principles are supported by institutional arrangements within the crisis management system: dedicated legal advice for legality, the architecture and escalation procedures for right authority, the recording disciplines established from the outset of the response for accountability. Right intention is addressed as a dimension of leadership in Section 3.5. Three principles, however, require judgements more vulnerable to the pressures described above, partly because the standards by which they can be assessed are more subjective. Necessity asks whether the proposed action is needed given the assessed picture, and whether less restrictive alternatives have been adequately considered. Proportionality asks whether the action is in line with the harm it seeks to prevent, and whether the risks of unintended consequences have been assessed. Effectiveness asks whether there are reasonable grounds for believing the action will achieve what is intended. The crisis management system cannot answer these questions for the decision-maker. They require those in the room to exercise judgement on incomplete information, and are the tests most at risk of being overridden by the instinct to act decisively, by political pressure to respond visibly, or by institutional momentum.

The first practical discipline is that decision-makers should accept that they will choose between courses of action on an imperfect picture. Under crisis conditions, the instinct may be to wait for a fuller picture before committing, or to attempt a systematic comparison of alternatives. Neither is realistic. **The discipline is to act on what is known, to choose the least bad course available rather than the best one, and to test that choice against necessity, proportionality, and effectiveness before committing to it**. A decision tested in this way may still prove to have been wrong, but it will have been taken on a defensible basis and can be honestly accounted for afterwards. In a hybrid crisis, this discipline has a further significance. A response that is unnecessary, disproportionate, or ineffective is precisely what the hostile actor may be working to provoke, and a government that tests its decisions against these principles is denying the attacker one of the outcomes the campaign was designed to produce.

Decision-makers can also take several specific steps to protect the quality of their judgements. How meetings are chaired affects the quality of decisions taken in them. Leaders and senior officials should chair to encourage honest input, hearing assessments and options before expressing a position. Where a senior figure states a preferred course of action at the outset, the group will tend to converge on it, undermining the ability of others with knowledge in the room to contribute. Decision-makers should also scrutinise the assumptions on which they are being asked to make decisions, explicitly asking CM team members what assumptions the options depend on. This need not be an extended exercise. A short, disciplined step ensures those involved know what they are relying on and creates the basis for knowing when to revisit the decision as the situation develops. Before committing to a course of action, those chairing may also consider putting a specific question to the team: if this measure is implemented and does not achieve what is intended, what is the most likely reason? This focuses attention on the risks of implementation and may surface practical obstacles or unintended consequences that would not otherwise emerge until the decision has been acted on.

Decision-makers can also test their assumptions and decisions in two further ways.

- First, they should ensure they are hearing from those closest to the effects of the crisis and the response, not only from reporting that has been filtered through departmental hierarchies. Where the response involves measures that restrict rights or impose burdens on the population, this is one of the most reliable ways of testing whether a proposed course of action remains proportionate to the situation on the ground.
- Second, building deliberate challenge into the decision-making process is valuable before a significant decision is confirmed. A structured challenge function can be achieved by directing an individual to argue the case against the proposed course of action or by assigning a standing responsibility to identify what has been missed. How the function is structured matters less than its objective: ensuring that someone has been required to look for the weaknesses in key decisions and that they have been heard. Where the CM team reaches rapid agreement on a question that ought to be difficult, that should be treated as a reason to pause rather than as confirmation that the answer is obvious.

Alongside these disciplines at the point of decision, those managing the response should step back at defined intervals from the operational rhythm to conduct a broader review of the strategy. This is distinct from the routine adjustments to priorities and resources that form part of the normal operational cycle. Its purpose is to ask whether the overall strategy is achieving what it was intended to achieve, whether the assumptions on which it was built still hold, and whether the situation has changed in ways the current approach does not account for. Where the review concludes that the current approach is no longer adequate, the strategic body must be willing to act on that assessment, to change the strategic aim, to shift the balance between inward and outward-facing measures, or to accept that measures taken so far have not achieved what was intended and that a different course is required. These are among the most consequential decisions taken during a crisis, and the natural institutional tendency will be to defer them.

In a crisis caused by a hybrid attack, the review should address the government's objectives in relation to the hostile actor specifically. The strategic body should consider whether absorbing the campaign's effects while maintaining the state's capacity to function remains sufficient, or whether the situation requires the government to impose costs that deter further aggression or to take measures that actively disrupt the campaign. This is a strategic choice with significant consequences, and it should be made deliberately on the basis of the assessed picture rather than arrived at through incremental escalation or institutional drift. In considering that choice, response options should be assessed across all available domains, not only within the domain under attack. Diplomatic, economic, or legal measures may be more proportionate and more effective than responding in kind within a particular domain.

Decision-makers should also consider how the hostile actor is likely to react to the government's measures. A hybrid threat actor may be deliberately seeking to provoke a disproportionate response that can be exploited to undermine public trust, damage the government's international relationships, or justify further hostile action. The proportionality test set out in Section 1.3 applies with particular force in this context, and decision-makers should weigh not only the intended effect of a measure but also how it may be used against the government. An effective response will also consider what it is trying to get the hostile actor to do, not only what costs it seeks to impose, and should leave space for de-escalation where circumstances allow. The review should also assess whether the hostile actor may be changing its approach. An actor whose initial approach has been disrupted may escalate to more severe or more overt action, and calibrating the government's response to manage that risk, including through proportionate measures across domains rather than matching the hybrid threat actor's intensity in kind, is itself one of the most important functions of the review.

Attribution

Whether and when to attribute hostile activity to a specific actor is one of the most consequential decision points in a hybrid crisis. Attribution involves two distinct judgements. The first is the internal decision to treat activity as hostile and to direct the response accordingly, on the basis of the assessed picture, even where the evidence falls short of what would be needed for a public statement. The same discipline applies here as to other crisis decisions: the government should act on what the assessment supports rather than wait for a standard of proof that the hostile actor has specifically designed to deny. Where evidence is not conclusive, that does not mean it carries no weight, particularly where the consequences of it proving valid are serious. Where the CRIP indicates a pattern of coordinated activity consistent with a hostile campaign, decision-makers should be prepared to direct response measures on that basis while continuing to develop the evidential picture, rather than delaying until attribution is certain and allowing the campaign to develop further.

The second judgement is whether to attribute publicly by naming the actor responsible. In many cases, the barrier is not the inability to assess who is responsible but the political consequences of saying so. Public attribution is a strategic choice with diplomatic, legal, and security implications, and decision-makers should expect it to require escalation to the strategic body, with legal and intelligence advice, and should plan for it as a distinct decision point rather than allowing it to emerge from operational discussions. Where attribution is being considered, coordinating with allies and partners strengthens the position. The decision itself should be a measured strategic choice, not one forced by operational pressure or media demands for an answer. Those responsible for it need as much time and space as the crisis allows to weigh the evidence and its implications. The operational response should continue on the basis of the internal assessment regardless of whether public attribution has been made.

Both attributing and not attributing carry costs. Public attribution expands the government's range of available responses; without it, options such as targeted diplomatic action, coordinated sanctions, and counter-narrative strategies that name the source remain unavailable or lack legitimacy. But attributing on an insufficient evidential basis carries diplomatic risk and may expose the basis of the government's assessment. Not attributing concedes the narrative to the hostile actor and leaves the government unable to direct measures at the actor responsible. Where the assessed picture supports attribution but the decision is being deferred, decision-makers should recognise that deferral is itself a consequential choice, not a neutral position. The development of the evidential basis for attribution should be treated as an active and continuing process through the crisis.

Case 4 United Kingdom, 2018: the Salisbury nerve agent attack[18]

On 4 March 2018, Sergei Skripal, a former Russian military intelligence officer who had worked as a double agent for British intelligence, and his daughter Yulia were found unconscious on a bench in Salisbury, England. They had been poisoned with Novichok, a military-grade nerve agent developed by the Soviet Union. The attack subsequently exposed a police officer and, months later, two members of the public, one of whom died. One of Russia's objectives appears to have been to demonstrate that those who betray the Russian state will face consequences, wherever they are, while simultaneously testing the limits of what a Western government would tolerate on its own soil.

The UK government's response was coordinated through the National Security Council, which met repeatedly in the days following the attack, directing the approach towards attribution, imposing costs, and ensuring consistency in attribution and public messaging. Multiple departments and agencies were involved in the response, with communications closely coordinated to reduce opportunities for disinformation and contradictory messaging. The government moved rapidly to public attribution: on 12 March, the Prime Minister told Parliament that it was "highly likely" Russia was responsible, a formulation that reflected the intelligence assessment. Allied governments were briefed on the evidence, and within two weeks more than twenty-five countries and NATO had expelled over 150 Russian intelligence officers in a coordinated diplomatic response. The Organisation for the Prohibition of Chemical Weapons confirmed the identity of the nerve agent, and UK counter-terrorism police subsequently identified two GRU officers as suspects, publishing their identities and travel records.

The case illustrates the value of public attribution coordinated with allies. The UK's willingness to attribute rapidly, share the evidential basis with partners, and sustain a clear public narrative transformed what could have remained a bilateral incident into a collective response. The coordinated expulsions imposed a significant intelligence cost on Russia and demonstrated allied solidarity. The response was not without limitations. The attack was itself a deterrence failure, following the assassination of Alexander Litvinenko in London in 2006, after which the UK response was widely viewed as limited relative to the scale of the attack.

18 Joshua Stewart. "The Grey Orchestra: Elastic Communications and the UK's Response to Salisbury." RUSI Journal, 2022; Duncan Allan, "Managed Confrontation: UK Policy Towards Russia After the Salisbury Attack," Chatham House Research Paper, October 2018; David Omand, "From Nudge to Novichok," Hybrid CoE Working Paper No. 2, April 2018.

3.5 Leadership and people

Right intention

Accounta-bility

Effective crisis management requires effective leadership in ways not fully addressed in earlier sections: interpreting the crisis to those involved in managing it, maintaining the welfare and capacity of the people on whom the response depends, sustaining public confidence through the conduct of the response, and holding the response together over time. These are also the aspects of crisis management where **the principles of right intention and accountability** are most directly tested, and where hostile actors may be working to fragment coherence within government, exhaust those managing the response, and erode public trust. How leaders handle them determines whether the operational system and decision-making disciplines described in earlier sections function effectively over the course of the crisis.

Effective leadership across these disciplines depends on having the right people in the key crisis management roles. One of the most consequential early decisions for the person leading the response is whether they do. The individuals who happen to hold relevant posts when a crisis breaks may not always be the best available for managing it, and senior leaders should be willing to make changes early rather than waiting to see whether those in place prove adequate. Replacing personnel during a crisis is disruptive and can affect morale, but the cost of retaining someone who is not equipped for the role compounds as the crisis develops and becomes harder to correct the longer it is deferred. This applies both within government, where individuals with more relevant experience or stronger crisis management capabilities may be available from other parts of the system, and beyond it, where the crisis may involve domains or techniques for which the government does not have sufficient in-house expertise. Bringing in external specialists, whether on attribution, strategic communications, or the specific sector under attack, is a sign of effective mobilisation, not a sign of failure.

Senior leaders should provide those involved in the response with a continuing interpretation of the crisis: what is happening, what the response is trying to achieve, and why. This is a continuing responsibility between the defined points of the operational cycle, directed at the CM team and the wider government apparatus, and goes beyond the strategic aim that is formally set at those points. When briefing the CM team or chairing meetings, senior leaders should set out not only what has been decided but the reasoning behind it, so that those carrying out the decisions understand the judgement on which they rest. Where the picture is incomplete or uncertain, they should say so, clearly enough that those involved are not working on false assumptions, while maintaining confidence in the direction the response is taking. When the situation changes or earlier assumptions prove wrong, senior leaders should explain what has shifted and why the approach is being adjusted, rather than simply issuing new direction without context. Beyond the CM team, the direction issued after meetings should include sufficient reasoning for recipients to understand not only what is required of them but why, so that the departmental representatives described in Section 3.2 can carry the interpretation back to their own departments.

Leadership of the response also extends to the welfare of those managing it. The roster depth, rotation planning, and shift disciplines described in earlier sections provide the structural basis, but they depend on active leadership. Senior leaders and shift supervisors should monitor the condition of key personnel as a continuing responsibility, watching for signs of deteriorating performance, shortened temper, narrowing attention, or withdrawal. They should intervene when those signs appear, including by directing individuals to rest or rotating them out of the team even where they resist. The practical challenge is that the most capable and committed people are often those most reluctant to step back and most likely to be retained beyond the point where their performance has begun to decline. Senior leaders set the standard. If those leading the response do not themselves observe the shift boundaries, or are visibly working to exhaustion, they signal to everyone else that the welfare disciplines do not apply under pressure.

Accounta-bility

The **principle of accountability** depends on the culture that leaders maintain during the response, not only on recording and oversight mechanisms. Under crisis pressure, setbacks easily produce blame rather than learning, and where blame is the institutional norm, people stop reporting problems and decision-makers become risk-averse, preferring safe choices to the difficult judgements that effective crisis management demands. Leaders should work actively against this. When failures occur, they should direct attention to what happened and what needs to change rather than to who was at fault. They should make clear, early in the response, that the recording of decisions exists to support honest review, not to build a case against individuals. They should protect those who report problems, challenge the prevailing assessment, or bring forward information that contradicts what senior leaders have stated. They should also actively seek out bad news rather than waiting for it to be reported, by asking direct questions about what is not working and creating regular opportunities for honest assessment. Where blame is entrenched, protection alone will not overcome the reluctance to report. And they should be seen to act on what honest reporting reveals, because what happens to those who first report shapes whether others will do so. These are difficult institutional behaviours to uphold under crisis pressure, and maintaining them requires sustained leadership attention.

Right intention

The **principle of right intention** places a particular responsibility on political leaders, who are the visible face of the response and whose conduct, tone, and visible priorities shape public perception of whether the government is acting in the interests of the population. In a hybrid crisis, political leadership is a direct factor in the effectiveness of the response, because hostile actors may be working to erode public trust in government and deepen social divisions. Crisis conditions can also create strong incentives to act for political reasons, for example, to be seen to respond, to avoid blame, to wrong-foot opponents, or to consolidate authority. To promote trust and avoid the perception of politicisation, political leaders should ensure that response measures, particularly those that restrict rights or impose burdens on the population, are visibly connected to the protection of the public rather than to the preservation of the state's authority or the government's political position. A government whose crisis measures appear self-serving or disproportionate provides material for the hostile actor to exploit. Where the crisis affects different communities or regions unevenly, or where the hostile actor is deliberately targeting social divisions, political leaders should consider whether response

measures risk deepening those divisions, even where the measures are operationally sound. A government that is seen to be functioning effectively, acting honestly about difficulties as well as progress, and orienting its decisions towards the population's welfare denies the hostile actor one of the outcomes the attack was designed to produce.

Hybrid crises present a further leadership challenge in sustaining the response beyond the acute phase. A hybrid campaign may last months, and the hostile actor may deliberately reduce the intensity or visibility of its activity to encourage the government to stand down prematurely, before resuming or shifting to a different domain. There is a natural tendency among both political leaders and officials to draw the response down once the immediate pressure eases, particularly where the crisis has not produced the kind of dramatic events that sustain political attention. The decision to end or significantly reduce the crisis response should be a deliberate strategic judgement, taken by the strategic body on the basis of the assessed picture, not the gradual result of institutional attention moving elsewhere. To prevent this drift, the operational cycle can be reduced in tempo but not abandoned, with the information management function continuing to monitor for renewed or shifted activity. The strategic body continues to meet at defined intervals, reviewing the assessed picture and confirming that the conditions for reducing the response have genuinely been met rather than simply assumed. Trained personnel are retained in their crisis management roles rather than released back to normal duties, preserving the capacity to scale back up at short notice. Where the assessment indicates that the hostile actor has paused rather than ceased activity, the response is maintained on the assumption that further action is likely.

3.6. Strategic communications in a crisis

When a crisis is activated, the communications preparations described in Section 2.5 will need to function in an environment that a hostile actor may already be working to shape. The government's ability to establish a credible public account quickly, to communicate honestly when the picture is incomplete, and to sustain a coherent message across government while responding to hostile information activity is an operational requirement of the response. Everything the government says and does during the crisis will be read simultaneously by the domestic public, the hostile actor, and international partners.

In a hybrid crisis, hostile actors may already be shaping public perception before the government has released any communication. The communications lead should therefore prepare the first substantive public statement as early as the situation allows, adapting prepared holding statements and templates to the specific crisis based on whatever the initial assessed picture provides. The individual chairing the response clears the content before it is issued, but this should be a rapid check against the known facts and the strategic aim, not an extended drafting exercise. Beyond the initial statement, the communications lead should prepare a communications brief for each meeting of the strategic body to report what is being said about the crisis, what questions are emerging, where hostile narratives are gaining traction, and where the government's own messaging is not reaching its intended audience. On that basis, and reflecting the direction confirmed at each meeting, the communications lead prepares the next public statement or briefing. The aim is that the government communicates, as best it can, on its own terms and at a rhythm it sets, rather than waiting for media enquiries or hostile claims to force a response.

Substantive public communications during the response should reflect what is known on the basis of the current assessed picture, what the government is doing, what is not yet known, and a commitment to providing further information at a specified time or when significant developments occur. This discipline has direct operational value in a hybrid crisis. A government that overstates what it knows gives the hostile actor material to work with when the record has to be corrected. Corrections will be necessary in any case, and where earlier statements prove inaccurate or incomplete they should be issued promptly, openly, and with an explanation of what changed in the assessed picture. In some cases, operational security, intelligence considerations, or a pending attribution decision will constrain what can be disclosed. Where these constraints exist, the public communication should reflect a deliberate decision about what to share, and where the government cannot explain its reasoning fully it should acknowledge that constraint directly rather than attempting to conceal it. A government that says it cannot yet share its full assessment is more credible than one that appears to be evading the question.

The strategic narrative framework developed in Section 2.5 provides the common reference point for communications across government. After each meeting of the strategic body, the communications function updates the narrative and the current lines to reflect the direction issued, and circulates both to the departments and agencies involved in the response. The communications lead does not need to clear every departmental statement before it is issued; attempting to do so will create bottlenecks, slow the response, and in practice will be circumvented as departments find themselves unable to wait. What the communications lead does need to do is ensure that departments receive the updated lines before they communicate, and that the narrative framework is concrete and current enough for departments to apply it without further interpretation. Where the monitoring function identifies that a department is communicating in ways that contradict the government's position or that are being exploited by hostile actors, the communications lead should address this directly, distinguishing between a failure to receive updated lines, a genuine difference in assessment, or an institutional interest being pursued independently. The same coordination cycle should ensure that government personnel receive the government's own account through official channels before they encounter it through the media or through hostile information directed at them.

Responding to hostile information operations during the crisis requires judgement about which narratives to engage and how. The communications function should draw on the monitoring capability established in Section 2.5 to track which hostile narratives are circulating, where they are gaining traction, and which audiences they are reaching. Not all hostile narratives require a direct response. Engaging with every claim risks amplifying material that would otherwise reach a limited audience, and risks allowing the hostile actor to set the terms on which the crisis is discussed. Where the government's own communications are reaching their intended audiences and providing a credible account, that itself may be an effective counter to much of what a hostile actor produces. Where the communications lead judges that a direct response is needed, it should be factual, tied to what the government is demonstrably doing, and issued through the channel most likely to reach the audience the hostile narrative is targeting. For narratives directed at specific

communities or exploiting specific grievances, this may mean working through civil society partners, local authorities, or trusted media outlets rather than through central government channels. Crisis management leaders should also guard against the communications effort becoming dominated by rebuttal. In a prolonged hybrid crisis, the accumulation of hostile claims can draw the communications function into a reactive cycle, and the proactive communications agenda established earlier in this section is the principal defence against this.

There are limits to what the communications function can achieve against a sustained hostile information campaign, and crisis management leaders should not overestimate the government's capacity to control how the public understands the crisis. Hostile narratives are more effective where they describe something people can observe for themselves. A government whose response is visibly failing, treating communities unevenly, or serving those in power rather than the population gives the hostile actor material that no communications discipline can overcome. What the government can control is whether its own conduct makes the hostile actor's task easier or harder, and how honestly and effectively it communicates about what it is doing.

The attribution decision discussed in Section 3.4 requires specific communications preparation. Before the strategic body takes the decision, the communications lead should prepare messaging for both outcomes, so that the government is ready to communicate coherently whether it attributes or not. Where the decision is not to attribute publicly, the communications function must sustain a coherent account of the crisis and the response without naming the actor responsible, at a time when the media may be speculating, the public demanding answers, and the hostile actor exploiting the gap. This is more manageable where the government's narrative has been grounded from the outset in what is happening and what the government is doing rather than in who is responsible. Where public attribution is being considered, the communications lead should coordinate timing and wording with allied governments so that statements can be aligned. The CM team should also assess the hostile actor's likely response, so that the communications function can prepare follow-up messaging accordingly. The communications function should be prepared for the period immediately following any public attribution, when media and public attention will be intense, the hostile actor will be actively contesting the claim, and the government will need to sustain its position with consistent, factual follow-up rather than allowing the announcement to stand unsupported.

In a prolonged hybrid crisis, communications fatigue is a specific risk. Spokespeople lose impact through overexposure, messaging that conveyed urgency in the first days becomes routine, and public attention declines even where the underlying threat has not. The communications lead should adjust the tone and content of communications as the crisis moves between phases, sustain public engagement when the situation no longer commands attention on its own terms, and consider rotating spokespeople where appropriate. A hostile actor may also deliberately reduce the intensity of its campaign to encourage the government to lower its guard, and the communications function should maintain public awareness of a threat that no longer feels immediate.

04 Training and Exercises

Training and exercises are essential to ensuring that crisis management responses to hybrid threats are both effective and consistent with democratic principles. The structures, plans, and procedures set out in the preceding sections can be designed and put in place but a programme of training and exercising is needed to develop the people who will operate the crisis management system and identify weaknesses before a real crisis exposes them. This section addresses how to build that programme.

Figure 8 Training and exercises

Purpose of training	Developing officials' roles, decision-making, and the team as a coordinated unit
Forms and designs of exercises	Different forms of exercise, designed to build judgement under crisis conditions
Specialised exercises for hybrid threats	Scenarios that test detection and coordination, and training in specific response challenges
Sustaining the training programme and learning	Resourcing the programme, and supporting learning that improves plans, procedures, and approaches

Note: training and exercises are part of preparation.

The central purpose of training is to develop the capacity of politicians responsible for crisis management, senior officials and other members of the CM team to operate effectively under crisis conditions. Three aspects are especially important.

- First, those who will fill crisis management roles need to understand the crisis management system and their place within it. This includes understanding what their role requires, how the procedures and reporting systems work, and how their responsibilities connect to the wider response.
- Second, training should develop officials' capacity to make sound decisions under crisis conditions, including building the ability to assess an evolving and ambiguous situation, choosing a course of action with limited information, anticipating how choices are likely to play out and how to use the seven principles as practical tests at the point of decision.
- Third, training should develop the CM team's ability to function as a coordinated unit rather than as a collection of individuals who happen to know their own roles. This means building a shared understanding among team members of how each operates, what information each needs from the others, and how decisions are communicated and acted on, so that when a crisis occurs the team can coordinate effectively from the outset rather than spending the early stages learning to work together.

The most effective way to develop these capabilities is through **scenario-based training**, in which participants work through a simulated crisis that evolves as they respond to it. Unlike briefings on the plan or instruction in procedures, which can convey knowledge but cannot test whether people are able to apply it under pressure, scenario-based training places participants in conditions that approximate those of a real crisis and requires them to exercise judgement in real time. It can take several forms. Discussion exercises, in which participants talk through a scenario around a table with a facilitator, are the simplest and least resource-intensive format. They require no specialist facilities, can be arranged at relatively short notice, and can be completed in a few hours. Despite this, they are among the most valuable elements of a training programme. A well-designed discussion exercise will test whether senior officials understand the decisions that would fall to them in a crisis, whether coordination arrangements between departments work as intended, and whether the assumptions built into the plan hold up when examined against a realistic scenario. They are also an effective way of introducing officials to scenario-based training for the first time. Command post exercises are more demanding. The CM team operates from the crisis coordination facility, working through a scenario managed by directing staff who feed in information, simulate external developments, and maintain the pressure of an evolving situation. This format tests not only the team's decision-making and coordination but also the facility itself, the communications systems, and the information management procedures on which the response depends. Live exercises are the most comprehensive format. Staff and assets are physically moved and deployed across large areas, both where the impact of a crisis may occur and in planning areas, rather than being notionally simulated by directing staff in the crisis management centre. This is the only format that extensively tests whether the arrangements work end to end, from the decisions taken in the crisis coordination facility through to their implementation on the ground. It is also significantly more complex, disruptive, and expensive to organise. Alongside these scenario-based formats, simple tests of key systems or procedures also play an important role, such as testing whether crisis communications systems work, whether secure channels function under the conditions they would need to operate in, or whether the crisis coordination facility can be activated and staffed within the required timeframe.

Regardless of scale, each exercise should have a clear aim that specifies what is being tested, whether that is a particular function such as the invocation procedure or the information management team's reporting cycle, or the coordination of the full crisis management system under a developing scenario. The scenario itself should be built around a realistic situation but include specific elements that go beyond allowing the plan to run its course. These include information that is incomplete, ambiguous, or contradictory, so that participants must assess what is happening rather than receiving a clear picture; points at which departments or agencies must provide information to one another or coordinate their actions, so that the dependencies between them are tested under pressure; and developments that the plan did not anticipate, so that the team is required to adapt rather than follow a script. The programme of training should use a range of crisis types rather than rehearsing a single scenario repeatedly, so that participants build experience across the conditions the crisis management system may need to handle. For command post and live exercises, those running the exercise should manage the evolution of the scenario in real time, injecting new information, simulating

external pressures such as media reporting or public reaction, and adjusting the pace and complexity to maintain realistic pressure on participants. The scenario should be designed so that each member's role is genuinely engaged rather than present but passive, and decisions and communications should be recorded throughout so that the material is available for the debrief that follows.

There may be value in structuring training activity into a progressive programme, beginning with discussion exercises and building towards more demanding formats as the team's familiarity develops. Those who are new to their crisis management roles, or who have not previously taken part in scenario-based training, should begin with discussion exercises before being placed in more demanding formats. Not every government will be in a position to run the full range of formats, and the choice should reflect what is being tested and what resources are available. But a systematic and sustained programme will be more effective than occasional training and exercises. The capability that builds from these depends on regular practice, and a government that runs a consistent cycle, even around discussion and command post exercises alone, will be better prepared than one that invests in a single large-scale exercise and then allows the programme to lapse.

Hybrid campaigns create specific conditions that exercises should be designed to test. The first is detection and assessment under conditions of deliberate ambiguity. Scenarios for hybrid threat exercises should be tailored to reflect the multi-domain, multi-vector character of a hybrid campaign as described by the CORE model, with activity unfolding across several domains simultaneously and producing effects that cascade between them. Rather than presenting participants with a single, clearly defined incident, the scenario should require them to assess what is happening across a picture in which individual events may appear unrelated, the significance of particular developments may be unclear, and the involvement of a hostile actor is not established from the outset. This kind of scenario tests whether the information management and assessment functions can draw together reporting from across government and produce the cross-domain picture on which an effective response depends. One approach that can be particularly useful for hybrid threats is to ask participants, after a phase of the scenario has played out, to identify what preparations they now realise would have helped if they had been in place before the crisis began. This technique can surface gaps in preparedness that are difficult to identify in the abstract but become apparent once officials have worked through the practical demands of responding to a hybrid campaign. Exercises for hybrid threats should also bring together the full range of departments and agencies that the crisis management system encompasses, including those from non-traditional sectors that may not have participated in crisis exercises before. The coordination problems described in Section 3.3 will not surface unless those actors are present and genuinely engaged rather than observing from the margins.

Three further aspects of responding to hybrid attacks may also warrant specialised training.

- First, training scenarios can test how participants handle the attribution decision described in Section 4.4, for example by presenting evidence that is suggestive about a hostile actor's involvement but not conclusive alongside simulating pressure to make a definitive public statement before the assessment fully supports one. These scenarios can also require participants to work through the consequences of attributing or withholding attribution.
- Second, those responsible for strategic communications should receive training in how hostile information campaigns operate, so that they have a working understanding of the techniques involved and of how they differ from conventional negative media coverage. This does not require every communications official to become a specialist in information operations, but it does require sufficient familiarity to carry out the functions described in Section 3.6 (e.g. monitoring hostile narratives, distinguishing between material that requires a response and material that would be amplified by engaging with it).
- Third, exercises should test the process by which the strategic body develops and decides on outward-facing measures directed at the threat actor, requiring participants to work through escalation risks and the coordination of measures across diplomatic, economic, and other domains. This tests whether the departments responsible for those instruments are brought into the common operational cycle rather than operating on a separate track.

The value of training and exercises depends on whether they generate genuine learning, which means that any problems identified result in the implementation of changes to how the crisis management system operates. Learning in this sense requires several things in practice. Every exercise should conclude with a structured debrief, conducted promptly while the experience is still fresh, in which participants review what happened, what worked, what did not, and why. The conclusions should be recorded as a statement of lessons identified, together with an action plan specifying what changes will be made to the plan, the procedures, or the training programme as a result. The same rigour should be applied, not only to exercises, but to situations in which the system came under strain but the failure did not materialise, or in which a crisis was narrowly averted. Understanding why the system held in those circumstances, and whether it would hold again under slightly different conditions, is as valuable as understanding why something went wrong. Learning should also extend beyond a government's own direct experience. Many governments have already managed significant hybrid activity and allies can draw on their experience as material for scenarios and as a source of transferable lessons. Review after exercises and real events should include whether the seven principles were applied effectively at key decision points, making them a practical evaluation tool as well as a guide to action. Each of these inputs should feed back into the design of the next exercise and, where relevant, into changes to the crisis management plan, the procedures, or the system itself. It is this cycle of identifying problems, making changes, and testing those changes that turns a series of individual exercises into a programme that builds capability over time.

Everything described in this section depends on sustained institutional commitment. The official or body responsible for the crisis management system should ensure that the programme of training and exercising is resourced, scheduled in advance, and built into the regular planning cycle, with progress reported to senior leadership and defined obligations on departments to participate. Without this, training and exercising will lose ground to the competing demands of day-to-day government business. Exercises in particular face institutional resistance. They pull people away from their normal responsibilities and carry the risk of exposing weaknesses that individuals or departments would prefer not to have scrutinised. The learning cycle faces its own pressures. Post-exercise and post-crisis review can become entangled with questions of blame, and where that happens the programme may continue to run exercises but will stop generating the honest assessment on which genuine improvement depends. The most important safeguard against this is to adopt a no-fault approach, **where exercises operate on an explicit basis that the purpose is to find and fix problems, not to judge those who surface them. Those leading the programme should actively protect this principle, especially when institutional pressures work against it**.

05 *Recovery and transition*

As a crisis draws to an end, or appears to, key decisions need to be taken that can have significant consequences for whether the government is better prepared for what comes next and whether public confidence and democratic legitimacy are maintained or restored. This section covers the transition from response to recovery, recovery itself, and the review and learning process through which the experience of a crisis feeds back into the system's future capability. For hybrid threats, the post-crisis period has distinctive characteristics that complicate each of these. The threat actor's campaign may not end when the acute phase of the crisis subsides, and the post-crisis environment itself may become contested ground.

Figure 9 Recovery and transition

Transition from response to recovery	Recovery	Review and learning
The decision to stand the response down, weighed against operational and political conditions	Restoring what was disrupted, strengthening the system, and returning to normal governance	A structured review of the response, which serves accountability and translates learning into change

Three issues require attention at broadly the same time, each placing demands on leadership and on institutional capacity. The first is that the decision to transition from crisis response to recovery carries consequences. Standing down the crisis regime too early can create vacuums in coordination and service delivery and can damage public trust if affected populations perceive that the government is deprioritising the damage caused by the crisis. Maintaining the crisis regime too long carries different risks, including that the continued concentration of authority creates the conditions for emergency measures to become normalised. For hybrid threats, this decision is harder to time, because the end of the acute phase may be a pause in activity or a shift to a different domain rather than a definitive conclusion. The second issue is recovery itself: restoring the functioning of affected systems and, where possible, strengthening them against future disruption. It requires its own strategic direction, leadership, and sustained resources, and the challenge is that it must be planned as a strategic undertaking under conditions where institutional energy is depleted and political attention has moved elsewhere. Where the crisis was caused by a hybrid campaign, recovery that restores the previous state without addressing the vulnerabilities the campaign exploited leaves the same points of entry available to the threat actor. The third issue is the accountability process, through which the decisions taken during the response are subjected to scrutiny. **Accountability** is essential both for democratic legitimacy and for learning, but it is also a political process that creates a contest over what the crisis meant, who bears responsibility, and what should follow. In the aftermath of a hybrid campaign, the threat actor may seek to shape this contest, and a degeneration into blame dynamics can undermine the honest assessment on which genuine improvement depends.[19]

Accountability

19 For a fuller treatment of the political dynamics of crisis termination and accountability, see: Boin et al., The Politics of Crisis Management.

The decision to transition from crisis response to recovery requires two conditions to be assessed. The first is operational: whether the conditions that triggered the crisis response are sufficiently resolved that the crisis management system can be stood down without creating gaps in coordination or capability. The second is political: whether the crisis issues have receded sufficiently from public and institutional agendas that normal governance can resume. The transition should be a deliberate decision taken by the strategic body informed by an honest assessment of both dimensions. But there may be tensions between them. The operational picture may indicate that the response can be wound down while the political consequences of the crisis are still unfolding, or political pressure to end the crisis may build before the operational situation is genuinely stable. Where tensions exist, the strategic body needs to understand which is driving the pressure to transition and make a conscious judgement rather than allowing one to override the other by default. The assessed picture produced by the information management function should inform the transition decision in the same way it informed operational decisions during the crisis. And the crisis measures still in place should be tested against the same principles that justified them. For hybrid threats, both dimensions of this assessment are harder to read, for the reasons described above. The threat actor may also be working to influence perceptions of whether the crisis is over, whether by encouraging premature stand-down or by sustaining a sense of crisis to exhaust the government and erode public confidence. The strategic body should account for these possibilities in its assessment, and the system should retain the capacity to reactivate if the picture changes.

How governments organise the recovery effort will depend on the scale and nature of the crisis. A major crisis with sustained cross-government consequences may require a dedicated recovery coordination body with its own leadership and resources. Where the effects fall primarily within one sector, the lead department may resume responsibility within its normal mandate, with lighter coordination from the centre. Whatever the institutional arrangement, effective recovery requires designated leadership with the authority to sustain it, a strategic direction that goes beyond restoring what was disrupted, and access to the records and institutional knowledge built up during the response. Without this, recovery risks drifting once the institutional urgency of the crisis has passed. Once the strategic body has confirmed the transition, the crisis response unit should be wound down through a structured handover to these arrangements rather than allowed to dissolve as personnel return to their normal responsibilities. The records created during the response – the CRIP, decision logs, and the communications record – should be consolidated and transferred to the recovery leadership and to whatever review or accountability process follows. Actions from the response that have not yet been fully implemented should be allocated clear ownership, so that they are tracked to completion rather than lost in the handover. Personnel who staffed the crisis response unit should provide handovers to those taking up the response before they are released. For hybrid threats, the information management function may need to continue in a reduced form beyond the formal transition, maintaining monitoring for any resumption or shift in hostile activity and preserving the capacity to reactivate the crisis management system if the assessed picture changes.

At the point of transition, decision-makers also need to consider the strategic character of recovery itself. Recovery usually involves the restoration of any services, systems, and functions that were disrupted, and these often command the most immediate attention, because affected populations need visible progress and because of political pressure. But it also provides an opportunity to **use what the crisis revealed about the system to strengthen it against future threats**. Every crisis exposes weaknesses that were not fully visible beforehand and, immediately after one, political and institutional conditions for strategic recovery are often strongest, when the case for change is hardest to dispute. But these conditions erode as other priorities reassert themselves and public attention moves on.

The officials responsible for the crisis management system can prepare the ground for strategic recovery by commissioning a structured assessment of what the crisis revealed. This assessment should distinguish between weaknesses that fall within the crisis management system itself, such as gaps in information management, coordination arrangements that did not function as designed, or training deficiencies, which officials can begin to address through updates to the crisis management plan and the training programme, and weaknesses that require political decisions, such as legislative change, institutional reform, or significant resource allocation. For the latter, officials should present prioritised recommendations to political leadership while the impetus for change exists, with a clear account of the evidence on which they are based. In both cases, accountability for implementation should be built into the recovery arrangements, so that commitments are tracked to completion rather than allowed to lapse as the crisis recedes.

Where the crisis response involved extraordinary measures, such as emergency powers, restrictions on rights, or the suspension of normal accountability mechanisms, recovery should include a deliberate plan to restore normal governance arrangements. The longer emergency measures persist beyond the point at which they are justified, the greater the risk that they become embedded in how government operates and, potentially, the higher the political cost of reversing them. Restoring normal governance requires political leadership to commit publicly to the withdrawal of extraordinary measures and to a timetable for doing so. The officials responsible for the crisis management system can prepare the ground for these decisions by identifying which extraordinary measures remain in place, assessing whether the conditions that justified each still apply, and recommending a sequence for their withdrawal or formal review against the same necessity and proportionality tests that governed their introduction. For hybrid threats, this carries a further dimension. A threat actor that sought to provoke an overreaction or to erode democratic norms during the crisis benefits directly if those effects persist into the post-crisis period. Where the government's crisis response restricted rights or concentrated authority in ways that the threat actor can point to as evidence of democratic failure, allowing those arrangements to continue hands the threat actor a post-crisis narrative advantage it did not need to construct. The government's credibility in the recovery period depends substantially on its ability to demonstrate that extraordinary measures were temporary and reversed when no longer justified.

Accounta-bility

A structured review of the crisis response is essential both for accountability and for improving the system's future capability. The review should establish what happened, what decisions were taken and on what basis, what worked, what did not, and why, covering the full scope of the response from the preparations that were in place through to the transition to recovery. Review after a real crisis is harder than review after an exercise because the stakes are higher and the process is subject to a tension that can distort it. The political accountability process, establishing who was responsible and whether they acted appropriately, and the learning process, establishing what needs to change in the system, serve different purposes and operate under different logics. Where the two are not distinguished, the political dynamics of accountability can suppress exactly the honest reporting on which learning depends. Two specific risks follow: that accountability is suppressed to protect those in power, which deprives the system of learning and erodes public trust; or that it is weaponised against political opponents, which turns the review into a continuation of the crisis by other means. The review should therefore be commissioned promptly, while the experience is fresh and personnel are still available, and based on the records maintained during the response rather than on recollection alone. Its terms of reference should focus on what happened and what should change, not on assigning individual blame. Where the scale or political sensitivity of the crisis warrants it, consideration should be given to using external facilitators who bring independence from the institutional dynamics that might otherwise constrain the process. Failures should be examined as symptoms of systemic weakness rather than attributed to single causes, since the conditions that produced them are likely to involve multiple contributing factors across the system. For hybrid threats, the review should also assess what was deliberately targeted by the threat actor and how effectively the system detected, assessed, and responded to activity that was designed to be ambiguous.

The value of the review depends on whether its findings are translated into changes to how the crisis management system operates. Some findings will fall within the authority of the officials responsible for the system, such as updating the crisis management plan, adjusting coordination arrangements that did not function as designed, revising information management procedures, or redesigning the training programme to address specific weaknesses the crisis revealed. Where the review reveals that the seven principles were not applied effectively at key decision points, this should inform both training and any structural changes to how decisions are taken and challenged. It can be especially valuable to examine whether the crisis was, in whole or in part, the surfacing of a slow-burn problem that the system failed to detect or acknowledge earlier. Where the evidence suggests it was, the review needs to go beyond the response itself and ask what in the monitoring architecture, the institutional culture, or the political environment prevented earlier recognition and action. These are often the most consequential findings, because the conditions that allowed a slow-burn to develop undetected are likely to produce further crises if they are not addressed, and they may demand broader changes, for example, to the legal framework, institutional reform, or significant resource allocation, which require political decisions. Officials should prepare prioritised recommendations with the evidence to support them. Where the crisis was caused or exacerbated by a hybrid campaign, the review's findings should inform not only the crisis management system but the

government's broader assessment of the threats it faces and the vulnerabilities the campaign exploited, feeding back into the resilience framework described in Section 1.2. The findings from a real crisis also become material for future exercises, and the discipline of lessons identified, implementation, and testing described in the preceding section applies with equal force here. The learning from each crisis feeds back into the preparations described in Section 3 and into the training programme, and the quality of that learning determines whether the system is genuinely strengthened by the experience.

The cycle described in this section, from transition through recovery to review and learning, is where those responsible for the crisis management system either strengthen it or fail to. How a crisis is managed directly affects the resilience of the state and society afterwards. The post-crisis period is where that effect is determined and whether the government learns from what happened, addresses the weaknesses the crisis exposed, restores the governance arrangements that a democratic society depends on, and emerges better prepared for what comes next.

Case 5 - Moldova, 2024–2025: election interference and institutional learning[20]

In the run-up to Moldova's October 2024 presidential election and EU referendum, Russia mounted a multi-domain interference campaign. Kremlin-linked networks distributed prepaid financial cards and other incentives to large numbers of Moldovan voters. Disinformation campaigns saturated social media. On election day, cyberattacks, including DDoS activity, targeted the Central Electoral Commission and bomb threats disrupted polling stations. Less than a year later, Moldova held parliamentary elections in September 2025 under a comparable barrage of interference, including vote-buying via cryptocurrency, AI-generated disinformation, paid protests, and further cyber attacks on election infrastructure.

The 2024 elections were the first real test of an institutional infrastructure the government was still building. The Centre for Strategic Communication and Countering Disinformation, established only in 2023, identified and countered hostile narratives but was still in the process of becoming fully operational. Police confiscated over a million dollars in alleged electoral funds from organised groups returning from Moscow and investigated the vote-buying networks, but the scale of the operation became apparent only late in the campaign. Some analysts and observers assessed the response as reactive and poorly coordinated between agencies. The government used the period between the two elections to address the weaknesses the 2024 experience had exposed. The Anti-Corruption Prosecutor's Office initiated criminal cases against vote-buying organisers. Voters alleged to have accepted bribes were in some cases fined. The Central Electoral Commission strengthened its campaign finance oversight and cyber defences. EU assistance was expanded, including cyber and hybrid threat support. By the 2025 elections, the enforcement response was more systematic, resulting in a series of criminal cases and over a hundred detentions, and a more coordinated approach across law enforcement, strategic communications, and cyber defence.

In Moldova the government demonstrated a capacity to protect the integrity of democratic processes under sustained hybrid pressure, even with severe resource constraints, and to learn from crises. The response incurred costs: the intelligence service's blocking of hundreds of websites during the 2025 campaign was domestically contested, coordination between institutions remained imperfect, and Moldova's resilience continues to depend heavily on EU support. International election observers nonetheless assessed the 2025 response as decisive and measured, and the enforcement measures taken between the two elections demonstrably improved the government's ability to detect, disrupt, and prosecute interference.

20 Anastasia Pociumban, Moldova's Response to Hybrid Attacks: A Learning-by-doing Strategy, HCSS, November 2023; Dumitru Minzarari, "Population-centric: Lessons from Russia's hybrid war in Moldova," ECFR, March 2023; Pup, Antonia-Laura. "How the EU Rewrote its Cyber Diplomacy Playbook in Moldova's 2025 Elections." Georgetown Journal of International Affairs, 31 January 2026; Matthew Schaaf and Andrew Rogan, "A Lesson in Resilience: Moldova's Resistance to Election Interference," IFES, 2025.

06 References

Allan, Duncan. "Managed Confrontation: UK Policy Towards Russia After the Salisbury Attack." Chatham House Research Paper, October 2018. https://www.chathamhouse.org/2018/10/managed-confrontation-uk-policy-towards-russia-after-salisbury-attack.

Ålander, Minna. " Death by a Thousand Paper Cuts: Lessons from the Nordic-Baltic Region on Countering Russian Gray Zone Aggression." Carnegie Endowment for International Peace, November 2024. https://carnegieendowment.org/research/2024/11/russia-gray-zone-aggression-baltic-nordic.

Boin, Arjen, Paul 't Hart, Eric Stern, and Bengt Sundelius. The Politics of Crisis Management: Public Leadership Under Pressure. Cambridge University Press, 2016.

Brattberg, Erik, and Tim Maurer. Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks. Carnegie Endowment for International Peace, 2018. https://carnegieendowment.org/research/2018/05/russian-election-interference-europes-counter-to-fake-news-and-cyber-attacks.

Bronk, Chris, Gabriel Collins, and Dan S. Wallach. "The Ukrainian Information and Cyber War." Cyber Defense Review 8, no. 3 (Fall 2023). https://cyberdefensereview.army.mil/Portals/6/Documents/2023_Fall/CDR_V8N3_Fall_2023_03-Bronk.pdf.

Cabinet Office (UK) and BSI Knowledge. "PAS 200:2011 - Crisis Management - Guidance and Good Practice." 2011. https://knowledge.bsigroup.com/products/crisis-management-guidance-and-good-practice.

Finlex. "Act on Temporary Measures to Combat Instrumentalised Migration (Finland)." 2024. https://www.finlex.fi/en/legislation/translations/2024/eng/482.

Flin, Rhona. Sitting in the Hot Seat: Leaders and Teams for Critical Incident Management. Wiley, 1996.

Hybrid CoE. "Hybrid Threats." Accessed 2026. https://www.hybridcoe.fi/hybrid-threats/.

Hybrid CoE. The Landscape of Hybrid Threats: A Conceptual Model: Public Version. Publications Office, 2021. https://doi.org/10.2760/44985.

Hybrid CoE and European Commission. Hybrid Threats: A Comprehensive Resilience Ecosystem. Publications Office of the European Union, 2023. https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/.

Klein, Gary A. Sources of Power: How People Make Decisions. MIT Press, 2017.

Kvartsiana, Khrystyna. Ukraine's Cyber Defense: Lessons in Resilience. German Marshall Fund of the United States, December 2023. https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf.

Minzarari, Dumitru. "Population-centric: Lessons from Russia's Hybrid War in Moldova." European Council on Foreign Relations, March 2023. https://ecfr.eu/article/population-centric-lessons-from-russias-hybrid-war-in-moldova/.

Multinational Capability Development Campaign / Ministry of Defence (UK). Countering Hybrid Warfare Project: Countering Hybrid Warfare. 2019. https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf.

Pup, Antonia-Laura. "How the EU Rewrote its Cyber Diplomacy Playbook in Moldova's 2025 Elections." Georgetown Journal of International Affairs, 31 January 2026. https://gjia.georgetown.edu/science-technology/how-the-eu-rewrote-its-cyber-diplomacy-playbook-in-moldovas-2025-elections/.

Toucas, Boris. "The Macron Leaks: The Defeat of Informational Warfare." Center for Strategic and International Studies, 2017. https://www.csis.org/analysis/macron-leaks-defeat-informational-warfare.

Omand, David. "From Nudge to Novichok: The Response to the Skripal Nerve Agent Attack Holds Lessons for Countering Hybrid Threats." Hybrid CoE Working Paper No. 2, April 2018. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-2-from-nudge-to-novichok-the-response-to-the-skripal-nerve-agent-attack-holds-lessons-for-countering-hybrid-threats/.

Omand, David. How to Survive a Crisis: Lessons in Resilience and Avoiding Disaster. Viking, 2023.

Pociumban, Anastasia. Moldova's Response to Hybrid Attacks: A Learning-by-doing Strategy. Hague Centre for Strategic Studies, November 2023. https://hcss.nl/report/moldovas-response-to-hybrid-attacks/.

Redhead, Matthew R. Old Wine, New Bottles? The Challenge of State Threats. Serious Organised Crime & Anti-Corruption Evidence Research Programme, 2025. https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/67852e69ff4ff4079a9c3000/1736781420568/SOCACE-RP32-OldWineNewBottles_final.pdf.

Schaaf, Matthew, and Andrew Rogan. A Lesson in Resilience: Moldova's Resistance to Election Interference. International Foundation for Electoral Systems, 2025. https://www.ifes.org/publications/lesson-resilience-moldovas-resistance-election-interference.

Stewart, Joshua. “The Grey Orchestra: Elastic Communications and the UK’s Response to Salisbury.” RUSI Journal, 2022. https://www.tandfonline.com/doi/full/10.1080/03071847.2022.2075117.

StratCom, NATO Strategic Communications Centre of Excellence. "Strategic Communications Hybrid Threats Toolkit." 2021. https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213.

UNHCR. "UNHCR Urges Finland to Protect the Right to Seek Asylum." May 2024. https://www.unhcr.org/europe/news/press-releases/unhcr-urges-finland-protect-right-seek-asylum.

Vilmer, Jean-Baptiste Jeangène. The "Macron Leaks" Operation: A Post-Mortem. Atlantic Council / IRSEM, 2019. https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf.

Folke Bernadotte Academy (FBA) is the Swedish government agency for peace and security. As part of Sweden's international development cooperation, we promote peace in conflict-affected countries. We offer training and advice and conduct research to strengthen peacebuilding and governance, in peace and security contexts. Moreover, we deploy civilian personnel to peace operations and election observation missions primarily led by the UN, EU and OSCE. The agency is named after Count Folke Bernadotte, the UN's first peace mediator.

For updates and latest publications, follow FBA on:

linkedIn.com/FolkeBernadotteAcademy

instagram.com/FolkeBernadotteAcademy

facebook com/FolkeBernadotteAcademy

fba.se/en

Folke Bernadotte Academy
Swedish agency for peace and security

FBA