NATO UNCLASSIFIED

17 June 2026

DOCUMENT
PO(2026)0184
Silence procedure ends:
18 Jun 2026 – 09.00

To: Permanent Representatives (Council)

From: Secretary General

2026 BASELINE REQUIREMENTS, RESILIENCE GUIDELINES AND EVALUATION CRITERIA

1. On 17 June 2026, the Resilience Committee agreed the enclosed 2026 Baseline Requirements, Resilience Guidelines and Evaluation Criteria.

2. I do not believe that the issues covered in this document require a Council discussion. Therefore, **unless I hear to the contrary by 09.00 on Thursday, 18 June 2026**, I shall assume that Council has approved this document, and agreed to forward it to Defence Ministers for their endorsement.

(Signed) Mark RUTTE

1 Annex
1 Appendix

Original: English

Development and agreement of this document took 10 hrs and 20 minutes in the Resilience Committee.

ANNEX 1
PO(2026)0184

2026 BASELINE REQUIREMENTS, RESILIENCE GUIDELINES AND EVALUATION CRITERIA

BACKGROUND

1. Resilience at NATO is the capacity to prepare for, resist, respond to, and quickly recover from strategic shocks and disruptions, and ensure the continuity of the Alliance's activities. Ensuring national and collective resilience is critical to NATO's core tasks of deterrence and defence, crisis prevention and management and cooperative security, and underpins efforts to safeguard our nations, societies and shared values.

2. Resilience has three core functions: ensuring continuity of government and essential government services, continuity of essential services to the population, and civil support to military operations through peace, crisis and conflict.

3. The 2021 Strengthened Resilience Commitment[1] stresses that NATO's Baseline Requirements[2] for national resilience are essential to deterrence and defence and the effective enablement of our armed forces. The Baseline Requirements define NATO's level of ambition for national and collective resilience and underpin the ability of an Ally to support NATO's objectives throughout peace, crisis and conflict. Their implementation is a key driver of Allied civil preparedness and their fulfilment a strategic necessity.

4. Strengthening resilience requires a whole-of-government approach, supported by whole-of-society considerations that recognise the importance of citizens and societies as fundamental actors in enhancing national resilience.[3] Allies also acknowledged and emphasised the critical role that the private sector plays in bolstering national and Alliance-wide resilience, as it owns and operates much of the critical infrastructure and supply chains that sustain transportation, communications, energy, food and water supply, medicine, government administration, and information flow.[4]

5. Allies' commitment to develop national civilian planning[5] hinges on the implementation of the Baseline Requirements and of the Resilience Objectives[6] and aims at ensuring coherence between NATO and national planning for deterrence and defence, and national resilience efforts.

---

[1] PO(2021)0221, Strengthened Resilience Commitment.
[2] Assured continuity of government and critical government services; resilience energy supplies; ability to deal with uncontrolled movement of people; resilient food and water resources; ability to deal with mass casualties; resilient civil communications systems; resilient civil transport systems.
[3] PO(2023)0369 (INV), Non-Binding Guidance to Enhance Societal Resilience.
[4] PO(2025)0388, Guidance for Enhancing Public-Private Cooperation for Resilience.
[5] PO(2025)0144, Non-Binding Guidance to Support National Civilian Planning.
[6] PO(2023)0226 (INV), 2023 Alliance Resilience Objectives.

6. The Baseline Requirements are periodically updated to reflect the evolving challenges and priorities of resilience at NATO. Their last revision took place in October 2021 and addressed, among others: lessons from the COVID-19 pandemic, particularly on crisis response and public communication across all levels of government; the need for more resilient critical infrastructure and supply chains; broader planning for large-scale evacuations.[7]

7. The North Atlantic Council tasked the Resilience Committee, supported by its Planning Groups, to update the Baseline Requirements, Resilience Guidelines and Evaluation Criteria to reflect findings from the 2022 Resilience Assessment, relevant strategic direction as well as lessons learned and considerations from recent events[8]. It is informed by the progress made by Allies on resilience and civilian planning, and the guidance given by Policy Directors for Resilience on the need for more measurable and outcome-oriented Baseline Requirements, Resilience Guidelines and Evaluation Criteria. It considers the need to adapt national and collective resilience to the deterioration of the security environment as outlined in the 2022 Strategic Concept and in response to the long-term threat posed by Russia to Euro-Atlantic security and the persistent threat of terrorism. Accordingly, it reflects Allies' need to intensify their risk-informed planning against all scenarios, including armed conflict with a peer adversary.

AIM AND SCOPE

8. The aim of this document is:

I. To update the seven Baseline Requirements, Resilience Guidelines and Evaluation Criteria taking into account the evolution of the strategic environment since 2021, and NATO's adaptation to it;

II. To set a way forward on how to continue to strengthen and assess the resilience of Allies and of the Alliance, including through the Planning and Review (P&R) cycle for Resilience and the NATO Defence Planning Process (NDPP), and with a view to informing national civilian planning as well as NATO's defence planning.

NATO'S ADAPTATION AND THE NEED FOR REVISED BASELINE REQUIREMENTS

9. With the adoption of the Concept for the Deterrence and Defence of the Euro-Atlantic Area (DDA) and its Family of military Plans (FoP), NATO and Allies operate under a single, coherent framework to organise deterrence and defence activities across SACEUR's Area of Responsibility (AOR).

---

[7] PO(2021)0372, Revised Baseline Requirements, Resilience Guidelines and Evaluation Criteria.
[8] PO(2022)0423 (INV), 2022 Resilience Assessment.

10. In response to the long-term threat posed by Russia to Euro-Atlantic security and the persistent threat of terrorism[9], NATO has accelerated its military adaptation and has undertaken the biggest reinforcement of its collective defence in a generation. It has bolstered its posture, especially in the Eastern flank, ensuring that in-place, combat-ready forces are supported by rapidly available reinforcements. This includes improving the capacity to project and sustain forces for high intensity warfighting at speed and scale, relying on effective logistics support, in particular through the provision of Host Nation Support (HNS).[10]

11. NATO's military adaptation must be met with faster, stronger and more consistent efforts to strengthen resilience, especially civil support to military operations. This is especially true as the Alliance becomes increasingly interconnected, geographically and across domains, and where challenges to the resilience of an Ally may have cascading effects throughout SACEUR's AOR. The fulfilment of national civilian planning against operational requirements, including the HNS Minimum Operational Requirements (MOR), reinforces credible deterrence and defence by ensuring that military forces are adequately supported with civilian resources and infrastructure. Further, strengthening resilience through a whole-of-government and whole-of-society approach demonstrates the Alliance's resolve and blunts our adversaries' strategic intimidation.

12. The implementation of the Baseline Requirements requires Allies to:

a) Establish an effective governance framework for national resilience that clearly identifies roles and responsibilities across whole-of-government and whole-of-society stakeholders, while coordinating with the military in peace, crisis and conflict;

b) Account for reliable and sustained resource planning. At their 2025 Summit in The Hague, Allied Heads of State and Government agreed to account for up to 1.5% of GDP for defence- and security-related spending, including in the areas of resilience and civil preparedness;[11]

c) Deliver civil effects to support the execution of NATO's military plans, including through rapid implementation of the NATO Response Measures[12] as well as by providing Host Nation Support (HNS) in a contested environment.[13]

---

[9] PO(2025)0159-FINAL, The Hague Summit Declaration.
[10] PO(2026)0048, Political-Military Advice on Host Nation Support for Collective Defence.
[11] PO(2025)0174, The NATO Defence- and Security-Related Investments Definition, Paragraph 6. Expenditures for resilience, civil defence, and civil preparedness are included, as long as the expenditure is based on national resilience planning or required to enable the execution of a NATO defence plan or national plans.
[12] Response Measures EDA, EDB, EDC, LEA, LEB, LDA, LDB, MHA, MHB, MHC, MHD, MDA, MDD, MDE, MEA, MEB, MGA, MGB, PHA, PHB, PIA, PIB, QAA, QAB, QCA, QCB, QDA, QDB, RAA, RAB, REA, REB, RFA, RFB, RGA, RGB, RIA, RIB.
[13] PO(2024)0196, Resilience Committee Advice on the Civilian Aspects of the Final Host Nation Support Concept for Collective Defence. AC/305-D(2026)0011, NATO Contested Logistics Concept.

13. Coherence between national and NATO planning for deterrence and defence will ensure that civil and military plans and capabilities reinforce each other. It will also ensure that Allies can de-conflict needs for civil, military and commercial resources so that both the requirements to support national armed forces and those to deliver HNS to reinforcing forces can be balanced and fulfilled, while mitigating the impact on the population, including the provision of essential services.[14] This should also facilitate and encourage respective civil and commercial stakeholders to consider including contingencies for crisis and conflict situations into their respective business continuity planning.[15]

CROSS-CUTTING CONSIDERATIONS FOR THE REVISED BASELINE REQUIREMENTS

14. Allies have demonstrated that the best and most effective response to all threats and hazards is through cross-sectoral, whole-of-government coordination, supported by whole-of-society considerations. This reflects not only the many interdependencies across the baseline areas, but also the coordinated effects needed to respond to broad and far-reaching challenges to resilience. National and NATO-organised exercises, including NATO's Crisis Management Exercises (CMX), provide opportunities for relevant authorities to test resilience at the national and Alliance levels.[16]

15. Allies have made substantial progress to adapt to a dynamic and evolving strategic environment. However, the continuous degradation of the security environment demands a more thorough, risk-informed approach to ensuring resilience and a better focused set of Resilience Guidelines and Evaluation Criteria for Allies to self-assess their ability to prepare for, resist, respond to, and quickly recover from strategic shocks and disruptions.

16. Additional cross-cutting risks**,** challenges and threats that have been considered for the 2026 revision of the Baseline Requirements include:

a) The potential for armed/physical attack on citizens and/or critical infrastructure, including acts of sabotage;

b) More frequent and damaging cyberattacks, which can cripple the delivery of essential services to the population and civil support to military operations and create unique economic and political challenges for the Alliance and individual Allies;

[14] PO(2024)0196.
[15] PO(2026)0048, paragraph 13.
[16] This includes, among others, developing, testing, and exercising procedures aimed at ensuring that Civil Situation Reports (CIVSITREP) are provided in a timely manner and with relevant information to NATO.

c) The challenges associated with emerging and disruptive technologies (EDTs) impacting resilience and civil preparedness as well as military effectiveness[17];

d) Harmful economic activities and strategic dependencies, which may hamper Allies' ability to promptly react to strategic shocks and disruptions and have a potential significant impact on industrial capacity and supply chains, during crisis and conflict;

e) Extreme weather, natural disasters**,** space weather and changing environmental conditions, which inflict increasing strain on resilience across the Euro-Atlantic area, potentially compounding the effects of hostile activity;

f) The need for stronger and more reliable restoration and repair capabilities to improve Allies' abilities to quickly recover from strategic shocks;

g) The inherent vulnerabilities caused by the increased dependence of essential functions on space-based assets and related technology, including societal functions but also military capabilities.

WAY FORWARD ON THE PLANNING AND REVIEW CYCLE FOR RESILIENCE

17. The endorsement of Alliance-wide Resilience Objectives by Heads of State and Government in 2023 provided Allies with a framework to develop national goals and implementation plans to support the achievement of specific, measurable, achievable, relevant and time-bound targets, in line with the established four-year planning and review (P&R) cycle for resilience.[18] This revision of the Baseline Requirements resets the P&R cycle. As part of the 2026 Resilience Assessment, Allies will also consider adapting the Resilience Objectives for the following cycle.[19] The overall implementation of the Baseline Requirements and Resilience Objectives will be supported by a sustained rhythm of resilience activities and will continue to be monitored and evaluated, including in the context of the next iteration of the NDPP.

18. Starting in 2027, an Annual Report on Resilience will become the single reporting and tasking vehicle for the North Atlantic Council to provide timely guidance on how to take forward the work on civil preparedness.[20] This report will offer an overview of the Alliance-wide implementation of the Baseline Requirements, based on input from the Planning Groups, and national replies to the Defence Planning Capability Survey (DPCS). The Planning Groups will develop this input by providing an update on their activities and an

[17] PO(2021)0059, Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies.
[18] PO(2023)0226 (INV).
[19] Ibid, paragraph 7.
[20] PO(2026)0075, Optimisation of Reporting to Council.

assessment of the progress achieved in their area of expertise. In line with its Terms of Reference[21], the Resilience Committee will direct and ensure coherence of the work of its Planning Groups, and will provide relevant direction and guidance, including through the Annual Report.

19. The production of revised Regional Civil Assessments (RCAs)[22] will be further aligned with NATO's Regional Plans and the timeline for their revision[23], to more directly inform Allied civilian planning, military adaptation and future posture adjustments. Allies will forward the revised RCAs to Defence Ministers through the Annual Report on Resilience.

RECOMMENDATIONS

20. The Resilience Committee recommends that the North Atlantic Council:

a) Approve this document and agrees to forward it to Defence Ministers for endorsement in June 2026;

b) Encourage Allies to fully implement the Baseline Requirements, Resilience Guidelines and Evaluation Criteria to further strengthen national and collective resilience, including in support of HNS implementation;

c) Recalling the tasking to prepare an Annual Report on Resilience in time for the June Defence Ministers Meeting starting in 2027[24], task the Resilience Committee to take into account the additional guidance provided in this document;

d) Task the Defence Policy and Planning Committee to take into account this document to inform Political Guidance for Defence Planning 2027;

e) Task the Resilience Committee to review the Baseline Requirements, Resilience Guidelines and Evaluation Criteria in four years, or as deemed necessary, in coordination with the NMAs.

[21] PO(2022)0036, Terms of Reference for the Resilience Committee.
[22] PO(2023)0227, PO(2023)0228, PO(2023)0233, PO(2023)0377, PO(2023)0450.
[23] PO(2025)0148, 2025 Comprehensive Report on Deterrence and Defence.
[24] PO(2026)0075.

APPENDIX 1 TO THE 2026 BASELINE REQUIREMENTS, RESILIENCE GUIDELINES AND EVALUATION CRITERIA

1. NATO's military adaptation must be met with faster, stronger and more consistent efforts to strengthen resilience, especially civil support to military operations. This is especially true as the Alliance becomes increasingly interconnected, geographically and across domains, and where challenges to the resilience of an Ally may have cascading effects throughout SACEUR's AOR. The fulfilment of national civilian planning against operational requirements, including the HNS Minimum Operational Requirements (MOR), reinforces credible deterrence and defence by ensuring that military forces are adequately supported with civilian resources and infrastructure. Further, strengthening resilience through a whole-of-government and whole-of-society approach demonstrates the Alliance's resolve and blunts our adversaries' strategic intimidation.

2. The implementation of the Baseline Requirements requires Allies to:

a) Establish an effective governance framework for national resilience that clearly identifies roles and responsibilities across whole-of-government and whole-of-society stakeholders, while coordinating with the military in peace, crisis and conflict;

b) Account for reliable and sustained resource planning. At their 2025 Summit in The Hague, Allied Heads of State and Government agreed to account for up to 1.5% of GDP for defence- and security-related spending, including in the areas of resilience and civil preparedness;[1]

c) Deliver civil effects to support the execution of NATO's military plans, including through rapid implementation of the NATO Response Measures[2] as well as by providing Host Nation Support (HNS) in a contested environment.[3]

3. Coherence between national and NATO planning for deterrence and defence will ensure that civil and military plans and capabilities reinforce each other. It will also ensure that Allies can de-conflict needs for civil, military and commercial resources so that both the requirements to support national

---

[1] PO(2025)0174, The NATO Defence- and Security-Related Investments Definition, Paragraph 6. Expenditures for resilience, civil defence, and civil preparedness are included, as long as the expenditure is based on national resilience planning or required to enable the execution of a NATO defence plan or national plans.
[2] Response Measures EDA, EDB, EDC, LEA, LEB, LDA, LDB, MHA, MHB, MHC, MHD, MDA, MDD, MDE, MEA, MEB, MGA, MGB, PHA, PHB, PIA, PIB, QAA, QAB, QCA, QCB, QDA, QDB, RAA, RAB, REA, REB, RFA, RFB, RGA, RGB, RIA, RIB.
[3] PO(2024)0196, Resilience Committee Advice on the Civilian Aspects of the Final Host Nation Support Concept for Collective Defence. AC/305-D(2026)0011, NATO Contested Logistics Concept.

armed forces and those to deliver HNS to reinforcing forces can be balanced and fulfilled, while mitigating the impact on the population, including the provision of essential services.[4] This should also facilitate and encourage respective civil and commercial stakeholders to consider including contingencies for crisis and conflict situations into their respective business continuity planning.[5]

4. Allies have demonstrated that the best and most effective response to all threats and hazards is through cross-sectoral, whole-of-government coordination, supported by whole-of-society considerations. This reflects not only the many interdependencies across the baseline areas, but also the coordinated effects needed to respond to broad and far-reaching challenges to resilience. National and NATO-organised exercises, including NATO's Crisis Management Exercises (CMX), provide opportunities for relevant authorities to test resilience at the national and Alliance levels.[6]

5. Allies have made substantial progress to adapt to a dynamic and evolving strategic environment. However, the continuous degradation of the security environment demands a more thorough, risk-informed approach to ensuring resilience and a better focused set of Resilience Guidelines and Evaluation Criteria for Allies to self-assess their ability to prepare for, resist, respond to, and quickly recover from strategic shocks and disruptions.

6. Additional cross-cutting risks, challenges and threats that have been considered for the 2026 revision of the Baseline Requirements include:

a) The potential for armed/physical attack on citizens and/or critical infrastructure, including acts of sabotage;

b) More frequent and damaging cyberattacks, which can cripple the delivery of essential services to the population and civil support to military operations and create unique economic and political challenges for the Alliance and individual Allies;

c) The challenges associated with emerging and disruptive technologies (EDTs) impacting resilience and civil preparedness as well as military effectiveness[7];

d) Harmful economic activities and strategic dependencies, which may hamper Allies' ability to promptly react to strategic shocks and disruptions and have a potential significant impact on industrial capacity and supply chains, during crisis and conflict;

---

[4] PO(2024)0196.
[5] PO(2026)0048, paragraph 13.
[6] This includes, among others, developing, testing, and exercising procedures aimed at ensuring that Civil Situation Reports (CIVSITREP) are provided in a timely manner and with relevant information to NATO.
[7] PO(2021)0059, Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies.

e) Extreme weather, natural disasters, space weather and changing environmental conditions, which inflict increasing strain on resilience across the Euro-Atlantic area, potentially compounding the effects of hostile activity;

f) The need for stronger and more reliable restoration and repair capabilities to improve Allies' abilities to quickly recover from strategic shocks;

g) The inherent vulnerabilities caused by the increased dependence of essential functions on space-based assets and related technology, including societal functions but also military capabilities.

Baseline Requirement 1: Assured Continuity of Government and Critical Government Services

***Objective 1**: A formalised, tested and exercised plan or system for the continuity of government, including*[8]*:*

a) The ability to exercise sovereign authority and sustain representation and decision-making at NATO under all conditions.

b) A line of succession of the leadership and clarity of the decision-making process and chain of command in the national government in the case of a potentially destabilising event throughout peace, crisis and conflict.

c) Identification and prioritisation of National Essential Functions, critical governmental agencies, critical services including supporting obligations under the Concept for the Deterrence and Defence of the Euro-Atlantic Area (DDA) and its Family of Plans (FoP) (e.g., Host Nation Support (HNS) and Enablement functions, such as the provision and delivery of food, water, fuel, electricity, heat, transport, financial services, specialised goods, medical/pharmaceutical/personal protection products and equipment).

***Objective 2**: A comprehensive system of national capabilities for civil protection/civil defence that is resilience-based and preparedness driven.*

***Objective 3**: A hardened and resilient, both environmentally and physically protected, crisis management centre and alternative arrangements to ensure continuity of government operations and other critical services, during crises and conflict with redundant capacities to operate for at least one month with support systems (e.g., power; communications; food and water; and CBRN collective protection for a period of time as determined by the national risk assessment).*

[8] For further guidance, see Planning Framework for Nations on Assured Continuity of Government and Critical Government Services (AC/98-D(2019)0010 (INV)).

Resilience Guidelines	Evaluation Criteria
a) Establish a national continuity of government and critical government services plan or system that identifies and prioritises government agencies, government services, critical staff positions, and delineates the line of succession, in peace, crisis and conflict.	1) Does the plan or system: a. Identify and prioritise essential government agencies, National Essential Functions and services? b. Identify private sector roles, contractual dependencies, and market-based service delivery risks? c. Address the line of succession and delegation of authority for the head of state/head of government and other key leadership positions? d. Include a clear decision-making process/chain of command in crisis and conflict? e. Address executive decisions to activate the continuity of government/continuity of operations plan? f. Reflect coordination horizontally and vertically across different organisations, including the military as well as different levels of government? g. Include coordination with public and private sector critical infrastructure operators, in line with the Guidance for Enhancing Public Private Cooperation for Resilience?[9] h. Enable the nation to meet its international commitments, including representation to NATO, and, as appropriate, requirements related to NATO business continuity planning for NATO headquarters[10] or installations located in the nation[11]? i. Incorporate procedures to implement all NATO Response Measures addressing continuity of government and critical government services? j. Include arrangements for devolution and reconstitution, including, where appropriate, triggers, authorities and alternate plans?

[9] PO(2025)0388.
[10] EM(2021)0054, NATO Headquarters Business Continuity Plan.
[11] Those NATO Bodies that are part of the NATO Enterprise as listed in PO(2023)0302 (NU).

	k. Reflect consultation of civil society in national preparedness and response? l. Address national guidance on strategic/critical stockpile requirements? m. Address the different levels of risks based on an all threats and hazards approach? n. Envisage appropriate geographical and risk-based separation (to include multiple distributed leadership nodes) in the line of succession to ensure national decision making? o. Include endorsement/approval by the Head of State or Government (or equivalent government executive)? p. Include the necessary legal and operational arrangements to enable continuity of government and essential services? q. Establish a continuity of essential records and digital government capability, including cloud and offline backups, data integrity validation after a cyberattack and continuity of digital identity and registries? r. Identify and train critical civilian staff (from government and critical infrastructure service providers) and relevant military personnel? s. Establish arrangements for Information and Communications Technology (ICT) systems (including alternative and classified systems); crisis management; secure communications to exchange classified information, including with NATO; shelters, including with Chemical, Biological, Radiological and Nuclear (CBRN) protection; stock capacities and coordination or service provision agreements concerning resources owned by the private sector.
b) Implement and maintain a robust system and procedures which enable essential communications across government agencies; between government and critical service providers**;** and between	1) Does the system have redundant capacities allowing for priority communication between: a. Government agencies including military? b. Government and critical service providers? c. Government and civil society? d. Critical national and international points of contact? 2) Are redundant communications systems periodically tested and exercised, and enhanced as required?

	government and civil society and all other relevant stakeholders.	3) Does the system provide for secure essential communications (including when primary work locations are not usable (e.g., alternate locations/telework, etc.))? 4) Does it include an effective early warning, situational awareness, reporting and alerting system with public and private sector stakeholders? 5) Does it include proactive public communications, taking into account crisis communications and risk, as well as coordination and guidance to key stakeholders? 6) Does the system provide for back-up communication platforms to enable effective public communications and are back-up power supply arrangements included for critical communications systems? 7) Do critical service providers have a legal obligation to continue the delivery of essential services under all conditions?
c)	Ensure that planning includes/ addresses preparedness activities and coordination, evaluation of risk, continuity of operations, the ability to rapidly scale-up whole-of-government crisis response and sufficient alternatives for the provision of critical services.	1) Does planning address continuity of services, facilities, and infrastructure critical to the functioning of government and essential services, including pre-crisis monitoring and evaluation of risk and coordination? 2) How are the national obligations to support the DDA FOP (including HNS obligations) implemented and do they reflect involvement and coordination with all necessary stakeholders through a whole-of-government and whole-of-society approach? 3) Does planning recognise the potential need for plans for the rapid scaling-up of crisis management measures, in the event of a high impact and/or transnational crisis or conflict? 4) Does planning identify the organisations and processes to provide continuity for critical services? Does it include business continuity plans in case of crisis and conflict situations? 5) Does planning enable continuity of operations via continued delivery of identified critical services/functions when disruptions occur, or devolution is required (unable to work/provide services from primary buildings**,** offices**,** or remotely) or in the case of severe disruption to workforce availability?

	6) Are contracts for goods and services that support the continuity of government awarded to companies with verified business continuity plans, and does the government support restoration of these goods and services? 7) Do critical service providers plan for swift repair and rapid recovery if critical infrastructure or essential services operations are disrupted by kinetic or non-kinetic means? How does the government support these repair and recovery efforts, in particular in a contested environment? 8) Does planning include provision for redundant and secure communications able to withstand cyberattacks or other network disruptions? Are infrastructure necessary to support the execution of the DDA FoP considered as part of national critical infrastructure protection measures/plan?
d) Implement and maintain a national civil protection/civil defence organisation/mechanism, including warning systems, evacuation and sheltering resources, and public preparedness.	Does the national civil protection/civil defence organisation/mechanism include: 1) Consequence management plans for emergency/civil protection/civil defence services that include scenarios such as large-scale sabotage, kinetic or non-kinetic attacks from state and non-state actors, crisis and conflict? 2) Increased preparedness to activate the national civil protection organisation/mechanisms and surge capacity for additional manning and specialised equipment? 3) Specialised training programs and procedures for consequence management for large-scale kinetic or non-kinetic attacks and conflict scenarios (urban S&R, shelters etc)? 4) Emergency provisions, taking into account basic human needs[12], such as health, water, sanitation, psycho-social care, food, physical security and transport? 5) A system for providing/requiring shelters or safe rooms in houses, workplaces, schools, universities, hospitals and other public facilities? 6) Surge capacity and specialised training of emergency/civil protection/civil defence services?

[12] PO(2017)0013 (INV), NATO Policy on Civil Preparedness for Population Movement in Crisis and Collective Defence.

	7) Tailored national alert systems for crisis and conflict contingencies, that includes warning the civilian population, using all communications means/systems (e.g. radio, sirens, cell broadcast, social media) on BMD attacks,[13] Air Alerts, CBRN incidents, sabotage and other potential imminent kinetic scenarios including but not limited to, evacuation or sheltering of the civil population? Is it integrated or connected with relevant NATO systems and processes? 8) Does national continuity training incorporate exercising public communications?
e) Periodically review, train on, exercise and update national continuity plans/systems.	1) Does the national continuity plan/system include requirements for regular system tests, training and exercises? 2) Do national continuity training events and exercises address plans and capabilities that involve multiple levels of government and address critical infrastructure vulnerabilities, cyber risks and other sources of interdependencies, such as supply chains (to include devolution/loss of the capital, and NATO-integrated crisis decision-making)? 3) Do national continuity training events and exercises test continuity of operations plans, capabilities and systems and involve all relevant civil and military stakeholders? 4) Does the national plan include a systematic process to ensure implementation of lessons learned from training, exercises, and events for enhancing national continuity plans and capabilities? 5) Are corrective action plans developed following major continuity exercises? 6) Does the nation develop periodic reports on national continuity of government preparedness, and submit a report to national leadership?
f) Designate a crisis management centre and alternative	1) Is the crisis management centre:

[13] AC/98-D(2018)0003, CEPC Advice on the proposed BMD Passive Defence and Consequence Management Requirements, 24 May 2018; PO(2015)0007, Plan for minimising/limiting the consequences of a ballistic missile that reaches a target in NATO Europe, 6 January 2015; PO(2014)0200, Report on the NATO Civil-Military Interface to National Authorities, 24 March 2014; PO(2012)0204, Ballistic Missile Defence - Plan for Minimising/Limiting the Consequences of Intercept/Engagement, 11 May 2012.

arrangements to support the continuity of essential government functions. Provide redundancy in the event that the primary crisis management centre is compromised.	a. Designated as part of national critical infrastructure and adequately resourced (essential and backup staff, equipment, power supply, maintenance and periodic upgrading)? b. Environmentally protected (such as CBRN filtration and ventilation) for personnel and operating systems (i.e. computer servers)? c. Protected from physical, cyber and other threats as identified in the national risk assessment(s)? d. Able to meet national and NATO communications requirements, including secure communications? e. Able to operate autonomously for at least one month, based on the national risk assessment, until normal operations are resumed (with self-contained capacity to provide critical services such as power, food, water, accommodation and planned re-supply as required)? f. Able to support crisis communications, including addressing appropriately information threats[14]? g. Periodically activated and tested/evaluated for its usability? 2) Is a backup crisis management centre established to replace the primary centre if necessary? 3) Are primary and backup centres: a. Regularly tested and operated to include transfer from one to the other? b. Able to meet national and NATO communications requirements (static or deployable CIS assets) and the essential functions of the primary crisis management centre?
g) Establish requirements to ensure continued availability of essential	1) Do these requirements:

[14] PO(2024)0337, NATO'S Approach to Counter Information Threats, paragraph 2: 'Information threats describe intentional, harmful, manipulative and coordinated activities by state and non-state actors in the information environment with an actual or potential negative impact on NATO and Allies. This includes, but is not limited to, information operations, information manipulation and interference by foreign actors, and disinformation.'

	personnel for critical services under all conditions, including crisis and conflict.	a. Identify essential personnel required to support essential functions in sectors, such as energy, communications, health, transport and food and water, including first responders, in the event of severe disruption to workforce availability throughout the peace, crisis, conflict continuum? b. Identify a legal obligation for essential personnel for critical services to continue their work throughout peace, crisis, and conflict? c. Prioritise the supply of critical services for essential personnel? d. Establish arrangements/exemptions to ensure cross-border movement of essential personnel to ensure the functionality of critical supply in support of the HNS requirements, among others? e. Include social and welfare support arrangements for personnel working in critical governmental services? f. Include plans for physical protection of essential personnel for critical services, including the ability to provide support during crisis and conflict? g. Include plans to continue their work throughout the peace, crisis, conflict continuum? h. Incorporate potential use of volunteers in supporting functions? i. Include a de-confliction mechanism of personnel between civilian and military needs. j. Identify surge staffing? k. Address fatigue and mental health resilience of essential staff? l. Enable secure telework at scale? m. Enable continuity of security clearances and personnel vetting?
h)	Strengthen societal resilience by enhancing the involvement of civil society and citizens in effective response to crisis and conflict. [15]	1) Does your national system include provisions to involve civil society and citizens in civil preparedness, including through risk assessments, situational awareness, planning, and communication?

[15] For further guidance, see the Non-Binding Guidance to enhance Societal Resilience (PO(2023)0369).

	2) Do you incorporate civil society capabilities and initiatives in your government´s efforts to enhance societal resilience? 3) Do you offer regular information, education, training and exercises for individuals, households and communities in the fields of national security, civil preparedness, civil defence, risk awareness and psychological resilience? 4) Does your national curriculum for primary, secondary and tertiary education include age-appropriate civil preparedness education components? 5) Do you cooperate with civil society organisations to enable citizens to be self-sufficient for a defined period of time during crisis or conflict, based on your national risks assessment? 6) Do you issue guidance on what emergency provisions are required to be self-sufficient during a certain period of time?
i) Establish and implement a national communications strategy to ensure proactive and consistent public communications across all levels of government (local, regional or national).	1) Does this strategy adopt an objective-driven approach aiming to build and maintain public trust and support? 2) Does this strategy provide clear structural roles of respective actors across all levels of government (local, regional or national) in order to effectively disseminate information to media, citizens and civil society in all types of crisis and conflict situations? 3) Does this strategy identify key target audiences and channels? 4) Does the strategy address media engagement? 5) Does this strategy address tailored crisis communications? 6) Does this strategy outline methods to mitigate the impact of information threats? 7) Does this strategy allow for flexibility and take into account potential shifts in demand as situations or circumstances evolve? 8) Does this strategy establish appropriate education to increase cyber awareness and build the resilience of citizens against misinformation and information threats? 9) Does this strategy incorporate methods and mechanisms for ongoing evaluation to ensure tactics and messaging are effective and reaching key target audiences? 10) Is this strategy continuously used (not only during crisis and conflict)?

	11) Does the strategy incorporate media into national whole-of-government and whole-of-society exercises (in order to exercise media role in all kinds of crisis and conflict situations but also to help communicate important information to the public)? 12) Are media companies defined as national essential services and consequently receive priority support in case of crisis and conflict? 13) Does the strategy incorporate alternative broadcasting solutions (SATCOM, social media, etc.) if the regular transmission means have been disrupted?

Baseline Requirement 2: Resilient Energy Supply

Objective 1: *Continued access to reliable energy supplies, particularly in crisis or conflict, taking into account the potential impact of industrial capacity[16], interdependencies, cascading effects and potential secondary impacts. This should be underpinned by mitigation plans for the full spectrum of risks and threats and identified vulnerabilities, the ability to scale up energy production and distribution to meet wartime demands, and the ability to ensure priority access in line with the requirements for Host Nation Support and the revised NATO Response Measures.*

Objective 2: *Resilient capabilities to mitigate threats and respond to energy supply disruption, and verified and exercised repair and restoration plans, developed and implemented with infrastructure operators. This could include plans for the segmentation of networks, flexible operator training and integrated exercises, and the diversification of routes, supplies and energy resources, including critical equipment, spare parts and commodities.*

Objective 3: *Tools to identify and prioritise critical supply chains and interdependencies (including energy-related industrial base, cross-border interconnections, cross-sectoral and within sectors), including legislation or robust contractual agreements with private sector owner/operators and means to mitigate potential risks associated with potential harmful economic activities.*

Objective 4: *Implementation of information sharing and awareness raising protocols and procedures resulting in the provision of timely, actionable information across all relevant national and international stakeholders, including infrastructure operators, to strengthen national and societal resilience and support collective defence.*

Objective 5: *Identification and assessment of risks and opportunities offered by existing and evolving technologies and the evolution in concepts to ensure the continued resilience of energy systems*.

[16] Consistent with the principles agreed in PO(2025)0388, “Guidance for Enhancing Public-Private Cooperation for Resilience”, paragraphs 7-11.

Resilience Guidelines	Evaluation criteria
a) Inform energy resilience and security planning with appropriate, comprehensive risk assessments and awareness developed and shared with all relevant civil and military stakeholders.	1) Is there a robust, regular sector-wide risk assessment that evaluates, inter alia: a. Impacts of armed attack and physical security of energy infrastructure? b. Personnel Security? c. Cybersecurity (including both Information Technology and Operational Technology)[17]? d. Sabotage and other hybrid actions from state and non-state actors? e. Extreme weather and natural disasters? f. Mass health crises and pandemic events? g. CBRN risks and threats? h. Regional agreements or arrangements? i. Impacts on military forces and capabilities? j. Vulnerabilities associated with critical interdependencies? k. Vulnerabilities related to international trade systems, transport and logistics? l. Trends and changes in economic, environmental and policy factors affecting the energy sector, for example liquid fuels refining? m. Impact of harmful economic activities**,** ownership and control of critical infrastructure, technologies and systems? 2) Does risk assessment and awareness consider all aspects of critical energy infrastructure, including production/generation sites, distribution nodes and networks, storage facilities**,** operations/command and control centres, offshore infrastructure, and critical undersea infrastructure? 3) Does the risk assessment draw upon all relevant stakeholders, including civilian authorities, regulators, infrastructure operators, and civilian and military end-users? 4) Is the risk assessment and other information used to evaluate the ability of energy systems/supply networks to adapt their capacity to evolving threats and hazards?

[17] Operational Technology (OT) refers to computational assets for controlling services for the operation of industrial processes, such as at critical energy infrastructure, including electrical switches, relays, transformers, etc. Information Technology (IT) refers to the use of computers to manage data needed by the organisation's enterprise processes.

	5) Are the risk assessment and other threat information and alerts (including classified information as appropriate) shared with operators and other necessary stakeholders in a timely fashion?
b) Take measures to protect critical energy infrastructure from all relevant threats, including physical, cyber, hybrid, personnel, human-induced and natural hazards**,** health crises and the impacts of changing environmental conditions[18].	1) Drawing on the risk assessment, does a comprehensive legislative/regulatory/voluntary preparedness plan exist to mitigate vulnerabilities and protect energy infrastructure against risks and threats of all types? 2) Do necessary legal and operational arrangements ensure a comprehensive approach to critical energy infrastructure protection, including against armed attack and asymmetric threats during crisis and conflict, to enable NATO and national military plans, including the DDA Family of Plans? Inter alia, this could include: a. Operational physical and cyber security arrangements, capabilities and standards, including military protection and protection from insider threat. b. Preventative measures, such as securing oil and gas storage facilities and refineries. c. Construction standards for critical infrastructure. d. Safe and secure deployment and awareness of Emerging and Disruptive Technologies. e. Redundant personnel resources, installation of protection protocols, and effective countermeasures at vulnerable energy assets to minimise cascading effects; f. CBRN detection and decontamination capabilities; g. Measures to secure access to critical supply chain components, including necessary expertise to maintain and operate critical systems; h. A mechanism to communicate information on all threats and hazards between government, industry and, when relevant, the public; i. A process to monitor and assess harmful economic activities, and address ownership and operational control of critical systems and infrastructure by potentially malicious actors; j. A process to monitor, identify and escalate response to incidents of abnormal activity or patterns impacting energy systems, which could be indicators of sabotage and other hybrid actions; k. Established information sharing protocols to identify similar patterns in other critical sectors.

[18] For further guidance, see Recommendations and Best Practices on the Protection of Electricity, Gas and Oil Critical Infrastructure (AC/331-D(2017)0001).

	3) Are preparedness and mitigation measures regularly reviewed, updated and exercised with all relevant stakeholders, including civilian and military authorities, and energy system operators?
c) Integrate robust continuity procedures into day-to-day operations, including the ability to rapidly restore energy systems and ensure essential energy supplies throughout crisis or conflict.	1) Drawing on the risk assessment, do energy supply restoration plans and procedures include: a. Clear assigned roles and responsibilities for civilian authorities and regulators, infrastructure operators, suppliers and major end users including the military? b. Assessments of minimum and maximum energy supply and demand in crisis and conflict to identify potential system stability issues in advance and mitigate them appropriately? c. Standing and surge personnel capabilities and identified rosters of critical skills to evaluate damage and rapidly repair energy infrastructure? d. Identified essential personnel required to support essential functions and measures to ensure their availability, in the event of severe disruption to workforce availability? e. Necessary stockpiles of critical equipment, spare parts**,** and raw materials**,** and access to spare parts and components to enable timely restoration? f. Diversification of supply routes for energy, critical spare parts and components, suppliers and energy resources? g. Identified, redundant energy systems (generation, transmission**,** storage and distribution), with mitigation plans? h. Sufficient energy supplies to support critical military operations, for example through fuel reserves, backup generation, and long-term restoration? i. Reactive measures, including emergency power supply arrangements and release of reserve oil and gas supply, and alternative methods for power distribution, including non-market based temporary solutions, to ensure access to reliable critical services? j. Established national arrangements for Public-Private sector platforms and protocols to exchange threat information, mitigate vulnerabilities and national priorities? k. Procedures and resources to increase monitoring and, if needed, implementation of response plans for the protection of the national energy sector in crisis situations? l. Tailored and periodically tested emergency measures, including appropriate resources (staffing/redundancy)?

	m. Systematic update/implementation of national procedures and regulatory arrangements to take account of existing and emerging risks? n. Pre-arranged contracts for energy supply, maintenance and relevant commodities, reflecting anticipated supply and demand in crisis and conflict**,** and supported by a network of multiple alternative suppliers? 2) Do energy continuity plans specifically enable priority access to energy supply for NATO assets, installations and operational forces, if applicable, in case of major disruptions, in line with NATO business continuity planning and the requirements for Host Nation Support? 3) Is there a national crisis communications plan to convey public information about energy disruptions, restrictions and prioritisation in crisis or conflict, to combat information threats and promote societal resilience?
d) Conduct regular crisis management training and periodic restoration exercises, including for widespread and long**-**duration disruptions.	1) Is there a comprehensive education, training and exercise programme, which includes: a. Key public sector/private owners and operators, including third party contractors (gas, oil**,** electricity, heat, cooling and hydrogen)? b. Other critical sector interdependencies, including military? c. A comprehensive approach that addresses the impact of different risks and threats to the supply chain and critical infrastructure? d. Scalable exercises and restoration plans (from small outages to wide-scale disruption) covering crisis and conflict? e. Cross-border cooperation, including information sharing, risk mitigation and response through national and international stakeholders and structures, as appropriate?
e) Develop national arrangements to assess critical cross-border interdependencies, including international cooperation, and support restoration and protection activities.	1) Do these national arrangements include: a. A detailed assessment of critical cross-border and internal supplies, supply chain requirements, energy delivery systems and related dependencies? b. Procedures to share information with relevant international organisations**,** as appropriate? i. Do these consider timely notification in the event of a potential impact on NATO operations, missions and activities? ii. Are they able to integrate information from private sector operators?

f) Establish appropriate arrangements (national or multinational) to identify, coordinate and prioritise civilian and military energy needs throughout crisis or conflict.	1) Do national energy supply prioritisation arrangements include: a. An effective national process to coordinate and deconflict civilian energy requirements with military requirements, including to ensure the fulfilment of Host Nation Support requirements? b. A national energy allocation mechanism? c. Flexible continuity of operations including pre-identified contingency arrangements for sources of supply/networks and storage capacity? d. Clarity on governance arrangements for energy storage capacities, including the respective roles of civilian and defence stakeholders and the conditions under which priority access to civilian stocks may be ensured for the armed forces where appropriate? e. Energy surge capacity and scalability? f. Public communication and guidance on consumer usage and/or prioritisation of critical supply in the event of disruption or shortages? g. Contingency planning for critical energy infrastructure to ensure alternative energy supply options?
g) Identify alternative supply options to mitigate energy vulnerabilities**,** including through the use of innovative energy sources**,** and implement multiple supply arrangements to ensure energy redundancy and diversity, including long-term transition plans.	1) Do national energy supply arrangements include: a. Diversification of energy sources of supply, storage, transport and distribution**,** including through the use of innovative energy generation and storage, such as conventional and alternative drop-in fuels and fusion? b. Diversification of technology supply chains for energy transmission and storage, including industrial control systems, transformers, inverters, and batteries at all scales? c. Diversification of supply chains of minerals critical for energy technologies, including rare earth minerals, lithium, cobalt, nickel and copper? d. Strategic energy stockpiles, stockpiles of critical component for energy networks, and distribution capability? e. Related measures to support continued and reliable access to liquid fuels, for example through industrial refining capabilities? f. Pre-arranged contracts for alternative suppliers and energy inventory/storage? g. Risk assessments and mitigation strategies to address the impacts of sabotage and other hybrid actions and strategic competition in the energy sector?

h) Establish robust protocols and procedures covering cyber resilience.	1) Do your cyber resilience protocols and processes in the energy sector: a. Understand and mitigate cyber risks to security of supply as a continuous process? b. Include detection, response and resilience to the full spectrum of cyber incidents and events? c. Cover cyber resilience, both Information Technology (IT) networks and Operational Technology (OT) networks? d. Incorporate security by design: secure production, from secure suppliers, with secure development lifecycles? e. Apply appropriate standards and best practices pertaining to risk management?

Baseline requirement 3: Ability to Manage Controlled and Uncontrolled Movement of People

Objective 1: *National arrangements and contingency plans to address and mitigate the impact of controlled and uncontrolled movement of people from within and outside the national territory, including a mass influx of people that exceeds 2% of the nation's total population, based on national risk assessments, taking into account basic human needs.*[19]

Objective 2*: National arrangements for controlled evacuation of the civil population from crisis and conflict areas. Ensure, if necessary, the protection of the population through restriction of movements, in the event of life-threatening dangers, taking into account basic human needs.*[20]

Objective 3: *Preplanning and exercising handling of the simultaneous movement of people and deploying military forces within the same geographic area via limited transportation routes. This includes a de-conflicting mechanism to prioritise the movement and support of civilians and the military.*

Resilience Guidelines	Evaluation criteria
a) Ensure national arrangements and contingency plans are in place to manage controlled and uncontrolled movement of people from within and outside the national territory, including an influx of people that exceeds 2% of the nation's total	Do national arrangements account for: a. Realistic planning assumptions based on risk assessments**,** the most demanding potential scenarios, and analysis of unfolding events? b. Legislation that provides the competent organisations with the required authority and resources to implement population movement plans and operations, underpinned by relevant organisational considerations and management structures?

[19] PO(2017)0013 (INV).
[20] Ibid.

population, based on national risk assessments[21].	c. Provisions for basic human needs[22] such as physical security, sheltering, food, water, health, sanitation, psycho-social care, education and transport, taking into account the specific needs and requirements of vulnerable people? d. Provisions to establish reception centres, conduct registration, and, if needed, determine legal status and security screening, all taking into account the specific needs and requirements of vulnerable people? e. Measures and arrangements for public health and emergency services to meet the need for surge capacity when managing population movements? f. Designated routes/corridors for transporting people and emergency services that do not interfere with the movement of military forces? g. Arrangements to deconflict civilian and military requirements, taking into account potential competition amongst surge capacities to support military operations? h. Relevant information and guidance to the public? i. Measures to monitor population movement and exchange information with relevant stakeholders, including NATO HQ, other Allied nations, relevant NMAs, the UN and other specialised IOs and NGOs, to maintain situational awareness? j. Procedures for requesting and receiving international assistance? k. Procedures to implement NATO Response Measures addressing controlled and uncontrolled movement of people? l. Cooperation with other nations, including Allied nations that are part of the same Regional Plan, to deal with cross border population movements?
b) Ensure national arrangements are in place for controlled evacuation of the	Do these national arrangements account for: a. Realistic planning assumptions identifying which segments of the population should be moved in different scenarios?

[21] For further information, see Planning Guidance for Nations on Population Movements (AC/98-D(2019)0011 (INV)).
[22] PO(2017)0013 (INV).

population from crisis and conflict areas.	b. Legislation that provides the competent organisations with the required authority and resources to implement controlled evacuation of the population, underpinned by relevant organisational considerations and management structures? c. Mechanisms to deconflict the simultaneous movement of civilians and military forces? d. Provisions to establish secure hubs for the provision of essential services to evacuees, taking into account the specific needs and requirements of vulnerable people? e. Provision of essential information to the population? f. Cooperation with other nations, including Allied nations that are part of the same Regional Plan, to deal with cross border evacuations?
c) Ensure there is a process to develop provisions for restrictions on the movement of people under exceptional circumstances, such as an obvious danger of loss of life due to natural disasters; life threatening epidemics, pandemics and other Chemical, Biological, Radiological and Nuclear (CBRN) threats; or to support NATO or national military requirements (e.g. to prevent interference with the movement of military forces).	Do these provisions take account of: a. Applicable international law and regulations dealing with the movement of people and restrictions[23]? b. Clear communication to the population about the purpose and length of these movement restrictions if predictable, targeted group/groups of people, and a clearly established process for recovery? c. Exceptions for specific groups, such as identified essential personnel (e.g. health care workers and workers supporting other critical services, including child-care, care for aged and disabled people, essential personnel for public utility services, etc.)? d. Arrangements to allow citizens from other nations to return back to their home countries if desired/feasible? e. The social and economic consequences of long-term movement restriction or lockdown, including impacts on the provision of critical public services? f. Guidance to support citizens to be self-sufficient for a defined period of time during crisis and conflict?

[23] PO(2017)0013.

d) Validate national arrangements through regular training and exercises involving all relevant stakeholders (civil, military, private and voluntary sectors).	Do training and exercise programmes address: a. National arrangements dealing with population movement, including civil-military cooperation, and the role and responsibilities of key stakeholders? b. Lessons identified/learned and corrective action processes to reflect exercises and real-world events? c. Public communications, including crisis communications?
e) Ensure a legal framework is in place for the government to acquire the necessary transport capabilities, taking into account the potential need for simultaneous movement of civilians and military troops.	Have the necessary transport capabilities been identified and is there a legal framework guaranteeing assured access to them?
f) Ensure arrangements to de-conflict the simultaneous movement of the civilian population and incoming military forces are included in Host Nation Support Minimum Operational Requirements.	Are arrangements in place and do they address: a. The restriction and prioritisation of the use of main transportation routes, Reinforcement and Sustainment Network (RSN) assets and infrastructures as well as facilities designated for Reception, Staging and Onward Movement (RSOM)? b. Identification of and specific plans for the most challenging areas for de-confliction? c. Provisions for civilian and military authorities to coordinate and continuously reassess planning assumptions in a crisis or conflict? d. Inclusion of international and/or non-governmental organisations, as appropriate? e. Identification and support of critical nodes for continuity and security of supply chains, and specific provisions for deconfliction of movement?

Baseline Requirement 4: Resilient Food and Water Resources

Objective 1: *Ensure situational awareness, early warning and protection for food and water resources, and critical infrastructure, including against all threats and hazards.*

Objective 2: *Comprehensive contingency plans* **–** *regularly exercised nationally and/or with other Allies* **–** *to secure food and water supply, particularly during crisis and conflict, to ensure provision of food and water to civilian population and in support to military operations in line with the Host Nation Support (HNS) requirements and the NATO Response Measures.*

Objective 3: *Continuity of essential functions in food and water sectors under sustained crises, addressing, workforce availability and capability, critical inputs, supply and cross-sector dependencies, and risks associated with potential harmful economic activities.*

Resilience Guidelines	Evaluation criteria
a) Ensure food and water resilience and security through situational awareness, comprehensive risk assessment – developed and shared with all relevant civil and military stakeholders – and horizon scanning.	1) Have you identified critical systems, infrastructure, and stakeholders across the entire food and water value chain – from primary production through processing, distribution and retail – to ensure they meet security, civil protection/defence and military requirements (e.g. HNS)? 2) Is there a comprehensive, regularly updated sector-wide risk assessment that evaluates and accounts for: a. Risk and impacts of armed attack on food and water systems and infrastructure? b. Cyber risks? c. Sabotage and other hybrid actions? d. Extreme weather, natural disasters**,** space weather and the changing environment? e. Mass health crises and pandemic events?

	f. CBRN risks? g. Impact of harmful economic activities, ownership and control of critical infrastructure, technologies and systems? h. Vulnerabilities related to international trade systems, transport and logistics? i. Vulnerabilities associated with critical interdependencies? i) energy sector; ii) civil communications sector; iii) civil transport sector; iv) external suppliers and digital systems; v) critical input such as fertilizers, feed, seed and packaging; vi) workforce availability? j. Emerging (e.g. global navigation satellite system jamming and spoofing) or low-probability, high-impact risks? k. Impacts of assessed risks on military forces and capabilities? 3) Does the assessment draw upon intelligence and other input from all relevant stakeholders, including civilian authorities, private sector and the military? 4) Is information on risks and incidents, including hybrid, reported and shared (including classified information) nationally, with neighbouring Allied countries and NATO, to support shared situational awareness and timely decision-making?
b) Link relevant national and regional stakeholders and their capabilities to support timely detection, assessment and reporting of kinetic or hybrid activities, affecting food and water systems, including critical infrastructure.	1) Are there established links between relevant civil, military and private sector stakeholders in food and water sectors? 2) Are these relationships maintained and further developed? 3) Is there a mechanism to share classified and unclassified information and assessment on all threats and hazard between government, private sector stakeholders and, when relevant, the public?
c) Develop and implement risk mitigation measures to reduce	1) Drawing on the risk assessment, do plans/measures exist to mitigate vulnerabilities and protect food and water systems and infrastructure against disruptions and attacks?

vulnerabilities of food and water systems to disruption and attack, including in support of collective defence.	2) Do they include: a. physical and cyber security; b. alternative supply sources; c. redundancy (e.g. back-up power, stockpiles); d. repair capability? 3) Are national authorities cooperating with private sector stakeholders in designing and implementing these measures? 4) Are essential personnel and operational responsibilities necessary for the successful operation of food and water systems in crisis and conflict defined and communicated? Does this include: a. key maintenance engineers; b. highly specialised personnel; c. sectoral points of contact and d. decision-making authorities? 5) Do these mitigation measures account for HNS requirements? 6) Are additional measures and resources (e.g. protective measures, testing protocols, surveillance) for risk impact mitigation accounted for by national authorities and private sector? 7) Do national authorities have tools to incentivise the private sector to support mitigation measures? 8) Do national authorities have legal mechanisms to direct the agri-food and water sectors and tools to address any dependencies? 9) Do mitigation measures include awareness raising programmes or campaigns aimed at civilian population and private entities?
d) Establish and maintain an inclusive, sector-specific crisis management and response capability to ensure rapid	1) Have roles and responsibilities for key personnel/functions with decision making authority in crisis and conflict been established? 2) Do your response processes and procedures: a. ensure coordination of actions between key stakeholders and sectoral points of contacts;

operational response and continuity of essential functions during crisis and conflict.	b. account for security alternate/back-up arrangements for supply for food and water; c. include prioritisation arrangements, including for military needs; d. align with the relevant NATO Civil Preparedness-related Response Measures? 3) Do you ensure coordinated, reliable and transparent crisis communication to build and maintain trust and support within civil society, to disseminate reliable information and to address information threats? a. Does it include guidance to different stakeholders, taking into account potential shifts in demand and consumer behaviour in crises and conflict?
e) Develop and conduct a comprehensive training and exercise programme (including with other Allies) to validate contingency plans, test interdependencies, and strengthen preparedness for all threats and hazards affecting food and water systems.	1) Are sector-specific trainings and exercises conducted on regular basis? 2) Are these conducted on various levels (e.g. national, sub-national level)? 3) Do these involve all relevant stakeholders (e.g. public, private, civil and military)? 4) Are lessons learned from training and exercises, as well as real crises and conflicts systematically collected and used to bolster resilience? 5) Are lessons learned shared with all relevant stakeholders? 6) Do sectoral trainings and exercises address interdependencies of food and water and other sectors, such as energy and transportation?

Baseline Requirement 5: Resilience To Deal With Mass Casualties And Disruptive Health Crises

Objective 1: *Strengthen resilience and readiness through a whole-of-government and whole-of-society approach to preparedness and planning to address mass casualties and disruptive health crises, ensuring the provision of essential healthcare services to the population and in support of the national and NATO military forces.*

Objective 2: *Enhance mechanisms and procedures to share health and medical information and situational awareness between civil and military medical authorities and other key stakeholders as well as relevant international organisations.*

Objective 3: *Create a comprehensive and secure overview/database/inventory of the emergency civil and military healthcare capabilities and capacities.*

Objective 4: *Develop comprehensive and integrated contingency/emergency plan/planning addressing/responding to mass casualties in an emergency and times of crises and conflict.*

Objective 5: *Design robust and diversified national stockpiling and security of supply arrangements for medical supplies, equipment, pharmaceuticals and/or active pharmaceutical ingredients, as well as blood and blood products.*

Objective 6: *Conduct comprehensive civil-military training and exercises to test plans, procedures and cooperation among all relevant stakeholders.*

Resilience Guidelines	Evaluation criteria
a) Build resilience to facilitate the response to mass casualties and disruptive health crises.	System: 1) Are the roles and responsibilities, including legal authorities and limitations, within the health system clearly defined and understood? 2) Are regular health preparedness assessments conducted of the national health care systems/services? 3) Do these authorities facilitate and address the civil-military medical joint planning, coordination and/or transfer of authorities in the transition from peacetime, through crisis, to conflict, to recovery, and back to peacetime? 4) Is a standard triage system used and are first responders and clinical staff trained accordingly? In extreme situations, is it possible to use the reverse triage system? 5) Do you have guidelines and recommendations (for instance disaster medicine guidelines) on how to manage and allocate resources in the event of mass casualties? Space: 6) Are key healthcare infrastructure and resources inventoried/tracked digitally (e.g. geo tagged) and updated regularly? 7) Is the inventory/database secured/protected? 8) Does it include resources of key private sector and other vital health service providers? 9) Have the key health infrastructure, services and resources been assessed against threats of all types (e.g. terrorism, hybrid, extreme weather, natural disasters, and changing environmental conditions as well as conflict) and take into account cross-sectoral dependencies (e.g. transport; energy, communications, and water)? 10) Has the capacity of hospitals, alternative treatment sites and shelter areas been identified and evaluated? Do shelters provide capacity for patient treatment?

	11) Are coordinated programmes/strategies and funding in place to assess and enhance the resilience (structural and non-structural) of health/care system? Are there incentives/funding to reinforce hospital infrastructure (e.g. underground facilities/hardening) and/or to create redundancy/spare capacity (e.g. electricity supply (generators, fuel reserves) to be able to run health/care facilities autonomously) Staff: 12) Do you track the number of (potential shortfall of) healthcare personnel, personnel that are also reservists; and/or personnel citizens of other countries? If you experience a shortfall in healthcare personnel, have you put a programme/strategy to mitigate it?[24] 13) Do you have plans, procedures and funding to move and/or surge staff (e.g. task transfer, extension of duties/duty hours, use of retired doctors and nurses, medical students and others)? Do you have procedures in place addressing/lifting liability/indemnification/recognition of certification/credentials? 14) Are robust arrangements in place to enabling a (coordinated) shift from conventional to contingency to crisis care? Is this exercised? 15) Are coordinated (civil/military; national/regional/local) plans and procedures in place to evacuate/relocate large number of patients?[25] Does it include the activation and establishment of evacuation-coordination cells and/or mechanism to direct/manage flows of patients (national to local and across borders)? Does a, coordinated, established (national) system enable the exchange of patient data, information and tracking of patients? Are relevant cross-border agreements in place, including bordering/regional

[24] AC/345-D(2024)0017 – Strategies to address the Shortfall of Healthcare Workers
[25] AC/345-D(2024)0018 – Non-Binding Guidance for Civil-Military Cooperation for the Evacuation of Patients in Large Scale Emergencies; see also AC/320-N(2024)0012 - The revised Allied Command Operation Patient Flow Management Guideline.

	Allies? Are arrangements and resources in place to surge coordination cells for prolonged operations? 16) Is there a comprehensive planning and/or a programme to promote a coherent and integrate communication/information system and/or common standards for information management and sharing? 17) Are comprehensive, coordinated crisis communication plans/strategies in place, including to promote societal resilience? Do these take into account the need to address potential of information threats? Do they contain clear messages/instructions to the public, using multiple platforms based on target audiences? Stuff: 18) Are thresholds and processes for access/requesting regional/national/international assistance/resources (e.g. NATO EADRCC, UN OCHA, WHO, EU ERCC, as well as NGOs) well established? Are the time lags in receiving such assistance understood? 19) Is the additional assistance pre-packed/mobile? And, relevant transport capabilities pre-identified/earmarked? 20) Have bi-lateral, multilateral and cross-border agreements for requesting and/or providing assistance (e.g. staff, medical supplies and equipment, transport/treatment of patients) been put in place?[26] Are potential liability issues addressed? 21) Does the guidance to citizens on personal resilience/emergency kits cover guidance on medical supplies to keep at home and on first response measures?
b) Establish mechanisms and procedures to share, health and medical information and situational	1) Does a national public health information collection and analysis network exist? 2) Does this network extend/include specialist areas (e.g. pandemics, antimicrobial resistance, CBRN, including pandemics, burns and intoxications)?

[26] This may require agreeing/arranging the details of receiving and onward transport of patients, including the handling of relevant technical equipment and machines.

awareness between civil and military medical authorities and other key stakeholders as well as with relevant international organisations.	3) Is medical/health information collected, analysed and shared across government? Does it include military/civil information and feed into a broader situational awareness picture? Does it cover, for example, environmental health and epidemiology? 4) Is it linked to existing international early warning systems (e.g. all hazards notification as per International Health Regulation) and does it enable information exchange in health crises? 5) Are there standardised approaches and methodologies for information collection across the country, including for the analysis of open-source information? 6) Have integrated and harmonised processes been put in place to ensure a swift exchange of information, including between relevant national authorities, private sector providers and organisations? 7) Is there a nationally approved list of critical information requirements (content, format and frequency)? Is the process to collect this information in place and regularly exercised? 8) Are there means to share classified information? Are individuals authorised to deal with classified information? 9) Is there an established national/regional/local first responder communications platform or network that can be used during the early phases of an event? Is it centrally coordinated? Does it include all first responders and hospitals? 10) Have the hospital/health care information systems/technologies been vetted/screened for potential vulnerabilities (e.g. harmful economic activities; insufficient or improper cybersecurity measures and protocols)? 11) Are regular updates and basic cyber hygiene training required/performed? 12) Has a comprehensive plan for national warning with pre-defined and tailored messages for mass casualty and disruptive health crises (e.g. CBRN incidents) events been integrated into the overall warning system? 13) Are national plans and procedures in place to implement relevant NATO's Response Measures related to medical support for a potential emergency, crisis and conflict?

	14) Have relevant agreements, personnel, and means of communication been identified/designated to liaise and exchange information with national and NATO military personnel (e.g. NATO Military Authorities/Joint Force Commands)?
c) Define and monitor critical assets to deal with mass casualties.	1) Have the critical resources, including critical and priority medical countermeasures, to cope with mass casualties been identified, including deployable teams, tent ambulances, technical equipment and assets? 2) Have potential shortfalls been identified? And, potential mitigation measures (e.g. use of private sector) been identified? 3) Do they include civil (public and private) and military infrastructure, medical and rescue capabilities? 4) Do they include identification of critical healthcare workers (including mental health care providers) required to support essential functions, in the event of severe disruption to workforce availability during a high impact crisis, including pandemics? 5) Are medical evacuation assets (sea, rail, rotary/fixed-wing and ground) available? Are these readily available and/or are procedures in place to requisition them? 6) Have relevant CBRN (civil and military) capabilities been identified and included?[27] 7) Are hospitals prepared for the management of mass casualties? And are emergency plans in place for hospitals? 8) Are relevant specialist and specialist capabilities foreseen (e.g.: psychological capabilities, turnkeys)? 9) Is knowledge transfer ensured (i.e. does new scientific evidence get to where it needs to be implemented, e.g. in the hospital)?

[27] For further information, see Non-Binding Guidelines for Enhanced Civil-Military Cooperation to Deal with the Consequences of Large-Scale CBRN Events Associated with Terrorist Attacks (PO(2019)0054).

	10) Does it include key pharmaceutical and medtech companies; key vaccine stocks/supplies; biomedical equipment; blood and blood products (including transport); mortuary; main crematoria and storage facilities; relevant transfer and transport assets; volunteer services that may provide important assets and resources, as well as capabilities for the identification of victims? 11) Is the information regularly updated? Are civil and military, as well as international capabilities, reflected? 12) Is this overview maintained in real-time in a central information system or does it rely on information/input from various sources? 13) Have security measures been put in place to ensure first responders are able to respond in a safe environment and have access to personal protective equipment and decontamination capabilities? 14) Do all authorities have the necessary, independent and integrated portable and mobile communication equipment? 15) Are capabilities needed to deal with waste management included? 16) Are potential alternative sites of care and resources (public, military, commercial) identified/inventoried?
d) Develop and/or enhance the resilience and sustainability of national security of supply arrangements.	1) Do national security of supply arrangements[28]: a. Correspond to a comprehensive national threat and vulnerability assessment that takes account of/prioritises a variety of scenarios, including terrorism and pandemics as well as crisis and conflict? b. Rely on data/modelling/understanding of consumption levels and existing utilisation**,** as well as take into account potential (exponential) peak demands?

[28] See AC/98-D(2019)003-REV1 (INV) - Guidance to National Authorities for a Robust Security of Supply and Supply Chain Arrangements and AC/98-D(2022)0004 – Guidance to National Authorities on Medical Countermeasures.

	c. Rely on pre-determined stockpiles (incl. blood and blood products) or national production capabilities and/or contracted stocks? d. Are these stocks/reserves kept within the country? Have physical and cybersecurity measures been identified/applied? e. Cover civil (e.g. general practitioners, hospitals, nursing/retirement care home staff, NGOs) and military requirements (including requirements linked to Host Nation Support)? f. Assure security of supply including through stockpiling of critical items, for a minimum of 3 months of regular use? g. Consider and mitigate potential dependencies on external suppliers of raw materials/active ingredients? h. Take into account the potential break-down and/or failure in supply chains and/or export limitations? i. Foresee coordination and exchange of information with the private sector, including key pharmaceutical/medical industry? Are contingency and continuity plans and/or planning requirements identified for these private sectors? j. Include emergency funds/resources available to compensate for- or to purchase relevant resources? k. Assure a clear management and administrative structure established for any national security of supply arrangement, managed centrally or through a government agency and/or private sector? l. Ensure relevant transport assets are available for timely distribution and resupply? m. Include/foresee the use of alternative sites for diagnosis and dispensing medicines? n. Include arrangements to release relevant resources from the security of supply arrangement and/or enable national authorities to steer/direct the production of supplies and/or distribution of assets/resources?

	o. Is there a national capacity to develop, produce and store vaccines? To shift production capabilities? Are emergency regulation/procedures in place to activate and resource such a shift? 2) Is the supply arrangement, incl. information on the scope and status of supplies, shared/coordinated between national civil and military authorities? 3) Does national regulation/legislation speed up the regulatory approval and facilitate the movement, cross-border donations/supply of medicines and equipment, especially in times of crises and conflict? 4) Include reporting requirements to notify shortages/shortfalls, which are centrally managed and updated regularly? 5) Put in place crisis communications strategies/information to address public concerns over the dangers/quality vaccines and essential medicines, availability and access to supplies as well as responding to information threats? 6) Does it include guidance to citizens on personal resilience also on medical supplies (e.g. guidance on medical supplies to keep at home; regular first aid courses)?
e) Develop an integrated, civil-military contingency/ emergency plan.	1) Has an integrated, comprehensive, civil-military contingency/emergency plan been developed and is it based on realistic/national scenarios?[29] 2) Does planning cover single, large-scale incidents (e.g. terrorist attack) involving 1000 casualties or more?[30] 3) Does planning cover a protracted crises (in a contested environment) with a continuous inflow of casualties over months?[31]

[29] For further information, see Guidance to National Authorities for Planning for Incidents Involving Catastrophic Mass Casualties (AC/98-D(2018)0002-REV1, multiref). Please see also the Total Battle Casualty Rate Estimate Guidelines for Defence Planning (NR) (PO(2025)0331).
[30] For further detail on the injury pattern please see AC/98-D(2018)0002-REV1.
[31] In Ukraine, between Feb 2022 and Dec 2025, more than 14,500 civilians have been killed and more than 53,000 were injured. Assuming a population of around 40 mil., the ratio of civilians injured (per thousand, per month) has been around 0.0086 killed and 0.0313 injured. These calculations are based on figures taken from the United Nations.

	4) Does the plan cover all steps: first response, pre-hospital care, transfer/transfer mechanisms, primary care and hospitals, forensic and mortuary facilities and funeral arrangements? 5) Are roles and responsibilities (public, military, private, including NGOs) assigned, including information on potential volunteer services, nursing associations, etc.? Have command and control and points of hand-over or transition of authorities (e.g. local to regional, civil to military) clearly been identified/defined ahead of time? 6) Are medically, ethically and legally agreed recommendations developed on how to allocate/distribute (limited) medical resources or on when to apply alternative and/or crisis standards of care? Is it clear who authorises their application? 7) Are both quantitative and qualitative capabilities included in this plan? 8) Does it cover the needs of vulnerable groups and/or populations at risk? 9) Does the plan address and prioritise multiple requirements on the same resources, including Host Nation Support requirements? 10) Does the plan establish a coordination mechanism between relevant civil and military authorities at all levels (e.g. POCs, procedures), including for the evacuation/transport of a large number of victims? 11) Does the plan address zones of safety and security (incl. potential areas/shelter for hospital personnel)? 12) Does it set out direction and procedures to manage large numbers of deceased (including mortuary facilities, victim identification and repatriation of remains, burial sites)? Does it cover how to deal with fatalities from a potential exposure to and/or contamination with CBRN agents? Does it take into account requirements for criminal investigation and coordination with the police and justice services?[32]

[32] AC/345-D(2026)0007 – Non-Binding Guidelines for the Planning and Management of Incidents with large number of Fatalities

	13) Are relevant stakeholders included in the development? Has the plan been shared with relevant stakeholders (including field practitioners)? Where relevant, has the public been informed? 14) Is the plan regularly reviewed and updated, including information based on lessons learned and experience? 15) Is there a linkage between the activation of the national contingency planning and the NATO Response System? 16) Do legal provisions foresee extraordinary measures, such as a declaration of state of emergency, to acquire additional resources? 17) Does preparedness legislation take into account the flexibility required for the recognition of the qualifications of medical professionals/practitioners (link to surge capacity and/or crisis standards of care)?
f) Develop and implement a training and exercise programme that tests plans and procedures, and brings together relevant stakeholders.	1) Has a robust and inclusive exercise and training programme been put into place? 2) Does the training of medical students/doctors and nurses include/cover military medicine and/or training of civilians to work alongside military personnel? 3) Is first aid training (including on application/use of personal protection equipment) provided to the general public and is it institutionalised? 4) Is training regularly provided to the different responders (including First Aid, triage and treatment options)? Are the offered courses both online and offline? 5) Are exercises conducted regularly? 6) Are exercises conducted at different levels, in different formats (table top format to field exercises), and do they cover civil-military aspects? 7) Are different aspects of a response to mass casualties trained and exercised? Is the response plan exercised? 8) Has a training and exercise calendar been shared with relevant civil and military stakeholders?

	9) Do national, joint training and exercises take place to test the provision of civil medical support to military forces? 10) Do exercises involve relevant public and private stakeholders (e.g. NGOs; industry)? 11) Has a lesson's learned process (and potential R&D) been established and shared? Does it include a corrective actions plan? 12) Are tests conducted (scheduled and unscheduled)? 13) Are cross border emergencies exercised (bilaterally, multilaterally)? 14) Is the provision of psychological support part of the training?

Baseline Requirement 6: Resilient Civil Communications Systems

Objective 1: *Continued availability of reliable, resilient and secure civil communications services. This should include continuity and contingency planning for crisis and conflict situations, and be underpinned by national legislation and crisis management arrangements in cooperation with private sector and military stakeholders.*
Objective 2: *Comprehensive and regular national risk assessments of the full range of risks and vulnerabilities, considering also risks in a situation of crisis and conflict. The risk assessments should include physical and digital risks, as well as the cascading effects of disruptions on civil support to the military, continuity of government, and other sectors including emergency services, energy, transport and health care.*
Objective 3: *Establish and maintain an overview of supply chains, including sources of critical components, dependencies, foreign ownership, and control of vendors and service providers that are critical to the availability of communications networks, systems and services. Consider the availability of critical supply chains and managed services in a situation of crisis or conflict.*
Objective 4: *Ensure priority access to civil communications networks and services to support both societal resilience and military enablement, and including for the national and Allied military and Host Nation Support (HNS) requirements.*
Objective 5: *Assured capability and mechanisms to support communication between the authorities and civil population, including during crisis and conflict. This should include national capabilities of alert and warning systems to the population in case of an emergency situation.*

Resilience Guidelines	Evaluation criteria
a) Establish national cooperation structures for preparedness planning, situational awareness and crisis response with key civil and military authorities and private sector stakeholders.	1) Has the national authority identified the relevant key stakeholders, including civil and military authorities, and public and private sector telecommunication operators? 2) Has the national authority established cooperation structures with the identified stakeholders to assess and coordinate network functionality, crisis response and maintain situational awareness? a. Are the identified stakeholders, including private sector operators and military authorities, included in the regular cooperation mechanism? b. Does the cooperation structure support planning and crisis response throughout peace, crisis and conflict? c. Is the cooperation underpinned and enabled by a legal/regulatory framework? 3) Have national authorities established a process to ensure that: a. Information is exchanged in a timely, systematic and secure manner; b. Coordination is effective and incident response happens in a timely manner; c. Private sector communication service providers are aware of the requirements and crisis response arrangements, including those relevant during crisis and conflict? 4) Has the national authority established cross-border cooperation with neighbouring Allies, in particular those that are part of the same Allied Regional Plan, for preparedness planning, technical interoperability and crisis response during crisis and conflict?
b) Identify and classify communications services and infrastructure that are critical for the continuity of government, civil support to the military and provision of critical services.	1) Is there a nationally agreed methodology in place, involving the key stakeholders, for identifying critical networks, network elements, communication services and critical dependencies of those systems? a. Does it include a clearly defined classification scheme with defined availability and recovery objectives? 2) Do public-private partnerships develop, and does the national regulator/authority maintain, a high-level knowledge base of critical networks, systems and services? a. Is it updated regularly to reflect existing and evolving technologies?

c) Assess civil communications resilience and security with appropriate, comprehensive risk assessment, including risks relevant during crisis and conflict.	1) Is there a comprehensive and regular sector-wide risk assessment, involving the key stakeholders, that evaluates, inter alia: a. Physical security of civil communications infrastructure; b. Personnel security; c. Cybersecurity threats from state or non-state actors; d. Sabotage and other hybrid actions from state and non-state actors; e. Risks and impacts of armed attack, including kinetic, CBRN and EMP threats; f. Vulnerabilities associated with critical dependencies, such as power supply, critical undersea infrastructure, GNSS-based synchronisation services and alternative PNT solutions[33]; g. Risks and impacts of emerging and disruptive technologies, such as evolving 5G technologies, the operational use of artificial intelligence (AI), and the impacts of quantum technologies[34]; h. Extreme weather, natural disasters, and the changing environment; i. Mass health crises and pandemic events? 2) Does the risk assessment consider all aspects of critical civil communications infrastructure, inter alia: a. Critical network elements, and their dependencies on the underlying physical infrastructure, datacentres and cloud services; b. Network operations and managed services; c. Physical location of these services. 3) Does the risk assessment consider access to critical supply chains during crisis and conflict, including, inter alia: a. Access to critical components, necessary expertise and repair/restoration capabilities;

[33] For further guidance, see AC/121-D(2025)0003 The Impacts of GNSS Interference on Resilience, and AC/345-D(2025)0017
[34] For further guidance, see AC/121-D(2025)0004 The Impacts of Emerging and Disruptive Technologies on the Resilience of Civil Communications

	b. Access to managed services, vendors and service providers that are critical to the availability of communications networks, systems and services; c. Identification of systemic and concentration risk, including dependency on a limited number of critical third-party ICT service or digital infrastructure providers? 4) Does the risk assessment consider the dependencies on critical civil communications infrastructure, including from: a. Other critical sectors such as transport, energy and healthcare; b. First-responder/emergency communications use of civil communications networks; c. Military use of civil communications networks; d. Host Nation Support (HNS) requirements, especially the HNS Minimum Operational Requirements (MORs)? 5) Are the risk assessment and threat alerts shared with operators and other necessary stakeholders in a timely fashion? a. Are the required mitigations of high-risk gaps prioritised with the operators and other key stakeholders? b. Is there a mechanism to ensure the mitigation of high-risk gaps within a defined timeframe?
d) Establish measures to identify and mitigate the potential risks of harmful economic activities that could have implications for national or Alliance security.	1) Have the national authorities established a process to monitor and assess harmful economic activities, ownership and operational control of national communications networks, including managed services, supply chains, and the personnel supporting critical services? 2) Have procedures or a formal mechanism been established to identify, evaluate and potentially address/mitigate any national security risks resulting from harmful economic activities?
e) Take measures to protect critical civil communications infrastructure from all relevant threats.	1) Do public and private sector communications service providers use standards-based and compatible methodologies for business continuity, contingency planning and risk management? a. Are they underpinned by national legislation and regulation? b. Are such plans shared with the national regulatory authority? 2) Drawing on the risk assessment, do comprehensive preparedness and contingency plans exist to mitigate vulnerabilities and protect civil communications infrastructure? Do they include, inter alia:

	a. Redundancy requirements; b. Physical and cyber protection considerations; c. Access to critical supply chains, and consideration of near-shoring of supply chains and 3rd party support; d. Identification and prioritisation of critical roles/workforce, considering also the expertise provided by managed service providers and subcontractors; e. Contingency arrangements for critical dependencies, inter alia, power supply, network synchronisation and critical undersea infrastructure; f. Provisions for national roaming; g. Alternative means, such as satellite communication, for critical communications requirements? 3) Do the measures include the protection and hardening of civil communications networks that support critical locations, such as HNS MOR infrastructure[35]? 4) Are specific requirements defined for mission critical use of civil communications networks, including first-responder and military use of commercial mobile radio networks? a. Are these aligned with STANAG 5665 Cellular Communications for Defence?
f) Establish robust cybersecurity protocols/procedures, including recovery capabilities from major cyber incidents.	1) Are cyber risks assessed and security controls developed and maintained with standards-based methodologies? 2) Do cybersecurity risk assessments include a process to review risks associated with: a. Relevant cloud platforms used to operate civil communications systems; b. Emerging and evolving technologies, such as 5G, AI, and the adoption of post-quantum cryptography? 3) Do security controls and protocols include, among other considerations: a. Appropriate cybersecurity protection systems, which are regularly maintained and updated? b. Appropriate network and system monitoring for cybersecurity situational awareness.

[35] As defined in the HNS MOR Infrastructure/Pillar I.

	c. Capability to proactively find and remediate cyber compromises through threat hunting operations? d. Capabilities and resources to manage significant cybersecurity incidents affecting critical infrastructures? e. Recovery capability from a major cyberattack, including comprehensive backup processes, testing routines and recovery exercises? f. Flexible and scalable procedures to cope with evolving cyber threats? 4) Are there mechanisms to communicate cyber risk information between private sector stakeholders and civil and military authorities, and with NATO and Allies?
g) Ensure that key stakeholders have developed and implemented crisis response arrangements, and that a mechanism is in place to notify military authorities of attacks on civil communications systems that may impact NATO's core tasks.	1) Are national arrangements in place for crisis response, including civil, military and private sector stakeholders? 2) Are the crisis response arrangements supported by relevant national emergency legislation and regulation in the telecommunications sector? 3) Is there a mechanism to notify national authorities of incidents that affect civil communications services? a. Is incident reporting aligned with the identified critical networks, services and systems, to ensure that private sector operators have the ability to identify and prioritise incidents impacting national resilience and civil support to the military? b. Is incident reporting mandatory? c. Is incident reporting timely to enable adequate crisis response? 4) Are the national arrangements aligned with the NATO Response System and the relevant Response Measures? a. Have specific national authorities been designated to notify the appropriate national and NATO military authorities according to the NATO Response System? 5) Do your crisis response processes and procedures ensure coordination of actions between key civil, military and private sector stakeholders? a. Have you established roles and responsibilities for key personnel/functions with decision making authority in crisis and conflict?

	6) Do the crisis response arrangements allow prioritisation of recovery and restoration in line with national civil and military priorities?
h) Establish and implement an assured capability and mechanisms to support communication between the authorities and the civil population.	1) Do national early warning, reporting and alerting systems exist to communicate with the public? a. Does it ensure robust and fast alert and warning mechanisms with redundant multi-channel capabilities and contingency options? b. Is it supported by relevant telecommunications and broadcasting legislation/regulation? c. Is it frequently tested and known to the public? 2) Have you established means to ensure that the public can communicate with the authorities during crisis and conflict situations?
i) Establish and implement an actionable national prioritisation plan for access to and use of civil communications networks by civil and military priority users.	1) Have national authorities developed prioritisation arrangements, including lists of critical users and locations, which are regularly updated? 2) Do the priority arrangements include, inter alia: a. Military and first-responder use of civil communications networks? b. Prioritisation of HNS requirements, especially the MORs? c. Communication services and infrastructure for NATO installations/headquarters, if applicable, in line with NATO business continuity planning? 3) Does the plan include a coordination mechanism for de-conflicting military and civilian communications requirements? 4) Do you have capabilities and authorities to transfer the required frequencies to the national and Allied forces, in line with the NATO Frequency Plan and the NATO Response System? 5) Is there legislation, regulation or other arrangements in place to ensure implementation of the priority access plan by public and private network owners and operators? 6) Does the plan include public communication and guidance on consumer usage and/or prioritisation of critical services in the event of disruption or limited capacity?
j) Establish a training and exercise programme to test and assess nation-wide and operator-wide network outage restoration	1) Is there a comprehensive training, exercise and evaluation programme involving civil and military authorities, and private sector operators and service providers? 2) Does the programme include public-private and civil-military liaison arrangements, contact points and responsibilities that would be needed during crisis and conflict?

procedures and crisis response arrangements.	3) Does the programme include appropriate training and exercising national crisis response arrangements, including in the context of the activation of the NATO Response System 4) Does the programme include cross-border exercises with neighbouring Allies? 5) Is there a lessons-learned system through which best practices are identified, disseminated and incorporated in existing procedures?

Baseline Requirement 7: Resilient Civil Transportation Systems

Objective 1: *Have legislation, policies and arrangements in place, necessary for continuity of essential civil transport services and civil support to military, including implementation of the NATO Response Measures, that:*

a) identify, test, prioritise, de-conflict, ensure access to, protect, and restore civil/commercial transport assets, infrastructure, services, transport routes, and personnel in a timely manner, to support national and Alliance priorities throughout peace, crisis and conflict;
b) allow border crossing within required timelines to support the freedom of movement of NATO forces, through a single national point of contact supported by a national cross-government network of relevant ministries;
c) provide war risk insurance or establish alternative means to indemnify carriers, within 48 hours of the initial entry of NATO forces into the theatre of operations so that civil transport assets can operate in areas where commercial insurance is not available;
d) maintain an up-to-date national inventory of critical transportation assets, infrastructure and services, also taking into account military requirements;
e) establish cross-government coordination protocols clarifying roles and responsibilities of all relevant authorities and stakeholders.

Objective 2: *Ensure that civil transport infrastructure and services remain resilient so that they are agile and able to withstand and recover, whilst minimising disruption, from:*

a) the impact of a range of potential risks, including both chronic (e.g. changing environmental conditions, information threats, increasing reliance on digital services) and acute risks (e.g. human-induced and/or natural disasters, hybrid threats, cyberattacks, pandemics);
b) the consequences of harmful economic activities and strategic dependencies; as well as
*c) potential vulnerabilities associated with existing and evolving technologies (e.g., GNSS, 5G and next generation communication networks)**,** and potential vulnerabilities associated with prolonged crises, including concurrent and complex crises, as well as cascading effects.*

Objective 3: *Keep transport information (IT) and operational technology (OT) systems, as well as transport-related emerging and disruptive technologies and communications, resilient, so that they are agile and able to perform essential functions. This would be supported by:*

a) a detailed overview of prioritised critical transport-related digital (i.e. IT and OT) infrastructure;

b) back-up and alternative systems as well as redundancies;
c) a mechanism for notifying NATO of significant disruptions on transport systems that have a potential impact on the Reinforcement and Sustainment Network (RSN);
d) a digital system allowing secure exchange of classified information among national authorities responsible for transport resilience, with NATO, as well as with appropriate links to critical network operators;
e) a mechanism to communicate and engage with owner/operator companies providing national and international critical transport assets, infrastructure, and services, throughout peace, crisis and conflict, including at a classified level.

Objective 4: *Ensure resilience of civil transportation systems to support cross-sectoral resilience through:*

a) Identifying interdependencies with other baseline areas, given the critical enabling role of transport for all sectors;
b) Establishing networks with lead authorities for other resilience areas to capture specific transportation needs of respective sectors (e.g. medical, agriculture, etc.);
c) Developing arrangement to meet transportation capacity required for continuity of essential services and civil support to military across all baseline areas.

Resilience Guidelines	Evaluation criteria
a) Establish a national cross-government network responsible for the full range of national regulations that may be applicable in case of a deployment.	1) Are cross-governmental coordination mechanisms in place to ensure a smooth deployment of NATO Forces to include border crossing and freedom of movement? 2) Have a 24/7 national cross-government network of relevant ministries and a coordinated national system been established to control movement of NATO forces into, across and from sovereign territories? 3) Has a single National Point of Contact (sNPOC)[36] been established and authorised to overcome obstacles that might impede border crossing and the rapid deployment of NATO forces? Has the relevant information been circulated to stakeholders and other Allies, as required? Is there an established communication procedure for the

[36] For further information, see guidance on Single National Points Of Contact (AC/98-N(2018)0006).

		sNPOC to contact civil transport operators and infrastructure managers when necessary? 4) Are the cross-governmental coordination mechanisms, including the sNPOC, regularly tested and exercised?
b)	Identify and resolve challenges around national legislation on border crossing and NATO requirements and agreed timelines for border crossing of NATO forces.	1) Does national legislation and relevant procedures allow NATO requirements and agreed timelines for border crossing to be met, and include: a. Special arrangements for different civil and military transport assets, modes and routes involving Allies and non-NATO nations? b. Special arrangements for military equipment, oversized/heavy vehicles and dangerous goods? c. Civil transportation providers operating on behalf of Allied forces? d. Simplified customs, border crossing and movement permissions regulations? 2) Does the nation have the ability to create special transport corridors for prioritised military and civilian cargo? 3) Has the nation reviewed legislative restrictions on the movements of personnel and material on the basis of NATO and Status of Forces Agreement (SOFA) requirements? Have there been legislative changes to facilitate border crossing, where suitable? 4) Is national legislation on border crossing regularly exercised to ensure rapid crossing of borders according to NATO requirements and agreed timelines?
c)	Provide war risk insurance or establish alternative means to indemnify carriers to operate in areas where commercial insurance is not available.	1) Are there arrangements in place to obtain war risk insurance or alternate means to indemnify carriers? 2) Do such arrangements include coverage of civilian/commercial and governmental operators? 3) Can these arrangements be activated within 48 hours? 4) Are these measures regularly tested and exercised? 5) As regards critical transportation entities, is there a negotiated indemnification scheme that would apply when commercial war risk insurance is not available?

	6) Are there mechanisms to ensure war risk insurance cover is promptly available for eligible interests and risks, during activation periods? 7) Have critical partnerships been established between civil transportation industry and different ministries/departments to support timely activation of the relevant war risk insurance/indemnification scheme when needed?
d) Identify critical transportation infrastructure and develop scalable methods for their protection. Analyse the effect of possible disruptions to or unavailability of critical transportation infrastructures on NATO's ability to conduct operations.	1) Are critical transportation infrastructure and routes (rail, road, air, and national waterways) to support national priorities during crises clearly identified, catalogued, and risk-assessed? Are these mapped against infrastructure identified in relevant NATO documents (e.g. Host Nation Support Minimum Operational Requirements)? 2) Do they have back-up capabilities, including the use of alternative transport modes? Do operators of such critical infrastructure have the means in place to switch to alternate sources for energy or 'manual' operating mode in case of communication disruptions? 3) Are there mechanisms to provide ongoing and scalable physical protection and to ensure operational continuity in the event of human-induced and/or natural hazards, hybrid threats, cyberattacks, pandemics or other crises? Are these regularly exercised and tested? 4) Is there a national protection and resilience plan for critical transportation infrastructure in place? If yes, has the plan been validated through a whole-of-government approach and integrated with national and Allied resilience frameworks, as necessary? 5) Is there oversight and planning in place to ensure that critical transportation infrastructure operators meet updated resilience standards? 6) Are there partnerships and a common plan of action established with critical transportation infrastructure operators? 7) Have military transport corridors been identified, including all relevant civilian transport assets and infrastructure required? 8) Are arrangements in place to prioritise and de-conflict civil and military transport requirements, in cases of heavily reduced transport capacity? Do military planners,

	civilian planners and commercial transportation providers work together in peacetime to plan for scenarios of increased demand, reduced capacity and/or competing civil/military priorities? 9) Is there a mechanism to provide advice and guidance to transport operators that are subject to different regional/local regulations?
e) Maintain national, regional and local route mapping including border crossing points.	1) Is national, regional and local route mapping regularly updated, including technical specifications (e.g., bridge height clearance, tunnel width) capacity and limitations? 2) Is there a system of alternative routes in place? Is it regularly tested? 3) Does a system exist to monitor real-time network traffic, freight travel and border crossing times, as well as supply chain flow and disruptions? 4) Is there a backup system for monitoring in place, that might include other means of monitoring? 5) Is there an established communication procedure with civil transport operators and infrastructure managers to monitor real-time traffic? Are interruptions and works on transport infrastructure, which cause reduced transport capacity, regularly communicated? Are response procedures developed and regularly tested?
f) Establish provisions to access, use or dispose of national and foreign-owned transport resources [37]	1) Do provisions exist to ensure national access to, prioritise and de-conflict transport resources (infrastructure, installations, systems, services, assets, and personnel) for exercises, operations and declared emergencies? Do these also take into account relevant stakeholders and operators? 2) Do these provisions cover foreign-owned and operated critical infrastructure and capabilities? 3) Have procedures or a formal mechanism been established to identify, evaluate and mitigate any potential national security risks resulting from foreign ownership, control, or direct investment?

[37] For further information, see Guidance to Assist Allies in Establishing Legislation/Standards for Strengthening Transport Infrastructure and Development of Operational Protocols to Deny/Limit Access to Transportation Resources (AC/98-N(2017)0055-REV1).

	4) Has a mapping of infrastructure, assets and capacity been completed, in collaboration with transportation operators and critical transportation infrastructure operators? 5) Are there legislative or contractual mechanisms to ensure access to transportation requirements?
g) Establish legislation or standards for strengthening infrastructure to facilitate military deployment capabilities and develop operational protocols to deny or limit access to transportation resources as a defensive manoeuvre.	1) Are there plans and resources to update design and construction standards to improve the resilience and military suitability of transport infrastructure (e.g. hardened seaports, and increased maximum weight for road networks)? 2) Are transportation resources (including personnel) sufficient to facilitate military deployments? a. Do these protocols deny or limit access to transportation? b. Have continuous fuel supply needs been considered? c. Are these protocols tested and exercised regularly? d. Are there means to prioritise civilian cargo that facilitates military deployments? e. Is there a strategic plan for transportation management that reserves a percentage of capacity to guarantee civilian transport? 3) Are legislation and/or crisis response measures in place to require civil/private industry to give priority use of transportation assets and services to deploying NATO Forces or other national crisis/security needs? 4) Does the nation carry out regular drills, testing defensive transport protocols, conducted with government and operators?
h) Establish a protocol for warning and notifying national transportation authorities. Conduct regular training and exercises for the established protocols.	1) Is there a protocol for national transportation warning and notification? In what form is this protocol activated? Through which channel is it activated? What is notified to the relevant national authorities? 2) Which national authorities are responsible? Is a linkage to NATO and the NATO command structures, in particular, foreseen?

		3) Is this protocol periodically tested and exercised? Are the exercises performed at the national level including wide-scale and long-duration disruptions? 4) Are transportation emergency operations integrated into national crisis management centres? 5) Is there a network of communications among transportation stakeholders and other members of civil society combining open and secure channels? Is this network tested through regular exercises?
i)	Put in place a mechanism to notify NATO of disruptions to transport systems, which may impact NATO operations.	1) Have protocols to notify the appropriate NATO bodies, including NMAs (e.g. ACO/JSEC) been established? Do they include notification requirements and processes that apply to critical transportation infrastructure operators and infrastructure owners? 2) Are these protocols regularly tested through exercises? 3) Have notification protocols for disruptions to critical transport infrastructure been integrated into the national process of cascading notification, including the national protocol for NATO notifications?
j)	Establish and maintain an up-to-date list of key stakeholders (infrastructure and transport providers) that may need to be involved in movement of NATO forces.	1) Does a list of key stakeholders exist? Does the selection of key stakeholders (across government, industry and civil society) meet a broad range of possible multimodal transportation scenarios/risks? 2) Which national authority is responsible for updating the list of stakeholders, including maintaining a record of adequate security clearances? Are organisation and personnel changes within these stakeholders notified and updated regularly? 3) Are there any security measures foreseen for stakeholders required to ensure transportation infrastructure and services continuity in response to crisis or conflict?
k)	Prepare for Host Nation Support (HNS) responsibilities in the transportation area.	1) Are the HNS requirements in the transportation area clearly understood, including roles and responsibilities of different ministries/agencies that will need to deliver effects to the armed forces? 2) Have commercial carriers that will provide transport services to NATO forces as part of HNS requirements been engaged by your national authorities?

		3) Are transport-related HNS requirements understood and negotiated, as appropriate, between ministries of defence and transport? 4) Are HNS transport plans reviewed and tested regularly?
l)	Identify critical transport technology infrastructure of importance to NATO, and analyse the effect of possible disruptions to or unavailability of critical transport technology infrastructures on NATO's ability to conduct operations.	1) Is critical transport technology infrastructure, of importance to NATO clearly identified and prioritised (e.g. management control centres covering surface, maritime and air, cargo clearance and tracking systems, mobile communication systems, satellite-based position and navigation systems)? 2) Does infrastructure design take account of the potential vulnerabilities associated with existing and evolving technologies? Are risk management plans and procedures flexible, scalable and adaptable? 3) Have vulnerabilities been identified and mitigated for: a. Existing technologies? b. Emerging technologies, before integration into transportation systems? 4) Are total system capabilities tested and exercised? 5) Have industry transportation infrastructure technology protection standards been adopted? 6) Are there backup systems to ensure operational continuity, including for power and communications? 7) Are there alternate plans for continuity of transportation services in the event of a technology failure?
m)	Establish robust protocols for cyber incidents, as well as vulnerabilities associated with existing and evolving technologies. IT and OT security protocols must include backup and alternate systems as well as testing routines, including manual and other arrangements	1) Are cybersecurity software and other protections regularly upgraded to keep up with risks associated with emerging and evolving technologies? 2) Have protocols for testing backup systems been established? 3) Are all IT/OT capabilities and systems tested through exercises? 4) Are cybersecurity protocols/procedures communicated to personnel? 5) Are there mechanisms in place to monitor compliance of transport IT/OT systems with cybersecurity requirements?

	where backup systems do not work (e.g. power outage).	6) Have secure communication protocols between transportation operators and government authorities been formalised to ensure continuity of information exchange during cyber incidents or technology failures? 7) Have national Cybersecurity standards been established and enforced among all regulated critical transportation infrastructure operators?
n)	Ensure the transport system supports sustainable and resilient supply chains in all critical sectors.	1) Are nationally-owned or controlled transport resources able to mitigate and manage disruptions to the supply chain of critical sectors? 2) Do national supply chain strategies exist for mitigating the impact of a reduced or depleted workforce? 3) Has the capability of the national transport system been identified, planned for, and tested on the ways to mitigate any potential shortfall in the energy supply chain, distribution of food, water, medical resources and movement of essential personnel? 4) Are interdependencies among critical infrastructures listed and analysed by the competent authorities? Are they tested in exercises? 5) Is there a mechanism to monitor and prioritise shipments within the supply chain? 6) Is there a contingency plan in support of all of the above? 7) Does the contingency plan include measures to ensure that critical transport infrastructure is protected against physical, cyber and other threats and vulnerabilities, including pandemics? 8) Have contingency plans been developed for critical supply chain nodes, taking into account the needs of civil society and transport operators?
o)	Establish arrangements to ensure transport systems' workforce remains resilient.	1) Are transport workers (across all sectors, including transporters, support employees, and technical representatives) identified as "essential personnel" to ensure that they are able to keep national and international supply chains operating? Is there any national legislation or procedure for identifying essential workers in the transport sector, and for ensuring they have the relevant skills? 2) Have positions or functions within the national transportation sector been identified, which might be: (a) called up for military service or other public services; (b)

	essential to civil transportation services and, therefore, should not be called up for other duties; or (c) needed for civil support services to national or NATO armed forces? 3) Are these designations coordinated between/across jurisdictions? 4) Have procedures been established to facilitate the expedited movement, safety, health care and protection of transport workers? 5) Have consistent medical and sanitation protocols for transport workers across all points of entry within the nation been adopted? Is the application of these protocols consistent with other Allied nations or recommended international norms (e.g. IMO, ICAO)? 6) Have critical skills and labour needs in the transportation system been identified? Are there training programs in place to ensure their availability? 7) Have networks, relationships and legal and contractual mechanisms with industry and labour unions been established to facilitate a resilient transportation workforce? 8) Have plans to access non-traditional labour pools in the transportation sector in times of crisis and conflicts been developed? Are these plans being tested?