



University  
of Exeter

Centre for the  
Public Understanding  
of Defence and Security



## Putting Homeland Defence in its Place

Educating and Exercising, from Whole-of-Nation  
to Whole-of-Region

**Paul Mason, Frances Tammer & Frederick Harry Pitts**

Centre for the Public Understanding of Defence &  
Security, University of Exeter

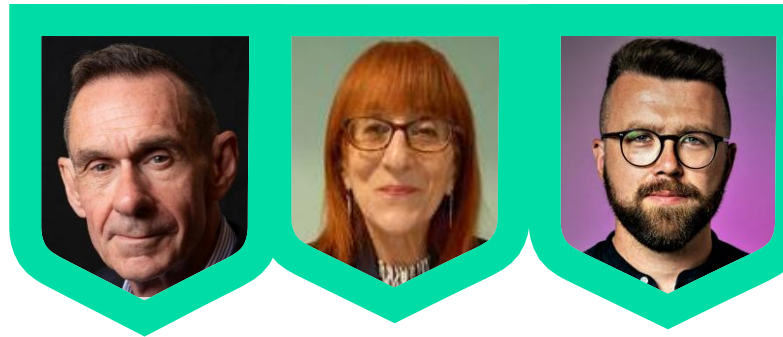
October 2026

**CPUDS**

Centre for the Public Understanding of Defence and Security

# Putting Homeland Defence in its Place

## Educating and Exercising, from Whole-of-Nation to Whole-of-Region



### Executive Summary

- UK awareness of Homeland Defence and whole-of-society resilience is gradually kicking into gear but must gather pace at speed and scale; a crucial task of this emerging national conversation is to bridge the gap between national ambition and regional and local capability, drawing in the general public.
- Homeland Defence ultimately has to be delivered by networks of actors at regional and local level including neighbourhoods. This must span the military, local government, emergency services, critical infrastructure, industry, civil society and the general public.
- Situated under clear national co-ordination, the region is a key unit of analysis and action; preparedness cannot simply be prescribed nationally, but must reflect the specificities of different geographies.
- As different regions have distinct vulnerabilities, infrastructure, industrial assets, social characteristics and governance arrangements there needs to be a practical means of bringing a range of regional stakeholders together to understand, test and strengthen resilience before a crisis or simultaneous crises take place.
- In July 2026 a pilot Home Defence training programme and tabletop exercise (TTX), co-produced with partners and stakeholders, tested the proposition that regional defence, security and resilience preparedness and readiness is strengthened when shared education precedes realistic multi-agency exercising.
- However, the TTX exposed a system-integration problem. Organisations could act effectively within their remits, but collective interaction was constrained by security boundaries, infrastructure dependencies and weak ownership of the information space.
- The exercise reinforced the case for treating preparedness as a capability built before crisis through doctrine, relationships, rehearsal, evaluation and lessons learned.
- The exercise further reinforced that the regional level provides the bridge between national direction and local delivery because it is where cross-boundary systems, distinctive vulnerabilities and the relevant institutional networks come together.
- The proposed next step is a repeatable, nationally co-ordinated and regionally adaptable model for driving and evaluating the national conversation on defence and security at different geographical scales, and which joins assessment, education, exercising, learning and measurable improvement.
- This would be anchored by universities in collaboration with Joint Military Commands, Regional Defence & Security Clusters, Local Resilience Forums and other partners, with an iterative loop between:
  - understanding a region's risks, resources and responses;
  - educating stakeholders across public, private and third sectors;
  - exercising the system with place-based TTXs; and
  - capturing lessons with evaluation and strengthening preparedness by shaping planning.
- Securing the resources and funding to sustain this activity and ensure its alignment with the national Homeland Defence programme is a key question and problem.



## Background and introduction

The UK's awareness of Homeland Defence and whole-of-society resilience has begun to build limited momentum. The practical challenge is to connect national ambition to regional capability and local action with the general public knowing what role it will need to undertake, but all at speed and scale. A previous paper published by the Centre for the Public Understanding of Defence & Security (CPUDS), *Making Sense of Home Defence: From Planning to Practice*, defined homeland defence as the interaction of military aid, societal resilience and a whole-of-society approach. The central issue in making this all cohere is not simply whether powers and plans exist, but whether institutions, relationships, knowledge, capabilities, public legitimacy and learning systems make them practical and enduring.

Co-produced at a Sandpit event in November 2025 with partners from government, the military and the emergency services, our team put these propositions to the test in July 2026 with a pilot training programme and tabletop exercise (TTX) bringing together a whole-of-society cohort from central and local government, the Armed Forces, emergency services, critical infrastructure, industry and civic society. This consisted of a two-day programme combining curated education with a realistic cross-domain TTX for all participants from central and local government, the Armed Forces, emergency services, critical infrastructure, industry and civic society.

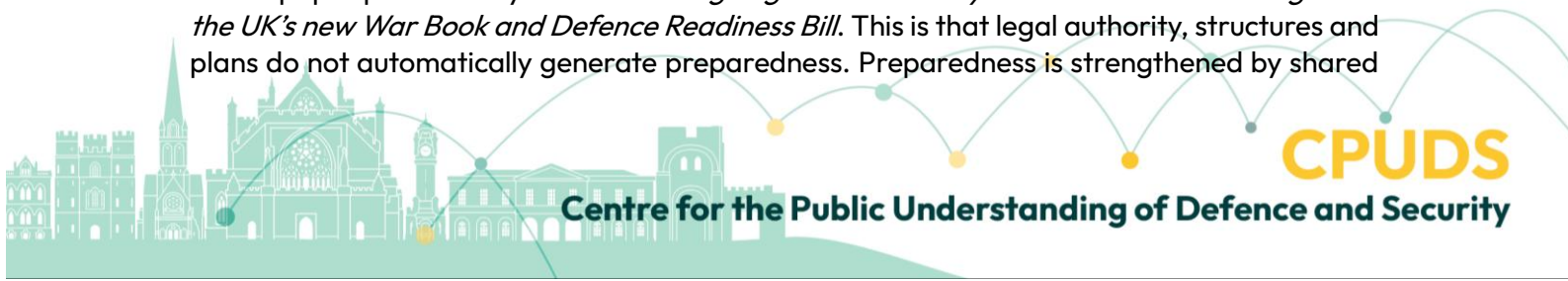
The wider regional relevance of this work was subsequently presented in October 2026. at a major military and civilian Home Defence conference hosted by the British Armed Forces and run by a Joint Military Command. The conference brought together a similar set of representatives from the Sandpit event with stated aims to improve understanding of the strategic context and threat picture, invest in partnerships and networks, strengthen preparedness and identify opportunities for regional cooperation. The University's contribution focused on professional education and TTXs as practical means of helping organisations understand how they could work together, test complex decisions and identify preparedness priorities.

This paper develops that account by setting out the educational model, the regional proposition and the evidence generated by the July exercise.

## Aims of training and education

The development of the pilot was in response to the identification of a specific education and training gap. In a sequenced timetable, Day One was designed to establish common understanding before participants were asked to act under pressure on Day Two. The stated objectives were to gain a common and deeper understanding of Homeland Defence; understand whole-society cross-domain working; focus on behavioural and effective planning and activity; test the complexity of decision-making in a TTX; and identify issues whose resolution would lead to better preparedness. The programme progressed from the operating environment and multi-agency definitions of Homeland Defence through public education, the information space, partnership working, layered resilience and risk mitigation before moving into the exercise.

This design reflected a wider proposition in our team's policy working informed by another recent paper published by CPUDS – *Designing the 21<sup>st</sup> Century Wartime State: Challenges for the UK's new War Book and Defence Readiness Bill*. This is that legal authority, structures and plans do not automatically generate preparedness. Preparedness is strengthened by shared



understanding of the resilience architecture, common vocabulary, knowledge of partner roles and responsibilities, awareness of cross-sector dependencies, and repeated opportunities to explore complex scenarios collectively before crisis. Information-sharing powers are necessary, but confidence, familiarity and experience are required to use them effectively. Institutional capability develops through repeated training, exercising, reflection and adaptation rather than planning alone.

On this basis, good Homeland Defence education is multi-agency, applied and connected to exercising. It should clarify doctrine and roles, expose cross-sector dependencies, build habits of co-operation, and prepare people to work across differing organisational cultures, professional practices, information requirements and security arrangements. It should also connect professional preparedness to public understanding and participation. This reinforced the need for sustained public engagement at individual, neighbourhood and community levels including schools, alongside professional programmes for officials and stakeholders.

## Why a region-specific approach is necessary

It is assessed the region should be at the centre of the delivery of Homeland Defence. There are already existing institutions on which to draw. For example, the basic unit of UK resilience on the ground is the Local Resilience Forum (LRF), comprised of multi-agency partnerships made up of representatives from local public services, including the emergency services, local authorities, the NHS, and the Environment Agency. These agencies are known as Category 1 Responders, as defined by the Civil Contingencies Act. Above the LRF is the Joint Military Command. HMG's *Rewiring the State* makes clear that the Mayoral Strategic Authority is the "right sized" unit of governance for the UK devolution agenda.

Preparedness must, therefore, connect clear national direction with regionally organised delivery and local action. The region is where national objectives can be translated into co-ordinated activity among local government, emergency services, infrastructure operators, industry, universities and civil society while reflecting the distinct assets, dependencies, vulnerabilities and governance arrangements of different places. The alignment of military, governmental, economic and societal activity must be tangible in its execution, not remain in the abstract.

This matters because functional systems do not map neatly onto administrative boundaries and UK resilience boundaries are rarely coterminous. Against a backdrop of infrastructure and service dependencies whose disruption can cascade across services, communities and the economy, regional mapping of these factors is required to inform multi-agency education and exercising. In the South-West, defence installations, ports, energy and digital infrastructure, supply chains, universities, dispersed communities and differing sub-regional economies form a distinctive resilience landscape. A generic national assumption cannot by itself reveal how those systems interact.

A region-specific approach is not an alternative to national consistency or local knowledge. National government has a crucial role in strategic direction, doctrine and taxonomy, intelligence, large-scale exercising and hardened communications. Regional arrangements should identify cross-boundary interdependencies, convene organisations spanning several LRF areas, co-ordinate shared education and exercising and disseminate lessons. Local actors remain responsible for detailed risk knowledge, public information and practical delivery. The objective is a connected system rather than parallel or competing structures.



The regional proposition also addresses a recurrent finding from the July pilot: preparedness depends on working relationships that do not appear automatically when a crisis begins. Barriers came to light from organisational cultures, professional practices, information requirements and security arrangements. Shared activity builds familiarity, clarifies responsibilities, surfaces assumptions and dependencies, and develops confidence under disruption. For this reason, our approach treats preparedness as an operational capability that requires continuing investment, evaluation and improvement rather than a compliance process completed on paper.

Fundamental here is development of a feedback loop linking understanding systems, risks and interdependencies; education; exercising plans, relationships and assumptions; structured lesson identification; and implementation and improvement. The value lies in treating these as mutually reinforcing activities rather than separate tasks.

Universities have a supporting role in this model as civic anchors and trusted brokers able to convene actors across institutional and security boundaries and wrap research and evaluation around exercises. We have a wider ambition for a common but regionally adaptable framework that could be developed collaboratively with Regional Defence and Security Clusters (RDSCs), LRFs and other partners without displacing statutory responsibility.

This could play out over two possible sequences:

- Exercise-first: use the Home Defence course and TTX to convene stakeholders, identify vulnerabilities and generate the evidence base for a systematic regional assessment.
- Assessment-first: map strengths, vulnerabilities, dependencies and opportunities and then design a TTX around those findings. These strands are intersecting rather than competing, with the appropriate sequence depending on regional circumstances.

• EXERCISE OVAL

SCENARIO BACKGROUND

## SW England: July 2027

- South-West Peninsula Local Strategic Authority formed April 2027 (SWPLSA)
- Community Hubs cover 50% population
- NCSC: Low-grade cyber probes of:
  - Langage email system
  - SW Water control system
  - Exeter Council HR database
- NPSA: Tighter physical and CCTV security at critical sites needed
- 2x subsea data cables damaged by anchor drags
- Drone nuisance near GCHQ Bude



*Image: Slide introducing scenario background, July tabletop exercise*

## What the TTX told us

### Objective and design

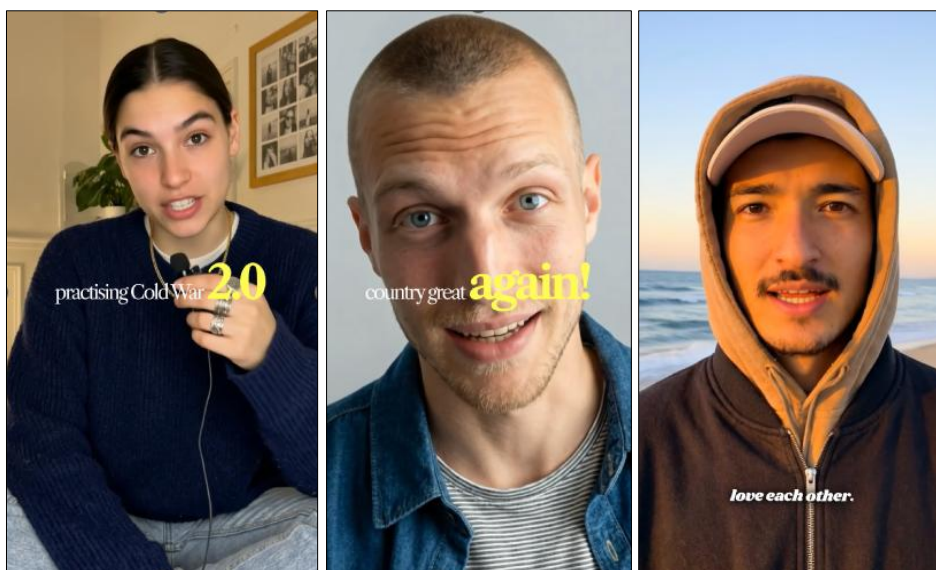
The pilot exercise was designed to test co-ordination, operational decision-making under stress and information flow between cleared and non-cleared professionals in four domains: regional military, emergency services, local government and Critical National Infrastructure (CNI). A strategic communications function was embedded in each cell. Cabinet Office Briefing Rooms (COBR) and the UK Intelligence Community were played by White, working from a script and setting broad counter-intelligence goals per turn.

The setting was July-December 2027, a near-future environment where the Defence Readiness Bill had been published but was stalled in Parliament, and a War Book had been agreed but remained TOP SECRET. The Russian aim was to destroy the UK population's willingness to resist: a clear cognitive goal, with all other actions subordinate to it. This goal was set in a human-authored operational order from STAVKA to the Russian hybrid agencies. The Director created a fictional South-West England Strategic Authority to overcome friction within current local-government, fire and police reorganisation programmes, and a fictional War Book based on the aforementioned paper *Designing the 21st Century Wartime State*, briefed towards the end of Turn 2.

### Scenario progression and key events

Over three turns Russia moved from “normal” hybrid and cognitive aggression in July and August 2027 to intensified hybrid activity from September to November, followed by a fourteen-day kinetic phase in which the UK was attacked by missiles from a Yasen-class submarine alongside sabotage and cyber-attacks. Red was played by a bespoke Claude Cowork agent, Feliks.ai, modelling the behaviour of ten Russian hybrid and intelligence agencies. Red engaged Blue dynamically, treating each Blue action as a potential new attack surface.

Turn 1: Russia established three proxy media products aimed at the green left, far right and alternative lifestyle demographics. SACEUR, the Commander of NATO Forces, ordered the South-West to host a Patriot battery.



Images (AI-Generated): Social media content propagating Russian narratives

Turn 2: Here, Russia subjected HMG to a welter of hybrid attacks causing a Cabinet meltdown, while increasing Doppelganger deepfakes to thirty times normal volume, focused on opposition to NATO enhanced Forward Presence and allegations of imminent conscription. Russian saboteurs then caused a major fire at a Plymouth oil terminal, coinciding with market manipulation that spiked global oil and gas prices. At this point COBR agreed to invoke the Civil Contingencies Act 2004 in the region.

Turn 3: Russia attacked Estonia and seized the strategic area, Svalbard, while a devastating cyber-attack hit the South-West's water supply and cascaded into the region's main gas-fired power station. HMG invoked substantial war powers using the War Book. A South-West Sub-Regional Seat of Government drew senior leaders into a command bunker, leaving the cells semi-autonomous to follow standard operating procedures and orders. At ENDEX the headquarters was functioning well, but subordinate units felt somewhat adrift and the strategic communications battle was going Russia's way.

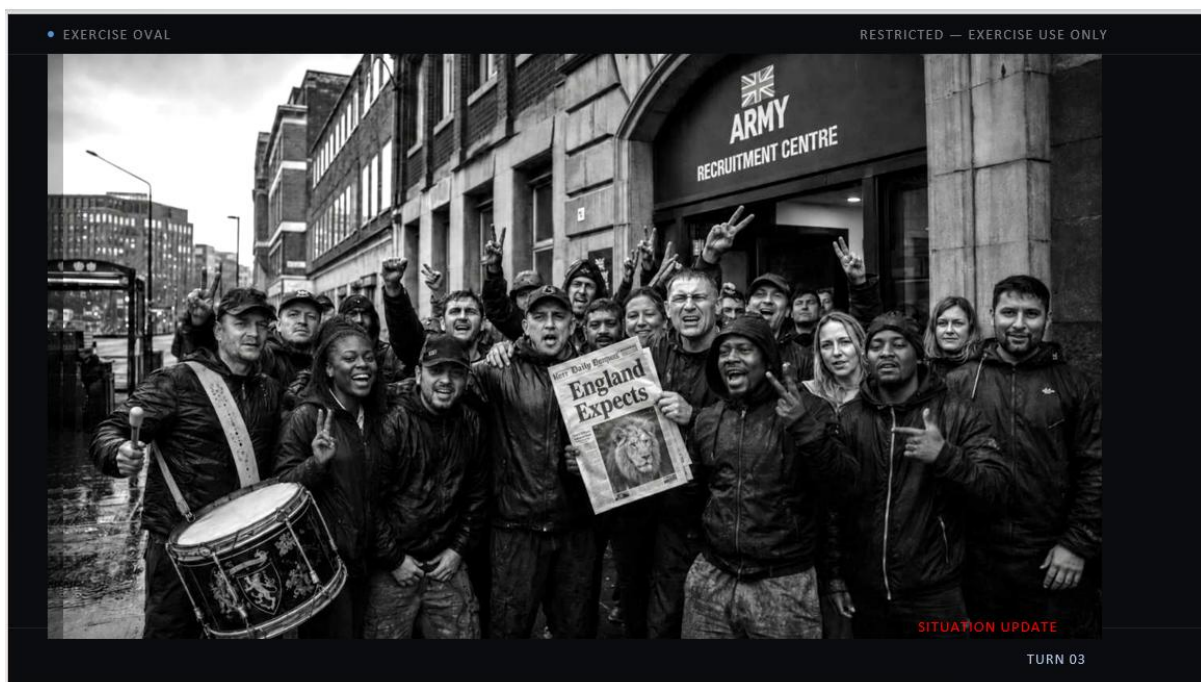


*Image (AI-Generated): Local residents mobilise as recruitment centres struggle to triage demand*

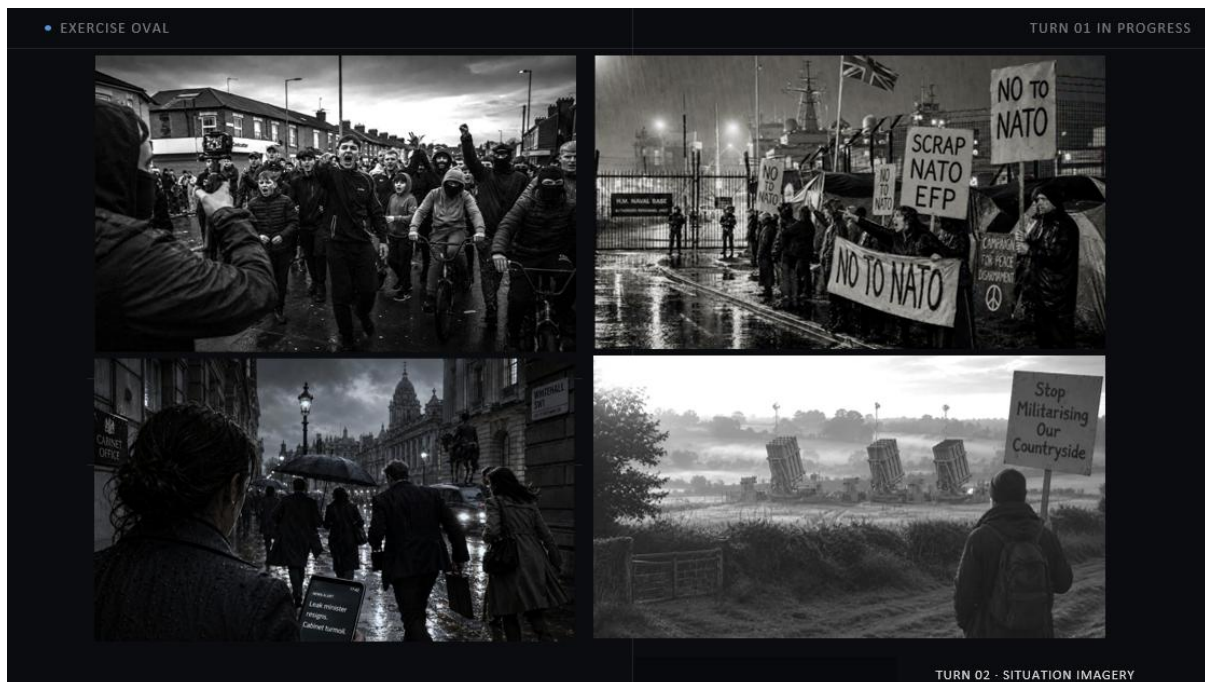
## Performance and principal findings

Each cell performed well under stress but stayed “in its lane”. Local government reported a rising loss of agency as COBR, the military and police made extensive demands upon it. Emergency services coped well. CNI, despite attempting to harden water, data and energy, was overwhelmed by the severity of the Russian effort. We judge that, had the game continued, the South-West would have faced catastrophic loss of water and energy supplies.

Throughout the exercise there was no clear regional responsibility for a unified strategic communications effort and no common lexicon for how to defend actively against cognitive attacks and fight back. The combination of missile, cyber and sabotage attacks with long-prepared disinformation networks was devastating in the game. The effect would have been greater had real-world political dissent been modelled.

The appearance of the War Book in Turn 3 catalysed creative and effective collaboration by the newly formed Sub-Regional Headquarters, but left many participants nonplussed at the scale of the duties imposed on them. The headquarters ended Turn 3 with a communications

plan but not a cognitive warfare strategy. Above all, despite Red's hybrid operational order focusing almost totally on cognitive goals, with sabotage and cyber-attacks as ways and means, Blue never developed a doctrine, objective or institutional means of fighting the information and cognitive battle. In Red's judgement, Red therefore won.



*Images (AI-Generated): Situation imagery from the tabletop exercise*

## Lessons and feedback from the TTX

Participant evaluation of the pilot – which was itself coproduced through the input of partners and participants in an earlier Sandpit – supports the aspirations with which our team set out on this initiative. Its content was pitched at the right level, while its breadth, logical flow, relevance, attention to human factors and use of the TTX proved valuable. Future iterations should provide a clearer definition of Homeland Defence and devote more attention to crisis planning and architecture, security, international comparisons, analogue failure and CNI.

A three-day course would allow greater breadth, interaction, discussion and questions; a systems-analysis approach could treat the challenge as a complex adaptive system of systems; and the programme could give more attention to the state-of-war context, defence readiness, communications, targeted resilience, lessons learned and connection to HMG objectives. The mix and sequencing should, therefore, be retained while the programme expands to three days, creating more space for the training and the exercise components to speak to each other in a way that is complementary.

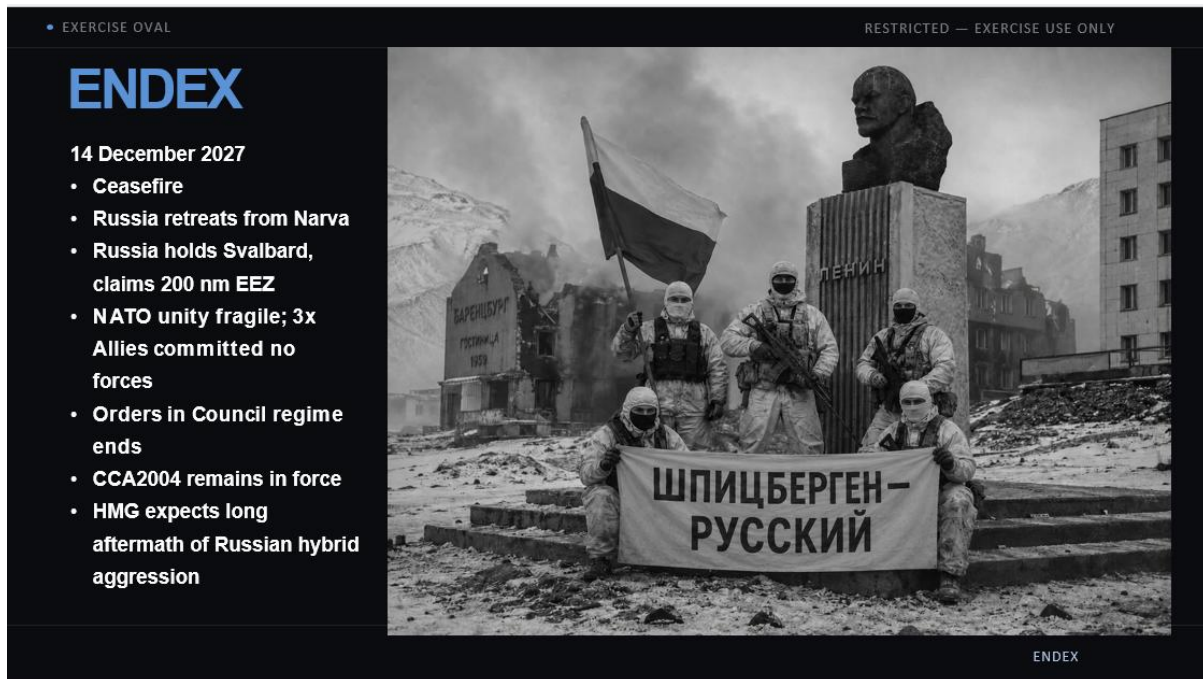


*Image: Slide outlining wider national/international outcomes of the exercise at its end*

From the findings above we can draw a set of lessons that should be retained in future development.

First, bottom-up modelling with real-world actors produced a dynamic that was primarily regional rather than sectoral. We would therefore argue that future national TTXs should not abstract regional dynamics and that real-world regional teams should be used to wargame regional effects.

Second, the central friction was communication between security-cleared leaders and non-cleared people in local government, emergency services and CNI. Participants improvised a way through, but a coherent answer to this issue must become a focus of training, guidelines and rehearsal.

Third, imposing a TOP SECRET War Book on people expected to enact it with little training or legal preparation was both catalyst and disruption. Therefore, we would recommend appropriately classified public-facing guidance and training at the level where new responsibilities would be carried.

Fourth, Category 2 responders, particularly CNI providers, should be brought systematically into the exercise loop.

Fifth, the exercise revealed the need for a central counter-hybrid capability, teachable and exercisable counter-hybrid doctrine, clearer institutional ownership and a named regional senior responsible owner. The announcement of the National Centre for Information Defence is to be welcomed in this regard, but its relationship to the Intelligence Community and regional delivery requires clarification.

Sixth, the TTX model is repeatable and scalable. We are working on developing the model using an open-source library of adversary hybrid doctrine and a synthetic regional population to log public mood and calculate effects. This is already available in Beta as a web interface, enabling future exercises to be run remotely and with significantly larger scale (e.g. the seven South West LRFs exercising together). Longer-term, this should incorporate richer digital data

collection, participation by politicians and less predictable adversary escalation. The final observation is a warning against scenario groupthink: repeated exercises may embed assumptions about a graduated path to kinetic conflict, so planners should introduce more randomness and dynamism into adversary action.

## Recommendations

Taken together, the analysis above points toward the following programme of action:

- Preserve the education-plus-exercise model but extend the course to three days, creating more space for discussion, systems analysis, communications, CNI and structured lesson identification.
- Establish a nationally co-ordinated but regionally delivered preparedness framework. National government should provide strategic direction, common doctrine and terminology, intelligence co-ordination, large-scale exercising and resources; regional arrangements should map dependencies, convene cross-boundary actors, coordinate education and exercising and disseminate lessons; local actors should translate preparedness into practice.
- Make communication across security boundaries a central training and exercising objective, with guidance and repeated rehearsal for the cleared and non-cleared actors who must cooperate in practice.
- Integrate CNI and other Category 2 responders more systematically into preparedness, planning, multi-agency exercising, information-sharing, evaluation and implementation of lessons.
- Treat strategic communications and cognitive defence as core resilience capabilities, with clearer national and regional ownership, doctrine that can be taught and exercised, and identified regional responsibility.
- Test regional command arrangements, the practical use of statutory and wartime powers, and participation by political leaders. Do not assume that publication of powers or a War Book creates the institutional familiarity needed to employ them.
- Build structured evaluation into the model. Exercises should capture evidence, distinguish observations from validated findings and lessons, assign recommendations to owners and assess whether preparedness capability actually improves.
- Scale flexibly through regional partnerships. A region may begin with assessment and design an exercise around identified vulnerabilities or begin with education and exercising to reveal what needs to be assessed. Universities, RDSCs, LRFs and other convenors can support delivery without displacing statutory responsibilities.
- Connect professional preparedness to public understanding and participation. National, regional and local systems must be matched by preparedness among the populations they serve, including the ability to understand warnings, identify reliable information, manage service interruption and support neighbourhood resilience.
- Identify and secure sustained central resources. Preparedness of duties and regional activity will remain theoretical if finance is not committed to implementation.
- Ultimately, our core proposition is that resilience is not generated by powers held in reserve. Preparedness is a continuing capability built before crisis through shared understanding, trusted relationships, practised cooperation, credible communication, realistic exercising, structured evaluation and mechanisms for learning.





University  
of Exeter

Centre for the  
Public Understanding  
of Defence and Security



## Further Reading

Paul Mason (2026) *Designing the 21st Century Wartime State: Challenges for the UK's new War Book and Defence Readiness Bill*. Centre for the Public Understanding of Defence & Security, University of Exeter.

[https://www.exeter.ac.uk/v8media/research/facilities/policy/P.\\_Mason\\_-\\_Designing\\_the\\_21st\\_Century\\_Wartime\\_State.pdf](https://www.exeter.ac.uk/v8media/research/facilities/policy/P._Mason_-_Designing_the_21st_Century_Wartime_State.pdf)

Frances Tammer, Frederick Harry Pitts, Gareth Stansfield (2026) *Making Sense of Home Defence: From Planning to Practice*. Centre for the Public Understanding of Defence & Security, University of Exeter.

[https://www.exeter.ac.uk/v8media/research/centres/CPUDS\\_Making\\_Sense\\_of\\_Home\\_Defence.pdf](https://www.exeter.ac.uk/v8media/research/centres/CPUDS_Making_Sense_of_Home_Defence.pdf)

## Authors

### Paul Mason

Honorary Senior Research Fellow, Centre for the Public Understanding of Defence & Security, University of Exeter

[p.mason3@exeter.ac.uk](mailto:p.mason3@exeter.ac.uk)

### Professor Frances Tammer

Professor of Practice, Strategy & Security Institute, University of Exeter

[f.tammer@exeter.ac.uk](mailto:f.tammer@exeter.ac.uk)

### Professor Frederick Harry Pitts

Director, Centre for the Public Understanding of Defence & Security, University of Exeter

[f.h.pitts@exeter.ac.uk](mailto:f.h.pitts@exeter.ac.uk)

## About CPUDS

The **Centre for the Public Understanding of Defence & Security** is a partner in the national conversation on defence, security and resilience. Bringing together government, industry, local authorities, emergency services, civil society and academia, the Centre provides a forum for informed debate, education and engagement on the issues that will shape the UK's security in the twenty-first century. Working with experts from the Strategy and Security Institute and beyond, CPUDS contributes to a whole-of-society approach to resilience, preparedness and homeland defence. Through research, publications, events, education and training, the Centre connects scholarship, policy and practice, helping to build the knowledge, partnerships and capabilities needed to meet an increasingly complex and uncertain security environment.

Find out more at [www.exeter.ac.uk/research/centres/strategy/research/public-understanding-defence-security](http://www.exeter.ac.uk/research/centres/strategy/research/public-understanding-defence-security)

**CPUDS**

Centre for the Public Understanding of Defence and Security