Wilton Park

Report: The Future Defence, Deterrence and Resilience Conference

Monday 07 – Wednesday 09 October 2024

Professor Julian Lindley-French &
General the Lord Richards of
Herstmonceux

In partnership with
The Alphen Group and
with major funding support
from NATO and
sponsorship from BAE
systems and Microsoft

In association with

BAE SYSTEMS

Report:
The Future Defence, Deterrence and Resilience Conference

Monday 07 – Wednesday 09 October 2024

In association with
The Alphen Group and with major funding support from NATO and sponsorship from BAE systems and Microsoft.

Summary by Dr Julian Lindley-French and General the Lord Richards of Herstmonceux

In memory and in honour of Robert G. Bell

Wilton Park reports are brief summaries of the main points and conclusions of a conference. The reports reflect rapporteurs' personal interpretations of the proceedings. As such they do not constitute any institutional policy of Wilton Park nor do they necessarily represent the views of the rapporteur. Wilton Park reports and any recommendations contained therein are for participants and are not a statement of policy for Wilton Park, the Foreign, Commonwealth and Development Office (FCDO) or His Majesty's Government.

An unabridged report by the authors, with details of thematic working group discussions, can be found here.

For the purposes of this report resilience is defined as the ability of a state, institution and democratic society to recover from shock and maintain capability and functionality under extreme duress.

"Too many leaders do not recognise we are in a state of conflict, maybe in a state of war. The Free World is moving into an era in which autocratic predator powers seek to prey on free open peoples. For too long Western leaders have enabled the transformation of their open societies into prey. It is time the predators re-learned simple lessons: freedom is not weakness, and prey have hard shells and sharp claws".

- Julian Lindley-French

Key takeaway

The core contention of this conference was validated: that the capacity to project legitimate coercive power is central to credible defence and deterrence but that such power can only be credible if Allied and Partner societies are demonstrably secure to friends and foes alike. The key to effective resilience and thus credible defence and deterrence is shared, well-designed, and responsive architecture built on a range of critical partnerships. These partnerships must be deeper and more planned than hitherto between NATO and the EU, between member states and partners, but above all, between governments and civil society. There is much to relearn from civil defence during the Cold War.

Introduction

The Future Defence, Deterrence and Resilience Conference was the third in a trilogy of policy-focused future war/defence conferences. The 2022 Future War and Deterrence Conference considered defence strategy going forward in an uncertain and strategically competitive world for the Alliance and Partners. The 2023 Future War, Strategy and Technology Conference examined the impact of Emerging and Disruptive Technologies (EDT) on Allied and Partner defence strategy. The 2024 Future Defence, Deterrence and Resilience Conference focused on the balance to be struck between people protection and power projection, civil defence and military defence in the face of the hybrid war in which autocratic powers are already engaged against open, democratic societies. As such, the Conference explored the civil military partnerships that will be vital to affecting such resilience.

All three conferences revealed the urgent need for choices to be made by the governments of free nations if a balance is to be struck between capability, capacity, resilience and affordability to meet the challenge going forward of preserving a just peace and the Western way of life. Credible deterrence rests as much on convincing an adversary that society and governance is sufficiently secure to resist all forms of aggression, of which the fielding of adequate and legitimate military power is a vital, albeit only one, part. Hybrid or 'grey zone' war comes in many forms, but it essentially seeks to disrupt, destabilise and disinform, possibly as a prelude to decapitation and destruction of a state. The threat must thus be seen as precisely that.

Systemic hybrid war by a peer competitor would also involve a sustained and systematic campaign to denude and degrade a state's communications and energy

nodes and infrastructure, as well as systems vital to the critical functioning of the state, continuity of government and governance, and the resilience and robustness needed to minimise the impact of attacks. Effective resilience demands effective consequence management, strong cyber defences (and offensive capability), civilian structures vital to the maintenance of the military effort and military mobility, and prevention of applied disinformation and propaganda on social media.

Core messages

Too many democracies have been asleep at the wheel in the face of oncoming threats to freedom and the systems that underpin it. Governments have chosen to see such threats as "wicked political problems" too challenging and complicated to deal with, even if the consequences of their inaction are dangerous, even potentially catastrophic. Adversaries such as China and Russia have used a series of crises and events – 9/11, the 2008-2010 banking and financial crisis, the refugee and migrant crisis, Brexit, and COVID 19 - to exacerbate divisions within open societies and thus weaken governance. They have also sought to dominate the digital domain and turn it from an enabler of communications into a weapon of misinformation.

There were several key themes that emerged during the course of the conference, focused on the need:

- to share resilience best practice between Allies and partners;
- for greater transparency between government, industry and citizens about the scope and scale of threats across the hybrid, cyber and kinetic war spectrum;
- to forge a much deeper partnership between the state and citizens;
- to build redundancy into critical national infrastructures allied to increased resilience;
- to involve the defence, technological and industrial bases and a wider supply chain in thinking, planning and action about resilience at an early stage;
- for a genuine EU-NATO strategic partnership across the defence, deterrence and resilience posture; and
- for whole-of-government approaches that underpin whole-of-society responses to ensure effective consequence management.

Above all, there was broad agreement that a very real threat is posed to democratic societies and their capacity to deter adversaries and defend themselves if current attempts by autocratic states to undermine resilience succeed. Above all, there is a

pressing need for all Allies and partners to know the state of resilience in their respective countries by undertaking national audits based on a shared NATO and EU methodology.

Deterrence is only credible in the minds of an adversary if they are convinced that under no circumstances will they achieve expansionist and adventurist goals through coercion, be it real or virtual. Traditionally, deterrence has been built upon the credibly demonstrable capacity to project military power. In the 21st century power projection demands clear evidence of people protection, meaning that open societies have the political and social resilience to withstand All-Threats Warfare. Over the past thirty years Western societies have become ever more complex and diverse as well as ever more open.

Given that such openness is the very quality the West sees as essential to its way of life, defending it is unlikely to succeed unless there is also a new form of adaptive deterrence built upon resilience. That is why people protection is as important as power projection. Resilience means not simply the capacity to resist imposed shocks but to recover rapidly from them governmentally, societally and economically, allied to an indisputable capability to impose unacceptable shocks on adversaries and their societies and thus directly threaten the ability of autocrats to remain in power. Therefore, the West not only needs to get sharper, but it also needs to get harder.

Summary of findings

The Conference was centred on six high-level working groups:

- Technology, Deterrence and Resilience: The Foundation of Future Defence;
- Building a Strategic Public-Private Partnership;
- Consequence Management, Critical Protection, and Civil Defence;
- Ensuring the Integrity of Democracy;
- Economic and Energy Security: The Critical Vulnerabilities; and
- Reinforcing Resilience: People Protection, Power Projection, Pan-Institutional and Whole of Government Solutions.

Enhanced Resilience

Resilience can best be defined as the individual and collective will and capability to recover from all conceivable and unconceivable shocks. It is vital that resilience forms a

foundation for both deterrence by denial and by punishment. A new Alliance framework is needed that links not just deterrence, defence and resilience, but also enables such synergies to create enhanced resilience because the nature of contestation is leading to major disruption.

To serve as a critical strategic enabler for vital deterrence by denial enhanced resilience must be defined broadly if an all-important whole-of-society approach to defence and deterrence is to be forged. Enhanced resilience must be mainstreamed into all aspects of deterrence, including a compelling definition of economic deterrence.

Allies and partners must far more actively prepare collectively and individually their respective societies for persistent hybrid threats across the contested domains of cyber, infrastructure, economic, life fundamentals (food, water, energy etc), and the governance and democracy battlespace.

Layered Resilience

Effective deterrence requires a mix of effective protection and rapid attribution of responsibility built on several assumptions: the West might not yet be facing a monolithic threat but it is sufficiently dangerous to require adaptive defence and deterrence; the human element will be as important as technological capability; there is a vital need for more effective and responsive indicators and metrics; and a vital need to win the battle of narratives in hybrid warfare.

Tools that cut across threats are needed to identify, quantify, and respond. Such cross-cutting tools include the need for holistic strategies and capabilities to ensure resilient energy supply; the ability to deal effectively with the uncontrolled movement of people; mitigating the impact of climate change on security; the capacity to deal with mass casualty events and highly disruptive health crises; ensuring resilient civil communications to underpin effective civil defence; the protection of critical underwater infrastructure and consequence management; and ensuring resilient civilian transportation systems and the capacity to identify and respond to anomalous shipping movements.

EU-NATO and the Nations: Latvia's experience

The need for the EU and NATO to forge a real strategic partnership across defence, deterrence and resilience is vital. Such a partnership has been made easier by the accession of both Finland and Sweden to NATO. Latvia offers a case study for the

future relationship between the EU and NATO for the provision of enhanced deterrence, defence and resilience. For example, the EU has been instrumental in helping Latvia integrate into law measures to accelerate the dangerous movement of goods across borders as part of efforts to improve military mobility, together with the establishment of joint EU and NATO strategic communications. The EU has also invested in Latvia and the other Baltic States in their efforts to create a new north-south rail corridor to strengthen military mobility and logistics.

National efforts are being aligned with EU and NATO planning. Latvia's 2025 government budget will make security the priority in addition to spending 3% GDP on defence, thus harmonising civilian efforts to enhance resilience with military measures. Such measures will include a new Joint Baltic Defence Line and efforts to strengthen air defences against drones and other threats. Latvia will also adopt measures to prevent the mobility of enemy forces and reinforce resilience against hybrid warfare, including coerced illegal migration by Belarus and Russia.

Technology, Deterrence and Resilience: The Foundation of Future Defence

Unobstructed access to critical information.

The primary technology-enhanced threat identified that needs to be mitigated is the ability of adversaries to **flood the zone with disinformation**. There are several opportunities for improving resilience of critical information production and dissemination. These include conducting a risk assessment of putting government data on a public cloud or government server, the construction of an artificial intelligence content verification and public awareness system, and sharing resilience lessons between nations.

A second threat is an adversary's ability to interfere with **crisis communication systems and hotlines**. Stronger attribution and retribution capabilities are needed, allied to a bespoke system for deterring cyber-attacks. "Responses need to be tethered to transgressions in order to establish that attacks have unpalatable consequences".

A third threat concerns that posed to critical national infrastructure (CNI), which is increased by the interdependence of civil networks, many of which do not maintain adequate cyber hygiene. In response, there is a pressing need to use emerging technologies such as AI to build and maintain a **live understanding** of complex systems, which in turn would enable a more holistic approach to system monitoring.

There is also a critical need to standardise communication amongst relevant stakeholders to promote a shared awareness of emerging threats. Given the vital role the private sector must play, opportunities to pre-negotiate contracts for crisis response should be explored. This would allow the private sector to budget and plan for such emergencies.

Above all, government responses to intrusions into critical national infrastructure need to be enhanced by technology, with intrusions of any kind – not just cyber –more proactively dissuaded. **Best practice** might be better promoted if NATO articulated policies that spelled out precisely what the Alliance would do in response to an attack on CNI.

A fourth threat concerned territorial integrity. The 2014 Russian annexation of Crimea demonstrated the vital need for a host of technology-enhanced responses. Accelerated attribution and **identification of hybrid forces and stealth territorial acquisition** was the primary recommendation to improve deterrence postures, including using new technologies to record actions and build accountability.

Further use of technology to enhance resilience in the face of territorial aggression included dispersed **Citizen Intelligence Surveillance and Reconnaissance (ISR)** capabilities through which citizen resistance groups could be organised. Some form of national service could help improve societal cohesion in States that are open to it.

Building a Strategic Public Private Partnership (PPP)

It is time to develop and deploy a **comprehensive, national level, whole of society resilience planning framework, planning activity and exercising schedule** that involves government, industry, charities and relevant NGOs from conception and at every stage through to implementation. This national level activity needs to take into account partner nation plans **and** NATO-level resilience planning policy/doctrine as well as the associated obligations stemming from both. These conclusions lead to a host of recommendations regarding strategic PPPs as follows.

- **Allies and partners learn from each other** by strengthening international engagement with front line states (using Ukraine, Latvia/Finland/Sweden/Estonia as exemplars) and those such as France that have recently conducted a 4* sponsored **Resilience Audit**.
- Leverage the alliance as a **School of Resilience**.

- **Involve industry and other stakeholders from the start of planning** and cast the net wide by stressing the corporate social responsibility of involvement (and the **financial benefits** of being ready for a resilience shock).
- Reach out to critical industries, government departments, local authorities, charities and NGOs.
- Ensure that larger businesses look hard at their **supply chains** and invite those deemed critical to the table. Recommend appointment of a designated **Chief Resilience Officer** at senior level of companies.
- Run **training/planning exercises and conferences** with government stakeholders to build out a network of resilience leads across government and industry and share findings with Allies and partners through the EU and NATO.

Set up the right behaviours to build a partnership of equals. There are already good examples of such partnerships of equals to learn from. These include the UK Defence Nuclear Enterprise and Aircraft Carrier Alliance as well as unmanned aerial systems (UAS) procurement for Ukraine across NATO nations. Such partnerships must be built on principles.

- *Lead with empathy and listening* along with a focus on the culture and values of the partnership.
- *Recognise incentives and disincentives; c*ommercial profit and commercial interests can align with resilience needs of the government.
- *Educate each other* on individual motivations, fears and desired outcomes to build trust.
- *Recognise the limitations in labelling contractors and/or actors* – not every actor required to engage on resilience is a current contractor *and* contractors need to recognise they are wider actors (and carry increased responsibility in the resilience space).

Build on **Specialist Reserves and** scale them up to a greater level across infrastructure, cyber and utilities resilience and redundancy. There are pockets of specialist reserve services already, but they need to be at national level and forged in planning and policy with both NATO and the EU to ensure consistency and considered escalation in response to established indicators as crises evolve. Direct industry to deliver against an escalating **Service Level Agreement (SLA)** with **Key Performance Indicators (KPIs)** as the civil defence situation deteriorates**.** Such a **planning and metrics approach** would allow businesses to plan and provide assurances that governments will pay them for their time when they activate this

service and pay more as each bespoke SLA becomes more onerous on an industrial partner. Measure the readiness of businesses by creating an **annual quality assurance audit** on companies.

Devise new legislation and policies on resilience, possibly built on the experience of Dutch readiness/resilience laws. **Leadership** will be vital**.** Someone needs to own resilience at a national level, departmental level and industrial level. To that end**, assign leaders for each nation** and for each business and government department. **To promote affordability,** options must be crafted to ensure there is money and it is spent on the right things to reinforce resilience. Create **escrow accounts** with more than one stakeholder access and multi-stakeholder approval.

Establish a binding Joint National Resilience Contingency Fund between governments and industry. A **National Resilience Tax Scheme** could be examined, although it would have to be seen as a structural tax, much like VAT and not as a windfall to ensure it did not have a counter-productive impact on investment. Create **a comprehensive communications plan** that targets multiple audiences with tailored messages to support a genuinely public private partnership with all stakeholders.

Make the economic case for resilience. There is a genuine economic case for investment in resilience as an essential element of sound national infrastructure that attracts (and retains) long-term structural investment and defrays the down-side risk associated with rapid flights of capital that occur when crises hit unprepared states. **Soliciting investment from industry** beyond their own fiduciary duties will require open sharing of what risks are being secured against, where government will own contingency and how that contingency will be made available to the private sector, both in planning for resilience and in activating capability and capacity as a crisis unfolds.

Consequence Management, Critical Protection and Civil Defence

It is vital that a rapid and greater awareness is generated of the threats societies face and the need for a renewed partnership between government and citizens. One danger is a level of naivety and short-term thinking at the local level. Realisation of the **threat landscape** is growing in Europe, but at too slow a pace. Politicians have sometimes reacted cautiously to warnings by intelligence agencies of malign efforts to undermine societal resilience, worried about causing panic in society. This attitude not only under-estimates the resilience of populations in democracies but prevents the all-important establishment of a **Resilience Partnership** between the state and

the people. Therefore, it is time to treat people as citizens in a common struggle for freedom and, to do that, the state needs to be honest about the level and nature of contemporary threats.

Resilience is also generally weaker the further one is from the Russian border. There is a critical lack of understanding and appreciation of the proximity of threats. This **lack of cognisance** across societies needs to be **addressed holistically** by NATO and the EU and then targeted specifically to meet differing national needs. Improved strategic communications between the state and population, allied to improved education over the **responsibility of the citizen in civil defence** is urgently needed. **Resilience education** should start with targeting younger members of society, at an early age, to understand the effects of disinformation from threats (internal, such as extreme nationalism supported by outside states, as well as external, such as direct state activities).

The **Chief Enabler for Resilience** at every level will be the capacity to exploit new technology to bring together more effective civil and military cooperation. More effective whole-of-society responses need functioning **digital interoperability**, detailed planning, and contingency testing through exercises. AI could help fuse information requirements and prioritise data for decision-making and prioritisation. **Single Synthetic Environment (SSE) technology should be adopted rapidly** to facilitate multi-domain operations (MDO) cooperation, test ideas, exercise and further develop the 'War Books' recommendations. Consequence mapping is now so complex that it exceeds human capacity – SSEs offer a route through this – and provides an invaluable decision support tool for the modern operating environment.

To increase resilience at home and abroad a **fundamental rethink of the provision of reserves is required.** Across the Alliance many more reserves, not only for the military but also for emergency services and other enablers, are needed urgently. The various systems for mobilising reserves will differ across the Allies, and whilst conscription works for some, it is not suitable for all. That said, the scope for companies to second paid critical expertise to the state should be explored.

Ensuring the Integrity of Democracy

The most **fundamental source of national power** is the belief of the population that their government is serving their interests. Support of the population for their political system and active engagement in it are key. In an age of individualism, a bottom-up approach is required to ensure that the system is serving the people; they are

therefore willing and able to defend it against external and internal threats, and supportive of making sacrifices toward that end.

What must be defended is not just a system of democratic voting **but the principles of individual liberty and the rule of law – in other words, "liberal democracy".** The threats to liberal democracy include both externally generated challenges and those that arise within democratic systems. Today's external threats emanate particularly (and mainly) from autocratic regimes in Russia, China, Iran and North Korea, but not exclusively so.

The **vulnerabilities are manifold** with opportunities for attacks on liberal democracy magnified when publics are dissatisfied and mistrustful of their government. Sources of dissatisfaction can include economic, social, being left behind by technology and technology that contributes to fragmentation of the information base.

There are three forms of resilience; active defence, the restoration of trust and diminution of fragmentation, and the education of populations. **Active defence** will be built on a stronger partnership between state and citizens through greater transparency regarding the sources of disinformation, particularly content generators. It is very important for the public to be aware of who and for what purpose information is being created and circulated. This may require providing far more open access to classified information when release would enhance defence against attacks while not revealing sources and methods.

Restoring trust and diminishing fragmentation can only be achieved if populations know that they are being heard and listened to and that the system of governance is agile enough to respond to inequities and any shortcomings of the system that may punish one or other community. Finally, **educating populations** requires the use of all available means and events to help promote critical thinking and civics, starting at the earliest stages of the education process and continuing through adulthood. This may require creating new institutional frameworks or the enhancing of existing ones across the Euro-Atlantic and global democratic communities aimed at promoting a better understanding of the requirements for and benefits of resilient liberal democracy.

Ensuring Economic and Energy Security

An **Economic Security Alliance** of likeminded Western states would enable economic challenges, including those impacting on energy security, to be discussed

and mitigating measures to be developed. There are a range of steps that need to be taken and which such an alliance might help foster.

1. **Invest in multi-domain monitoring** capabilities, either by reallocating existing means or developing new ones. This should enhance situational awareness and may contribute to preventing threats to the integrity of energy infrastructure.
2. **Threat signalling** by governments may allow Western nations to take countermeasures and convince the potential attacker to change course. The willingness to attribute grey zone activities to a perpetrator might also offer options for de-escalation.
3. Allies and partners must consider formalising **proportionate strategic retribution**, ranging from targeted economic measures (e.g., sanctions, export controls, trade measures, industrial policy), to well-considered covert operations.
4. NATO should explore the creation of an **investment vehicle** to provide additional maintenance capabilities for critical energy infrastructure. This mechanism, which could be developed from within NATO's Innovation Fund, should also include NATO's four Asia-Pacific Partners.

There needs to be a much fuller appreciation by policymakers of the vital leveraging and influence **role that economics, and in particular trade, plays in security policy**. Specifically, much more attention needs to be paid to the **long-term goals pursued by strategic competitors**, notably China, to force Western countries into **dependency**, including using renewable energy. To prevent such economic/energy warfare, Western countries should make a greater effort to adjust and strengthen their respective national legislation, create redundancy by finding new partner countries with whom to forge energy partnerships; and take a closer look at the longer-term consequences of subsidising certain national industries. Perhaps the most important immediate step would be for the West to better understand how its own financial system could act as an enabler to compete more successfully against adversaries. This is particularly important, considering regulatory and fiduciary constraints on financial institutions in funding the defence industry in Europe. Create **financial mechanisms for co-investment and funding of defence and security supply chains**, and to mandate European public investment banks and other large funds to invest in these supply chains.

Given the importance of **stockpiling critical energy resources** for coping with at least short-term disruptions, a broadening of a **Solidarity Principle** would

communicate a determination to respond collectively to what will remain a long-term challenge. To do this, leaders will need to change their mindsets and recognise together that economic and energy security will require **painful trade-offs.** They will also need to confront together contradictory and sometimes outright irresolvable policy conflicts, such as the profound tension between energy and environmental concerns. One element of any such change could be the re-branding of certain policy goals. For example, describing the green transition as a security gain (fewer dependencies) instead of a climate change mitigation measure.

Reinforcing Resilience, People Protection, Power Projection, Pan-Institutional and Whole of Government Solutions

Partnerships are the essence and foundation of resilience. Therefore, spaces must be created in which industry and technology can plug into civil-military structures. This is because industry and tech are critical to redundancy and robustness; "whilst deterrence is what you know, resilience concerns what you don't".

Societal resilience is fundamental to delivering future international resilience and this will depend upon strategic partnerships between nations, international organisations, and industry. NATO and allies can reinforce international resilience in the following ways: **Engage industry** in the planning and decision-making for critical national and international defence and security capabilities; **establish the legal and procedural processes** required to protect, leverage or mobilise populations during the transition period from peace to war; use **foresight techniques** to develop strategic deterrence and resilience communication plans and public messaging campaigns for future war scenarios; **undertake collective training and exercising** with allies and partners to test physical, digital and societal resilience, strengthen partnerships and better understand communication networks; and **conduct regular continuity of government and business exercises** to test the whole of society's resilience during future war scenarios.

Two further minimum critical resilience requirements should be established: financial & economic and information & communications. Lessons from the Russo-Ukraine War also need to be documented and analysed so that best practice models can be developed and whole-of-society solutions adopted.

Julian Lindley-French

Wilton Park | 01 November 2024

Wilton Park is a discreet think-space designed for experts and policy-makers to engage in genuine dialogue with a network of diverse voices, in order to address the most pressing challenges of our time.

enquiries@wiltonpark.org.uk

Switchboard: +44 (0)1903 815020

Wilton Park, Wiston House, Steyning,
West Sussex, BN44 3DZ, United Kingdom

wiltonpark.org.uk