REINVIGORATING CIVIL–MILITARY RELATIONSHIPS IN BUILDING NATIONAL RESILIENCE

VLASTA ZEKULIĆ, CHRISTOPHER GODWIN AND JENNIFER COLE

Russia's application of a sophisticated hybrid strategy and the rise of Daesh (also known as the Islamic State of Iraq and Syria, ISIS) have been drivers for change in the complex security environment of the twenty-first century. While the significance of these threats does not preclude the conventional aspect of national defence planning, it does complicate societal preparedness. Vlasta Zekulić, Christopher Godwin and Jennifer Cole examine the relevance of NATO resilience policies and propose a synchronised approach to crisis decision-making, civil preparedness planning and national and collective defence to ensure they are balanced, mutually supportive and incur manageable cost.

Since the turn of the twenty-first century, there has been a significant shift in the global geopolitical landscape, which has had noticeable implications for the perceived security situation in many Western states. The ramifications of this change have been felt across governments and financial and economic sectors. It has also been documented within populations, highlighting the interdependency between all domains of society and raising awareness of the need to build mutually supporting mechanisms to address these emerging challenges.

This has triggered references to the Cold War, when national unity of effort and civil preparedness walked hand- in-hand with military readiness. Yet, it often had its greatest use in times of crisis not driven by hostile threat, but by other drivers of instability, such as famine, economic collapse or natural disaster.[1] This article will demonstrate that while preparedness as it once was is impossible to revive, it can be rebuilt to fit the modern era.

In understanding how these strategic shifts have occurred, and why many governments and societies in the West have gradually moved away from the Cold War-era approach to civil–military relationships, it is necessary to consider several interrelated occurrences in recent history.

Changes in the Modern Security Environment

With the fall of the Berlin Wall, on 9 November 1989, the biggest existential threat the West had faced for 50 years disappeared almost overnight. Many of the former Warsaw Pact and Soviet Union states were quick to embrace Western democratic and economic ideals, and began negotiating a process of accession to NATO and the EU. From the perspective of Western democracies, this period signalled the continuation of the 'long peace', the absence of major conflict in Europe that followed the end of the Second World War.[2] In the UK, this also coincided with the end of the 30-year conflict in Northern Ireland and a reframing of UK policy away from domestic hostile threats, as well as from the threat of external state aggression: a military approach was no longer the most appropriate.[3]

Security threats did not, however, simply disappear – they changed. The West was faced with soft-security challenges spilling over from war-torn former Yugoslavia,[4] followed by an emerging global terrorist threat, as demonstrated by the 9/11 attacks. In response to the severity of these challenges, Western governments

began to look beyond their immediate borders to try to engage security threats at source, causing a shift from a homeland defence posture to one that was more expeditionary.[5]

One consequence of increased involvement in expeditionary operations was a gradual over-reliance on contracted civilian support for many logistical and some security functions of the military. Logistical outsourcing, which had been practised to a lesser extent since the 1980s, became the new NATO norm.[6] Although cost effective, it drew the focus away from national level civil–military cooperation, as competitive tendering not only called for contracting of the cheapest labour and services on the market, but also of a reduction in the spare capacity that could be held on standby and used by civil structures when needed.[7] In the UK, the civil defence structures were also moving further away from the Cold War mechanisms and, with the Good Friday Agreement of 1998, a complete overhaul of the Emergency Powers Act 1964 was required. The focus was now on a more agile 'all hazards' approach that included all types of threat.

At the same time, natural disasters, such as the Indian Ocean earthquake and tsunami in 2004 and the Haitian earthquake in 2010, or threats stemming from climate variability, demographic change, economic restructuring and, more recently, infectious disease in the form of the West Africa Ebola outbreak, were also drawing on concerted international responses from the civil sector on a scale only previously required in wartime.

From the NATO perspective, the combined effect of the events outlined above has meant that many Western states have become one-dimensional in their assessment of the geostrategic environment. Just as the UK National Risk Register[8] makes no reference to war, many other states re-postured themselves, believing the threat posed by a particular country, especially one closer to home, has significantly diminished when compared with the threats posed by terrorism or a non-state actor.

However, Russia's actions in and around Ukraine in late 2013 have caught the EU and particularly NATO off-guard to the extent that they have been forced to reconsider their posture, from a political, civil and security perspective.[9] Russia has demonstrated the ability to apply an aggressive hybrid strategy that aims to exploit adversaries' vulnerabilities across all levels of national power and society.[10] It is designed to complicate decision- making, particularly at the strategic political level, by remaining ambiguous and non-attributable and by operating below the level that would perceivably generate a coordinated response.[11] The strategy is commonly referred to as 'hybrid', because it uses a synchronous application of different levers of national power (economic, political, military and diplomatic) dependent upon the situation and desired strategic end-state; it is rarely constrained by time.

Importantly from a civil–military perspective, the response to hybrid threats requires an equal level of coordination across institutions, governments, alliances and the private sector, which may be best placed to identify early attacks or hostile reconnaissance. Franklin Kramer, Hans Binnendijk and Daniel S Hamilton explain that:

> When war changes, so must defense. New efforts are urgently needed that extend traditional activities directed at territorial protection and deterrence to encompass modern approaches to building a society's capacity to anticipate and resolve disruptive challenges to its critical functions, and to prevail against direct attacks if necessary.[12]

It is precisely in trying to formulate an adequate response against a hybrid opponent that many Western states have begun to understand the extent to which civil–military cooperation has deteriorated since the end of the Cold War.

Although preparedness planning for civil protection has continued through concepts such as the UK's Critical National Infrastructure,[13] joint planning between the military, national civil defence structures and pan-European constructs, such as the EU Civil Protection Mechanism,[14] it focused only on the non- military response to perceived threats and often lacked in-depth coordination. The need for resilience is therefore reconverging not just because hybrid warfare has changed the landscape of conflict, but also because it targets all aspects of states and their societies, which must be able to collectively prevent, resist and recover from aggressive action when and if required.

Understanding Different Meanings of Resilience

The UN defines resilience as '[t]he ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner'.[15] While resilience in civilian terms has been analysed in detail (psychological, environmental, societal, among others), until recently it has not been viewed from a comprehensive security perspective.

The civilian agencies responsible for national policy and operational response are, by definition, not the owners of the response to a military threat and in fact, in UK terms, it can be argued that no one 'owns' resilience. While the Cabinet Office is the doctrinal authority, with a coordinating role in strategy, policy, doctrine, response and recovery, all sectors of government and society have a role to play. Some organisations' planning assumptions and capability assessments necessarily fall short of military intervention, and as capability and assets have shrunk for both civilian and military agencies, it has become essential to ensure there is still sufficient overlap and that domains are joined up, leaving no gaps.

This is not entirely at odds with NATO's approach to resilience. The work of the Civil Emergency Planning Committee on the impact of hybrid warfare and collective defence operations recognises a resilient country as one capable, in times of crisis, of simultaneously safeguarding the continuity of governance, maintaining the delivery of essential services to the population and providing support to military operations. These broad guidelines are detailed in NATO's Seven Baseline Resilience Requirements,[16] which NATO members committed to implement at the 2016 NATO Warsaw Summit.[17] The necessity for concurrency in these capabilities is highlighted by Matthew Grant, who puts the case for why an over-emphasis on safeguarding the continuity of government above all else, with little regard for the impact this would have on the wider population, could potentially leave no one for the continuing government to govern.[18]

With this approach, NATO is trying to help its member states redefine resilience in order to build their capacity to *deter* and *defend* against contemporary security threats. [19] While the exact nature of the vulnerabilities of concern to NATO is classified, it can be framed as 'building capacity to detect, absorb and recover from all threats and hazards, along with a strong understanding of which sectors are critical enablers for strengthened military posture'.[20] Although the underlying tenets of civil preparedness and military response do not necessarily coincide, this does not mean that they are incompatible, nor that either should compromise their core tenets; their differences do need to be recognised and respected.

Why Cold War Resilience Cannot be 'Resurrected'

The security environment within which civil–military cooperation must be built to enhance national resilience represents a distinct shift from the environment of the Cold War years. Furthermore, restructuring resilience is also constrained by several important characteristics of the modern era that define how societies, states, organisations and corporations function and react against contemporary threats and disruptive challenges.

First, many institutions and organisations that facilitated a homeland defence posture on a national level during the Cold War, such as the Civil Defence Corps and the Royal Observer Corps in the UK, where civil–military cooperation was paramount, no longer exist. Others, such as the Civil Defence College (now Emergency Planning College) at Easingwold, have moved away from the military to an outlook and operational remit in line with the all-hazards approach.

At the multinational strategic level, Civil Emergency Planning (CEP) in NATO, originally established in the early 1950s[21] to develop plans for the mobilisation of civil resources and to recommend measures to be taken by governments in peacetime that would be readily available during war, downsized from fourteen CEP groups to a single Civil Preparedness Section within the Civil Emergency Planning Directorate.[22] Messages from the 1956 Report of the Three Wise Men on Non-Military Cooperation in NATO – stating that 'From the very beginning of NATO ... it was recognised that while defence cooperation was the first and most urgent requirement, this was not enough ... security is today far more than a military matter'[23] – were forgotten. Today, NATO CEP increasingly relies on a pool of civil experts to support military engagement. However, this represents a twofold challenge: first, questionable granularity of understanding within the civilian sector of the security challenges as perceived by NATO; and second, lack of assured access to these experts if they are focused on different types of disruption (such as severe flooding or earthquake damage).

Second, many military and national civilian capabilities to support military operations have been significantly degraded due to an over-reliance on contracted support during 20 years of expeditionary operations. Meeting military requirements in a non-competitive environment within a functioning state has been manageable as available provisions and infrastructure could be provided to military forces and the population, but the changed security environment may require deployed multinational troops to compete for the same civilian resources, transportation and infrastructure as the local population.[24] Although this scenario is not new, national and NATO plans that were in place during the Cold War to address this type of challenge mostly no longer exist, and those that do no longer lie with the military, but have been moved to civilian agencies. For example, in the UK, it is the Cabinet Office, not the Ministry of Defence, that sets policy, strategy and guidance on dealing with mass casualties, planning major evacuations, and feeding and sheltering large numbers of displaced populations, with the actual delivery enacted by the designated Lead Government Department (for example, the Department of Health in a public health emergency) under the coordination of the Cabinet Office Briefing Room Committee.

Third, the recent global financial crisis has not only resulted in an underinvestment in the military,[25] but also a strain on overall national budgets, which has meant an increasing reliance on a 'just enough, just in time' approach.[26] In turn, this has increased the risk of the possible effects caused by disruption to supply chains, which may be particularly vulnerable to cyber attack, presenting a 'potentially existential problem'.[27] This vulnerability of modern economic practice has grave implications for the military, and society at large, due to the outsourcing of significant military and civil defence capacity and the exposure of a state's industrial base to the competitive globalised market. The same dependency exists in both the military and civil sectors and they may find themselves competing in times of crisis for critical resources and services.

Fourth, the rapidly evolving and readily accessible development of modern and cheap technologies presents a different type of challenge to states as they strive to become more resilient. Potential adversaries are now able to acquire weapons and capabilities that have previously been available only to states.[28] As mentioned previously, cyber is one of the most serious. A cyber attack may be enacted by hackers in more than one country over systems and networks passing through several others before reaching their target. This threat became particularly relevant in the aftermath of the cyber attacks on Estonia in 2007 and on Ukraine in 2015.[29] Although NATO states committed to enhance their cyber security at the Warsaw Summit in 2016,[30] and additionally as part of the commitment to enhance resilience,[31] it is still predominantly a military domain issue alongside land, maritime, air and space. Cross-governmental and organisational cooperation is vital in addressing industrial, IT and cyber threats, as the technology being exploited is often owned by the private sector. This can limit the government's ability to oversee or intervene in its operation, and the point of origin of the attack can be almost impossible to pinpoint.

Last, this dynamic can be further exploited by access to the global audience, enabled through the internet and social media, but also by the thirst for information generated by 24/7 media coverage. Unlike during the Cold War, or even relatively recently, where information was subject to screening or editing and the cost of live broadcasting was extremely high, an actor wishing to influence or subvert a target audience can now do so independently and freely at little or no cost. This trend has been widely recognised, prompting renowned Kremlin propagandist Dmitri Kiselyov to declare that '[i]nformation war is now the main type of war'.[32]

All the above factors combine to illustrate how the world has changed since the Cold War. The military tools and mechanisms that were once effective in deterring adversaries are not necessarily obsolete, but rather no longer as accessible and available to response agencies, nor are they appropriate to face the challenge from non-state actors. Similarly, the civilian tools and mechanisms that have replaced the Cold War apparatus may be suitable for civil protection, but not for supporting military action in defence of a nation. Renewing national resilience against contemporary threats requires a cross-governmental and comprehensive approach, reinvigorating civil–military cooperation, and creating the support systems that understand the deep interdependencies between the military, civil and private sectors.

How to Build Resilience Against Contemporary Threats

Enhancing national resilience requires a whole-of-nation approach to merge resources, knowledge and mechanisms of government organisations and bodies, communities and the individuals within them. It also

requires governments to reassess where the drivers of insecurity may begin, for example the drought or flood that causes food shortages and thus migration, and/or the deliberate actions of a hostile enemy.

By slightly modifying Paul Arbon's concept of 'community resilience'[33] to a wider range of security challenges, this article proposes how countries should consider strengthening and synchronising four mutually interdependent areas to build resilience: identifying key threats, vulnerabilities and associated risks; the ability to make synchronised and joint decisions; building the required capacity across civil–military domains; and balancing the allocation of available resources to operationalise capacity and capabilities.

Identifying Vulnerabilities and Risk

As states recognise that they will always be the first responders, many are re-evaluating their own vulnerabilities[34] and preparedness to effectively deter and defend against contemporary security challenges. However, there is a need for a common understanding of what national and NATO vulnerabilities are, both from a civilian and military perspective, and how they may affect the stability and functioning of national and international systems. In broader terms, the threat to any NATO member is potentially a threat to all, just as vulnerability in one can become a vulnerability for all.[35]

This collective consciousness requires risk assessment of national and NATO critical values and vulnerabilities, but also an understanding of those that may be of interest to adversaries. Diego Ruiz Palmer suggests that the hybrid warfare model conceptualises 'dynamic interaction between hard and soft power ... that extends the military contest to society as a whole ... [making it] an accomplished form of "control war" over the ends, ways and means of nations, communities and societies'.[36] Therefore, while there is a strong chance that many vulnerabilities may be mitigated by military presence, military dependence on civilian infrastructure or assets may also make them a more attractive target for a potential adversary.

Although military and civilian plans are primarily developed in isolation from each other, restricting risk analysis and mapping of vulnerabilities, increasing understanding of the impact of potentially adverse events enables governments to develop adequate response mechanisms and manage consequences. In the UK, government ministers have become much more focused on risk prevention in recent years, rather than on response and recovery, with an accompanying focus of where investment is targeted, evidenced through investment in the Prevent strand of the CONTEST (Counter-Terrorism) strategy, the Centre for the Protection of National Infrastructure and the National Cyber Security Centre.[37]

Cross-Governmental Decision-Making

Many states have well-developed civilian crisis response systems and procedures for risk assessment and mitigation.[38] However, most of these plans are not coordinated with those of the military. The UK's National Security Strategy and Strategic Defence and Security Review 2015 explicitly positions resilience as one of the pillars of national security.[39] In practice, this has helped with the development of joint doctrine and generic capabilities that are positioned to deal with the consequences of a range of risks, and a general lowering of the distinction between counterterrorism and civil emergencies, where commonalities matter more than differences. However, a consequence of the shift may have been a sidelining of the military as the threats that traditionally require a military response have been seen as less likely and consequently of less immediate concern.

In the changed security environment, this traditional and stove- piped division of labour between the military, police, intelligence, customs and financial enforcement bodies is proving to be inadequate in responding to the challenge, particularly as adversaries manoeuvre and exploit seams in authority. Shrinking resources, increased centralisation of services and outsourcing diminishes the ability to absorb even minor disruptions, a trend that may be further exploited by potential adversaries. These organisational seams must be bridged, and information merged in order to expose adversarial intentions, actions and networks. Formalising integration and cooperation must be proactive and start at the planning phase.

In the context of hybrid threats, regardless of whether they are applied by a state or non-state actor, the target may be more than a single country or organisation, and consequently beyond the capability of any single entity to address. Similarly, a national response may not be enough, as a weakness exposed within one

country, especially within the European Schengen Area,[40] can easily transfer to another. Natural disasters respect no geographic boundaries, and can be compounded by their simultaneous impact on a number of neighbouring states which may have been previously providing aid. Finland provides a good model of how to move forward in its recognition that 'national preparedness measures should be supplemented and strengthened through the membership' of different international organisations.[41] Some measures are already in place, such as an EU directive aimed at protecting critical infrastructure that serves two or more member states.[42] However, this dynamic must further be reflected across NATO and the EU as it reinforces the need for the ability and capacity to contribute to integrated civil–military analysis and planning activities across the DIMEFIL (Diplomatic, Information, Military, Economic, Financial, Intelligence and Legal) spectrum.

Furthermore, in planning to counter contemporary threats and challenges, the private sector must be considered as it provides key elements of security and critical infrastructure, especially in the fields of energy, fuel and communication. While governments cannot 'command' the private sector, they may be able to impose a legal framework or regulations to dictate a level of responsiveness and responsibility to protect systems, services and infrastructure of national interest, regardless of ownership,[43] as the UK Cabinet Office approach referenced previously has identified. This is particularly important in the context of resilience, where a state may need to mobilise aspects of its industrial or resource base to support military and civilian operations within its borders in response to an internal or external threat or natural hazard.

Civil Preparedness and Civil–Military Relations

Dealing with contemporary security challenges requires a whole-of- government and whole-of-society approach. Civil preparedness for crises is critical in sustaining overall defence because the effective delivery of forces and military capabilities relies on resilient civilian resources. At the same time, the civilian population and critical infrastructure, upon which the military may rely, are highly vulnerable to external attack and internal disruption, which they may not have the resources or capabilities to address. Therefore, civil preparedness enables military sustainability, while military capabilities help to protect civil vulnerabilities.

Governments should be transparent and agile in communicating potential security threats and associated risks to their societies. In considering how NATO should respond to increasing security concerns in the Baltic, Henrik Praks noted that 'an important element raising resilience will have to include strengthening of internal societal cohesion'.[44] This is because every decision or action a government takes may have an impact on the population, for which it must be prepared. In understanding threats, vulnerabilities and risks, society may become more willing to accept the consequences of disruptive events. Civilians should not be viewed solely as victims or objects of protection, but as important and vital building blocks of a resilient society.

Although the military, civil and private sectors may approach resilience from different angles, in the contemporary security environment they are becoming more interdependent. The military has an increasingly important part to play due to its inherent interconnectedness, which may act as a lever for cohesion across its member states, and its ability to help to drive change. This calls for a more coherent and coordinated approach, which would benefit from enhanced military involvement, particularly from a planning and educational perspective.

Available Resources

There is growing recognition of the need for a more territorial response to security threats, but also of the potential burdens of financing and supporting such adaptations.[45] Re-establishing links between the civilian and military community under strong and transparent planning assumptions, and political and crisis decision-making, embodied in Norway's 'total defence' concept[46] – mutual civil–military support and coordination across an entire spectrum of crises, from peacetime via crisis to armed conflict and war – is one of several ways to enable cost-sharing. Another way might be to demonstrate how reinvesting in defence may also become an investment in civil preparedness.[47] If compatible and interconnected systems are purchased, shared and exercised such that they can be used in times of crisis, all agencies will benefit. Similarly, investing in infrastructure while considering possible military utility becomes an investment in preparedness and responsiveness. But for this to be an attractive proposition to the civilian sector, the utility the military offers must be understood as more than just defence against hostile external threats.

This is, for example, recognised by Finland (which is not a member of NATO) in its *Security Strategy for Society*, which states, 'the public administration is to a large extent and increasingly dependent on the functioning of the common information systems and networks that have been specifically designed for the entire administration, security authorities and the state leadership'.[48] Investing in organisational adaptation with a more civil–military bias may also enhance responsiveness. In essence, these concepts are known as dual-use and should be seen as the most efficient way to support military activity and capability through civil investment, and vice versa.[49]

Although the military embraces the tenets of capacity and redundancy to support sustainability and therefore resilience, the private sector, upon which it relies heavily, functions on a different set of assumptions and principles. It is driven mostly by the need to be profitable and efficient, tenets that do not necessitate concentration of capacity. In recent years, this has led to numerous cascading crashes of industrial activity, in which a small and local breakdown in the flow of physical goods or finance has triggered a shutdown of systems across the globe.[50] These examples are themselves illustrative of another dimension of the changing nature of threat: not from malicious actors, but from modern organisational processes. This has had consequences for the civil and military sectors, and illustrates why national governments must engage with multilateral organisations to understand how to mitigate against them. Appropriate measures may include diversification of supply, resources and services.

Conclusion

Resilience is a re-emergent theme that has assumed increasing importance to states as a result of the changed security environment. Russia's actions in and around Ukraine have refocused the West's attention on issues closer to home after decades of out-of- area military operations. In internally refocusing their efforts, many have looked to reinstitute practices that existed during the Cold War in an attempt to understand how they once more may become more resilient against a powerful and aggressive state actor or even the innovative and aggressive non- state actor, such as Al-Qa'ida or Daesh (also known as the Islamic State of Iraq and Syria, ISIS). However, this capacity needs to exist alongside the continuing requirement to assist civil structures in managing natural disasters, economic uncertainty, pandemics, power outages and supply chain failure, which are all potential drivers of instability.

This article has shown that the solution is broader than purely resurrecting old institutions as the threat is no longer singular and hostile actors are no longer easily recognisable. The emergence of non-state actors with access to modern technologies has significantly complicated the dynamics of the contemporary geostrategic environment. This is the security challenge of the twenty-first century.

To address resilience in this context, this article proposes an approach that states should consider that not only revives the whole-of-nation approach of the Cold War, but also how to rebuild resilience by embracing what is new. The way vulnerabilities can be exposed and exploited in modern societies requires a fresh approach to understanding and mitigating risk, and in understanding what triggers decision-making in a volatile and austere information environment. This calls for efforts in enhancing societal awareness, preparedness and responsiveness in support of national politics through transparency, training and education.

Set against this requirement is the importance of the relationship between civil and military sectors, not only because of their interconnectedness but also their interdependency. Moreover, modern-day resilience may likely require a regional approach or multinational cooperation, and will almost certainly need to consider the requirements of the private sector. Although the military has the capabilities and skills to drive change, the first step required to build resilience is focused civil leadership, educated and capable to assess risk, mitigate vulnerabilities, invigorate society and efficiently apply the required resources. NATO's ability to work together with civil structures to enact this, so that military capability and assets can be deployed in defence of states when needed, but also in support of them when required, against a multitude of vulnerabilities, will be key to a more stable and secure future for all its member countries.■

Vlasta Zekulić, after 20 years in the Croatian Army, is now an officer in NATO Headquarters Operations Division. Her PhD is in International Relations and National Security from the University of Zagreb.

Christopher Godwin served for 30 years in the Royal Navy. With Vlasta Zekulić, he championed work on resilience from the NATO perspective while serving at Allied Command Transformation in Norfolk, Virginia.

Jennifer Cole ran the Resilience and Emergency Management programme at RUSI until August 2017. She holds a PhD in Computer Science and Geography from Royal Holloway, University of London.

Notes

1 In the UK, for example, the largest deployment of the Civil Defence Corps (which came under the Home Office but was intended to provide assistance to the community in the aftermath of a nuclear strike on the UK) was in response to severe flooding in 1953 and the catastrophic collapse of a colliery spoil tip on to the Welsh village of Aberfan in 1966. See Matthew Grant, *After the Bomb: Civil Defence and Nuclear War in Britain, 1945–68* (London: Palgrave Macmillan, 2010). The Civil Defence Corps was officially disbanded in 1968. The capabilities to respond in this way are now dependent on private sector contractors.

2 Richard Ned Lebow, 'The Long Peace, the End of the Cold War, and the Failure of Realism', *International Organization* (Vol. 48, No. 2, Spring 1994), pp. 249–77.

3 Jennifer Cole, 'Securing our Future: Resilience in the Twenty-First Century', *RUSI Journal* (Vol. 155, No. 2, April/May 2010), pp. 46–51.

4 Mark Galeotti, 'The Challenge of "Soft Security": Crime, Corruption and Chaos', in Andrew Cottey and Derek Averre (eds), *New Security Challenges in Post-Communist Europe: Securing Europe's East* (Manchester: Manchester University Press, 2002), pp. 151–62.

5 The requirement to engage and sustain military operations further afield than the traditional area of operations.

6 A study conducted by the US Congressional Budget Office in 2005 concluded that organic support cost approximately 90 per cent more than using contractors. However, by 2012, there was an increased awareness that this was not necessarily the case because of the additional costs and risks associated with enhanced contractor presence in operations. At the height of the war in Afghanistan, the cost of getting fuel to a remote forward-operating base was as high as $400 per gallon. See Committee on Appropriations, 'Report on the Department of Defence Appropriations Bill, 2015', Report 113–211, 113th Congress, 17 July 2014; and US Government Accountability Office, 'Report on Defence Management – DOD Needs to Increase Attention on Fuel Demand Management at Forward- Deployed Locations', February 2009.

7 An example is the UK's decision not to replace the Ministry of Defence- owned 'Green Goddess' fire engines (held in reserve since the Second World War), which had proved critical during the fire-fighters' dispute of 2002–03.

8 Cabinet Office, 'National Risk Register of Civil Emergencies', 2015 edition, March 2015.

9 NATO, 'Wales Summit Declaration', press release, 5 September 2014.

10 See Kremlin, 'The Russian Federation's National Security Strategy', Russian Federation Presidential Edict 683, 31 December 2015; and President of the Russian Federation, 'The Military Doctrine of the Russian Federation', 26 December 2014.

11 For more on hybrid warfare, see Can Kasapoglu, 'Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control', *NATO Research Paper* (No. 121, November 2015); and Charles R Burnett et al., *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlyle, PA: US Army War College Press, 2016).

12 Frankin D Kramer, Hans Binnendijk and Daniel S Hamilton, *NATO*'s *New Strategy: Stability Generation* (Washington, DC: Atlantic Council and Center for Transatlantic Relations, 2015), p. 8.

13 For more information on the Centre for the Protection of National Infrastructure, see <https://www.cpni.gov.uk/critical-national- infrastructure-0>

14 European Commission, European Civil Protection and Humanitarian Aid Operations, 'EU Civil Protection', factsheet, April 2017.

15 UN Office for Disaster Risk Reduction, 'Terminology', <http://www.unisdr. org/we/inform/terminology#letter-2>, accessed 12 July 2017.

16 Jamie Shea, 'Resilience: A Core Element of Collective Defence', *NATO Review*, 2016.

17 NATO, 'Commitment to Enhance Resilience', press release, 8 July 2016.

18 Grant, *After the Bomb*, pp. 97, 190–92. 19 NATO, 'Deterrence and Defence Posture Review', press release, 20 May 2012.

20 Remarks by Civil Preparedness Section Head Lorenz Meyer-Minnemann at the Chiefs of Transformation Conference, Norfolk, Virginia, 8–10 December 2015.

21 The original fourteen Civil Emergency Planning groups can be found at NATO, 'Draft Resolution Concerning the Establishment of a Civil Emergency Planning Committee', C–M(55)95, 3 November 1955.

22 NATO, 'Civil Preparedness', 26 April 2017.

23 NATO, 'Report of the Committee of Three on Non-Military Cooperation in NATO', 13 December 1956, para. 15.

24 For example, the presence of displaced civilians or refugees may restrict normal throughput of transportation networks, and significantly hamper security forces' movement plans.

25 Years of underinvestment in defence has forced countries to prioritise military capabilities required for current missions and operations at the expense of maintaining more organic capabilities and capacities for home defence. See NATO, 'Secretary General's Annual Report 2012', 31 January 2013.

26 The 'just in time' production technique is designed to speed the flow of materiel and capital through manufacturing systems. The result is a significant reduction in inventories of both raw and processed materials.

27 Barry C Lynn, 'Shock Therapy: Building Resilient International Industrial Systems in 2030', in Erik Brattberg and Daniel S Hamilton (eds), *Global Flow Security: A New Security Agenda for the Transatlantic Community in 2030* (Washington, DC: Center for Transatlantic Relations, 2015), pp. 207–26.

28 The implications of additive manufacturing for the battlefield are immense. Researchers at the University of Virginia have 3D-printed a drone in a single day and, by adding an Android phone, made it autonomous for a total cost of $2,500. See T X Hammes, '3-D Printing Will Disrupt the World in Ways we can Barely Imagine', *War on the Rocks*, 28 December 2015.

29 Stephen Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Reponses', *Journal of Strategic Security* (Vol. 4, No. 2, Summer 2011), pp. 49–60.

30 NATO, 'Cyber Defence Pledge', press release, 8 July 2016, <https://ccdcoe. org/sites/default/files/documents/ NATO-160708-CyberDefencePledge. pdf>, accessed 19 July 2017.

31 NATO, 'Commitment to Enhance Resilience', para. 7.

32 Peter Pomerantsev, 'Inside Putin's Information War', *Politico*, 4 January 2015.

33 In 2009, the Council of Australian Governments agreed to adopt a whole- of-nation resilience-based approach to disaster management, which recognises that a national, coordinated and cooperative effort is required to enhance capacity to withstand and recover from emergencies and disasters. In response, the Torrens Resilience Institute, led by Paul Arbons, developed a community disaster resilience model and assessment tool. See Paul Arbon, 'Developing a Model and Tool to Measure Community Disaster Resilience', *Australian Journal of Emergency Management* (Vol. 29, No. 4, 2014).

34 European Commission, 'Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures More Secure', SWD(2013) 318, 28 August 2013.

35 For example, Turkey has dealt with the Syrian migration crisis for four years, taking in more than 2 million refugees. It continually warned against the threat of the conflict spilling over to Europe, and when that happened in 2015, almost no country was ready to deal with the flow of refugees.

36 Diego A Ruiz Palmer, 'Back to the Future? Russia's Hybrid Warfare, Revolutions in Military Affairs, and Cold War Comparisons', *NATO Research Paper* (No. 120, October 2015), pp. 7–8.

37 Cabinet Office et al., '2010 to 2015 Government Policy: Counter-Terrorism', updated 8 May 2015.

38 For example, Poland has a single national crisis directive, cascading through regions and counties to more than 2,000 local plans.

39 HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, Cm 9161 (London: The Stationery Office, 2015), p. 9.

40 The European Schengen Area is a challenge for police and intelligence agencies, as the free flow of people and goods also enables terrorists and weapons to move from one country to another. This was recently highlighted during the November 2015 Paris attacks, about which Belgium's Prime Minister Charles Michel said, 'Almost every time [there is an attack], there's a link with Molenbeek'. See *The Economist*, 'Jihad at the Heart of Europe', 21 November 2015.

41 Finnish Ministry of Defence, *Security Strategy for Society*, Government Resolution 16.12.2010 (Helsinki: Finnish Ministry of Defence, 2011), p. 10.

42 Council of the European Union, 'Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection', *Official Journal of the European Union* (L 345/75, 23 December 2008).

43 Lynn, 'Shock Therapy'.

44 Henrik Praks, 'Hybrid or Not: Deterring and Defeating Russia's Ways of Warfare in the Baltics – The Case of Estonia', *NATO Research Paper* (No. 124, December 2015), pp. 219–44.

45 On the eve of the Paris attacks in November 2015, the UK announced a 15 per cent increase in the size of its security services, and a doubling of spending on cyber defence. See *The Economist*, 'How to Fight Back', 21 November 2015.

46 Norwegian Ministry of Defence, 'Capable and Sustainable: Long Term Defence Plan', June 2016.

47 An example might be the procurement of a modern communications system that is interoperable across military, police and civil emergency organisations. This would have mutually beneficial implications through interconnectivity, mobility and in coordinating response across all state security functions.

48 Finnish Ministry of Defence, *Security Strategy for Society*, p. 5.

49 If procured equipment has a proven civil–military dual-use capability, part of the cost can be sourced from EU common funds, making them an attractive and cost-effective solution.

50 The first major international supply chain crash was in September 1999, after an earthquake in Taiwan cut off the flow of specialised semiconductors. Within days this resulted in the sudden closure of factories across Asia and the US. It happened again after the 9/11 attacks in 2001, the eruptions of the Icelandic volcano Eyjafjallajökull in 2010 and the 2011 floods in Thailand, to name a few.