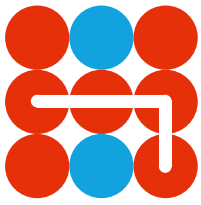
Working Paper • April 2019

Building Resilience: Hybrid's Weakness?

ROGER CLARKE & OWEN JACKSON



Hybrid CoE

Working Paper

Building Resilience: Hybrid's Weakness?

Summary

The fluidity of 'Hybrid Threats' makes them hard to theoretically grasp, and practically counter. This Working Paper encourages security practitioners to draw on insights from established work on resilience and civil preparedness. Resilience ensures that households, communities, societies, infrastructure and states are able to withstand and recover from shocks. Building resilience is an important part of the answer to hybrid threats, with its objective of normality juxtaposed to the chaos in which such threats thrive.

By:

Roger Clarke, Baltic Resilience Advisor, Foreign & Commonwealth Office, UK Government

Dr Owen Jackson, Assistant Director – International Resilience, Civil Contingencies Secretariat, Cabinet Office, UK Government

‘Hybrid Threats’, the bogeyman of contemporary security policy…

International organisations, national governments and security think tanks have effectively made ‘hybrid threats’ a standing agenda item in conferences, seminars, briefings and assessments. This focus is fuelled by real-world events in Salisbury and the Sea of Azov, and theoretical work on related concepts such as asymmetric and unconventional warfare. The amorphous nature of ‘hybrid’ negates the possibility of a universal and precise definition, but it is generally implied to be secretive, malignly powerful, and difficult to counter. In debates, planning and crisis exercises hybrid adversaries are invariably endowed with clear strategic objectives, coherent networks of supportive agencies, superb organisational skills, excellent situational awareness and no moral or legal constraints to limit an endless toolkit of un-attributable capabilities.

…but is this reputation entirely deserved?

Over the past few years this view has been moderated somewhat, propelled by the international response to events such as Salisbury. There is an increasing appreciation that states using hybrid ways and means suffer negative consequences, such as diplomatic condemnation, isolation, sanctions and strategic positioning by other states. At an operational level, there are signs that initiatives to counter disinformation and cyber-attacks are bearing fruit, and in the UK new tools such as Unexplained Wealth Orders and a closer scrutiny of foreign investments will further enhance our ability to respond.

Policymakers are increasingly developing tools to deter future hybrid attacks by denial, punishment, defiance, degradation, delegitimisation and collaboration. These are sensible, and move the debate forward by providing tangible options for decision-makers seeking to neuter such threats. However, as with wider discussions on hybrid, there is a risk that in crafting new tools for new security challenges we overlook well-established concepts that have continued, and possibly increased, relevance.

Resilience: activity, objective, mindset

The concept of resilience is almost as fluid as that of hybrid, yet this has not prevented it from shaping civil preparedness policies over the past few decades. For the purposes of this Working Paper we will conceptualise resilience in three ways, and for each highlight its relevance to debates on how to counter hybrid:

Resilience as an activity

Work to improve the resilience of key infrastructure assets, critical sectors and societies provides a risk-agnostic rationale for a wide range of activities. Resilience relates to managing the consequences of all threats and hazards, since for emergency responders it does not really matter whether a power station has been destroyed by floodwaters or explosive devices, or whether a telecommunications supply chain has been compromised by cyber-attacks or software glitches.

Separating highly classified threat assessments from generic consequence management allows a much greater number of actors to plan for, exercise and respond to crises. It also avoids a duplication of efforts by security-focussed military organisations and business continuity-focussed civilian organisations, since by working to similar planning assumptions expertise and resources can be pooled and optimised.

For countering hybrid threats this characteristic of resilience is particularly important. Despite many discussions about hybrid threats being highly classified, many of their impacts are identical to the consequence of a technical failure or natural hazard. Activities to build resilience can include hybrid threats as one of the many risks that feed planning assumptions, and in doing so foster a genuinely whole-of-society approach to this security issue.

Resilience as an objective

It is inevitable that hazards and threats will periodically shock societies, which should make resilience an easy objective for politicians and the public to support. Efforts to build resilience by reducing risks, whether through infrastructural changes (eg. improved water management) or financial measures (eg. reinsurance, climate and development financing[1]) are available and have been utilised to differing extents around the world. Countries that experience repeated disasters often lead the way in implementing these solutions, since the political pressure exists to effect change. Elsewhere, resilience practitioners sometimes struggle to achieve resilience through prevention because of political pressure to spend on more visible aspects of the risk cycle (ie. response and recovery).

Where countries do not have a recent history of catastrophic disasters, investing in resilience may be difficult to justify. This is a particular problem when considering hybrid threats, since the intent of hostile actors is to cause pain to their adversary while keeping activity below the threshold for decisive action. This makes it all the more important for countries to carry out holistic risk assessments and plan resilience interventions based on risk impacts (such as the UK's National Resilience Planning Assumptions). We have yet to see how long the current focus on 'hybrid' endures. However, regardless of what label we use, officials must continue to respond to the threats it describes. By making proposals that mitigate multiple risks, and drawing clear links to how they can prevent disruption to people's lives, policymakers can future-proof their initiatives.

Resilience as a mindset

Building situational awareness and capabilities is a proactive process. Resilience practitioners aim to make an asset, sector, or society, stronger and more able to withstand shocks. They embrace an interventionist approach that monitors current trends and makes informed changes where it is most useful to do so.

Work to counter hybrid threats is eminently worthwhile and needs to increase. However, we could usefully supplement this reactive, defensive mindset with a more proactive one that aggressively seeks and mitigates vulnerabilities. This would emphasise the deterrence aspects of resilience[2], and demonstrate to the

1 See, for example, Watson, C. et al (2015), Financing for Disaster Risk: 10 things to know; Overseas Development Institute

2 See, for example, RUSI's Modern Deterrence project https://rusi.org/projects/modern-deterrence

public and our adversaries the strength and agility of national government and international organisations to the public.

Conclusion: banishing the bogeyman

Politicians, policymakers and security analysts are increasingly engaged in substantive debates about how to deal with a range of hybrid threats that are secretive, malignly powerful, and difficult to counter. In doing so, there is a growing realisation that hybrid threats are not omnipotent, and new strategies show promising signs of success. However, we should avoid overlooking existing approaches in the field of resilience, since these provide valuable lessons in how to share classified information with large groups of stakeholders, how to convince decision-makers to support work that deals with both malign and non-malign risks, and how intervening proactively to reduce the risk of systemic shocks occurring, while sometimes difficult to prove and justify to the public, can have a disproportionate impact in improving national resilience and security.

It is important not to underestimate the step-change in response necessitated by the (re)discovery of 'hybrid'. However, we also should not overestimate this threat. Doing so does our adversaries' work for them, and distracts us from the tools we already have at hand, and activity we are already engaged in, to keep societies safe.

Authors

Roger Clarke is the UK's Baltic Resilience Advisor based in Riga. He runs cooperative projects with Estonia, Latvia and Lithuania on issues related to civil preparedness and crisis management. These cover areas such as critical national infrastructure, exercising, consequence management and crisis governance. As part of his work, Mr Clarke engages with a large number of stakeholders, including centres of excellence, NATO organisations, civilian ministries and tertiary institutions. He previously worked on crisis communications for a Public Relations firm in New Zealand, where his projects included running the communications response of a major infrastructure operator to the 2016 earthquake. Prior to that, Mr Clarke worked in the UK's Civil Contingencies Secretariat. While there, he coordinated the Government's response to a diverse range of national crises, carried out risk assessments of critical sectors and led contingency planning for a number of threats and hazards.

Dr Owen Jackson is Assistant Director for International Resilience in the Civil Contingencies Secretariat in the Cabinet Office. The Civil Contingencies Secretariat ensures the UK is planning for, preventing where possible, able to respond to and recover from any natural hazards or man-made threats. He leads the team representing the UK on a number of international working groups in the EU, UN and NATO, develops bilateral relationships with other national civil protection authorities, and is responsible for developing the UK's international policy in the fields of civil protection, risk and crisis management. He leads a small team of resilience advisers based in UK Embassies, ensuring close collaboration between the UK and its international partners to build national resilience. He is the UK National Focal Point for the Sendai Framework for Disaster Risk Reduction.

Literature:

Allcott, H., Gentzkow, M. and Yu, C., 2019. *Trends in the diffusion of misinformation on social media* (No. w25500). National Bureau of Economic Research.

Keen, F., 2017. Unexplained Wealth Orders Global Lessons for the UK Ahead of Implementation. *RUSI Occasional Paper, September*.

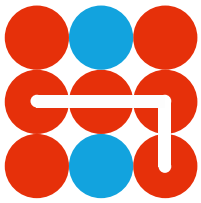
Levy, I., 5 February 2018, Active Cyber Defence – One Year On. *National Cyber Security Centre*. https://www.ncsc.gov.uk/content/files/protected_files/article_files/ACD%20-%20one%20year%20on_0.pdf

Johnson, R., 2018. Hybrid War and Its Countermeasures: A Critique of the Literature. *Small Wars & Insurgencies*, *29* (1), pp.141-163.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi

ISBN ISBN: 978-952-7282-16-8

Hybrid CoE is an international hub for practitioners and experts, building member states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland



Hybrid CoE