At a glance
June 2015

Understanding hybrid threats

'Hybrid threats' are often invoked in reference to the ongoing conflict in Ukraine and the ISIL/Da'esh campaign in Iraq. As policy-makers struggle to grasp what hybrid threats mean for national security, it is pertinent to recall the origins, the meaning, and legal challenges associated with this concept.

Evolving security environment

Concerns about hybrid threats were first reflected in NATO's new Strategic Concept of 2010 and incorporated in the NATO Capstone Concept, which defined hybrid threats as 'those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives'. Recently, the concept of hybrid threat has been revived in relation to Russia's actions in Ukraine and the ISIL/Da'esh campaign in Iraq. At an informal meeting in Riga, in February 2015, EU Defence Ministers called for more unity and concrete action at EU level. In May 2015, the European External Action Service circulated a discussion paper on 'Countering hybrid threats', which reaffirms that the EU needs to be able to recognise the overall effect of hybrid threats, and counter them by building more resilience.

Hybrid threat, hybrid conflict and hybrid war

The term 'hybrid threat' is a metaphor that brings complexities and dilemmas related to a changing global environment to the fore. It is often used interchangeably with references to hybrid war, to capture the interconnected nature of challenges (i.e. ethnic conflict, terrorism, migration, and weak institutions), multiplicity of actors involved (i.e. regular and irregular forces, criminal groups) and diversity of conventional and unconventional means used (i.e. military, diplomatic, technological). Taking into account different levels of intensity of a threat and intentionality of actors involved, it is possible to distinguish between hybrid threat, hybrid conflict and hybrid war:

- **Hybrid threat** is a phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat. Hybrid conflict and hybrid war are two specific categories whereby some hybrid tactics are used by a state to achieve its strategic ends.
- **Hybrid conflict** is a situation in which parties refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation (falling short of an attack), exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives.
- **Hybrid war** is a situation in which a country resorts to overt use of armed forces against another country or a non-state actor, in addition to a mix of other means (i.e. economic, political, and diplomatic).

Challenge one: Intentionality and proportionality

Most references to hybrid war encompass the notion of an adversary who controls and employs a mix of tools to achieve their objectives. Establishing responsibility and intentionality of actions is necessary to ensure that the policy response is legitimate and proportionate. However, this is not always easy in practice, due to the limitations of international law, technological constraints, or the diffusion of power to non-state actors, which increase the opportunities for deniability. For instance, due to technological limitations and the involvement of non-state actors, it is almost impossible to attribute, beyond any doubt, a cyber-attack to a specific country. Nonetheless, the US government has in the past indicted Chinese officials suspected of involvement in cyber-attacks against its computer networks, and imposed sanctions on North Korea following the attack on Sony Pictures Entertainment. The NATO Summit in Wales in 2014 confirmed the application of Article 5 of the Washington Treaty in the event of a cyber-attack, but has not established any threshold that would trigger a collective-defence mechanism.

EPRS | European Parliamentary Research Service
Author: Patryk Pawlak, **Members' Research Service**

PE 564.355

Disclaimer and Copyright: The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to the Members and staff of the EP for their parliamentary work. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy. © European Union, 2015.

Challenge two: International law and global governance

Even though no international legal framework specifically regulates hybrid warfare, any use of force in international relations is regulated by the United Nations Charter, which states clearly that, in the absence of an armed attack against a country or its allies, a member state can use force legally only if authorised by a United Nations Security Council resolution. Rules and principles regarding armed conflict are laid down in international humanitarian law and human rights law. With regard to hybrid conflict and threats, a patchwork of legal instruments covers specific policy areas, including the seas, counter-terrorism, money laundering and terrorist financing, and human rights. At the same time, the application of existing international law and the functioning of global governance institutions become increasingly complicated, as the boundaries of concepts such as sovereignty, legitimacy and legality blur. The continued military, economic and political action against the ISIL/Da'esh forces in Iraq, the debate about the application of existing international law in cyberspace, and maritime disputes in the South China Sea, are all good examples of the challenges stemming from this complexity.

Policy responses

The analysis of challenges posed by hybrid threats led to the emergence of a comprehensive approach blending all actors and available instruments: military forces, diplomacy, humanitarian aid, political processes, economic development, and technology. The EU's own comprehensive approach was adopted in December 2013. However, it is also important to understand that adjustments made to a security environment dominated by hybrid threats might have a long-term impact on the stability of the international order and may eventually have an impact on global power shifts. In that respect, several trends stand out:

- **Conceptual trends**: Government-led comprehensive approaches are increasingly complemented by whole-of-society strategies aimed at managing risks and building resilient societies. The focus on resilience helps to mitigate risks that might lead to hybrid conflicts in the future (i.e. over energy or access to water), and improves associated resource-management practices.
- **Material trends**: Resources to counter hybrid threats reside with many different stakeholders, including governments, civil society, the private sector and individual citizens. This joint ownership is reflected in public-private cooperation on security and development. At the same time, many governments have recently taken concrete steps to increase and modernise their civilian and military capabilities.
- **Legal trends**: Some of the present legal concepts and frameworks are anachronistic and do not always address hybrid threats adequately. This leads increasingly to incoherent application of the existing rules, whereby states use treaties and conventions selectively in order to justify their positions. The choice between status quo and new instruments might increase the need for alternative approaches (i.e. confidence building measures, law enforcement cooperation and mutual legal assistance).
- **Institutional trends**: Many countries have adjusted to hybrid threats by expanding the missions of existing institutions (i.e. new powers for intelligence agencies, bolstering EU strategic communication) or creating new organisations (i.e. the Ministry of Truth in Ukraine).

Examples of hybrid threats

Terrorism: terrorist organisations like Boko Haram, Al-Qaeda in the Arabian Peninsula (AQAP) and ISIL/Da'esh operate across the territories of many countries, and employ a variety of economic, military and technological tools to achieve their political goals.

Cybersecurity: the operations of state-affiliated hackers from Russia and China and the use of cyber-weapons are facilitated by difficulties with the attribution and the absence of norms of state behaviour in cyberspace.

Organised crime: armed criminal groups and drug cartels in Mexico resort to violence in the fight over territory and economic profits. Erosion of security, in turn, has a negative impact on the Mexican economy.

Maritime disputes: China is pursuing its aims in the South China Sea by combining economic and military pressure with extensive land reclamation projects in the Spratly archipelago.

Space: constraints on use of orbital space (and access to satellites) resulting from space debris – created, among other things, by anti-satellite missile tests.

Resource scarcity: resource-dependency between countries is increasingly used for political purposes. In 2010, China blocked exports of raw materials to Japan in response to the arrest of a Chinese fishing boat. In 2011, India’s refusal to adopt a water-sharing agreement with Bangladesh put additional pressure on bilateral relations.

Covert operations: Russia's strategic use of special forces (i.e. 'green men') and information in Ukraine.