The Hague Centre
for Strategic Studies

Between War and Peace

'Hybrid Threats' and NATO's Strategic Concept

Tim Sweijs

June 2022

The Hague Centre
for Strategic Studies

Between War and Peace

'Hybrid Threats' and NATO's Strategic Concept

Contribution by Tim Sweijs to the roundtable 'Between War And Peace: Increasingly Blurred Boundaries?' at the international seminar 'The Madrid Summit and the Future of NATO', hosted by The Institut Barcelona d'Estudis Internacionals (IBEI) https://www.ibei.org/en/international-seminar-the-madrid-summit-and-the-future-of-nato_266348.

With special thanks to Mattia Bertolini.

June 2022

In war studies one can distinguish between the futurists on the one side and the traditionalists on the other: those holding that everything in today's wars is new and unprecedented versus those holding that the nature of war is enduring and that what happens today on and off the battlefield has already been seen throughout history albeit in different guises. Within the debate between these two camps the question persists whether so-called hybrid war is war at all, whether we even need the 'hybrid' label, and whether we should not just focus on kinetic large scale warfare and allow the minor stuff to function as a safety valve to release tension.

Indeed, the traditionalists are right. There is nothing new about competition and conflict under the threshold of large scale political violence:

Globalisation and progressive digitalisation have changed the size and scale of hybrid threats.

- Political leaders from Nero to Napoleon to Nixon were Masters of Propaganda in manipulating political opinion to further their objectives.
- Proxy forces have been part and parcel of wars ranging from those between the Italian City States in the early Renaissance to those deployed by the superpowers in the periphery during the Cold War.
- Assassinations of opponents is not just used by the Russians, the Americans, the Israelis and the Iranians in modern times, but has been practiced for millennia. After all, the term 'assassin' derives from the Arabic term '*hashishi*', or those who smoke hashish, a Shiite sect in Syria and Iran who used to knife their political opponents between the 11th and 13th century.
- The targeting of vital infrastructures has also been done throughout history, from the poisoning of the wells to the destruction of waterworks.
- Theft of critical technologies for security or prosperity is seen throughout history as well: from France stealing the designs of the Jenny spinning wheel in England in the late 18th century to the theft of nuclear enrichment centrifuge designs by Abdul Qadeer Khan in the Netherlands in the 20th century.

Yet, the futurists are right too. The size and scale of hybrid campaigns under the threshold of large scale political violence are of a different nature simply due to the onset of globalisation and progressive digitalisation, which have opened up new ways to project power and to wreak havoc on one's opponent. Cyber strategic actors can target vital infrastructures from afar and disrupt economic and societal activities; they can manipulate public discourses and undermine democratic decision-making processes on a larger scale and with greater speed than was previously possible. We have seen plenty of that in recent years:

- Shrewd disinformation campaigns executed by the Internet Research Agency in St Petersburg have found an audience in a minority yet sizeable part of the European population.
- We have seen real ripple effects of cyber-attacks in which the cyber payload was not contained but spread throughout our global networks. A key example is NotPetya with an estimated 10 billion USD of damages, including processes interrupted at hospitals, ports and industrial infrastructures.

- And things could be taking a turn for the worse. The advent and maturation of 5G will further boost the creation of an Internet of Things, which further increases the vulnerability of our infrastructures and societies. Plenty of new opportunities for manipulation of the minds of men and women will present themselves. Back in 2006, for example, YouTube was widely seen as a hobby-channel for people to share their personal lives; Twitter was still called Twttr with only twelve thousand users; and the smartphone did not yet exist. Then came the smartphone, 4G rolled out, App stores were created, and the world turned into a global beehive in which the social media virality of the 2010s replaced the CNN effect of the 1990s. Moreover, Augmented Reality, Virtual Reality, and Hologram Technology are maturing, and the fruits of the Third Summer of Artificial Intelligence that took off around 2011 are becoming more widely available. One should envision a Brave New World in which new forms of virtual societal warfare will appear, be it in the Metaverse envisioned by Mark Zuckerberg or in the Real World that us *homines sapientes* currently still inhabit.

The Russia-Ukraine war has major implications for the prospect of hybrid threats in the 2020s.

Implications of the Russia-Ukraine war for hybrid threats

The onset of one of the largest interstate, steel-on-steel, horrific wars in Europe since the Second World War might lead one to think that we should gear up and prepare for large scale war, rather than to ponder these smaller, lower level challenges. Indeed, NATO is well advised to ramp up its conventional forces, beef up its strength, replenish its stocks, increase readiness, and enhance mobility. Because if we do not, the opponent might come through the so-called front door. But once we secure this front door, it is likely that opponents will try to come in through the backdoor.

The Russia-Ukraine war has major implications for the prospect of hybrid threats in the 2020s. First, Vladimir Putin has crossed the Rubicon, and, regardless how the war will end, we have entered into an era of Persistent Confrontation. Second, Russia's miserable performance on the battlefield, its inability to gain air supremacy, the poor management of its logistics and supply chains, and its disastrously amateurish tactics combined with top down command and control, stands in stark contrast to Ukraine's unexpected ability to defend itself, and to impose real damage on the invading force through a hedgehog strategy made possible by extensive Western arm supplies. This sends a strong message to those considering entering into large scale conventional wars: they are enormously costly and the odds of success are far from certain. Third, from a strategic perspective it would be wiser for revisionist actors to either pursue a *fait accompli* strategy through quick land grabs or hybrid strategies in the grey zone to further their political objectives. Therefore, hybrid strategies can be expected to stick around in the 2020s.

What does this mean for NATO?

NATO is advised to move from a deterrence by reinforcement to a deterrence by denial posture, complemented with a deterrence by punishment option. In addition, the Alliance needs to step up its counter hybrid postures to deal with hybrid campaigns in an Era of Persistent Confrontation. What does that entail?

1. Bolster Resilience: Societal and Physical

- On a societal level, we should invest in *Humboldtisches* forms of education and nurture critical thinking, foster awareness through openness of governments and free media, and stimulate dialogue between Alliance members with different threat perceptions, as well as with societal groups other than those who are already aware.
- On a physical infrastructure level, one should devise infrastructure metrics for resilience, stimulate NATO-EU cooperation and the involvement of the private sector, and devise governance mechanisms.
- Moreover, economic collaboration between NATO allies should be encouraged within the context NATO's Article 2 in order to make sure that 'know thy vendor' legislation is in place and critical infrastructure is protected.
- Furthermore, resilience should be built through "continuous and effective self-help and mutual aid" and securing vital infrastructure (i.e., NATO Article 3). Note that this also serves the purpose of deterrence by denial by signalling to your opponent that attacks are unlikely to succeed.

NATO should move from a deterrence by reinforcement to a deterrence by denial posture.

2. Strengthen Deterrence

- Even though it is impossible to deter everything, it certainly is possible to lift the fog of unclarity over hybrid attacks that are aimed at avoiding detection by investing in attribution capabilities, both technical and forensic ones.
- This is necessary to identify actors conducting Computer Network Exploitation and even Computer Network Attack operations in one's infrastructure, and shed light on their modus operandi. Geopolitical expertise can help to 'connect the dots'.
- Note that attribution capabilities need to be matched by the political will to attribute – this is after all not a legal but a political act – which can be furthered by creating the interagency conditions to facilitate consultation, coordination and condemnation, both at the national level and the international level.
- This process in turn can be facilitated by the creation of international norms, aimed not just at shaping the behaviour of the opponent, but also at assembling the coalition of the able and willing to impose costs in case of transgression.
- And finally, it can be helped along by communicating up front what is unacceptable and what responses will follow. This can be done by codifying rules for the game in national strategies and doctrines, in high level political statements as well as in bilateral contacts, in regular exercises, and perhaps sometimes in small scale action, to showcase abilities and willingness.

NATO's Strategic Concept due in late June should take note of the developments in hybrid strategies and heed the recommendations above. In this way the Alliance is better equipped for the challenges of the future.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl