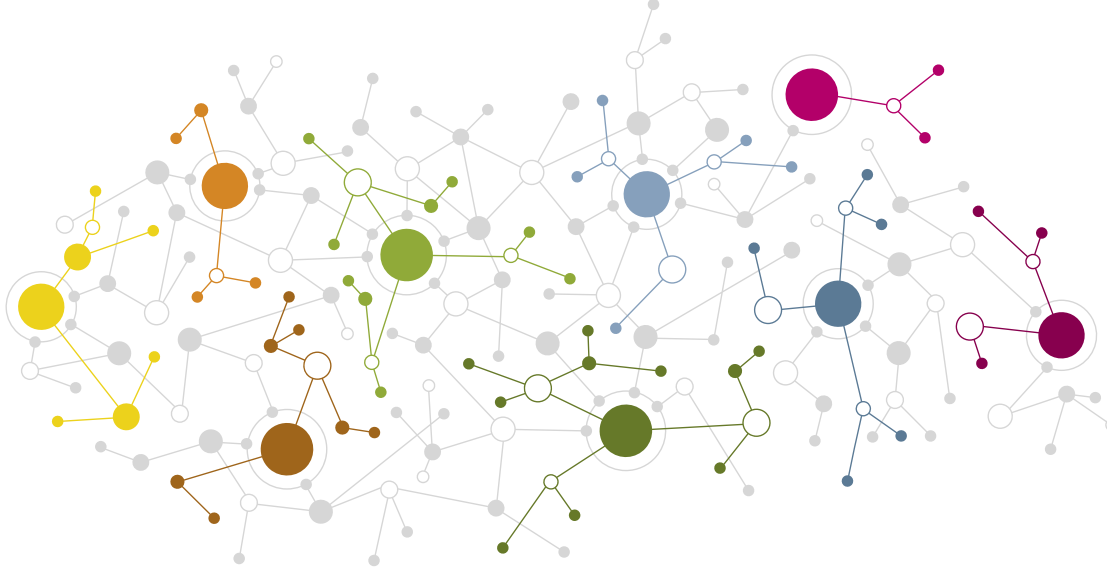
HYBRID CONFLICTS: THE NEW NORMAL?



TNO innovation for life

Frank Bekkers (HCSS)
Rick Meessen (TNO)
Deborah Lassche (TNO)

The Hague Centre for Strategic Studies

TABLE OF CONTENTS

INTRODUCTION

Manifestations of hybrid threats are in the news. The general public has become aware, maybe not of the full concept, but certainly of some of the more striking incidents. Institutions like NATO and the EU write policy papers and organize symposia and workshops to discuss it. Government officials warn us about it. But what exactly is this hodgepodge of little green men, disinformation campaigns, online recruiting of jihadists, cyber-attacks, strategic acquisitions, meddling with elections, etc.? This booklet will not give you the final answer. Not because we want keep it to ourselves, or that it would be too complicated for anyone but a small crowd of intimate experts, but for the simple reason that the very nature of the phenomenon itself makes it impossible to pinpoint what hybrid exactly is.

However, if you are a professional in the defence and security domain somewhat familiar with hybrid threats, looking for some structured way of thinking and discussing the phenomenon and suggestions for further reading: please read on! Or if you are personally interested in what 'geopolitics is back on the agenda' might mean for day-to-day processes within society - and how this might even affect your personal social media behaviour and daily news consumption - please read on! It is for you that TNO and HCSS have joined forces to create this booklet. We will discuss the What (What is it?), the Why (Why should we care?) and the How (How should we deal with its challenges?) of everything hybrid. We will raise a number of key issues and themes, and illustrate those with a number of examples to get a feel (rather than an exact description) of the subject and its issues.

We hope to answer some of your questions, but also leave you with new food for thought.

1. **HYBRID:** WHAT IS IT?

Hybrid threats – what are they? Hybrid threats (or hybrid warfare, hybrid conflicts, hybrid tactics, hybrid confrontations, hybrid operations and other hybrid 'things') involve the orchestrated use of a wide range of instruments of power to coerce an opponent, falling within the entire spectrum from peace to war. These instruments, such as cyber-attacks, economic blackmail, information warfare and exploitation of ethnic divisions, target various parts of society. Hybrid threats manifest themselves in quite different guises over time and with changing protagonists. Even the name of this 'new' (see Chapter 2 for a discussion on how new it really is) style of warfare is contested. 'Ambiguous', 'hybrid', 'irregular', 'political' and 'non-linear' warfare have all been suggested. Possibly the most accurate term for the phenomenon is 'multi-domain coercion'. By its very nature, the concept of hybrid threats defies fixed definitions. In fact, the European Union consciously refrains from using a formal definition because this might hamper the ability to conceptually and practically respond to the evolution of the real world manifestations of hybrid threats. It describes - not defines - hybrid threats as follows:

"Hybrid threats combine conventional and unconventional, **military and non-military activities** that can be used in a **coordinated** manner by **state or non-state actors** to achieve specific political objectives. Hybrid campaigns are **multidimensional**, combining coercive and subversive measures, using both conventional and unconventional tools and tactics. They are designed to be **difficult to detect or attribute**. These threats target **critical vulnerabilities** and seek to create **confusion** to hinder swift and effective decision-making. Hybrid threats can range from cyberattacks on critical information systems, through the disruption of critical services such as energy supplies or financial services, to the undermining of public trust in government institutions or the deepening of social divisions. As attribution is difficult, these challenges require specific and coordinated measures to counter; for example detection of the transfer of dangerous chemicals, reducing access to them, or decontamination."[1]

An example: hybrid or not? In June 2017, Greece blocked an EU statement on human rights violations by China, which was meant to be issued to a gathering of the UN Human Rights Council in Geneva. In order to issue such a statement, the EU needs the support of all 28 Member States. Greece refused to support the statement by saying that the EU should discuss this with China in private and not via the UN.

Critics say this is all because of the recent Chinese investments in Greece. For example, Chinese multinational COSCO owns 51 per cent of all stocks of the Greek harbour Piraeus. Fosun International, another Chinese multinational, has invested 200 million euro in the country and is working on one of the largest real estate projects in Europe, located at the old airport of Athens. Lastly, there is rumour of Chinese interest for taking over Greek state companies and banks that need to be privatized because of the countries poor economic situation.[2]

1 European Union. (2018). A Europe that protects: Countering Hybrid Threats, p. 1. Retracted from: https://eeas.europa.eu/sites/eeas/files/hybrid_threats_en_final.pdf
2 Visser, M. (2017, 9 May). Chinese investeerders geloven in Griekenland. Trouw. Retracted from: https://www.trouw.nl/home/chinese-investeerders-geloven-in-griekenland~ac8de71a/

SOME ESSENTIALS.

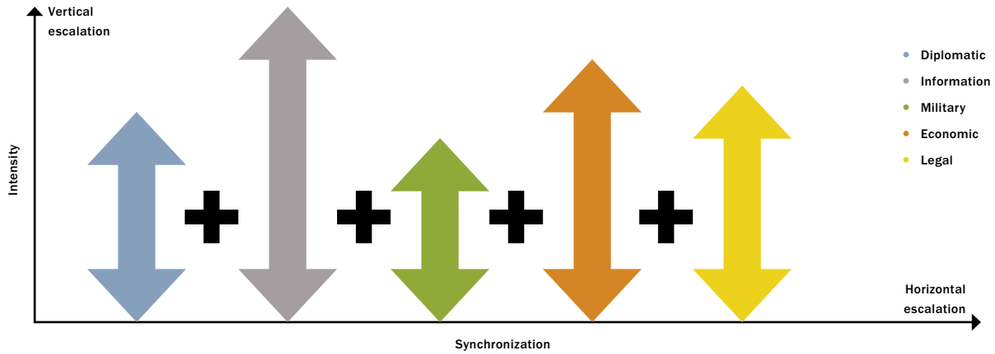
The EU description and the above example exemplify the wide ranging nature and, up to a point, elusiveness of hybrid threats. Nonetheless, a number of characteristics may be discerned:

- **Interstate.** Hybrid threats refer to (the confrontation between) state actors, or at the very least state-like actors[3], that possess or have access to a wide range of power instruments and the means to coordinate their use in targeting other states or societies. At the same time, hybrid activities are often exercised through covert methods and/or by non-attributable proxies - non-state actors that are tasked, supported or inspired by a state actor that remains behind the scenes and has plausible deniability for its involvement.
- **Asymmetric.** It is typically the weaker party that engages in non-military hybrid activities in order to avoid the opponent's superior military strength, and in covert hybrid activities so to lower the risk of retaliation. Political objectives are pursued without crossing the threshold of war, which would allow the stronger opponent to legally use its superior military force. Note that 'the weaker party' may change with the circumstances. Overall, Russia is militarily inferior to NATO, but is likely to have the upper hand in the initial stages of a military confrontation in the Baltics. Correspondingly, Russia uses hybrid tactics to test and possibly undermine the resolve of NATO; whereas NATO and the EU utilise a combination of military and non-military means to deter Russia from brinkmanship in the Baltic states.
- **Multi- and cross-domain (horizontal escalation).** The very word 'hybrid' refers to the variety of diplomatic, informational, military, economic/financial and legal instruments (often abbreviated as DIMEL[4]) that may be employed to affect elements of the target country's society, the so-called PMESIIP factors (political / governance, military, economic, social, infrastructure, information and physical environment). Furthermore, in the action-reaction chain, hybrid operations in a particular domain - say, cyber-attacks on government websites - may be countered with measures in a different domain - say, an economic boycott. Such horizontal escalation requires the coordination and release of control by different organizations in a whole of government or even a whole of society (WoG / WoS) approach.
- **Vertical escalation.** Next to horizontal escalation, hybrid actors typically move up and down the escalation ladder in what is called the 'grey zone' between war and peace, while avoiding the threshold that would lead to open (military) conflict. In doing so, hybrid techniques leverage conventional and attributable capabilities in threatening ways that reinforce the non-attributable efforts. Often the aim is to achieve military and political objectives rapidly, presenting a fait accompli – an outcome already accomplished and presumably irreversible – before an allied response can prevent it.
- **Probing, shaping, blurring and blending.** Hybrid activities are typically not outright attacks. With probing actions the defences and resilience of the target are tested. Shaping actions prepare the ground for possible future 'hot' confrontations. Blurring and blending actions are intended to create confusion, to remain invisible or to mislead (no clear attribution).

The different instruments of power, DIMEL, can be used in multiple dimensions and on multiple levels simultaneously. However, they are all aimed at the same goal and synchronized in order to strengthen each other. This is visualised in the figure above. On the horizontal axis, one can see the different kinds of instruments that can be used. On the vertical axis, the variety in the intensity of the use of each instrument is shown. Not every instrument needs to be used as intensely in order to achieve results. It is the optimal combination of instruments that counts most. Of course, the mix of instruments is also partly determined by the instruments available. The instruments of power used will thus depend on the capabilities of the hybrid actor and on the perceived vulnerabilities of its opponent, as well as the political goals of the hybrid actor and its planned ways to achieve those goals. In the process of using hybrid means, an actor can escalate by intensifying the use of a certain instrument (vertical escalation) or escalate by switching to a different instrument (horizontal escalation). The example below gives an impression of what a combination of DIMEL-instruments can look like.

3 Such as ISIS that, in its heyday, controlled significant territory where it exercised state-like functions such as raising taxes, issuing legislation and administering justice.

4 Also referred to as DIMEFIL, whereby the added 'F' stands for Financial and the 'I' for Intelligence. When using DIMEL, these factors are included under respectively the economic or the information instruments.



A combination of vertical and horizontal escalation of DIMEL instruments.[5]

EXAMPLE/CASES:

Russia's use of DIMEL instruments in Crimea

- **Diplomatic:**
  - Consistent denial of Moscow's involvement in the conflict and framing Russia as an interested power rather than a party to the conflict.[6]
- **Informational:**
  - Denial of involvement Russian troops.[7]
  - Exaggerated claims of Russia's military prowess and success.
  - Using Internet trolls to spread Russia's narrative and blacksheep Ukraine's leadership.
  - Use of Russian-language broadcasting tools for propaganda and psychological operations.[8]
- **Military:**
  - Snap exercises, done by little green men without insignes.[9]
  - Executing unannounced flights in NATO airspace.[10]
  - Threatening with using its nuclear weapons.

5 Based on the Multinational Capability Development Campaign's (MCDC) rapport 'Countering Hybrid Warfare - Analytical Framework' of 31 October 2016.

6 Renz, B. (2016.) Russia and 'hybrid warfare.' Contemporary Politics, 22:3. p. 288.

7 Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe, International Affairs, Volume 92, Issue 1, p. 175.

8 Kofman, M. & Rojansky, M. (2015). A Closer Look at Russia's 'Hybrid War.' Keenan Cable, no. 7 (Wilson Centre). p. 5.

9 Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe, International Affairs, Volume 92, Issue 1, p. 175.

10 Kearns, I. (2015). Avoiding War in Europe: The Risks From NATO-Russian Close Military Encounters. Arms Control Today. Available at: https://www.armscontrol.org/print/7244 [Accessed on: 31 October 2018].

- **Economic:**
  - Enforcing trade embargoes on the gas supply to Ukraine and Crimea.[11]
  - Targeting the Russian diaspora, making promises about pension money in Crimea.[12]
- **Legal:**
  - Defending the legitimacy of the referendum on Crimea for separation of Ukraine[13], by pointing to the supposedly-equivalent acknowledgment of the unilateral declaration of independence by Kosovo in 1990's by many Western states as a precedent.[14]

INTENTIONS VS. PERCEPTIONS - AT THE STRATEGIC LEVEL.

Whether a series of actions constitute a hybrid threat often entails an element of subjectivity and is open to interpretation. In his address to the Russian Parliament on 18 April 2014, in which President Putin justified the annexation of Crimea, he stressed the humiliation Russia had suffered due to many broken promises by the West, including the alleged promise not to enlarge NATO beyond the borders of a reunited Germany. Although it uses a different terminology, Russia sees the NATO enlargement as a 'hybrid threat', while NATO considers it a legitimate political choice made by sovereign countries. Furthermore, some actions are not only multi interpretable, but can indeed change character depending on geopolitical dynamics. In particular, many Chinese foreign investments have both an economical and a political rationale. While often left implicit, in certain scenarios the political rationale becomes visible and the associated activities may enter the realm of 'hybrid threats' for some observers. See the example above, in which it is claimed[15] that the Greek government's blocking of a joint EU statement to the UN Human Rights Council on Chinese human rights violations might have something to do with the fact that Greece has become increasingly dependent on Chinese investments since the 2008 financial crisis.

INTENTIONS VS. PERCEPTIONS - AT THE OPERATIONAL LEVEL.

The interpretation issue also plays at the operational level. We still lack shared metrics to unambiguously classify and quantify most hybrid activities - let alone unequivocally gauge a hybrid campaign. As an example, in January 2017 the French defence Minister Jean-Yves Le Drian warned that 2016 had seen 24,000 cyberattacks against French defence targets, and that the attacks were doubling every year. In the same month, EU security commissioner Sir Julian King said that there were 110 separate attempts to hack the European Commission's servers in 2016, a 20% rise on the year before; while NATO Secretary General Jens Stoltenberg claimed a monthly average of 500 threatening cyber-attacks against NATO infrastructure that required intensive intervention in 2016, an increase of 60% compared to 2015. Clearly, the figures are all over the place. This is not because France, the EU and NATO have completely different cyber-attack profiles, but because 'cyber incidents' are counted differently, using other standards and metrics. Is this a problem? Well, yes! Amongst others, it blurs the common picture of the seriousness of cyber-attacks, and therefore it is hard to agree on a common line of responding to cyberattacks. The legal definition of an attack is by international law defined through a threshold of significant death and/or destruction. According to most international law experts, this threshold has not yet been reached in cyberspace.[16] When we ever reach this point, do we then have the right standards and metrics in place ?

11 In 2014, a local gas company was first 'nationalized' by the authorities of Crimea, only to later become part of the Russian Gazprom. Russia also promised that Gazprom would finance an undersea gas pipeline to Crimea. (Stelmakh, A. (2014). The Crimean Crisis in Energy Terms. p. 3. Available at: https://ukraineanalysis.wordpress.com/2014/03/ [Accessed on: 31 October 2018]).

12 Kramer, A. E. (2014). Russia Raises Some Salaries and Pensions for Crimeans. New York Times. Available at: https://www.nytimes.com/2014/04/01/world/europe/russia-raises-pensions-for-crimeans.html [Accessed on: 31 October 2018].

13 Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe, International Affairs, Volume 92, Issue 1, p. 175.

14 Russia Today. (2014). Putin: Crimea similar to Kosovo, West is rewriting its own rule book. Russia Today. Available at: https://www.rt.com/news/putin-address-parliament-crimea-562/ [Accessed on: 31 October 2018].

15 See e.g.: Cumming-Bruce, N., & Sengupta, S. (2017, June 19). In Greece, China Finds an Ally Against Human Rights Criticism. Retrieved from https://www.nytimes.com/2017/06/19/world/europe/china-human-rights-greece-united-nations.html

16 Klimburg, A. (2017). The Darkening Web: The War for Cyberspace. New Jersey, United States of America: Prentice Hall Press.

IS IT WARFARE?

We prefer not to use the term hybrid warfare, even if this is a term often used in the media. Not because it isn't a real war[17] - that state in which a nation prosecutes its right by force - in which even those who don't want to take part have to behave in accordance with the laws of war[18]; but because the association with the (traditional) military ways and means to wage war is far too limited. Certainly in the Dutch translation of the term 'warfare' ('oorlog' or 'oorlogsvoering'), the association with the military is very strong. But while the military are part of hybrid warfare, they are not the only, and often not the principal, actor.[19]

TAKE-AWAY.

Hybrid threats are a dynamic phenomenon in many guises, impossible to clearly demarcate and often difficult to detect. Whether certain incidents are connected to constitute a hybrid conflict is partly in the eye of the beholder. A crucial issue is that the state actor behind a hybrid threat may use non-state 'proxies' to perform hybrid operations. In the end, behind a genuine hybrid threat sits the full range of state instruments, applied in concert across a range of domains, within the entire spectrum from peace to war. Recently introduced as a new term, hybrid threats are conceptually not new, but at the same time have acquired new dimensions and applications in the modern era. It is this new incarnation of an age-old way to confront opponents in the international arena that warrants focussed attention.

17 As Mark Galeotti, author of Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right, says: "The more I think about what we should be calling hybrid war, the more I think the answer is: war." See Pollock, J. O. H. N. (2017, April 13). Russian Disinformation Technology. Retrieved from https://www.technologyreview.com/s/604084/russian-disinformation-technology/

18 In this context, Trotsky's notorious epigram loosely translated as "You may not be interested in war, but war is interested in you" is very apt.

19 The Dutch ministry of Justice and Security therefore uses the t erm hybride conflictvoering (waging hybrid conflict) and, more recently, "A threat to national security by hybride conflictvoering". Within the Netherlands it is becoming usance to avoid the term oorlog (war) in association with hybrid activities.

Chinese companies invest large sums of money in Greek harbours. The price: having to prevent EU sanctions against China?

2. ‘HISTORY **DOESN’T REPEAT ITSELF**, BUT IT RHYMES’[20]: WHAT IS OLD, WHAT IS NEW IN HYBRID THREATS?

History rhymes ... Using a variety of power instruments in interstate confrontations is in itself nothing new. The famous general and military analyst Von Clausewitz (1780-1831) already pointed at this by stating: "War is the continuation of politics by other means". The Chinese military strategist Sun Tzu, who lived in the 5th century B.C., called it the supreme art of war to subdue the enemy without fighting. This could be linked to the use of disinformation. He advised to ‘appear weak when you are strong and strong when you are weak’ in trying to influence the enemy while avoiding open confrontation.

... But doesn’t quite repeat itself. So, although not new, the phenomenon of hybrid hostilities has acquired new manifestations in a globalized world that, by and large, has entered the information age. This requires rethinking of the subject in the current geopolitical landscape. The political, strategic, and technological contexts in which hybrid hostilities take place are not the same as they used to be. The new elements in contemporary manifestations of hybrid threats are in essence twofold:

- **Ends/targets:** States show an increased desire to avoid open military confrontation. The increased interconnectedness of a globalized world has made traditional wars less attractive. Think, for example, about how intertwined the world economy is today. This long-term trend is combined with the contemporary rise of national populism and strong men as leaders of great and middle powers, sometimes entertaining ‘zero sum gain’ world views. The combination has led to increased interstate confrontation, while falling short of open (military) conflict.[21] In addition, hybrid actors want to destabilize and cause friction in other states, but not at all costs (total war). They want to use subtle (de-)escalation mechanisms. So, for instance, closing down access to global markets and the ability to transfer money can be economically as devastating as dropping bombs and firing missiles against a state's infrastructure, without long lasting physical damage.
- **Ways and means:** The transition to the information age has led to the cyber and information domain emerging as the principal domain for hybrid threats and confrontations. Technological change and global interconnectivity has led attacks being done with more speed, on a larger scale and with more intensity. Most critical infrastructure today is connected to the Internet and, at least partly, operated and controlled remotely. Basic utility services such as electricity and water are prone to disruption and severe damage by cyber-attacks. The Ukraine power grid cyber-attack on 23th of December 2015 is considered to be the first known successful cyber-attack on a power grid. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers. With the advent of the Internet of Things, both industrial plants and domestic appliances have and will increasingly become targets. If almost everything is connected, a simple attack on one object can cause devastating cascade effects. Another phenomenon of the information age is that people have become dependent on smartphones to communicate with other people and services. This hyper connectivity allows for spreading fake news rapidly on a large scale. The Russian interference in the US elections demonstrates how a Russian troll factory, involving a small amount of IT/social media experts, could reach out to 126 million Facebook accounts by employing fake accounts. Facebook guessed that 120 fake Russian-backed pages created 80,000 posts, received by 29 million Americans directly, but reached a much bigger audience by users sharing, liking and following the post.[22]

TAKE-AWAY:
as a concept, the use of hybrid strategies and hybrid tactics to influence or coerce opponents is of all ages. However, continued globalization, the transition to the information age and rising geopolitical tensions have put new emphasis on hybrid hostilities that manifest themselves in a contemporary way.

EXAMPLES / CASES:

Hybrid tactics in Eastern Europe and WW1: nothing new.[23]
The role hybrid tactics played in the Russian infringement in Ukraine and the occupation of Crimea are well known, as is the fear of the Baltic States of becoming victim to the same tactics at some point in the near future. Let’s consider Estonia as a candidate target for Moscow. We would expect that the scenario will be as follows: Russian propaganda accuses the Estonian government of repressing the Russian-speaking minorities, following an incursion under the right to protect. Russian soldiers will enter the country in non-military clothing. Tallinn’s telecommunications will be targeted first. All hybrid tactics. However, this is not a future scenario but a throwback to 1924. Lenin had his sights set on Estonia, in order to annex the Soviet Union’s tiny neighbor. Occupying and controlling the telephone exchange can when sparking your imagination be compared to cyber hacking nowadays. And the ‘little green men’ of today are grandchildren of those Lenin ordered into Estonia.

If we even go further back to World War I, we see that the activities of code breaking and tapping into the undersea telegraph cables that linked London, Paris and Berlin resembles the digital espionage of today. Unrestricted submarine warfare and blockades resemble the economic sanctions of today. Propaganda labelled enemies as barbarians that committed endless atrocities against innocent civilians, while at the same time Zeppelins and Gotha bombers panicked Londoners with night-time terror bombings. Attacking random civilians in order to force governments to change their foreign policy, as was the goal of 9/11, is therefore also nothing new.

20 Quote by Mark Twain.
21 While direct military confrontations between the great powers are avoided, we see an (increasing) number of incidents, e.g. in the South China Sea between China en e.g. the US and Japan, and in the Baltics between Russia and NATO and EU countries Furthermore, great or regional powers participate - and occasionally engage with one another - in ‘proxy’ wars, such as in Syria and in Yemen.
22 Solon, O. (2017, October 31). ‘Russia-backed Facebook posts ‘reached 126m Americans’ during US election. 'The Guardian. retrieved October 15, 2018, from https://www.theguardian.com/technology/2017/oct/30/facebook-russia-fake-accounts-126-million.
23 Ullman, H.K. (2015, March 10). ‘Hybrid War: Old Wine a New Bottle?’ Huffington Post. Retrieved October 9, 2018, from https://www.huffingtonpost.com/dr-harlan-k-ullman/hybrid-war-old-wine-in-a-_b_6832628.html?guccounter=1

Renewed attention for hybrid tactics in this age.[24] Using hybrid tactics is, as shown above, an old way of warfare. However, the renewed attention for the method in this age started in 2006, in order to describe Hezbollah's strategy in the Lebanon war. Hezbollah is marked as a terrorist organization by the EU. The organisation was originally founded to fight for the liberation of South-Lebanon, after the occupation of the area by Israel in 1982 (Israel eventually left in 2000). Because Hezbollah consists of Shia militants, they have a strong connection with Iran, also a nation with a majority of Shia-Muslims. It is widely accepted as fact that Iran sponsors the group, for which Hezbollah in turn functions, at times, as a proxy of the Iranian state. However, they also have their own agenda.

During the Lebanon war, Hezbollah exercised hybrid tactics by using decentralized cells composed of guerrillas and regular troops. These regular troops were armed with weapons that nation states use such as precision missiles, rockets, armed unmanned aerial vehicles, and advanced improvised explosive devices. They communicated with encrypted cell phones, were able to take Israeli helicopters down and monitored Israelis with night vision and thermal imaging devices. Iranian special forces acted as mentors and suppliers. Next to acting like a proxy and having access to military goods, Hezbollah also dominated the perception battle by immediately distributing battlefield photos and videos through mass communication. Although the war resulted in an attack-free episode of several years for Israel - who had suffered over 200 attacks in the year before - Hezbollah was considered overall as the winner of the conflict, due to winning the perception war.

Hezbollah flag on missiles. The Lebanese militant group often functions as a proxy for Iran.

24 Piotrowski, M. A. (2015, March 2). 'Hezbollah: The Model of a Hybrid Threat.' Retrieved October 9, 2018, from https://www.pism.pl/files/?id_plik=19320

3. WHY SHOULD WE **CARE** (NOW)?

NOT BUSINESS AS USUAL.

Today's incarnations of the old concept of hybrid threats are not business as usual. In the digital domain, distances have disappeared; proximity is no longer a condition for exerting influence. This makes hybrid tactics a lot easier, much less conspicuous, and a great deal cheaper. It decidedly increases the variety of ways and means that can be employed in a hybrid campaign. Sophisticated military platforms tend to become ever more expensive with each new generation, a trend known as techflation. But the value proposition of the 'ugly stepsisters', various other (non-kinetic) means for creating strategic effects, has gone up dramatically. This gives a whole new dynamics to the whole hybrid phenomenon, providing hybrid actors the employment of 'cheap' hybrid tactics to exploit (western) societal vulnerabilities to create disunity and polarisation.

INFORMATION AND ICT-INFRASTRUCTURE AS A KEY VULNERABILITY.

Targets for hybrid operations reside wherever there are major societal vulnerabilities and the greatest asymmetry between the target's weaknesses and the source's strengths are found. In the information age, a nation's wealth is not just in tangible things, such as land, infrastructure and machines, but increasingly in intangibles such as information, IP, the educational system, and the knowledge economy (actually all relevant and critical functions for a well-being society). We have come to rely not just on physical assets to ensure our survival and well-being (such as dikes to keep the water out, roads to guarantee food supply, pipes for water supply and drainage, and cables for electricity), but increasingly also on digital services (that run on a physical infrastructure of their own). Furthermore, the physical and digital world have become intrinsically interwoven, with the physical domain very much dependent on information and guidance provided in the digital domain. Within our context, these facts lead us to two conclusions. First, competition between states is increasingly centred around information and knowledge as the key asset that determines a nation's competitive strength. Second, the whole information infrastructure, both the physical aspects (networks, servers, computers, data centres etc.) and the virtual aspects (the actual content of the various information systems) has become a key vulnerability and entry point for attack. With most of the information infrastructure being part of networks that, directly or indirectly, connect to the internet, these attacks can, in principle, be conducted from any other internet access point across the globe. This is what gives the age-old phenomenon of 'asymmetric warfare' a new face in contemporary 'hybrid threats'.

WAKE-UP CALLS.

On 17 July 2014, Malaysia Airlines flight MH17 crashed in the fields of eastern Ukraine after being hit by a Russian-made missile. 298 people lost their lives, including 196 Dutch. For the Netherlands, the downing of flight MH17 and the aftermath served as a wake-up call. It showed not only how a non-frontline state could be directly hit by tensions in the periphery of Europe, but also how Dutch society could become the target for modern disinformation campaigns. The MH17 incident also marked a Rubicon moment for the Russian disinformation machine: it was the first time that the full power of the state was trained on convincing the world to accept a false narrative of events, despite a preponderance of evidence to the contrary. Internet trolls, hackers, Kremlin-run media such as Russia Today (RT) and Sputnik, retired soldiers, public officials and anonymous programmers combined forces to

achieve a common goal: the discrediting of all those who claimed that Russia had some part in the missile attack. This has served as a catalyst for the Dutch government to think about how to organize its power instruments in a world of decreased interstate trust and with hybrid threats as a prime security challenge. We need to consider hybrid responses to hybrid threats: the integrated use of all instruments of state power to prevent, deter, mitigate or counter such threats (see Chapter 4).

For most of the Western world, the story of MH17 was a side issue. The Russian interference in the 2016 US presidential election, however, was all over the front pages. Emails stolen from the Democratic National Committee, sophisticated botnets, the use of fake Facebook accounts, similar attacks across Europe; the full extent of Russia's activities is still being uncovered. The realization that information has become weaponized and that some sort of information war is going on has now reached a substantial part of the population of Western countries.

A DYNAMIC PHENOMENON FITTING THE AGE.

Indeed, the most eye-catching instance of hybrid threats currently is Russia's '4D' approach: Dismiss, Distort, Distract, Dismay; never confess, never admit, raise confusion and keep on attacking. But the hybrid threat stemming for Russia certainly isn't the only one. Throughout this booklet, we describe a variety of real world cases of hybrid threats, giving an impressionistic image of a very dynamic phenomenon. These cases describe how the nature of international contestation is changing and will be fought out in today's world and the decade to come; and perhaps beyond that. It's an age where direct kinetic warfare - centred round military weapons 'that go bang' - is very expensive, in both political and economic terms; almost always prohibitively so. Instead, interstate rivalry will be fought out through a variety of means, many of which are covert, ambiguous and not habitually associated with 'war'.

TAKE-AWAY:
Our complex and open societies are increasingly vulnerable - i.e. offer ample entry points - for hybrid attacks, using modern technologies in a connected world to achieve effectiveness and efficiency. In practice, we see a (growing) number of incidents that can be classified as such, and/or point to probing and shaping actions for possible future attacks. Some of these are pretty clear cut (Russian influencing of the US elections, whether successful or not; Russian airspace intrusions). Others are more ambiguous (is Erdogan's Turkey a hybrid threat?). It may be argued that we - the West, NATO, the EU and the Netherlands - are in the 'grey zone' between war and peace, in which our strengths and weaknesses, political and societal resolve, and resilience - or lack thereof - are constantly tested by (hostile) hybrid operations.

EXAMPLES / CASES:

LikeWar: The weaponization of social media. In the book 'LikeWar: the Weaponization of Social Media', authors Peter Singer and Emerson Brooking (2018) describe how social media became a powerful weapon in conflict. Examples are, firstly, the Israeli defence led operation 'Pillar of Defence' against Hamas in the Gaza-strip in 2012. This could be identified as the first Twitter war. It lasted eight days, in which ten million Twitter messages were exchanged by online proxies in order to shape public opinion. In 2014, Al Shabaab attacked the Westgate shopping Mall in Nairobi, Kenya, and took several people hostage. The attack lasted three days, in which Al Shabaab tweeted the entire time. Because it took quite some time for the Kenyan authorities to react, Al Shabaab could use Twitter to influence the narrative of what was happening. Another example is the use of social media by ISIS. By mid-2014, ISIS started using social media to post videos of executions. After posting the video of the execution of the American journalist James Foley, research showed that more Americans were afraid of terrorism than during the immediate aftermath of 9/11. These examples show how powerful social media can be as a tool in conflict. As the authors put it: social media makes it possible to hack the people in the network, instead of the network itself.

Our neighbour Germany under hybrid attack of Russia
In our direct vicinity, Russia used hybrid tactics to discredit the German government and to create social unrest. Germany is the main initiator of EU sanctions against Russia in response to its March 2014 annexation of Crimea. Also, more recently, Germany has taken an increasingly assertive role within NATO, leading the multinational battle group in Lithuania under NATO's enhanced Forward Presence mission. Interestingly, Germany has a Russian minority of approximately 3 million, and in the East, many people take a positive stance towards Putin and Russia.

Germany has been under cyber-attack since 2015, almost daily. An example of how this has sought to influence Germany's public opinion is the Lisa case. In January 2016, rumours were spread on social media that a 13-year old Russian girl named Lisa was missing and had allegedly been raped by three refugees. Thanks to police investigations, it was discovered that the girl had been with a friend and had not been raped. However, Russian domestic and foreign media had already taken up the story and insisted it was true. Russian Foreign Minister Lavrov even accused the German authorities of a politically motivated cover-up of the story. This provoked uproar amongst Germany's Russian minority and right-wing sympathizers, who organized joint demonstrations in Berlin.[25]

Other examples include spreading conspiracy theories and the narrative that Germany is 'a puppet of the United States and NATO' by the German-language version of Russia Today. In December 2016, for instance, RT Deutsch reported that "the U.S. would deploy 2,000 tanks on German soil." In reality, the United States moved 87 tanks through Germany; and only to deploy them in Poland and the Baltic states. The infamous Russian social-media trolls are also active in Germany. Merkel's Instagram account was bombarded with abuse from thousands of Russian trolls just days after she set up her profile in June 2015.[26]

25 Meister, S. (n.d.-b). The "Lisa case": Germany as a target of Russian desinformation. Retrieved from https://www.nato.int/docu/review/2016/also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm
26 Sahin, K. (2017, July 26). Germany Confronts Russian Hybrid Warfare. Retrieved from https://carnegieeurope.eu/2017/07/26/germany-confronts-russian-hybrid-warfare-pub-72636

Influencing elections and people's opinions through the use of social media bots is a common tactic in hybrid conflicts. Is there enough public awareness and resilience?

4. WHAT ARE THE **KEY POLITICAL** AND **SOCIETAL CHALLENGES?**

IS THE WEST ABLE TO RESPOND?

Some observers hold that democratic principles and constitutional limitations hinder Western government's abilities to respond adequately to covert hybrid tactics aimed at undermining the values, norms, and institutions of the West. Robust responses are hampered because hybrid actions are primarily seen in terms of criminality, not in terms of transnational warfare. As a consequence, the threat is not conceptualized appropriately and the necessary security tasks, responsibilities and capabilities are not properly defined and distributed. This is something that also came out of the 'hybrid threats awareness' games TNO organised in 2017 and 2018 with a whole range of governmental representatives in attendance. In those games it became clear that most parties, up to a point, recognized and acknowledged the holistic and permanent nature of hybrid threats when confronted with them in the game scenarios, but that this realization hardly changed their behaviour. For instance, the municipalities are naturally concerned about the security of the Municipal Administration, but the distinction between a security breach by a 16-year opportunity hacker and intrusions with a more strategic character by a state actor - whether or not via 'proxy' parties - is hardly a consideration. Most parties look primarily at the National Coordinator for Terrorism and Safety (NCTV) and the Ministry of Defence (MoD) as problem owners for recognizing and countering (possible) integral hybrid threats. This applies a fortiori in low key hybrid confrontations where relatively harmless (in the short run) probing and shaping actions prevail, the possible coherence of various individual incidents is unknown or debatable and the involvement of state actors unclear. Both NCTV and MoD are seen as one of the few players that have, or should have, the mission, mandate and resources to consider (possible) hybrid threats and to put all relevant information pieces together ('connecting the dots') - and if necessary also to take action. But, in the Netherlands and in most Western countries, a comprehensive approach is lacking due to siloed mechanisms in government as well as public-private cooperation.

OVERVIEW OF CHALLENGES.

Conceptually, there are several key challenges our government and our society as a whole face in the context of hybrid threats. Leaving the international dimension aside for the moment, these challenges fall into four categories:

Recognizing a hybrid threat for what it is. It is difficult to provide conclusive proof of an orchestrated hybrid campaign, not in the least because hybrid actions are explicitly designed to stay under the radar, defy attribution or generate confusion. Furthermore, as discussed in Chapter 1, whether a particular incident or series of incidents constitutes a hybrid threat may be a function of the target's interpretation as much as the source's intentions. It often takes time to fully comprehend the extent of a hybrid threat.

Is this a hybrid threat? - "How China Got Sri Lanka to Cough Up a Port".[27]
As an alternative to force, in 2018 China assumed territorial control over a port and 15,000 acres of land in Sri Lanka, largely by means of its economic power. Under the burden of enormous debts and without feasible options to repay the loans, Sri Lanka saw no alternative to handing over the territory for 99 years, providing China with a strategic foothold along a critical commercial and military waterway.

It isn't war, but what is it? - "American Special Operations Forces Are Deployed to 70 Percent of the World's Countries".[28]
In 2013, US Special Forces were being deployed in over 130 countries throughout the world, with not only counter-terrorist raids and drone strikes in Somalia, Pakistan and Yemen, but also capacity building missions in Africa, mostly without a clear condition of war. Although, from our Western perspective, we do not tend to consider the American presence worldwide as a 'hybrid threat', the countries in question may beg to differ.

Mobilizing governmental and societal actors to act.
The Whole of Society targeting presents a great challenge to Western countries, as our siloed defence mechanisms do not work particularly well when the adversary strikes at soft targets throughout society. However, while autocratic nations may have an edge on the offensive side, all countries have an opportunity to organize their defences against hybrid threats. Since hybrid threats often have a long time horizon, this requires a process-oriented rather than an incident-centric approach. And because a hybrid 'war', unlike a conventional war, does not have a beginning and an end state delineating the 'war' period, defensive and possibly offensive (counter) measures have to be taken in the context of a normal political situation.

Coordinating cross-domain responses. Hybrid challenges are best met by hybrid responses, thereby capitalizing on one's own strengths and exploiting the opponent's weaknesses. A well-balanced, orchestrated use of the range of all measures in anticipation of and response to hybrid threats requires at least close intra-departmental and possibly supra-departmental monitoring, analysis, decision making and control functions. Certainly in the Netherlands, with its culture of independent departments, meeting cyber threats with economic measures (as an example) is not easy to organize. In practice, however, these kind of decisions need to be coordinated internationally. Decision making is then transferred to the EU, the NATO or the EU-US levels.

Taking a more active role in the game. This requires assets in place to deter the adversary, actions taken to deny adversary's access to their own and allies' instruments, and using one's own strengths to erode adversary's abilities to deploy hybrid operations. But we must be wary of going too far. Apart from the fact that uncontrolled escalation of events is in no nation's interests, Western countries should live up to their own norms and rules in order to remain credible - in the eyes of their own citizens as much as in the arena of international relations.

In the sections below, we elaborate on how to approach these four categories of challenges.

Situational awareness and situational understanding.
How do we 'connect the dots', i.e. detect and understand hybrid threats? Insights into how this threat is generated and orchestrated is essential for determining countermeasures and building resilience. This requires an integral and conceptual approach that combines knowledge of:

- the concept of coercion, ranging from strategies and tactics, and the effects that the opponent seeks to achieve through the use of a range of means in a variety of domains;
- international relations and the political and strategic culture of countries that apply hybrid tactics; and
- the strengths and weaknesses of the target countries.
  In the case of Russia, as an example, understanding the decision making system helps to see through the Kremlin's diversion-and-deception tactics, thus partly removing the element of surprise.

In particular, analysis and monitoring capabilities must be strengthened as part of a government-wide anticipation function to security risks and threats. Whereas in other areas the governmental role is to stimulate and facilitate rather than (trying) to control, in intelligence gathering and processing national intelligence agencies have a pivotal position, without denying the usefulness of open-source investigations performed by civil society actors such as Bellingcat.

Building resilience. It is important to build a more resilient society. This should not be viewed only as an extra burden, but also as an opportunity to get one's house in order. Why? Because the structures that allow a society to respond in an agile manner to hybrid threats can better cope with the complex underlying frictions that make our modern societies fragile. A more resilient society does not equate to a militarized or fear-driven society, but rather to a more functional one, as decision-making processes become more transparent and inclusive.

There are good international examples that may provide valuable benchmarks and lessons, such as the Finnish "comprehensive security" concept, in which there is a high alertness for hybrid threats in all societal domains and the ability to act cross-domain is provided. Of course this is inseparable from the Finnish geography and history. Inside the Kremlin House of Mirrors. How Liberal Democracies can Counter Russian Disinformation and Societal Interference provides insights into how to respond to Russia's hybrid activities in the information domain, based on case studies covering three 'frontline' actors, Ukraine, Latvia, and Finland, next to two international actors, the EU and NATO. One conclusion is that, instead of engaging in government-induced counter-propaganda, Western societies need to continue to rely to the power of free media and private organizations that reside outside governmental command structures.

People and organisations should be better equipped to deal with disinformation, fake news and 'algorithmic' online interference of the political discourse. J.W. Singer, author of Like War: The Weaponization of Social Media (2018), advises to employ a range measures, much like in public health, such as the equivalent of hygiene education, digital literacy, an emergency alert system, education programmes not only at schools, but also through, for example, public awareness campaigns. The targeting of superspreaders, the smaller subset of people who are at the core of viral outbreaks of fake news, is also part and parcel of a whole of society effort to inoculate vulnerable citizens against harmful misinformation.

A National Security Council? Last year, the authoritative Dutch Scientific Council for Government Policy (WRR, Wetenschappelijke Raad voor het Regeringsbeleid) recommended the establishment of a National Security Council (NSC), chaired by the Prime Minister, as the most appropriate official to guarantee focus and coherence of policy decisions and of subsequent actions.[29] The Scientific Council disputes the notion that smaller countries need no formal structures or plans because the number of stakeholders is limited, and therefore coordination can be arranged in a decentralized manner by careful interdepartmental power balance and/or through the interaction of individual functionaries. On the contrary, it argues, smaller nations by definition face a crow-

27 Abi-Habib, M. (2018, June 25). How China Got Sri Lanka to Cough Up a Port. Retrieved from https://www.nytimes.com/2018/06/25/world/asia/china-sri-lanka-port.html
28 Turse, N. (2017, January 5). American Special Operations Forces Are Deployed to 70 Percent of the World's Countries. Retrieved from https://www.thenation.com/article/american-special-forces-are-deployed-to-70-percent-of-the-worlds-countries/
29 Wetenschappelijke Raad voor het Regeringsbeleid. (2017). Veiligheid in een wereld van verbindingen. Een strategische visie op het defensiebeleid. (Nr. 98). Retrieved from https://www.wrr.nl/publicaties/rapporten/2017/05/10/veiligheid-in-een-wereld-van-verbindingen

ded internal and external security agenda and must therefore excel in strategy formation. This requires a powerful entity to structure and prioritize across a wide range of security issues stemming from the various departmental agendas. This recommendation, however, goes against the grain of the Dutch political culture. The Cabinet recently decided not to establish a NSC-like institutional structure.[30] Alternatively, the current interdepartmental consultation and coordination processes will be intensified, thereby to some extent establishing a networked NSC-like function. This networked approach can be flexible and powerful. But whether solid organisational structures with clear responsibilities and, if need be, the power to overrule and follow-through will not be sorely missed in times of real crises and tough choices remains to be seen.

International collaboration. Hybrid threats are forcing NATO and the EU to find new ways of working together.[31] "We have realised," says a NATO official, "that we are only part of the tool-box." The EU and NATO have managed to cooperate in the past. More than a decade ago, the EU took over stabilization missions in the Balkans that use NATO's command headquarters and planning capabilities. These arrangements allow NATO to support EU-led operations in which the alliance as a whole is not engaged. NATO and the EU also tried to form a civil-military partnership in Afghanistan, and both have deployed naval forces to fight Somali pirates since 2008.

Another example would be tighter cybersecurity collaboration within the EU and between the US and EU. Collaboration should include information and technology exchanges while also sharing exercises between militaries and civilian organizations. Private sector entities should also be involved.
The Centre of Excellence for Countering Hybrid Threats in Helsinki (2017) can be seen as another stepping stone. It functions as an international hub for practitioners and experts with the aim to assist both EU and NATO member states and institutions in understanding and defending against hybrid threats.

Respond 'in kind'. Up to a point, Western governments and societies can respond 'in kind'. We may dust off some old strategies, such as:
- Deterrence and containment.
- Partnerships in the EU neighbourhood.
- Capacity/resilience building in vulnerable countries.

In particular, the strategy of deterrence is very much back on the agenda. Old regimes and protocols from the Cold War are revisited; a whole generation of political and military leaders have had little or no experience with the concept. However, Cold War mechanisms no longer necessarily fit the new age. What does 'hybrid deterrence' look like? What, for instance, is the role of societal resilience? - after all, many hybrid activities target societal structures and processes.

Without in any way being exhaustive, other possible measures include:
- Continue to increase costs for 'hybrid' behavior. One form of cost imposing is economic sanctions. These need to be enforced closely while evasion mechanisms are identified and plugged. A particular apt measure is to deny source countries any Western developed dual-use cyber technologies.
- In addition to blocking access to Western capitals, safe havens for illicit funds should be denied, and flows of illicit funds should be more effectively blocked, as they serve Moscow's overall interests.
- Counterintelligence efforts should receive further resources to prevent any further penetration of Western societies by foreign intelligence agencies, and to begin to expose and roll back their existing networks in political, cultural, economic, and civil society circles.
- Greater transparency should be required from Western politicians, businesses, and civil society organizations to combat toxic economic connections, by which source countries penetrate our decision making systems and societies, corrupt them, and use them for their purposes.

TAKE-AWAY:
Hybrid threats impact all of society, requiring a coordinated whole of government – and even a whole of society – response. This is not easy to organise in typically siloed governmental structures; and without government control over societal stakeholders. The Netherlands organizes its emerging whole-of-government approach to security in line with its political culture: from the bottom-up rather than top-down. This might, however, provide insufficient follow-through power in the face of more severe hybrid threats. Building societal resilience and defence against hybrid conflicts, such as against disinformation, is still in its infancy, and needs focussed attention.

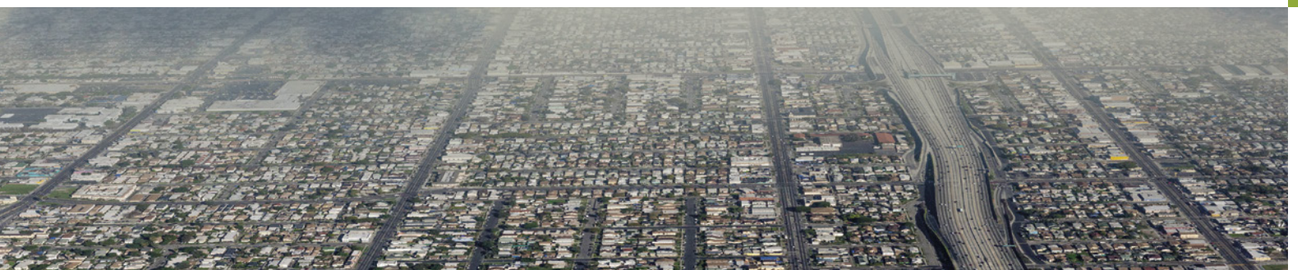
EXAMPLES / CASES:

Finland as an example of resilience.[32] The Finnish example in promoting societal resilience may be instructive for countering hybrid threats within the information realm. Russians are the second largest ethnic minority in Finland, and so there is ample Russian language media content available within the country. This has facilitated, in recent years, numerous fake news campaigns by The Kremlin. While direct measures to disengage informational cyber threats remain necessary, the Finnish case shows a whole-of-government approach based on educating key stakeholders is an effective way to build long-term resistance to disinformation campaigns.
In building resilience to Russian disinformation, educating actors at the governmental level was the first port of call in Finland. Multi-stakeholder collaboration was encouraged to increase understanding, demonstrated by the Government Communications Department receiving input from all ministries on a weekly basis on topics including Russian information operations. Furthermore, in 2015, a specific Committee was established to deal with Russia's disinformation practises.[33] The media in Finland are also important. Multi-stakeholder collaboration between government and media, such as through providing training, means that Finnish media outlets have become much more aware and critical of Russian behaviour. The government also works with private partners to develop a media landscape analytical dashboard, which will allow them to gauge different media sentiments, identify the dissemination of fake news, and tailor responses accordingly.

Priority is given to fact-checking messages with a potentially high impact for reaction, which the government says should ideally be countered within four hours of transmission. These practises mean that the Finnish government does not shut down Russian websites or radio stations spreading potentially harmful disinformation, but instead they approach these actors and provide them with a Finnish counter-narrative.[34] The Finnish outlook can be summarised as "[b]ecause society as a whole is being targeted and society as a whole needs to defend itself, the government acknowledges the need to involve as many stakeholders as possible."[35] This is seen in the multi-stakeholder collaboration at governmental level, and between government and media. The success of this approach is demonstrated by the Russian news agency Sputnik ceasing to operate in Finland due to failing to attract enough readers.

30 Minister of Defence. (2018b, March 28). Kabinetsreactie op het adviesrapport WRR 'Veiligheid in een wereld van verbindingen. Een Strategische Visie op het Defensiebeleid' [Kamerstuk]. Retrieved from https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2018Z05555&did=2018D21987
31 See also the EU-NATO joint declaration on Hybrid (2016), in which NATO and EU will combine hard and soft power to counter hybrid threats.
32 Extra reading: Nyberg, R. (2018) Hybrid Operations and the Importance of Resilience: Lessons from recent Finnish history. Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2018/02/08/hybrid-operations-and-importance-of-resilience-lessons-from-recent-finnish-history-pub-75490 [Accessed on: 31 October 2018].
33 Sweijs, T., Kertysova, K. & de Jong, S. (2017). INSIDE THE KREMLIN HOUSE OF MIRRORS: How Liberal Democracies can Counter Russian Disinformation and Societal Interference. The Hague Centre for Strategic Studies. p. 26. Available at: https://www.hcss.nl/report/inside-kremlin-house-mirrors-how-liberal-democracies-can-counter-russian-disinformation-0 [Accessed on: 31 October 2018].
34 Ibid., pp. 27-28.
35 Ibid., p. 30.

Current technological developments lead to a new and broader arms race, with civil actors as new players



5. WHAT ARE THE KEY **TECHNOLOGICAL CHALLENGES?**

HOW DOES TECHNOLOGY INFLUENCE THE USE OF HYBRID TACTICS?

In Chapter 2, we argued that the use of hybrid tactics is not altogether new, but that the ends and means have changed. Contemporary hybrid means can target specific communities very precisely. This enables hybrid actors to disrupt societies or states without causing too much collateral damage. In today's globalised world, after all, this collateral damage may well comprise their own interests. That is one of the major reasons why social media and cyber have become attractive as a means of exerting influence. These kind of developments point to the need for looking at existing and emerging technological developments from a 'hybrid' perspective. It seems that we have entered a new and different type of arms race. The conventional arms race was about weapon systems that cause physical destruction, such as bombers, submarines, tanks, artillery systems, and nuclear missiles. The current arms race is much broader, and includes weapons that create 'virtual' destruction or influence. In this new arms race, innovating cyber weapons or tools for targeting specific communities via social media with fake news has become as important as advancing conventional weapon technology.
Much of these innovations are based on market driven research and development. This also implies that the military should focus even more on commercial (civil) technology development. To a large extent, these developments are outside the purview of governments. Furthermore, access to the resulting technologies and applications is not restricted to the great powers. Smaller states, as well as non-state actors and terrorist groups, have access to state-of-the-art technologies fit for hybrid tactics. Therefore, a continuous tracking and assessment of technological developments within the civil sector is necessary in order to anticipate new ways and means for conducting hybrid activities.

TEN EXAMPLES OF 'HYBRID' TECHNOLOGIES.

To illustrate how civil technology can influence the military domain, the table below provides ten technological developments that can either evoke new hybrid tactics or empower existing hybrid tactics. Actually, the number of technological developments that will impact the manifestation and evolution of hybrid threats is far more encompassing. As always, the examples below underline the fact that technology is a two-edged sword, with both beneficial and detrimental applications.

The list is derived from TNOs yearly technology horizon scan, used by the Dutch ministry of Defence and currently extended for use by the ministry of Justice and Security. This horizon scan now includes more than 250 future technologies and innovations, all of which are assessed, for example, for their Technology Readiness Level and Impact in the military and/or security domain. This database can also prove useful for assessing current and future hybrid threats, when observed through a particular hybrid lens (see Chapter 6).

	Technology	Examples of hybrid applications
	Chemical, Biological, Radiological or Nuclear (CBRN) technologies	Invisible gasses that penetrate the skin without the victim noticing, subsequently manipulating the brain and influencing thoughts and behaviour.
	Manipulation of video: using a technique called real-time facial re-enactment, which enables the real-time transfer of facial expressi-ons from a person in a source video to a person in a target video	Manipulate videos in such a way that the audience watches a key leader making false statements, without noticing that it is fake and manipulated [see case-box below]. In the future, this could also be applied to a complete body, in order to make somebody appear 'live' on video while he or she is not there in real life .
	Artificial Intelligence: Intelligence demonstrated by machines and/or (semi-) autonomous systems	Employing (semi-)autonomous systems (drones, cyber weapons, etc.) for all kinds of tasks and missions, such as spying, disrupting the EM spectrum (radars, radios), but also to kill or neutralise persons and platforms. By using AI these systems can execute the assigned task or mission on their own, while being capable of adapting to new situations. Also, the attribution of responsibility, the who-is-behind-it, becomes difficult to determine.
	Quantum computing: Super-fast computers that utilise different algorithms to classical computers	Cracking cyber security codes with unprecedented speed, making cyber security even more difficult.
	The Internet of Things (IoT): The network of physical devices, vehi-cles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity, which enables these things to connect, collect and exchange data.	E.g. hacking future autonomous cars and traffic systems in such a way that the control of these cars and systems can be taken over. Once control is taken over the hacker can cause the cars to crash or to cause collisions in order to create chaos and casualties.

	Technology	Examples of hybrid applications
	Micro-targeting: The combination of several technologies (Big Data, IoT, Micro-robots etc.) in order to track, trace and eliminate (target) individuals	Employing slaughter bots[36] and use these to eliminate specific persons or groups. See case-box below.
	Malware: software that is used to disrupt computer systems, to collect sensitive data or to get access to private computer systems.	Manipulating air traffic control systems, resulting in operators who act upon false data and will issue wrong directions to pilots and aircraft, resulting in all kinds of dangerous situations.
	Bio-hacking: DNA sequencing and synthesis and the misuse of this	Creation of new biological weapons based on synthetic biology technology, such as viruses.
	Information revolution: increased global interconnectedness through internet, increasing access to infor-mation for all audiences	Videos on how to fabricate an IED on YouTube, but also enabling digital espionage for less sophisticated actors.

TAKE-AWAY:
Current hybrid actors will continuously exploit new ways and means of improving hybrid campaigns and their impact. They will look for new technologies or technological developments to incorporate these into hybrid strategies and means. For the EU, NATO and Western nations, often exposed to hybrid campaigns, it is eminent to anticipate these developments - and in particular the 'downside' of new technology, which can be used against them. Technology horizon scanning is, and remains, a powerful way of anticipating new developments in warfare in general, and hybrid threats in particular.

36 A video on slaughter bots was released on YouTube by the Future of Life Institute and Stuart Russell, a professor of computer science at Berkeley, on 12 November 2017, see https://www.youtube.com/watch?v=fPqmC16ewYgT

EXAMPLES:

Manipulation of video by using real time facial re-enactment. A technique that enables the real-time transfer of facial expressions from a person in a source video to a person in a target video. By doing so it is possible to take over the ad-hoc control of the facial expressions of the target actor. Combining this with recorded snapshots of audio, it is possible, for example, to manipulate videos in such a way that the audience watches a key leader, such as the US President, making false statements. For the audience the video seems to be authentic. In 2015 the University of Erlangen-Nuremberg, the Max Planck Institute, and the Stanford University were the first to publish a scientific paper on this novel approach and technique.[37] The first demonstrators have already been developed, and it is expected that the first applications employed in state-operated information campaigns will be used on short notice.

One step beyond this, is the real-time manipulation of a human body. It could create the perception that someone was at a crime scene or in a meeting in which he or she was actually not present. This would require everyone to have an alibi for every moment of his or her life, which is doubtful that one can succeed in this. The developments in this area can be speeded up when the entertainment industry will take it up. It will be difficult, apart from having an alibi, to prove that these videos are fake. It probably would require specific software that can determine authenticity of videos.

Micro-targeting. The concept of tracking and targeting specific individuals or vehicles. When using big data on IoT information and social media content, it could be possible to track and trace individuals almost everywhere and anytime. When using autonomous flying microrobots (the size of an insect), equipped with a small sensor and needles containing poison, one could not only track and trace an individual, but also eliminate an individual (temporarily). This would offer state actors and terrorist groups (even a single terrorist) huge opportunities to (temporarily) eliminate key leaders or persons without the chance of attribution. In particular, key persons that normally are well protected and not easy to approach would be at risk.

Microrobots are already operational, and it will only require a couple of years to develop a ubiquitous track and trace system based on IoT, Social media and Big data. Fitting the microrobots with micro sensors and weapons relies on developments in miniaturization and integration.

37 Thies, J., Zollhöfer, M., Stamminger, M., Theobalt, C., & Nießner, M. (2016). Face2Face: Real-time Face Capture and Reenactment of RGB Videos. Retrieved from https://web.stanford.edu/~zollhoef/papers/CVPR2016_Face2Face/paper.pdf

6. FINAL REMARKS: DEVELOPING AN EARLY WARNING FUNCTION

EARLY WARNING.
An important initial line of defence against hybrid threats is the early detection of signals that might point to hybrid activities being conducted or being prepared. These signals may trigger more focussed intelligence activities to further determine the nature of the possible threat, precautionary measures to minimize the potential for damage, or even pre-emptive counter measures. Below, we suggest three lines of development that might be pursued.

ASSESS 'HYBRID' TECHNOLOGIES.
As illustrated in Chapter 5, technological developments may generate novel ways of conducting hybrid activities. TNO already scans emerging and evolving technologies for potential impact on military/security threats applications. This technology watch and assessment (TWA) function is done on a regular basis for the ministry of Defence and, on a more ad-hoc basis, for the ministry of Justice and Security and the national police force. Based on this existing body of work, specific emphasis can be put on identifying and assessing technologies with particular 'hybrid' applications (defensive as well as offensive).

MEASURING HYBRID ACTIVITIES.
HCSS, together with the Clingendael Institute of International Relations, produces a yearly Strategic Monitor for the ministries of Foreign Affairs and Defence. The Strategic Monitor analyses trends and developments in the global security environment that may impact Dutch vital interests and values, partly based on quantifiable indicators that measure the propensity for instability and conflict worldwide and the strategic relationships between great powers, as well as between great powers and pivot states. In line with this effort, a valuable next step would be to build a framework to monitor and assess the level (quantitative) and severity (qualitative) of hybrid activities in Europe and in the Netherlands; and a dashboard to visualise this.

MEASURING SOCIETAL RESILIENCE.
As a mirror image of the above, creating a framework of quantifiable indicators for assessing the societal resilience against hybrid threats in Europe and in the Netherlands would be very helpful. It enables assessing a society's vulnerability against these threats and from there provides guidance for possible improvements and actions to be taken. In the end it would become less attractive for an actor to perform hybrid campaigning. This is actually reinforcing hybrid deterrence through societal resilience. In TNO's hybrid research programme (2019-2022, supervised by the MoD) the possibility of a dashboard providing such indicators will be explored.

KEY POLICY DOCUMENTS AND INITIATIVES

NL
Dutch Ministry of Foreign Affairs. (2018). Geïntegreerde Buitenland- en Veiligheidsstrategie.

EU
European Union. (2018). A Europe that protects: Countering Hybrid Threats.
European External Action Service. (2016). The EU Global Strategy.

The 'EU versus Disinformation' campaign
See www.euvsdesinfo.eu

The European Centre of Excellence for Countering Hybrid Threats
See www.hybridcoe.fi

NATO
EU-NATO Joint Declaration on Hybrid (2016).
Brussels Summit Declaration. (2018).

FURTHER READING

HCSS
- Bergema, R., Kertysova, K., & Roelen, M. (2018). Political Warfare by Russia. Global Security Pulse August 2018
- Rademaker, M., Sweijs, T., & Voorhoeve, J. (2017). Hoe beschermen wij ons tegen Russische desinformatie?
- Sweijs, T. & Kertysova, K. (2017). Inside the Kremlin House of Mirrors. How Liberal Democracies can Counter Russian Disinformation and Societal Interference.

TNO
- Duistermaat, M., Van Vliet, A. J., Van der Boor, R. A. E., & Van Daalen, A. F. (2017). Behavioural change as the core of warfighting - So now what? Militaire Spectator, 186(10), 424–438.
- Mente, R. & Kuijt, J. van de. (2017). Nederland blind voor hybride campagnes? Van nepnieuws tot militaire inzet. Magazine Nationale Veiligheid en Crisisbeheersing, 2017 (5/6), pp. 38-39.

TNO innovation for life

TNO.NL

18-10394 DECEMBER 2018