National Coordinator for Security and Counterterrorism
Ministry of Justice and Security

Χίμαιρα

An analysis of the 'hybrid threat' phenomenon

Reasons for declassification

This study, which was originally written in the autumn of 2016, was released for central government use in the first half of 2017, classified as 'restricted'. Given the ongoing relevance of this phenomenon and the need for parties outside central government to get to grips with it, the decision was made to fully declassify this report so that it can be read and used outside central government. It has not been revised or updated in the meantime, however. The examples cited therefore date mainly from the period of the initial, classified publication.

This analysis is based on content from a variety of sources, including research institutions, think tanks, foreign governments, the EU, NATO, the General Intelligence and Security Service (AIVD), the Defence Intelligence and Security Service (MIVD) and the National Network of Safety and Security Analysts. The AIVD and MIVD endorse the definition and concepts used in this publication.

'For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.'

Sun Tzu

Contents

Executive summary 6

The definition 9

Possible actors 15

Manifestations and potential consequences 18

What can we do to defend ourselves? 32

Executive summary

Although the term 'hybrid threat' is relatively new, the tactics it refers to are not. The concept has long been an element of interstate relations. In essence the term refers to threats that can assume various forms and impact on multiple national security interests simultaneously and thus pose a threat to national security. The word 'hybrid' refers to the use of a mix of tactics and to the threat's asymmetrical nature, polymorphous manifestation and wide-ranging impact. Given that recognition of the complexity and interconnectedness of threats is fundamental to our thinking about national security, the adjective 'hybrid' does not add anything new. To do justice to both the nature and origin of the threat, it is better to speak of 'a threat to national security from…' (e.g. 'hybrid conflict' or 'terrorism') than of 'hybrid threats', without any further qualification.

This document deals with the threat to national security from hybrid conflict, which is defined as follows:
A conflict between states that falls largely below the threshold of open armed conflict, and involves the integrated use of means and actors, in pursuit of certain strategic objectives.
This form of conflict is characterised by:

1. the integrated deployment of various military and non-military resources (e.g. diplomatic, economic and digital instruments), disinformation, manipulation, military intimidation, etc., which are among the set of instruments that states have at their disposal;
2. its function as part of a larger strategy/campaign;
3. the pursuit of specific strategic objectives;
4. the veil of misdirection, denial and ambiguity that often surrounds the actions in question, thereby making attribution more difficult and hindering an effective response.

The nature of conflict has evolved. This evolution is mainly the result of new technological developments turning new dimensions into 'battlefields'. Moreover, certain parties have become noticeably more active and increasingly deft at switching between instruments. Also new is the scale on which this integrated strategy is being deployed and the success it has had on the fringes of Europe.

The definition relates specifically to state actors, because it is highly improbable that non-state actors could meet the requirements for hybrid conflict (such as having strategic objectives or possessing sufficient state instruments to make the integrated deployment of such instruments possible). While they themselves do not meet the definition of instigators of hybrid conflict, they do fall within the scope of the definition, as 'instruments' (proxies).

This document uses real-world examples to outline the various ways in which hybrid conflict can manifest itself, explaining whether, and if so how, they can affect national security interests. The types of manifestations discussed are as follows: military, diplomatic and political, economic, digital, undesirable foreign interference (including political manipulation), and propaganda and disinformation. There has been a particular increase in the cyber and IT domain, due to the highly digitalised and networked nature of our society. Each of these manifestations has the potential to affect multiple national security interests.

Efforts to defend against hybrid conflict can be either specific or general in nature. In the case of the former, this means knowing your opponent, its strategic objectives and ambitions, its strengths and weaknesses, and connecting the dots. In the case of the latter, it means knowing your own vulnerabilities and acting with a view to limiting the *opportunities* of foreign powers, reducing the impact of hostile activities, and minimising your susceptibility to intelligence operations.

Χίμαιρα (Chimaera) or hybrid[1]

Background

Current developments in international relations, with certain state actors becoming increasingly aggressive in the integrated deployment of the instruments at their disposal, has necessitated further study of the phenomenon of 'hybrid threats', so as to enable the Dutch government to develop a position on the issue. The goal was to produce an analysis of the phenomenon that would:

- establish a definition;
- identify potential state and non-state actors;
- explain how this phenomenon can affect national security;
- give examples, wherever possible, of current manifestations of this type of threat.

1 The Chimaera is a figure in Greek mythology. It is a monstrous creature, composed of parts of different animals. In modern parlance the word can be used metaphorically to refer to an entity that is composed of parts of other (existing) entities. Another term for such an entity is a 'hybrid'.

The definition

The buzzword of the moment is 'hybrid'. Hybrid means the intermingling/combination or crossing of different things. This can occur in a variety of domains: biology (in animals as well as plants), technology, sport, etc.

Not a hybrid threat but a threat to national security

The term 'hybrid' is cropping up more and more in the security domain as well. People speak about 'hybrid threats', a term intended to encompass a wide range of events or phenomena with security implications. Depending on how it is used, the term may refer to migration, piracy, terrorism, ethnic conflict, Brexit, etc. This makes 'hybrid threat' an unwieldy umbrella term which muddies and confuses what could otherwise be a useful and substantive discussion. What is the added value of the term 'hybrid threat'? In essence the term refers to threats that can assume various forms and impact on multiple national security interests and thus be categorised as a 'threat to national security'. The word 'hybrid' refers to the use of a mix of tactics and to the threat's asymmetrical nature, polymorphous manifestation and wide-ranging impact (on multiple national security interests). Instead of referring to a 'hybrid threat', it is better to speak of a threat to national security. The complex and interrelated nature of threats is already a central part of our thinking about national security. The term 'hybrid threat' therefore adds nothing new and could even lead to confusion. As an umbrella term, 'hybrid threat' may mean one thing to one person and something totally different to another. To achieve and maintain clarity about what is being discussed, it is better to trace the threat back to its source and identify it accordingly. In one case it could refer to a systemic threat (such as Brexit), while in another it could refer to a terrorist threat.

So is 'hybrid warfare' a better term?

The term 'hybrid warfare' is slightly more concrete than 'hybrid threat'. Conventional warfare is an open conflict between states or within a state, conducted primarily – though not exclusively – by military means. In the case of hybrid warfare there is a blurring of the boundaries between war and peace; the battlefield is no longer a clearly delineated piece of territory. It usually involves the integrated use of conventional and non-conventional methods, open and covert activities and the deployment of military, paramilitary and civilian actors and means to create ambiguity and exploit the vulnerabilities of one's opponent so as to achieve geopolitical and strategic objectives. A hybrid conflict encompasses the integrated use of a wide spectrum of means, in the political, economic, military and intelligence spheres. Influencing and misleading opponents by means of information manipulation is a key aspect of hybrid tactics. Many of the activities that constitute hybrid warfare do not rise above the legal threshold[2] of armed conflict. Although this approach views the use of non-military means through a military lens, it does not mean that an approach rooted in the civilian domain would yield different insights. Both perspectives offer the prospect of conflict or aggression with the whole spectrum of instruments available to a state. The same semantic discussion is also playing out internationally, with 'hybrid warfare' being replaced by 'hybrid threats' so as to move beyond the purely military connotations of the former term.[3]

There are a number of interesting legal notions concerning opponents who avail themselves of the method of hybrid warfare, which do not feature in the various definitions but which clearly illustrate these actors' legal motives and options.[4] These include: making use of the complexity of international law on conflicts; exploiting the margin of legal interpretation associated with such laws; deliberately operating in under-regulated areas (such as cyberspace), or staying below the legal threshold of conflict. In other words, such actors deliberately operate in such a way as to remain below the threshold of what is generally qualified as 'armed conflict' in international law.

2 I.e. they fall below the threshold of what would generally qualify as 'armed conflict' under international law.

3 This international discussion also recognises the danger that an overly broad definition could become a meaningless umbrella term, while an overly narrow definition could be nothing more than a synonym for the Russian intervention in Ukraine.

4 Aurel Sari, 'Hybrid Warfare, Law and the Fulda Gap', in *Complex Battlespaces: the Law of Armed Conflict and the Dynamics of Modern Warfare*, March 2017, and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), Strategic Analysis January 2018: 'Blurred Lines: Hybrid Threats and the Politics of International Law'.

There is no single definition, but most[5] contain the following elements:

1. The integrated use of multiple military (convention and unconventional deployment) and non-military means, such as:
   - Military (conventional): e.g. concentration of troops on the border, for instance under the guise of alert exercises, military intimidation
   - Military (unconventional): e.g. non-identifiable troops (including special forces), private military contractors, 'volunteers' and proxies
   - Diplomatic: e.g. manipulating international structures by concluding/denouncing treaties or stalling/blocking decision-making in international forums
   - Economic: e.g. generating economic pressure, including by denying access to markets/energy supplies or interfering with commercial activity (including by military means)
   - Cyber activity (espionage, manipulation, attacks, sabotage)
   - Propaganda/disinformation
   - Influencing/manipulating/undermining (of intelligence)

Obviously, these examples are not meant to be exhaustive. In reality such an extensive toolbox is only available, in its entirety, to state actors.[6] While non-state actors can use one or more of these means, they cannot use all of them, limiting the range of capabilities at their disposal. The *diversity* of means employed is an essential quality of *hybrid* conflict, because of the varied mix that the term implies.

2. The aim is to achieve certain specific strategic objectives,[7] such as preventing Ukraine from joining NATO or the EU.
3. Orchestrated deployment as part of a larger strategy/campaign.
4. A key element of hybrid warfare is the veil of misdirection, denial and ambiguity that surrounds the actions themselves, making attribution more difficult and hindering an effective response.

5 As discussed in: European Parliamentary Research Service, 'Understanding Hybrid Threats', June 2015; https://www.hybridcoe.fi/hybrid-threats/; https://www.nato.int/cps/en/natohq/topics_156338.htm; Munich Security Report 2015; US Joint Irregular Warfare Center, 'Irregular Adversaries and Hybrid Threats: an Assessment-2011'; HQ, Department of the Army, 'Army Doctrine Publication (ADP) 3-0: Unified Land Operations', October 2011; Frank Hoffman, 'Conflict in the 21st Century: the Rise of Hybrid Wars', Potomac Institute for Policy Studies, December 2007. The last two of these centre mainly on mixed actors (state and non-state) and military capabilities, and on the nature of the conflict/mix of tactics. The Munich Security Report and the study by the US Joint Irregular Warfare Center, by contrast, focus more on the mix of instruments used (power instruments) and in that respect are similar to the NATO definition. These definitions stem from the military domain and view the use of civilian methods from this perspective, but it is also possible to view the concept from a civilian perspective.

6 See also the definition in the MIVD's 2016 Annual Report, p. 24, which also makes this distinction.

7 The MIVD makes a distinction between the use of hybrid warfare as an *end* and as a *means*. If it is used as an *end*, the focus will mainly be on influencing democratic decision-making processes. If it is used as a *means*, it should be seen as a strategic 'shaping operation' to acquire the most favourable possible political, economic and/or military position in the run-up to a conflict.

There are several observations to be made in this regard. To begin with, the integrated use of various means and methods in conflicts is not a new trend; indeed, it is as old as warfare itself. The concept of hybrid warfare, as it has been used since 2014,[8] is mainly a Western construct, resulting from Russia's successful intervention in Ukraine. In the context of Western thinking on conflict resolution, we also make use of a hybrid approach: the Comprehensive Approach, also known as the 3D approach (defence, diplomacy and development). You could say that hybrid warfare is like 'the comprehensive approach gone bad'.[9] What is new is the fact that since 2014 the threat has manifested itself on our borders and that the frequency, scale, level of aggression and success of such manifestations have taken us by surprise. An important substantive difference between the past and the present lies in the fact that the digital domain, including the scope for mounting 'influence operations' in a networked world, has acquired the status of 'battlefield'.[10] Thanks to the internet and social media, information operations have deeper penetration than ever before. They are quicker, reaching the target group more directly, and they can be modified in real time. All this makes them more effective. But does this new dimension, which is manifesting itself everywhere, warrant a new name?

Secondly, the term 'warfare' (wrongly) gives the impression that there is only a threat when a state of war exists. This suggests that aggressive, hostile actions undertaken by others in order to further their own agenda do not harm us unless we are in open conflict and headed for a state of war. It would therefore be better to speak of, for example, assertive (or aggressive) state action. Then it is clear that the assertiveness/aggression that is causing harm does not rise above the threshold of warfare, and also that even states that are our allies can act assertively, at the expense of our interests. The term 'assertive state action' was already being used, in line with international think tanks/research. All the means described above fall under the heading of 'assertive state action'. 'Assertive state action' does not necessarily imply the existence of a conflict: it mainly describes an assertive, sometimes bordering on aggressive, manner of promoting one's interests, whereby harm inflicted on other parties is considered 'collateral damage'. There is no deliberate strategy to inflict harm. In this way it can be distinguished from what is meant by hybrid warfare/hybrid threat, whereby the harm inflicted on others is intentional.

The term 'assertive state action' excludes non-state actors. Is this a problem?

There are other expressions that can be used to refer to the conduct of non-state actors. This more precise term clarifies the origin of the threat, without overlooking the relevant intentions, capabilities and possible impact, provided we remember that those intentions and capabilities may be evolving; out-of-the-box thinking and thorough analyses are indispensable in that respect. In recent years we have witnessed a growing threat on the part of states that deploy a range of instruments in an integrated way in pursuit of strategic objectives. At international level, there is a need to focus first and foremost on state actors. The distinctions implied by 'assertive state action' meet this need.

This term is also used in the National Risk Profile (NRP). The NRP specifically mentions hybrid threats as a phenomenon within a larger geopolitical context: 'The term "hybrid threat" is used to describe a conflict *between states*, usually below the level of armed conflict, involving the integrated use of a range of means: political, economic, sociocultural, military and intelligence-related. The aim is to achieve certain (specific)

8 The term 'hybrid warfare' has been in vogue for some time, and its popularisation is largely due to the work of Frank Hoffman in 2007. In that context the term referred mainly to the use of conventional and unconventional military means.
9 When the comprehensive approach is used to achieve illegal objectives or to achieve objectives by illegal means.
10 The globalisation and digitalisation of modern society means that the impact of economic and digital means tactics is greater than before (new arenas of interest). As a result, such means are being used more than ever.

strategic objectives, by means of influencing decision-making processes, among other things. To this end, the opponent's vulnerabilities are exploited. This is done by conventional and unconventional means, open and covert activities, using military, paramilitary and civil actors and means. The use of manipulated information for the purpose of influencing and misleading opponents is an important aspect of hybrid tactics. An important characteristic of such conflicts is often the deception, ambiguity and denial which accompanies the actions and which hamper attribution and response. An increase in this type of conflict has been observed.' The Hague Centre for Strategic Studies also prefers the term 'hybrid conflict' to 'hybrid warfare'.[11]

This raises the question: are we talking about a new phenomenon?

No – at least, not entirely. The use of unconventional means of warfare is as old as warfare itself. The ultimate objective is to strike the enemy, even if it means using clothes infected with smallpox,[12] the use of proxies[13] or the Trojan Horse. The integrated use of instruments of national power is nothing new. Even the practice of incorporating such ambitions into a larger strategy is not new. Nor is it the province of only one actor (the Russian Federation). In the US Army Doctrine 'strategy' is defined as 'a prudent idea or set of ideas for employing the *instruments of national power* in a synchronized and integrated fashion to achieve theater, national and/or multinational objectives'.[14]

What is so different now are the new technological possibilities, actors' increased skill at switching between various instruments, the scale on which this integrated strategy is being used, and the success it has achieved on the fringes of Europe. This marks an evolution in the nature of conflict: these technological advances are adding new dimensions, and the parties concerned are becoming more active.

Digitalisation and globalisation have opened up new arenas of interest, and as a result the impact of operations using, say, economic and digital means is greater than in the past. This has led to an increase in the use of non-military means. The use of information and influence operations, in particular, has also flourished. A key new aspect of this trend is digitalisation and the role that the internet and social media play in modern society. This serves as a catalyst for a great many 'traditional' tactics (e.g. espionage, sabotage and propaganda): they are now easier, cheaper and quicker to use, with a greater impact and added layers of ambiguity. It has been recognised for some time that cyber espionage is a growing problem. More recently, there has been a growing awareness of the dangers associated with the spread of disinformation via digital channels. The fact that the internet and social media make it possible to deliver a particular message *directly* to the target audience quickly, via various pathways and in various forms or voices means that propaganda/disinformation has grown in value as a weapon. This value is reinforced by the fact that people increasingly form their opinion on the basis of information on the internet and social media, where they mainly see their own world view confirmed. Attribution is very difficult in the digital domain, making it particularly suitable for covert operations.

11 'Coming to Grips with Hybrid Warfare', The Hague Centre for Strategic Studies, 2015, p. 12.
12 Used in the 18th century as a weapon by the British against Native Americans and against the American revolutionaries. Colette Flight, 'Silent Weapon: Smallpox and Biological Warfare', 17 February 2011, http://www.bbc.co.uk/history/worldwars/coldwar/pox_weapon_01.shtml.
13 There is a history of states supporting separatist movements or terrorist groups because this aided in their own strategic objectives.
14 Army Doctrine Publication (ADP) 3-0: Unified Land Operations, U.S. Department of Army, October 2011.

Conclusion: *The current use of the term 'hybrid' seems to refer mainly to the multiple guises that the threat can assume (including the cyber dimension).*[15] *The whole idea of national security is premised on a comprehensive approach to the threat, so as to ensure that complex threats are not underestimated and to foresee the possible manifold impact of simpler threats. To properly address the nature and origin of the threat, it is better to speak of 'a threat to national security posed by hybrid conflict', or 'by assertive state action' or 'by terrorism' than simply 'by hybrid threats', without any further qualification. Henceforth this document will deal with the threat to national security posed by 'hybrid conflicts', defined as a form of conflict between states, largely below the threshold of open armed conflict, involving integrated use of means and actors, in pursuit of certain strategic objectives. The need for a more in-depth interpretation of the phenomenon of 'hybrid threats' seems moreover to be prompted mainly by current international developments, whereby certain state actors are becoming increasingly aggressive with regard to the integrated deployment of the instruments at their disposal. The above definition meets that need.*

15 Whereas military specialists would say that hybrid tactics are less about the manifestation (the output) than about the integrated use of means (the input).

Possible actors

Which state actors make use of this integrated deployment of resources and actors to achieve their strategic objectives?

Obviously, there are many states that strategically deploy the various instruments at their disposal.[16] Not all states do so in the same integrated way, but a number of them have attracted attention on account of their high level of integration and activity, for example China and the Russian Federation. The activities of the Russian Federation have been particularly striking in the past few years due to their versatility, aggressiveness and frequency. There is little debate in international circles over the fact that Russia engages in hybrid conflict. Given the versatility and frequency of these activities and the clear use of military instruments, Russian activities are a particularly good illustration of how hybrid conflict works. Moreover, Moscow has elevated hybrid conflict[17] to the status of official strategy.[18] Reference is often made to the Chief of the Russian General Staff, General Valery Gerasimov, and his 'Gerasimov doctrine'.[19] It is not so much a doctrine as a meditation on the 'new generation of warfare'. For these reasons, examples from the Russian context are given below, even though there are also other states where manifestations of hybrid conflict have been observed. Wherever appropriate, references to these manifestations or states, which are active in the domain being discussed, have been added to the body of the text or the footnotes.

16 The most recent AIVD annual report mentioned China, Russia, Turkey, Iran and North Korea as countries that use the instruments at their disposal with malicious intent or in a way that harms Dutch interests. AIVD Annual Report 2018, 2 April 2019.

17 It is worth noting that in the Russian language, different terms are used, such as 'non-linear warfare'. The label 'hybrid warfare' comes from the West.

18 Because this is an official Kremlin strategy, employed in combination with Russia's activities in all arenas, Russian examples will be used in this document as an illustration: this makes it clear that actors exist that do indeed use the full range of the instruments at their disposal to achieve their objectives.

19 In the summer of 2014 Mark Galeotti coined the term 'Gerasimov doctrine', which has since taken on a life of its own, acquiring mythic proportions in the process. This was never Galeotti's intention; he was simply looking for a catchy title for a blog post. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

In February 2013 Russian General Valery Gerasimov formulated his ideas and ambitions on conflict in the *Military-Industrial Courier*, a Russian professional journal. In a speech and in this article Gerasimov expounded on the Western manner of warfare – as perceived by the Russians – and how the Russian Federation should arm itself against it. This was designated the 'Gerasimov doctrine', and its main features are as follows:[20]

- Blurring the boundary between peace and conflict; a very swift transition from one to the other.
- Twenty-first-century warfare/lessons from the Arab Spring: a well-functioning state can change into an arena of fierce fighting in a very short time (months/days), fall victim to foreign intervention and sink into a mire of chaos, humanitarian crises and civil war. This is typical of 21st-century warfare *[In his narrative Gerasimov frames the Arab Spring as the result of covert Western operations. The similarity with events in Ukraine is telling.]*.
- An increased role for non-military means in achieving political and strategic goals; they are often more effective than weapons.
- A shift in focus to the broad deployment of political, economic, information-based, humanitarian and other non-military measures. These are used in combination with *[or with a view to mobilising]* the population's 'protest potential' *[An interesting legal issue is that under international law a state is permitted to protect itself only against an outside threat, not a home-grown one.[21]]*.
- Waiting until a certain phase to openly use military means – under the guise of 'peacekeeping' or crisis management – particularly as a means to achieve the final victory *[In this way open armed conflict is a 'last resort'.]*.
- The advent of new military innovations at strategic, tactical and operational levels, thanks to new technology. The distinction between these levels and between offensive and defensive operations disappears. The defeat of the enemy's objects is conducted throughout the entire depth of his territory *[Nothing new under the sun, militarily speaking.]*.
- The prevalence of asymmetrical actions, which can be used to neutralise the enemy's advantages in an armed conflict [such as a better/larger army]. Asymmetrical actions include the use of special operations forces and internal opposition in order to create a permanent operational front throughout the territory of the enemy state, as well as information operations.[22] *[Note the deliberate use of internal opposition as a means of conflict. According to Gerasimov these new tactics can be found in the military doctrines of great powers and they are also deployed in practice, e.g. by the US in Iraq (in 1991 and 2003).]*.
- Major asymmetrical opportunities offered by the 'information space' to diminish the enemy's combat potential. North Africa is an example of how technology can be used to influence state structures and the population through information networks. It is necessary to perfect activities in the information space *[It appears that Gerasimov is alluding here to the role of social media in the uprisings in North Africa. The information domain is seen as a fully fledged combat domain, like land, sea, air and cyberspace.]*.
- The need to develop a system for the armed defence of state interests beyond your own national borders. Two ways of deploying your armed forces beyond your national border are 'peacekeeping' and humanitarian aid.
- The need for military science and leadership to be open to new ideas and non-standard approaches: however strong the enemy may be, there are always ways to defeat him. He will always be vulnerable in one way or another, and this means that there are adequate ways of fighting him *[Here we see a mix of pragmatism, opportunism and Realpolitik: use whatever means necessary to achieve your goal.]*.

20 Mark Galeotti, 'The "Gerasimov Doctrine" and Russian non-Linear War', https://inmoscowsshadows.wordpress.com/2014/07/06.

21 As Dr Aurel Sari (Senior Lecturer, University of Exeter, Director of Exeter Centre for International Law) stressed in his lecture, 'Legal Aspects of Hybrid Threats' at the European Security and Defence College course 'EU facing "hybrid threats" challenges', 6-8 December 2016.

22 But also the use of mercenaries/private military contractors, e.g. the 'Wagner Group' in Syria and Africa. The term 'information operations' refers to disinformation and psychological operations (PSYOPS), which are discussed in greater detail below.

Two things are worth bearing in mind in this connection: first, although this document uses the activities of the Russian Federation as an example, that country is by no means the only actor to use such instruments.[23] And second, Russia's actions are largely prompted by opportunism and pragmatism: its efforts are aimed not so much at creating suitable opportunities as identifying and exploiting them.[24]

Do non-state actors also engage in hybrid conflict?

No, as initiators (or perpetrators) of hybrid conflict, non-state actors fall outside the definition used in this report. This is because they are considered unable to engage in *true* hybrid conflict, as described by the definition. For example, it is highly unlikely that a non-state actor has specific strategic foreign-policy and security objectives or that it possesses the state instruments needed to pursue these objectives in an integrated fashion.[25] Although the media often characterise the actions of non-state actors as hybrid warfare, it is better to regard these actions as terrorism, insurgency, etc.[26] It should be noted that non-state actors are often themselves used as instruments (proxies) in hybrid conflicts.

23 For example, in recent years questions have increasingly been raised about China's economic activities: where in the past they were generally seen as benign, they are now perceived as instruments of broader Chinese interests and as (potentially) harmful to the national security interests of the West. China's ambitions and actions are also increasingly interpreted as an attack on Western values or as a threat to Western unity. See for example: 'Rethinking Security: China and the Age of Strategic Rivalry' in *China and the Age of Strategic Rivalry: Highlights from an Academic Outreach Workshop*, Canadian Security Intelligence Service (CSIS), May 2018; and MERICS and GPPi, *Authoritarian Advance: Responding to China's Growing Political Influence in Europe*, February 2018.

24 The idea that 'the Russians are behind it all' is a serious overestimation. At the same time it is good to keep in mind that 'being in conflict with the West' is the lens through which the Russian authorities view the world, and the events and developments in it.

25 In order for a strategy to qualify as 'hybrid', there must be a variety of instruments at play, but non-state actors are unlikely to have such a range of instruments at their disposal. It is always possible that future developments will bring non-state actors closer to falling within the definition. For example, the terrorist group ISIS had a broader spectrum of tools at its disposal than previous terrorist organisations; it also, of course, had aspirations of statehood.

26 Various experts have questioned whether certain terrorist organisations engage in hybrid warfare or pose a 'hybrid threat'. Opinions differ, however. Some authors who favour the term 'hybrid threat' for certain terrorist organisations as well, see the characteristics of a hybrid threat as follows: 1) the combination of 'conventional' military deployment with guerrilla tactics; 2) adaptability: the ability to adapt to changing combat conditions; 3) the use of terrorism; 4) propaganda & information warfare; 5) criminal activities (to generate funds); 6) disregard for international law. Some scholars and analysts have judged ISIS or Hezbollah by these criteria, as they possess some of the instruments associated with states, concluding that such organisations are also engaging in hybrid conflict. See, for example, Scott Jasper and Scott Moreland, 'The Islamic State Is a Hybrid Threat: Why does That Matter' in *Small Wars Journal*, December 2014. The question is whether this categorisation is correct; the terms 'hybrid threat' and 'hybrid warfare' are being stretched beyond the point of usefulness.

Manifestations and potential consequences

This section will look more closely at the various manifestations of hybrid conflict and how they can threaten or harm national security.

What national security interests are at play?

In 2007 the Dutch government adopted the National Security Strategy, a new approach to better protect national security.[27] According to the Strategy, 'national security is at stake if the national security interests of our society and/or state are threatened to such a degree that there is a (potential) threat of social disruption'. The Dutch government has committed to protecting the following interests:

Territorial security can be compromised in various ways: if part of our territory is rendered unusable or inaccessible for an extended period of time (e.g. due to a flood); or if the Netherlands' international position is compromised economically or politically (e.g. due to an international conflict or undesirable interference in the commercial sector); this interest can also be harmed by actions that seek to undermine the integrity of cyberspace[28] or of allied territory.

Physical security is at risk if there are casualties[29] (above a certain threshold) or a lack of basic necessities.

Economic security is compromised when the vitality of the Dutch economy is undermined by unemployment, a decline in confidence, non-operational sectors or if the Netherlands suffers financial/economic damage.

Environmental security is compromised when serious harm comes to the environment's ability to regenerate.

27 The National Security Strategy is central government's risk-management instrument, designed to better protect the national security interests of Dutch society and, in the process, to prevent social disruption resulting from a crisis. The Strategy applies the same analysis to different types of disasters and crises with a view to comparing them and consequently making more well-founded policy choices. For more information (in Dutch) visit: https://www.nctv.nl/organisatie/nationale_veiligheid/strategie_nationale_veiligheid/documenten.aspx.

28 This is compromised when the availability, confidentiality and integrity of essential information systems (e.g. the Personal Records Database) is affected. The process control systems of critical infrastructure are also considered an essential information service.

29 Fatalities, people with serious injuries and people who develop chronic conditions (including psychiatric disorders).

Social and political stability is compromised by disruptions to the daily lives of ordinary people, the undermining of democratic institutions[30] and norms and values, and destabilisation of the country's social climate. Disasters that disrupt critical infrastructure can quickly lead to serious disruptions to daily life. For large groups of people this means that for a certain period they cannot take part normally in society (i.e. work, school or social activities). Incidents or developments that lead to widespread public anxiety and/or anger (socio-psychological impact) can also harm social and political stability.
The international legal order is at risk when certain underlying principles of the post-war international legal order are compromised, including the norms of state sovereignty, peaceful co-existence and the settlement of disputes, as well as the effectiveness and legitimacy of multilateral institutions, such as the IMF, the UN, NATO and the EU.[31] This can occur, for example, as a result of the manipulation of elections, the undermining of fundamental principles of multilateral institutions and the paralysis of the decision-making of such institutions.

What means are used? How do they manifest themselves? What national security interests are compromised?

As described above, the 'hybrid' label applies to the integrated deployment of the whole range of instruments available to a state, including the following.

1. Military manifestations

Military manifestations can be subdivided into various categories:

A The demonstrative deployment of conventional military assets, such the concentration of troops on the border, for instance on the pretext of conducting alert exercises (messaging, intimidation). In recent years the Russian Federation has shown that it can rapidly deploy sufficient combat power to one of its borders in order to engage in a regional conflict. We have seen this along the Ukrainian-Russian border, and along the border between the EU/NATO and the Russian Federation.[32] Such a display of military power is sometimes referred to as 'strategic messaging'.[33] EA good example of this is the deployment of (strategic) bombers and fighter aircraft along the borders of and in the areas of responsibility of NATO Allies, often without their transponders switched on.[34] The purpose of these activities is to send a strategic message: demonstrating military capabilities for the purpose of deterrence and intimidation (regional deterrence).

30 External manipulation of political processes can compromise democratic institutions' ability to function and thus social and political stability.
31 The importance of the international legal order is also connected to the international financial and economic system and the functioning, legitimacy and observance of international human rights treaties.
32 Such as the transfer of a missile system to the Russian exclave of Kaliningrad. The missiles in question, which can be equipped with nuclear warheads, have a range of over 500 km, which is enough to reach the capitals of Poland, Lithuania and Latvia. This has led to concern in these countries: 'Rusland plaatst raketten aan Poolse grens' (Russia stations missiles on Polish border), *Het Parool*, *Nederlands Dagblad*, 11 October 2016. An Estonian military expert has gone so far as to claim that there is no comparable weapon in the Western arsenal. It should be noted that NATO also conducts exercises along the border with the Russian Federation, 'NAVO tart Rusland met grootste oefening ooit in Oost-Europa' (NATO provokes Russia with biggest-ever exercise in Eastern Europe), NOS.nl, 6 June 2016.
33 Strategic messaging: expressing extreme displeasure at security-related developments by flaunting both conventional and nuclear military assets, MIVD Annual Report 2016, 24 April 2017. Examples of this include: sending fleets to patrol the North Sea, submarines in the Kattegat and North Sea, military aircraft entering EU/NATO airspace without a flight plan or transponders (thus posing a danger to civil aviation) and exercises directed against NATO. Sweden is an ideal target in this regard, as it is a member of the EU but not NATO, so there is no risk of article 5 of the North Atlantic Treaty being invoked.
34 For example, the violation of Finnish airspace on 7 October 2016.

B Another instrument used is military interventions under the guise of peacekeeping or humanitarian aid. Russia's military intervention in Syria, at Bashar al-Assad's request and thus permissible under international law, successfully thwarted Western efforts. The situation in Syria has become more volatile, and the flow of refugees into the EU has increased (putting additional pressure on EU solidarity). The unconventional use of military means, such as unidentifiable troops, special forces, private military contractors and 'volunteers' is another notable feature. Of course, we have seen this in Ukraine, with disastrous consequences for that country: a (frozen) civil war.

It is also clear that other state actors also use such military tactics, below the threshold of armed conflict, to send strategic messages, as witness China's military activity in the South China Sea.[35] This is a disputed area: multiple countries have claimed waters and islands in this region.[36]

Potential consequences

These kinds of tactics can put pressure on the interests of the international legal order, due to their potential to undermine the fundamental principles of the international regime or lead to paralysis of decision-making within multilateral institutions. The current practice of strategic messaging entails risks:

- To begin with, these activities damage international relations, with the attendant risk of escalation and misunderstandings, or misinterpretation of the actions in question, which could trigger an armed response – for example if article 5 of the North Atlantic Treaty is invoked and this leads to an open military conflict.
- A risk to civil aviation is posed by military aircraft without transponders on that are engaged in strategic messaging activities.[37] It is not mandatory for military aircraft to operate with transponders on, but if they do not, this can lead to risks to civil aviation, especially in relatively tight airspace, like the Baltic Sea region. Dutch airspace is also small, but there is far less military air traffic here than over the Baltic Sea.
- Strategic messaging activities involving nuclear material heighten the risk of a nuclear incident with long-lasting repercussions for physical and ecological security in the area.

The military intervention in Syria has put pressure on Western alliances (NATO and the EU) because of its secondary effects (refugee flows). Incidents resulting from the crowded Syrian conflict zone could lead to escalation. A case in point was the downing of a Russian aircraft by the Turkish air force for violating Turkish airspace in November 2015. Turkey is a member of NATO, and this incident caused great consternation within the Alliance over a possible escalation with Moscow. This raises a difficult question: what sort of violation, involving which NATO Ally, would justifying invoking article 5? Debate and doubt surrounding this issue undermines the solidarity of the Alliance, and that is precisely one of the Kremlin's strategic objectives. The intervention also hamstrung Western efforts to further the peace process.

35 See, for example, 'Militaire oefening China zet conflict Zuid-Chinese Zee op scherp' (Chinese military exercise ramps up South China Sea dispute), *Trouw*, 5 July 2016 and 'Filipijnen roepen op tot "zelfbeheersing en nuchterheid" in de Zuid-Chinese Zee' (Philippines calls for 'self-control and restraint' in South China Sea), *Het Financieele Dagblad*, 13 July 2016. A week before the Permanent Court of Arbitration in The Hague was due to issue a ruling on Chinese actions in the area, China held military exercises there, thereby sending the signal that they did not intend to take any notice of an unfavourable ruling.

36 Other countries have made either territorial claims (on the Paracel and Spratly Islands) or maritime claims (on the sea and the seabed): Vietnam, Taiwan, the Philippines, Brunei and Malaysia. This is closely related not only to economic interests tied to trade routes, fisheries and oil and gas reserves, but also to geopolitical relations, military expansion and the right of free passage under international law.

37 In November 2014 both NATO and then foreign minister Bert Koenders warned about this possibility, because the number of airspace violations had tripled in comparison to the previous year. In such situations the pilots were not in contact with European air traffic control, they did not submit flight plans and they had turned off their transponders, which meant passenger aircraft could not see them coming. 'Koenders waarschuwt voor Russische luchtmacht' (Koenders sounds warning about Russian air force), *Trouw*, 24 November 2014. In 2014 various media outlets reported on incidents where civil planes had to take evasive measures to avoid Russian aircraft.

With the unconventional deployment of military assets in Ukraine, Moscow achieved one of its strategic goals: Ukraine is weak and divided and will not join the EU or NATO as long as the conflict there continues.[38] In this way these tactics could have an impact on the independence and policy of an alliance that is important to the Netherlands. A weakening of alliances to which the Netherlands belongs does not bode well for our international position and our efforts to promote our interests in the international arena.

2. Diplomatic and international political manifestations

The primary manifestation in this category is the suspension or denunciation of treaties.[39] However, it also refers to the use of delaying tactics in international forums (e.g. the UN Security Council), for the purpose of blocking or stalling decision-making, ideally in collaboration with parties that share the same anti-Western sentiments.[40] By forming alternative/competing alliances in existing, Western-dominated structures, an attempt can be made to create a new arena with different rules, which Moscow can then dominate. There are other state actors, like China, that would like to see Western-dominated rules marginalised.

Potential consequences

This has potential consequences for geopolitical relations. In the event of ongoing polarisation, it is possible that Vladimir Putin will go further in his pursuit of allies against the West, the US, NATO /the EU. As a member of various international organisations (e.g. the UN and the Council of Europe), the Netherlands will feel the effects of any such actions (e.g. the blocking or thwarting of decision-making in forums of which the Russian Federation is also a member). There could also be consequences for Western alliances that will be felt in the Netherlands, such as the stationing of additional troops in the eastern part of NATO/the EU, to which the Netherlands – as an ally – would have to contribute.
There will be tangible repercussions for Dutch-Russian relations as long as cooperation in numerous areas is suspended, including with regard to a number of agreements of importance to the Netherlands.

3. Economic manifestations

Russia has a broad range of economic instruments[41] at its disposal, the potential effects of which differ from country to country. The aim is to generate economic pressure on the target. In Western democracies, the economic impact on the general public would be more likely to influence government policy than it would in the Russian Federation.
The term 'economic instruments' refers to the following:

- limiting access to markets/trade routes/raw materials/energy supplies;
- disrupting commercial activities (possibly by military means);
- foreign takeovers/investment, with a view to influencing/manipulating the continuity of vital sectors, the integrity and exclusivity of information and the functioning of the democratic legal order;
- creating strategic dependence by monopolising essential raw materials (oil/gas/rare earth metals) and transit routes;
- imposing economic sanctions/boycotts.

38 If Ukrainian accession was an aim of NATO/the West, this has frustrated it. (It has never been stated that accession was indeed an aim.)
39 Such as the suspension of the US-Russia Plutonium Management and Disposition Agreement on 3 October 2016.
40 Without greater geopolitical authority Russia can do little more than sabotage Western political efforts.
41 It should be noted here that China has much deeper pockets than Russia and flexes its economic muscle all over the world. Questions can be raised about the underlying motives and the local impact. For more on this, see 'Belt and Road projects direct Chinese investments to all corners of the globe. What are the local impacts?', *Washington Post*, 11 September 2018.

Chinese economic activities are an outgrowth of its economic policy plans, such as Made in China 2025 and the New Silk Road (Belt and Road Initiative), through which it is seeking to broaden its economic and geopolitical influence.[42] China employs a wide range of (covert) methods, including economic espionage (in some cases by digital means).

Potential consequences

These instruments are used to generate pressure on individual countries in order to influence their policy and position vis-à-vis Moscow, and to play the members of alliances like the EU and NATO off against each other. This can prompt debate, especially in cases where a particular instrument hits certain member states harder than others, and this instrument can function as a wedge to break up European solidarity. This wedge function has three aims: 1) to erode support for European sanctions against the Russian Federation; 2) to sow discord within the EU and 3) to sow discord between the EU and the US.

Effects on energy supply security. The Kremlin could decide to deploy the energy weapon in response to international sanctions, although this is a double-edged sword which would have a major impact on Russian interests. Russia's dependence on oil and gas income is so great and the EU such an important customer for gas that it is unlikely that suspending gas deliveries to the EU would be a real option. Nevertheless, the EU is developing a European energy supply security strategy to reduce its dependence on Russian gas. This is also the subject of lively public debate, as witness the discussion on Nord Stream 2. Depending on how the plans set out in this document are put into practice, there may be consequences for Dutch gas extraction.

As a part of an international/global system, the Netherlands will suffer economic effects if the world economy is impacted by, for example, reciprocal economic sanctions, the shut-off of gas supplies and capital flight from Russia. But the Netherlands also faces the economic effects of the downturn in bilateral trade relations with the Russian Federation. A possible result of China's use of economic tactics to further its own interests is a reduction in the earning capacity of Dutch companies.[43] Over the long term such activity could even result in economic and political dependence.

4. Digital manifestations

This category does not so much encompass a specific instrument as a domain within which various instruments can be deployed. The AIVD has noted that Iran, North Korea, Russia and others have engaged in sabotage and/or misuse of IT infrastructure.[44] China, Iran and Russia have been shown to have offensive cyber programmes that target the Netherlands.[45] Moscow – and NATO as well – treats cyberspace as a new arena of conflict,[46] which takes its place alongside the existing arenas (military, political and economic). It also uses this domain in combination with military assets.[47] Moscow recognised the importance of cyberspace early on, investing substantially in offensive cyber capabilities, and is now a formidable opponent in this new domain.

42 AIVD Annual Report 2018, 2 April 2019.
43 China takes an interest in Dutch businesses in certain sectors in particular: high-tech, energy, maritime and life sciences & health. Ibid.
44 Ibid.
45 Ibid. We use the term 'offensive cyber programme' when states employ digital assets for the purpose of espionage and sabotage in pursuit of their own political, military, economic and/or ideological goals at the expense of Dutch interests.
46 NATO recently added cyberspace as a military domain, alongside land, sea, air and space.
47 As happened during the annexation of Crimea, when the main Ukrainian government website went down for 72 hours as a result of a cyberattack. Georgia experienced something similar in 2008. *Putin's Cyberwar: Russia's Statecraft in the Fifth Domain,* Policy Paper no. 9, Russia Studies Centre, May 2016.

Moscow deploys cyber capabilities for a variety of goals: to dismiss or distort information; to disorient countries; to distract from or support its own military activities and to disrupt civil infrastructure.[48] Russian hackers have carried out attacks on targets including governments, international organisations, industrial installations, financial institutions and the media. Over the past few years there have been various incidents that illustrate the use of cyber capabilities for purposes of manipulation, sabotage and disinformation:

- **The hacking of the Democratic National Committee (DNC)** The Americans publicly accused Moscow of involvement. According to some analysts the purpose of this campaign was to influence the presidential campaign in favour of Donald Trump, while others believe that the purpose of the leak was to disrupt and discredit the American political process more generally.
- **Cyberattack on the Bundestag** The network of the German parliament was subjected to extensive infiltration. The majority of the network – several thousand computers – had to be completely replaced. It took at least 15 weeks before the network was up and running again, with infected systems reinstalled and functionality restored. Most sources have attributed the Bundestag hack to a Russian state actor.
- **Cyber sabotage at TV5Monde** This attack succeeded in disrupting broadcasts and sabotaging the systems of the broadcaster. The hackers also posted an image on their website captioned *'Je suis IS'*, and divulged the CVs of members of the French military. The attack was carried out under the name of the 'Cyber Caliphate'.[49] On the basis of technical indicators, however, security firms traced the attack to an espionage campaign that multiple researchers have attributed to a Russian state actor. The same campaign was generally linked to attacks on military targets, security services and embassies of the United States and allies in Europe. Possible motivations for the attack include: Russian dissatisfaction with the reporting by TV5Monde on the Ukrainian conflict; a wish to distract attention from the Kremlin's operations in Ukraine by encouraging the West to focus on ISIS; or a desire on the part of Russian actors to show what they are capable of (large-scale media sabotage).
- **The 'close access' hacking attack at the OPCW**[50] During a press conference, which was broadcast live, the MIVD announced that on 13 April 2018 it had foiled an attempted hack by the Russian secret service on the OPCW in The Hague. The Russians had allegedly sought to penetrate the OPCW's wifi network. The attempted hack took place around the same time as the OPCW's investigation into the poisoning of the former Russian double agent Sergei Skripal and his daughter. At that time the OPCW was also investigating the poison gas attack in Douma, Syria. Russia is a key ally of the Syrian regime. So the OPCW was working on two cases that were sensitive from Moscow's perspective.
- **Trolls/Social Cyberattacks** Used to spread disinformation online and carry out other types of online information operations. For more on this, see manifestation 6 below: propaganda and disinformation.

48 MIVD Annual Report 2016, 24 April 2017.

49 This name was also used for the cyberattack on the website of CentCom, the US strategic headquarters that directs military operations in the Middle East and Central Asia.

50 Organisation for the Prohibition of Chemical Weapons. 'MIVD: we hebben Russische hack van OPCW in Den Haag voorkomen' (MIVD: we prevented Russian hack of OPCW in The Hague), NOS.nl, 4 October 2018, and letter to parliament from the Minister of Defence of 4 October 2018, Parliamentary Papers, 2018-2019 session, 33 694, no. 21.

Potential consequences

The potential consequences of the use of cyber capabilities are legion: from espionage to manipulation to disruption, depending on the intended goal. This means that the repercussions can be felt across a broad range of national security interests. Cyber sabotage of critical infrastructure can lead to physical and ecological damage, casualties and social unrest. Espionage compromises the integrity and exclusivity of information. Troll factories and 'social' cyberattacks (as part of a pre-existing campaign of manipulation) compromise political and social stability. They have the potential to undermine social cohesion and ultimately the very functioning of the democratic legal order. What they have in common is the harm they inflict on the reputation and finances of the victim (whether in the public or private sector). One of the things that makes cyberattacks so insidious is the problem of attribution: it is very difficult to say with absolute certainly who is behind a given attack or campaign. This makes it practically impossible to mount an appropriate political and diplomatic response. As a result, there is always room for doubt, which the aggressor can then exploit. Cyber capabilities are thus ideal instruments for hybrid conflict, as they combine versatility, secrecy and deniability. They can also cause digital, economic and physical damage.

5. Foreign interference (including political influencing)[51]

Covert action has long been part of the arsenal of instruments used by states to further their interests abroad. This includes interference in other countries' affairs. To achieve certain strategic objectives, states will sometimes employ means that will not achieve the goal directly, but which, in combination with other means, will make the goal more accessible. Foreign interference often involves attempts to influence members of that country's diaspora. This approach, which is sometimes collectively referred to as 'diaspora policy' or 'the long arm',[52] is a subversive[53] tactic that can be part of a broader campaign involving the use of the diaspora as an instrument. 'Such undesirable and covert activities on the part of foreign powers in the Netherlands infringe on Dutch sovereignty and can severely compromise national security.

Such interference can lead to serious violations of the country's political and administrative integrity, undermine the international legal order and stability, foster radicalisation among ethnic and religious minorities, compromise fundamental rights, undermine the Netherlands' vital sectors and weaken Dutch competitiveness.' [54] Yet foreign interference goes much further than simply influencing, manipulating or intimidating the diaspora.[55]

51 The Dutch government now has an official policy on dealing with foreign interference. In their letter to parliament of 16 March 2018 the Minister of Justice and Security and the Minister of the Interior and Kingdom Relations explained the government's definition of undesirable foreign interference. The letter also discusses the government's efforts to boost resilience to such interference. Parliamentary Papers, 2017-2018 session, 30 821 no. 42.

52 Generally, efforts to influence the diaspora are driven primarily by questions tied to the political or financial survival of the government in question: i.e. seeking to preserve the political status quo in the country of origin (including existing state structures, the role and position of the head of state, and the role and position of citizens, both within the country and abroad). To this end, 'dissident' voices, at home and within the diaspora, are suppressed. The country of origin also has financial interests with regard to the diaspora.

53 In terms of its effect, but sometimes also in terms of its intention.

54 AIVD Public Annual Report 2003.

55 The Dutch government recognises the danger posed by undesirable foreign interference. It set out its position on the matter in a letter to parliament of 16 March 2018, (Parliamentary Papers, 2017-2018 session, 30 821 no. 42. The letter offers the following definition of the term: 'Undesirable foreign interference' refers to deliberate, often systematic and clandestine activities by state actors (or parties connected to state actors) in the Netherlands or aimed at Dutch interests, which could undermine the political and social system as a result of the goals being pursued, the means employed or the eventual effects. The letter gives examples of various states that use the tactic of foreign interference. The 2018 AIVD annual report specifically mentions China, Iran, Russia and Turkey.

The National Risk Profile (NRP) includes the sub-theme 'Undermining democracy, the rule of law and the open society'.[56] This illustrates the current and enduring nature of the threat posed by foreign interference. The NRP discusses both short- and long-term efforts to undermine the political and social system of the Netherlands,[57] which can be described as 'a democracy founded on the rule of law' and an 'open society'.[58] 'These are systematic, deliberate and in many cases covert activities on the part of state and non-state actors, which can compromise, weaken, destabilise, undermine or sabotage democracy, the rule of law and the government that bears responsibility for upholding these structures, as a result of the objectives being pursued, the means used or the eventual effect. They also include activities that, on account of the goals being pursued, the tactics used or the resulting effects, cause serious harm to necessary social cohesion by undermining trust and solidarity among members of the public. In many cases this does not lead to direct, acute upheaval, but over the long term it can cause serious disruption to and dysfunction in the democratic legal order and open society.

State actors who use such tactics also include foreign powers with which the Netherlands is in conflict or on bad terms. Foreign interference employs a variety of methods to exert influence, and its target audience (whether students, the media, politicians or the general public) is not always aware that it is being manipulated. It can also involve clandestine financing. The tactics used also include disinformation, i.e. the dissemination of false rumours and conspiracy theories via less than reputable news sites and social media. These covert activities designed to exert influence and interfere in other countries' affairs are collectively referred to as 'active measures'.[59] According to the experts who contributed to the National Risk Profile, these measures pose a very real risk to national security interests. Multiple measures will often be used simultaneously, so that the party in question can exert influence in various dimensions of society.

The Russian Federation is highly adept in its use of 'active measures', a method that was called the 'heart and soul' of the Soviet intelligence machine.[60] The aim was not so much to gather intelligence as to engage in subversion with a view to weakening the West, driving a wedge between the Western allies (especially within NATO) and harming the reputation of the US/the West in the eyes of the world. Such measures serve to lay the groundwork for any eventual war.

Various Russian active measures have been observed or openly acknowledged. Most clearly, of course, in Ukraine, where influencing public opinion and decision-makers is the order of the day and where the local population is being encouraged to take up arms against their own government. But interference has also been observed in the West. One example is the provision of financial support to anti-EU parties (such as Marine Le Pen's Front National).

56 The NRP, which is the successor to the National Risk Assessment, is drawn up by the National Network of Safety and Security Analysts at the behest of the Steering Committee on National Security.
57 The full range of possible implications of influencing is broader than this quote from the NRP would suggest.
58 Or the 'democratic legal order' in its vertical dimension (the relationship between a government and its citizens, characterised as 'a democracy founded on the rule of law') and its horizontal dimension (the relationship between citizens themselves, characterised as 'the open society').
59 'Active measures' is the Soviet term for foreign interference, which encompasses the whole range of methods for exerting influence, from media manipulation to violence.
60 By former KGB major general Oleg Kalugin.

The Netherlands, as a member state of both the EU and NATO and especially as the lead nation in the investigation of the crash of flight MH17, is also a relevant target for influencing. This means that it is conceivable that the Netherlands will be subjected to undesirable interference from Moscow. The ideal time for this is at moments of significance for the state, such as elections. We have seen something similar in the US and witnessed the concerns of other EU member states that held elections in 2017.[61] Elections are the perfect time to influence political decision-making and public opinion. Various state actors stand to benefit from this, and they can employ a range of instruments to that end, such as disrupting the democratic process through cyber sabotage (e.g. manipulating voting computers or accounts/computers belonging to political parties),[62] influencing the choices of voters themselves (by means of propaganda, disinformation) or undermining the (perceived) reliability of the result. Such influencing can occur at various phases of the election: during the run-up/campaign, on election day itself and finally, in post-election coverage by the media. It was therefore conceivable that during the entire span of the election (before - during - after) the Netherlands would be confronted with attempts at influencing. The fact that two other key NATO and EU member states and participants in the anti-ISIS coalition – France and Germany – had elections in the same year, made the attempt to exert influence even more plausible. Elections were first held in the Netherlands, followed by France in April/May and Germany in September. France and Germany are bigger fish, but this could have made the Netherlands an attractive 'guinea pig'. With this in mind the Dutch elections were closely monitored, both domestically and internationally.

The National Risk Profile devoted attention to undesirable interference with a scenario which explored concrete examples of (covert) interference and influencing activities on the part of foreign governments. See the inset below for the scenario and the building blocks. The scenario was a worst-case scenario with a probability rating of 'likely': the scenario is thus highly conceivable and there are indications that it could actually occur. There was only a small degree of uncertainty with respect to this assessment. The impact on national security interests was as follows. In terms of territorial security there was a serious impact on our international position. No impact was identified on physical security. There was a considerable impact on economic security as a result of the costs incurred. No impact was identified on ecological security. But in terms of social and political stability, a very serious impact was identified on democracy and the rule of law, and our open society. The building blocks used are, however, only a selection of the possible methods that fall under the heading of 'active measures'. Another impact is certainly possible, both in terms of the interests affected and the severity of the repercussions.

Potential consequences

The potential consequences of foreign interference are also legion, depending on the goal, the target and the means (routes). This means that the repercussions could be felt across a whole range of national security interests.

61 'Maaßen warnt vor Einfluss Moskaus auf Bundestagswahlkampf' (Maaßen warns of Moscow's influence on Bundestag election campaign), *Hamburger Abendblatt Online*, 16 November 2016. Concerns still remain: 'Cyber attacks rob future elections of their legitimacy, Jeremy Hunt warns', *The Telegraph*, 7 March 2019. In this article UK foreign secretary Jeremy Hunt specifically refers to authoritarian regimes that target democratic processes in the West. He mentions Russia, China, Iran and North Korea as actors that have been behind various hacks and online campaigns.

62 'Microsoft spots Russian hacking campaign ahead of EU elections', *Sky News*, 20 February 2019.

National Risk Profile worst-case scenario: state actors – 'An undermining operation from abroad' – Storyline

In the Netherlands young people, the media and the elite (in business, politics and academia) are influenced via a range of covert and overt activities by a non-Western country which is seeking to undo the sanctions that have been imposed on it and undermine the EU. For example, rumours are being spread about alleged major fraud and corruption scandals within the EU (see 'tactics' in the building block table below for other activities that could be used). A number of Dutch civil servants and politicians see no other option but to resign (despite a lack of clear evidence). Conspiracy theories are spread about Dutch and European migration policy. It is also suggested that migrants have harassed women and that the authorities are not taking action. Eventually the Dutch people begin to lose their trust in the government, and doubt is rife about the EU and other international partnerships. An ultra-right-wing party with an anti-EU and anti-migrant agenda, whose activities are secretly sponsored by the country in question (something which is also occurring in other EU countries), sees a dramatic increase in support. The gulf between supporters and opponents of the EU becomes greater and greater. The Dutch anti-EU and anti-migrant party regularly holds demonstrations that degenerate into serious unrest. On social media Dutch politicians and civil servants receive a relentless stream of hate, intimidation and threats, which seriously impedes their ability to function.

National Risk Profile worst-case scenario: state actors – 'An undermining operation from abroad' – Building Blocks

The following building blocks were used in this scenario:

Actor = the governments of countries with which Europe/the Netherlands is on bad terms/in conflict.

Goals = weakening trust in the government;
undermining the legitimacy of the government;
gaining political influence;
compromising the image of the Netherlands/the West;
driving a wedge between EU member states.

Means = calling the legitimacy of the government into question and undermining it in practice;
intimidation;
exercising (covert) influence;
propaganda via traditional and social media;
disinformation via traditional and social media;
recruitment;
entering politics/joining political parties, municipal councils, official consultative bodies, etc. with a hidden agenda;
cultivating/tasking individuals with influence in the business community;
acquiring influence in the media in order to project a particular image;
acquiring influence in academia.

Targets = government, whether national or local;
the media;
academia;
the West/EU;
Dutch citizens/public opinion.

6. Propaganda and disinformation

The information domain and information confrontation occupy a central place in Russian military thinking. Information confrontation can be seen as an independent, free-standing threat: it is part of a greater plan, a coherent and complementary campaign. It is a recurrent theme in Moscow's approach to engaging in conflict. The aim is to infiltrate, and then delay and disrupt, the opponent's decision-making cycle.[63] One of the goals of disinformation is to foster indecisiveness, making the target vulnerable to a resolute opponent. Another is to discredit Western values.[64] For example, Western freedoms and achievements (such as the acceptance of homosexuality) are portrayed as signs of moral decline. This view of information confrontation also colours Russia's perceptions.[65] In other words, outside information (from the West) is received in a similar spirit: as part of an information operation.

This explains why it is so important to Moscow to maintain control over the media. For Moscow it is essential to acquire 'information superiority' over the West, as this is virtually the only way of compensating for Western military superiority. Information confrontation is an essential part of Russian hybrid conflict. A hallmark of this strategy is the creation of uncertainty by frustrating the decision-making processes of NATO and the EU, thereby creating the impression that these organisations are fragmented, indecisive and weak.

For Moscow propaganda and disinformation have always been important and frequently used instruments, but their role has increased with the advent of the internet and social media. A wide variety of actors use social media in their struggle; it is not unlike what happened in the 19th century, when the telegraph became a new weapon of war.[66] The example of MH17: The critical, contradictory and confusing reports that were spread from the Russian Federation about the circumstances of the crash of MH17 and the subsequent investigation. This campaign of disinformation was set in motion immediately after the crash. Moscow deploys disinformation in such a way that Russian news consumers will not know what to believe. And the international investigation into the crash will be discredited, thus further impeding any future legal proceedings.

The basis of disinformation: the strategic narrative

It is important to realise that Moscow makes use of a strategic narrative that serves as the basis for its approach to information confrontation: history as a never-ending dialogue between the past and the present. Within this frame of reference, allusions to and echoes of the past are used to interpret and give meaning to present-day events. The narrative legitimises the actions taken, and it is adapted to the audience in question, whether domestic or international.[67] With regard to Ukraine, the narrative of a shared cultural history is used (e.g. Kyiv as the mother of all Russian cities) to justify the argument that the Russian Federation and Ukraine must stay together. Moscow also makes frequent use of the Nazi/fascist narrative,

63 MIVD Annual Report 2016, 24 April 2017.

64 Disinformation seeks to ramp up social tensions and polarise the political spectrum, making it more difficult to form a government with popular support. By undermining trust in the Dutch government, established media and authorities in the national and international arenas, it can compromise Western values like democracy.

65 Mark Laity, former BBC correspondent and the current Director of the Communications Division at SHAPE/NATO, 'Disinformation as a weapon in hybrid warfare', 12 October 2016, Atlantic Commission Lecture.

66 Emerson T. Brooking and P.W. Singer, 'War goes viral: How social media is being weaponized across the world', www.theatlantic.com/magazine/archive/2016/11.

67 There is also apparently a special narrative for the Netherlands. When asked, Laity could not offer a good answer: 'That would be getting too political'. (12 October 2016). If nothing else, the goal is for MH17 to be shrouded in uncertainty. We are also fed the same narrative about the (moral) decline of the EU, a line that is fed to all member states.

because of the heroic role of the Soviet Union in the victory over Nazi Germany. This narrative is designed to appeal to that heroic perception and to portray opponents as Nazis/fascists (the least desirable role in modern history), a group that had already been defeated once before. The Russian intelligence services play a key role in shaping this narrative: they have obtained an ever greater grip on society, as well as on the writing and interpretation of history.

Manifestations of disinformation

In essence this is a matter of pursuing old tactics (delaying, deceiving, confusing) by means of modern methods (social media). During the Cold War, propaganda and disinformation (on both sides) was highly ideological in nature. Although the ideological foundations are less pronounced nowadays (again, on both sides), propaganda and disinformation are increasingly cast in ideological terms. We are witnessing a growing divide in norms and values.

A new phenomenon, which has arisen with the growth of the internet and social media, is that of trolls and 'social cyberattacks'. 'Trolling' involves creating confusion and spreading panic/hate by means of disinformation disseminated by 'real' users on social media. Some (state) actors have professionalised this tactic by means of 'troll factories': entire organisations composed of individuals who spend their days posting on social media.[68] For some time the Russian Federation has sought to spread confusion and panic in order to create conditions conducive to Russian interests. With the arrival of the internet age, the Russian Federation incorporated these new techniques into its arsenal, in the form of online disinformation campaigns, the dissemination of propaganda and the widespread deployment of internet trolling. According to Margarita Levin Jaitner of the Swedish Defense University, in addition to trolls the Russian Federation also uses 'opinion agents',[69] who are deployed to circumvent Russians' mistrust in mass media by bombarding them with 'truthful information' via social networks and blogs. Social media are a major source of news for the Dutch public as well. This is particularly true of people who are feel that mainstream media reporting does not adequately correspond to their own world view. The risk is that social media becomes an echo chamber, ensuring that its users see only the kind of reporting that supports or reinforces their own convictions. Even if retractions of incorrect information are posted, they are scarcely read or shared by the audience that the original false story reached. The NATO Strategic Communications Centre of Excellence analyses the strategic communication aspects of social media in the Russia-Ukraine conflict, exploring the use of PSYOPS (psychological operations) and social media and introducing the term 'social cyberattacks'.[70] This term refers to the practice of acting anonymously or under a false identity to spread manipulated messages or to manipulate existing messages in order to achieve chaos, panic and large-scale civil disobedience. The purely psychological effects were effectively deployed in the Russia-Ukraine conflict, in support of military operations.

68 It should be noted that not all of these troll factories are in Russia. A recent example is the Internet Research Agency, which is based in the US and operates from there, but pushes the Russian agenda.

69 This phenomenon exists in the Netherlands as well. It is uncertain whether these opinion agents have a link to Russia. What is clear is that Russian state media agencies are aware of what groups/initiatives/influencers are active on Dutch-language social media. These agencies make a point of following these people and regularly quote them in their own news stories.

70 As defined by Dr Rebecca Goolsby.

In addition Moscow uses old-fashioned methods like falsifying official documents and official communications from other governments so as to discredit them and compel them to issue explanations.
Here are a number of examples of flagrant disinformation and their repercussions:

- A video released around the time of the Ukraine referendum, which threatened violence in the event of a 'no' vote. Among other things it showed a Dutch flag being burned. Fortunately, this video was debunked within two hours.
- The Lisa case: the rape of a 12-year-old girl in Germany by asylum seekers. It took two days before this video could be debunked, and during that time hundreds of demonstrators took to the streets to protest against Chancellor Angela Merkel.

Russian disinformation capabilities

The Kremlin gives financial support to hundreds of media channels and many NGOs. This means that there are thousands of professionals working against the EU/NATO/the West/the US. They are capable of customising their activities, tailoring disinformation to a particular target audience or country. In the Baltic states, for example, the Russian-speaking minority is a crucial tool. The local population is also involved in disinformation (whether consciously or not), for example local reporters for international Russian media channels, such as news outlets of RT. This lends the appearance of impartiality to the disinformation. For Moscow[71] information confrontation is a 24/7 business, with short and direct chains of command.[72]

Potential consequences

In the Netherlands (and the West in general) there is now a greater vulnerability/receptivity to disinformation than ever before. The threat is significant, because the public is ripe for disinformation campaigns.[73] On the other hand, in recent years the threat has been recognised at both national and international level; there have been both private[74] and public[75] initiatives to research and combat disinformation. The considerable attention the media have paid to this issue has also helped raise awareness of its existence. In time this can boost resilience. The reason the public is ripe for disinformation campaigns is tied to its increased distrust in government, the traditional media and 'the establishment' more generally. It is this very distrust that disinformation campaigns are designed to exploit. Social polarisation is exploited in order to destabilise the EU. The fact that we in the West do not have a strong counternarrative of our own that we can deploy against the Russian narrative makes us more vulnerable. The fact that users of social media are not, like TV viewers, passive consumers, but are rather actively involved in the discussion and the information being shared means that they are also more likely to internalise this information. The impact of disinformation is thus much more direct, and its presentation can be modified in real time, depending on its effectiveness (or lack thereof).[76] Disinformation is thus highly flexible and, moreover, fairly inexpensive. A successful information confrontation could lead to serious polarisation or entice people to turn away from their own governments and institutions. Looking to the future, technological developments will throw up major challenges in the domain of disinformation: the popularisation of 'deep fakes', i.e. highly sophisticated manipulated videos.[77] The term 'deep fake' refers to audio and video recordings that are created by means of

71 And other major players.
72 'Disinformation as a weapon in hybrid warfare', lecture, 12 October 2016.
73 Ibid.
74 Such as Bellingcat and the Alliance for Securing Democracy.
75 Like the EU vs Disinformation initiative of the East Stratcom Task Force, EU European External Action Service.
76 If a particular storyline does not catch on, it will be discarded and replaced with something else.
77 'You thought fake news was bad? Deep fakes are where truth goes to die', *The Guardian*, 12 November 2018 and *VPRO Tegenlicht*, broadcast on 18 November 2018.

artificial intelligence. This technology makes it possible to create audio and video recordings in which real people say or do things that they never said or did in real life. Whereas this kind of trickery was once the province of the Hollywood special effects studios, the technology has since become more accessible to the masses. Moreover, the development of the technology has accelerated, and as a result video and audio material can be produced ever more rapidly and easily, resulting in an ever more realistic product. And while researchers attempt to unmask and defuse deep fake videos using algorithms, the self-learning algorithm ensures that these videos are becoming increasingly realistic and more difficult to detect. It is no coincidence that the US Department of Defence has classified deep fake technology as a threat to national security.

In conclusion, it can be observed that the manifestations described here can have an impact on all national security interests except ecological security. The potential threat posed by hybrid conflict is thus substantial.

What can we do to defend ourselves?

The question that then arises is of course: what can we do to combat the effects of hybrid conflict? Both a specific and a general approach are possible.

The specific approach is focused on the actor and requires a thorough knowledge of our opponent.
- If we know its strategic objectives and ambitions, we will know where it aims to go. From that point we can identify the possible routes that would lead to that destination. These routes can then be reinforced, monitored for misuse or equipped with bypasses.[78]
- A knowledge of its strengths and weaknesses. The opponent will use instruments and operate in domains in which it is superior, as a way of compensating for those instruments and domains in which we are superior. Knowing these strengths and weaknesses helps to estimate – predict, if you will – what instruments will be used or what domain targeted.
- Identifying cases of hybrid conflict is a matter of 'connecting the dots': identifying similarities in various manifestations of the phenomenon so as to discover/recognise the underlying pattern or strategy.

The general approach is about how we relate to ourselves:
- A knowledge of our own vulnerabilities, since these are the places where an opponent will first attempt to strike. These vulnerabilities may be either physical/material or immaterial in nature.
- Acting so as to limit the opportunities for foreign powers to exploit our vulnerabilities, for example by diversifying dependence on natural resources.
- Acting so as to reduce the impact of an opponent's activities, for example by ensuring the existence of analogue redundancy where digital solutions are used in vital processes.
- Acting so as to reduce our susceptibility to information operations. In the case of disinformation, the first step is unmasking the product in question, because it exposes the actions of the opponent. But having a good narrative of our own that is credibly articulated and widely accepted is important for boosting our own resilience. EU/European integration is actually a great achievement and shows the West's power to bring about a prosperous and egalitarian society by peaceful means. That would be a very strong narrative, were it

78 A bypass makes it possible to close the main route if the opponent happens to be on it, without obstructing our own access to the 'destination'.

not for the fact that it has largely faded in the collective memory. An international inventory could provide insight into what instruments (such as public diplomacy) other countries use to boost their resilience.

Hybrid conflict is very much like a game of chess: strategic goals are not achieved directly but rather through the path of least resistance or least visibility. And as with chess it is important to keep the entire board in view and not to focus solely on the movements of individual pieces.

Uitgave
Nationaal Coördinator
Terrorismebestrijding
en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
info@nctv.minjenv.nl
@nctv_nl

april 2019