Appendix 5
Deterrence as a security concept against ambiguous warfare

Rob Hendriks

Current situation

It appears time to recognise and acknowledge that a significant change has taken place in the prevailing paradigm of war. Paradigms play a major role in determining the nature of war. Insight into this change is therefore required to be able to understand and describe the threat of ambiguous warfare for the purpose of ascertaining the extent to which deterrence is still relevant. Roughly speaking, there have been three successive paradigms of war in recent history.[1]

The *state versus state* paradigm, sometimes featuring alliances between states, prevailed from 1648 to 1945. The Westphalian state system, its key elements being territorial integrity and non-intervention, led to *raison d'état* and the maintenance of sovereignty becoming the guiding principles of the foreign policy of states. Although there were protracted wars during this period, they did not involve a society in its entirety. Wars also included long periods of relative peace, even impasses, that were followed by fierce but nevertheless circumscribed battles. The overriding priority was the continued existence of the nation and armies were therefore never totally expended because they were needed to safeguard this continuity. These 'limited wars' changed in nature over time and, particularly after the Industrial Revolution, state versus state wars became increasingly 'total':[2] the entire society contributed in some way to, and also suffered from, the war being fought.

The *bloc versus bloc* paradigm dominated from 1945 to 1989. Based on mutually assured destruction (MAD),[3] NATO and the Warsaw Pact kept each other at bay. Nevertheless, there were a number of times during this period that the Cold War 'heated up' – in addition to rising tensions around Berlin and Cuba. Western nations had to deal with wars of decolonisation, many in the form of an insurgency by the native population and counterinsurgency on the part of the colonial power. The newly independent countries rapidly became part of the global game of chess between the two superpowers of the time, the US and the USSR. Both opted to exert their influence in the world through third parties. Although the proxy wars thus fought were not waged directly against the main adversary, they were aimed against the political and ideological system for which the adversary stood. The proxies came from the

1 The paradigms described did not exist in isolation. There were also conflicts from other paradigms in the periods of time referred to.
2 The United States versus the Confederate States in the American Civil War, the Franco-Prussian War, World War I and World War II, for example.
3 The nuclear arsenal that both blocs possessed ultimately guaranteed the total destruction of both sides should one bloc attack the other.

entire spectrum of actors, from state actors conducting formal opposition to guerrillas and even mercenaries.

The future of the world looked positive, at least from a Western perspective, following the fall of the Berlin Wall in 1989 and the subsequent disintegration of the Warsaw Pact and the USSR. The paradigm became one of *state versus non-state actors*. Globally, there were over 30 conflicts between states and non-state actors from 1989 to 2010. For Western states, involvement in war was mainly a choice rather than a result of a threat to sovereignty. International crisis management was the main reason for intervention, preferably on the basis of a mandate of the UN Security Council. In these 'wars of choice', which were usually but not always 'small wars', Western countries provided support to either the counterinsurgency or the insurgency depending on the nature of the actors involved. The Gulf War and Iraq War (1990/91 and 2003 respectively) must of course be mentioned here. Both were wars of choice, but they are also clear examples of the state versus state paradigm. For some time, they also served as proof of the West's military supremacy.[4] Although 'hard power' was essential in these conflicts, it was not adequate on its own. All capabilities available to a state,[5] including psychological operations and information operations, for example, had to be used. In addition, a comprehensive approach[6] proved necessary to deal with the complex conflicts as completely as possible. Developments in emerging states[7] and in states which had suddenly become independent were largely ignored at the political and strategic level, however. In a conceptual sense, notions of liberal peace or democratic peace dominated in this period relative to those of political realism.

As shown by, for example, the current IS crisis, the deployment in Mali and the continuing involvement in Afghanistan, the *state versus non-state actor* paradigm of the previous era still very much applies. Nevertheless, a new paradigm is now clearly emerging, namely a '*state versus state 2.0*' one. In the context of this paradigm, a state does not necessarily act like a state, or at any rate not in accordance with the rules of the international community. A current example of such conduct is Russia's approach to Ukraine,[8] an approach Russia first applied tentatively against Georgia in 2008. Countries such as India, Pakistan and China have also acted in a similar way in the past. Clausewitz's *Realpolitik* assertion that war is the 'continuation of policy by other means',[9] in the context of which a state also attempts to manipulate the psychological, moral and ethical dimensions, applies in this paradigm.

What types of warfare can be distinguished at the present time? Academic literature usually describes the types in pairs: regular versus irregular, conventional versus unconventional,

4 Although objectives were achieved at various levels, the conflict rapidly evolved into a state versus a non-state one. A key aim, the creation of a stable situation in the region, has not yet been achieved.

5 A state's instruments of power are Diplomacy, Information, Military, Economy (DIME).

6 In short, a whole-of-government approach, including, in addition, international organisations and non-governmental organisations (NGOs).

7 BRICS: Brazil, Russia, India, China and South Africa.

8 The arming and deployment of armed groups, the deployment of anonymised Russian armed forces in Ukraine and the positioning of regular military units along the border for the purpose of intimidating, the foregoing in combination with cyber operations and an information campaign in support (see the Ukraine case in this report for details).

9 The original German text repeatedly states 'mit Einmischung anderer Mitteln'. This certainly does not mean 'continuation by other means', since this formulation would imply that the means used up to the outbreak of a war that are available to political leaders (diplomacy, economic and so on) are no longer used during a war. The crux of the statement is precisely the combined use of all instruments of power.

symmetric versus asymmetric. The types thus juxtaposed differ in terms of one or more of the following: actors, resources, methods and objectives. Contemporary warfare, however, especially as conducted by and against non-state actors, is rarely one of the 'pure' types referred to. In practice, it is usually of a hybrid kind. Hybrid warfare incorporates all of the conceptual categories of warfare. It uses the elements that achieve the desired effects in the specific context of time and place. In addition, the mix of elements can continuously be adapted. This capacity to evolve results in continuously changing characteristics. It is therefore very difficult to find an adequate response to hybrid warfare.

In principle, all of the 'pure' types of warfare can occur in the *state versus state 2.0* paradigm. Current warfare, however, is characterised by a 'state 2.0' that, on the one hand, overtly acts as a power, possibly an impartial one, that uses all of the instruments of power of a state. On the other hand, it uses other actors (proxies) and, in addition, makes covert use of its instruments of power and of relatively new methods such as cyber operations and powerful information operations to support the covert aspects and justify the overt ones. This is not an entirely new phenomenon. History is full of examples of covert operations, agents deployed to a foreign location to engage in inflammatory activities and double agendas of states. The modern resources and methods now being used in combination with the increasing interconnectedness of interests as a result of economic globalisation make the hybrid approach more effective and potentially more destructive, however. When acting in an ambiguous manner, a state 2.0, unlike a non-state actor, can use the entire range of instruments of power, to an extent also covertly. The new Russian overarching doctrine for the armed forces,[10] for example, states that warfare is based on the use of all available means in all conceivable combinations and according to all methods of implementation possible, including covert operations. The covert aspects and the deniability that they provide[11] in combination with the overt dimension of an ostensibly impartial actor or even a bringer of peace that is above the parties make actions ambiguous. Seen in this light, hybrid warfare is a current starting point for a state 2.0 and the combination with ambiguity is a very valid possibility. Since this way of waging war is embedded in the new state versus state 2.0 paradigm, it may be stated that ambiguous warfare constitutes a current and remaining threat.

Ambiguity in warfare is almost as old as war itself. It has recently become the focus of attention, however, because of the presence of Russian troops in Crimea (in advance of its annexation by Russia) and in other parts of Ukraine. Although these troops were clearly present, they concealed their nationality (see the Ukraine box).[12] In addition to the deployment of anonymised Russian armed forces, Russia's ambiguous warfare includes arming and deploying local groups in Ukraine. It is striking that Russia, a permanent member of the UN Security Council and a very influential state, seemed to be formally denying its military interference while at the same time accepting that it was clear to all involved that the anonymised military units were in all likelihood Russian. A possible result of this is that ambiguity in warfare may in the future be used more frequently in a more or less open way by both small and large states. There is a concern that Russian action in Ukraine in

10 Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces, is seen as the architect of this doctrine.

11 The need to be able to deny responsibility for at least certain elements of ambiguous warfare happen to make it difficult to 'flawlessly' execute this kind of warfare.

12 See Nicu Popescu, 'Hybrid tactics: neither new nor only Russian' (ISS Issue Alert). Paris: European Union Institute for Security Studies, January 2015.

combination with rising geopolitical tensions will encourage other states to make greater use of ambiguous warfare than was the case in the past.

An increase in ambiguous warfare could be detrimental to Dutch national security in several ways. First, ambiguous warfare undermines the international rule of law, since ambiguity lowers the threshold for states to resort to war or further their interests by military means. Second, it increases the likelihood of the Netherlands becoming involved in an armed conflict, particularly if the issue concerns the security of NATO allies. Although Dutch territory is not located along a potential, physical front line, the territories of other members of NATO and the EU, alliances to which the Netherlands has strongly committed itself, are.[13] In addition, the territorial security of the Netherlands itself could be threatened in the longer term. Although protecting the territorial integrity of the Netherlands is primarily the responsibility of the Dutch government, it can only do so successfully by cooperating with foreign partners. Protecting the territory of allies and mutual assistance is therefore a matter of 'extended interests'. Third, an increase in ambiguous warfare could also result in Dutch security interests being threatened even if the Netherlands is only indirectly involved in a conflict, as a diplomatic actor rather than as a member of an alliance. The cyber domain could be used to attack vital Dutch infrastructure, for example, or the Netherlands could be affected by unannounced and deniable ambiguous economic sanctions. Such sanctions could undermine economic security or result in political and social unrest. In addition, even if the Netherlands is not involved in any way, vital infrastructure on which the country also depends could be attacked at the international level.

Expectation for the coming five to ten years

Ambiguous warfare will remain a threat to Dutch national security in the coming five to ten years. In terms of the EU's immediate environment, Russia will probably be the main source of this threat. Since other parties have so far failed to effectively respond to ambiguous Russian interference in Ukraine, it seems likely that Russia will again use the method if circumstances for doing so are favourable. If several large states resort to the method more frequently as a result, international tensions may become more pronounced. The increase in tensions, identified in the Clingendael Monitor, between the great powers that will occur in the coming years as a result of a shift in the balance of power is very relevant in this context. The Russian example aside, it is possible that, in the event of rising international tensions, large states will opt to limit the probability of military escalation by including ambiguity in their military action or involvement in smaller conflicts.

Ambiguous warfare is therefore likely to become more, rather than less prevalent in the coming years, not least because security interests are closely linked to each other and security itself depends to a significant extent on two things that are adversely affected by ambiguous warfare, namely credible alliances and a properly functioning legal order. In addition, there is a close relationship between external and internal security, which makes an open society such as the Netherlands more vulnerable to ambiguous warfare. For example, attacks that are not directed against the Netherlands or its allies can also have a significant

13 NATO as a political and military alliance with a traditional focus on the core duty of defending its territory and, in addition, with an assumed role of 'crisis response actor', and the EU as a political and economic union that originally focused mainly on the economy, and therefore also on economic security, but which has a growing role in terms of physical security, primarily as a crisis response actor.

impact on Dutch security interests. The consequences of ambiguous warfare directed against the Netherlands or its allies would be even worse.

In the context of the new paradigm in which a state 2.0 is willing and able to conduct ambiguous warfare, the probability of an actual threat to the Netherlands, especially an indirect one in the sense of one posed to an ally, is already clearly greater than was previously the case. Whether this probability will further increase in the coming five to ten years depends to a large extent on how the Netherlands, embedded in the international community, particularly as a member of NATO and the EU, responds to the Ukraine crisis.

The relevance of deterrence as a security concept

Even more than is the case with respect to conventional threats, deterrence against ambiguous warfare must be completely credible. This credibility must be based on three factors: awareness, availability and willingness. *Awareness* of the reality of ambiguous warfare is absolutely essential at the political and strategic level. The idea that modern 21st-century states will not resort to such means is incorrect. Recognising and acknowledging the fact that the paradigm of war has changed and that ambiguous warfare is a real threat that is here to stay must be the foundation of all thought and action in relation to the threat. Such an awareness must manifest itself in unquestionable solidarity and unanimity in NATO and the EU, a projection that supports the other two factors.

Availability concerns the presence of the capabilities required to create and make deterrence a reality. Ambiguous warfare, when it occurs, is best countered by ambiguous warfare. This would, however, mean consciously opting to reduce the degree to which the Netherlands complies with international standards and values and possibly even laws and treaties. The irony would be that the importance of maintaining such standards, values, laws and treaties is precisely one of the reasons why an adversary that is conducting ambiguous warfare must be dealt with. Hybrid warfare is an alternative. Deterrence with respect to ambiguous warfare therefore requires the open presence of the concepts, methods, means and skills required to conduct hybrid warfare. To begin with, there must be genuine conventional capabilities, not least because conducting meaningful hybrid warfare rests on the ability to effectively combine elements from all types of warfare. The NATO Readiness Action Plan, which provides for, among other things, an increase in the number of response troops and a reduction of the response time, is an example of a large-scale initiative that enhances availability.

In addition, it is important to realise that a great deal of knowledge and know-how necessary to conduct hybrid warfare against a state 2.0 was already acquired in the state versus non-state actor paradigm. NATO has a functional doctrine on psychological operations and information operations and a thematic doctrine on counterinsurgency (COIN). Like the Netherlands, various allies are developing cyber and counter-cyber operations. The thematic doctrine can be used in both Article 5 and non-Article 5 operations. There are also other instruments of power of a state that can be used by the Netherlands and its allies. In addition, likewise in various COIN crisis situations, actual experience was gained in the use of economic means[14] in parallel with diplomatic, information-related and military means. It is essential to realise that a comprehensive approach, which is standard when supporting

14 Both financial support to partners and financially blocking opponents.

a partner in a COIN or other crisis scenario, must also be applied, perhaps even more intensively, when acting against an adversary that is conducting ambiguous warfare.

A *willingness* to deploy available means is the final component that is necessary for credible deterrence. To an extent, such willingness is evidenced by the availability of the concepts, methods and means referred to above. Ultimately, however, actual deployment is the unequivocal proof of willingness. Nevertheless, taking hybrid action simply to demonstrate that it is possible is of course not a sensible *modus operandi*. In terms of deterrence, the closest thing to actual deployment are exercises. In response to ambiguous warfare against non-NATO and/or non-EU countries, and also to reassure worried allies in the eastern part of NATO territory, a comprehensive exercises programme was developed and has been partly implemented to reinforce the message that NATO will take armed action in the event of an attack on its territory. The US has publicly declared that it will respond to a cyber attack that costs lives or does major material damage and that the response may include the use of conventional weapons. It is not always easy, however, to identify the perpetrator of a cyber attack. Another option yet to be used is to regularly conduct hybrid warfare exercises that include cyber and information operations designed to achieve relatively harmless results that are nevertheless hard to achieve, that are subsequently made public. The thinking in this regard must be in parallel with that which applies to exercises involving conventional means. This will ensure that the standards and values of the Netherlands are observed while projecting a message that is loud and clear to a state 2.0. Ideally, such exercises should take place in partner countries that have EU and/or NATO external borders in order to amplify the message projected. What applies to actual deployment also applies to such exercises: political and moral courage is required, an overarching strategy that provides scope for the use of all instruments of power of a state and all required elements and doctrines of all types of warfare is essential, and all ethical and legal considerations must be clear before deployment is actually necessary.

The costs and gains assessment of states that are considering ambiguous warfare can be influenced in several ways. The costs side can be directly influenced by enhancing the threat of retaliation and making it more credible. Deterrence based on retaliation is difficult because of the attribution problem, however. Because of the very nature of ambiguous warfare, it may not be possible to identify the perpetrator. Implicit and unannounced economic or diplomatic retaliatory measures may be taken if there are serious suspicions or if the identity of the perpetrator is actually known, even if the perpetrator's identity cannot be proved directly. The problem with such countermeasures is that they contribute to undermining the international rule of law. The possibility of retaliation in the form of legal or political and military countermeasures is substantially increased if the identity of the party responsible for acts of ambiguous warfare can be shown to a sufficient extent.

In conclusion, it can be said that increasing the costs that potential perpetrators must incur can be achieved by investing in international standards that increase the risk of reputational damage on the part of those who engage in ambiguous warfare. If this kind of warfare is both internationally illegal and deemed to be morally reprehensible in the extreme, even the suspicion that a state is engaging in it could result in major damage to the image of that state. Depending on the situation at hand, this could make a shift to ambiguous warfare in an armed conflict less likely. In addition, the costs of ambiguous warfare could possibly be increased by investing in better information and intelligence capabilities and a robust communications strategy that makes use of international media and diplomatic channels. A higher probability of being exposed would perhaps make it more difficult for a party that

is conducting ambiguous warfare to deny that it is doing so. Specifically regarding the threat of ambiguous warfare conducted by Russia against NATO countries, investments by these countries in military means and cooperation will be effective if there is also a credible probability of exposure and retaliation, since Russia would then have to invest more.

Investments aimed at increasing the probability of exposure are also relevant to the gains side. Acts of ambiguous warfare would be more likely to fail and it would be pointless for the state that carried them out to deny them. However, since the probability of exposure would have to be 100%, it is almost impossible to ensure that an ambiguous attack will never take place. In complement to the above, the Netherlands can take measures that counteract the perpetrators' underling objective of creating confusion and anxiety. One such measure would be effectively preparing oneself for possible acts of ambiguous war at the international level that could be relevant to the Netherlands. In the case of measures on both the costs and gains sides, the Netherlands will be able to take far more decisive action by working together with other countries and international organisations.