Deterrence as a security concept against non-traditional threats

Frans-Paul van der Putten
Minke Meijnders
Jan Rood

In-depth study
Clingendael Monitor 2015

Clingendael
Netherlands Institute of International Relations

Clingendael
Netherlands Institute of International Relations

Deterrence as a security concept against non-traditional threats

In-depth study Clingendael Monitor 2015

Frans-Paul van der Putten
Minke Meijnders
Jan Rood

June 2015

June 2015

About the authors

Frans-Paul van der Putten is a *Senior Research Fellow* at Clingendael, the Netherlands Institute of International Relations. His work focuses mainly on the effects that the rise of China is having on the global balance of power.

Minke Meijnders is a research and project assistant of Clingendael's security research group. She focuses on international security issues such as maritime security, terrorism and peacekeeping operations.

Jan Rood is a *Senior Research Fellow* at Clingendael. He focuses on global issues and European integration. In addition, he is the Endowed Professor of European Integration in a Global Perspective at Leiden University.

Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Email: info@clingendael.nl
Website: http://www.clingendael.nl/

Contents

Deterrence as a security concept against non-traditional threats

Introduction

The main question in this part of the Clingendael Monitor 2015 concerns the extent to which deterrence, as a security concept and instrument, can in the coming five to ten years be a relevant and effective way of protecting Dutch security interests against international, non-traditional threats.[1] The 2010 report 'Defensieverkenningen' already noted the continuing importance of deterrence as a means of discouraging "activities that run counter to the security interests of the Kingdom and the international rule of law".[2] The focus was on deterrence in the form of establishing the prospect of credible retaliatory action against current, particularly military threats. Such action could include the use, in a NATO context, of conventional and nuclear assets. However, also the report observed that, in a global context, many threats are now not military in nature or are at any rate not immediately military in nature. It was therefore argued that a long-term approach to deterrence as an instrument is required, one that focuses on both current military threats and new and future threats of a different nature.

These non-traditional threats differ from traditional security threats in that the latter tend to be characterised by the visible use of military assets by a foreign state actor for the purpose of seriously undermining the national security of the Netherlands and/or its military allies. Due to the absence of clearly recognisable aspects associated with military and state intervention, non-traditional threats are both hybrid and diffuse. In concrete cases where a non-traditional threat has been initiated by a state actor, it may be advisable to view this threat in interrelation with possible traditional threats initiated by the same state actor.

Previous editions of the Clingendael Monitor confirm the existence of a more varied range of security threats to the Netherlands and its partners and allies.[3] In addition to the remaining possibility of hostile military action, the 'new' threats include cyber threats, religious terrorism, crime, and so on. This greater variety in the range of threats is the main reason that this study discusses the importance and effectiveness of deterrence as a means of countering the threats referred to in the light of future developments in this area.

Based on the conclusions of previous editions of the Clingendael Monitor, this study focuses on five main categories of threat and analyses the applicability of deterrence as an instrument

[1] The authors thank Nina Jolink and Anne Bakker for the valuable contributions that they made to this report as part of their research internships at Clingendael. The authors are likewise grateful to Bibi van Ginkel, Sico van der Meer, Sander Huisman, Peter van Bergeijk, Rob Hendriks, Margriet Drent, Kees Homan and Dick Zandee for writing parts of this report and/or for taking part in the preparatory sessions. We are also indebted to Franca van der Laan, Luc van de Goor, Ko Colijn and readers at various ministries for their valuable comments on previous versions of the text.

[2] Ministry of Defence, *Eindrapport verkenningen: houvast voor de krijgsmacht van de toekomst*, The Hague: Ministry of Defence, 2010, p. 196.

[3] See *Clingendael Strategische Monitor 2012*, *2013*, *2014*, *2015*.

in the context of each area. The focus is particularly on the international dimension of these threats, in other words, on threats that could affect the Netherlands through the international sphere in addition to the national sphere. The five main areas of threat selected for this study are as follows:

- Terrorism;
- Threats in the cyber domain;
- Organised crime;
- Threats in the economic domain;
- Ambiguous warfare.

These main areas of threat are discussed in terms of the following three subquestions:

1. What is the current situation with respect to the area of threat under consideration?
2. To what extent is the area of threat under consideration relevant to Dutch national security for the coming five to ten years?
3. In what way is deterrence as a security concept relevant to the protection of national security with regard to the area of threat under consideration?

This report summarises the key findings and conclusions of the exploratory analyses carried out on the basis of these questions and set out in the appendices.[4] At present, only a limited amount of literature is available on the subject of deterrence in relation to non-traditional security threats, both in a general sense and more specifically in terms of relevance to the Netherlands. This report must therefore be seen as an initial delineation of the field. In addition, the paucity of practical examples of successful or unsuccessful implementations of deterrence instruments that are of relevance to the Netherlands means that this study is more theoretical in nature and is not really aimed at presenting concrete policy options.

The concept of deterrence as used in this study will first be described in greater detail and placed in a historical perspective, after which a summary of the key findings and conclusions is presented. This summary is followed by an analysis of Dutch security interests and an outline of the global and regional context in which this study must be viewed. After these introductory sections, the report discusses current threats to Dutch security and which developments are expected in the next five to ten years. The concluding section provides an indication of the relevance of deterrence as a security concept in terms of the five main areas of threat. This report does not go into the question whether putting specific deterrence measures into practice is cost-effective or desirable from a political or social standpoint.

Together with ‘A world without order?’, the summary report, and a forthcoming study on economic vulnerability, this study constitutes the Clingendael Monitor 2015. The Clingendael Monitor is published each year as part of the Strategic Monitor of the Dutch government.

[4] The appendices were prepared based on the written contributions of subject experts that were edited by the authors of this report. Responsibility for the way in which insights from the appendices have been incorporated into the analysis included in this overarching text rests with the authors of the body of the report.

Deterrence

Deterrence has a long history in the context of maintaining law and order and as a military strategy. It became a tenet in the international security environment of the Cold War as a response to the existence of nuclear weapons. The concept has since been further developed in both academic and policy terms.

Deterrence is aimed at discouraging undesirable behaviour. The definition of deterrence used in this study is as follows:

An approach aimed at preventing an actor who is planning to seriously harm the national security interests of the Netherlands from actually performing the harmful act or acts by influencing his or her assessment of costs and gains.

Only measures *deliberately* aimed at discouraging would-be perpetrators and/or their facilitators (individuals who provide support and thereby make it possible for perpetrators to carry out their attack) form part of a deterrence strategy. Deterrence can be aimed at increasing the costs for the would-be perpetrator or at reducing the gains that the would-be perpetrator could achieve. A further distinction can be made in this context between direct and indirect deterrence measures.

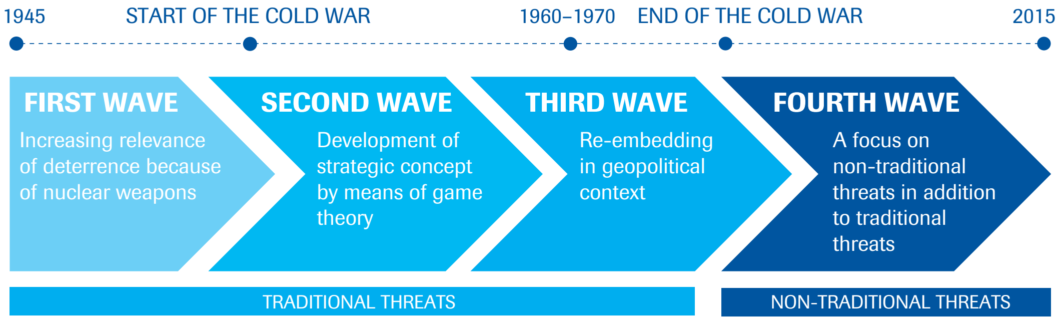
The following framework of analysis is used in this report with respect to the various forms that deterrence can take.

	Measures aimed at emphasising/increasing the costs that the would-be perpetrator must take into account:	**Measures aimed at reducing the gains that the would-be perpetrator could achieve:**
Direct	Convincing the would-be perpetrator that an attack or harmful act of any kind will trigger retaliatory action.	Reducing the opportunity to carry out an attack by visibly increasing the number and/or quality of security measures and increasing the operational risks to the perpetrator (reducing an attack's probability of success).
Indirect	Convincing the would-be perpetrator that a substantial investment is required for an attack.	Convincing the would-be perpetrator that performing the harmful act or acts will not contribute to achieving the intended objective (reducing the gains that can be achieved if an attack is successful).

Communication with the potential perpetrator is central to an effective deterrence policy: ultimately, it is about influencing the would-be perpetrator's assessment and, in this context, making it less attractive to perform the act or acts intended to cause harm. In other words, for a deterrence policy to work, communication about the measures that may be taken must reach the potential perpetrator and must be deemed to be credible by him or her.
A deterrence policy is based on the knowledge or suspicion that certain actors intend to perform acts that harm national security. To formulate the policy, it is therefore necessary to know who the potential perpetrators are. It is also necessary to be aware of their interests, motives and the resources at their disposal.

Developments in the thinking on deterrence in the context of international security

Current thinking on deterrence as an instrument for state actors to counter security threats at the international level is strongly informed by the development of nuclear weapons since the 1940s and is directly related to the bipolar world order in which the Soviet Union and the United States maintained an uneasy peace based on *mutually assured destruction (MAD)*. The nuclear strategy of *second strike capability* – that is, a power's assured ability to respond to a nuclear attack with a nuclear strike of its own – was a mainstay of the status quo at the time.


1945
START OF THE COLD WAR
1960–1970
END OF THE COLD WAR
2015
FIRST WAVE
Increasing relevance of deterrence because of nuclear weapons
SECOND WAVE
Development of strategic concept by means of game theory
THIRD WAVE
Re-embedding in geopolitical context
FOURTH WAVE
A focus on non-traditional threats in addition to traditional threats
TRADITIONAL THREATS
NON-TRADITIONAL THREATS

Political scientist Robert Jervis refers to *three* waves in the thinking on deterrence.[5] The *first* wave in deterrence theory started immediately after the Second World War, when writers such as Bernard Brodie concluded that the invention of the atomic bomb had fundamentally altered the nature of war. Brodie was of the opinion that a strategic revolution had taken place. Whereas before it had been about winning wars, preventing wars now had become the essential aim. According to Brodie, this strategic revolution had occurred because of the possibility of total destruction inherent in the use of nuclear weapons, which meant that defeating an adversary would serve no or virtually no purpose. The logical implication was that, when faced with an adversary that had nuclear weapons, a state could no longer protect itself on the basis of military superiority.

The *second* wave came against the backdrop of the Cold War. The strategic concept of nuclear deterrence was further developed using game theory and other methods. Thomas Schelling was one of the first to classify war as a bargaining process in which opponents attempt to influence each other's expectations and intentions by means of threats, promises and action.[6] He saw war as the art of deterrence, coercion and intimidation. In this context, he believed that nuclear weapons were sooner suited for punitive action than for conquering enemy territory. To make deterrence credible, the different phases of the escalation ladder had to be completely clear in order to limit a potential war to a certain phase (escalation control). At the same time, to achieve a deterrent effect, the phases had to remain undefined to a sufficient degree in order to exclude the risk of an actual war. In this view, a degree of uncertainty regarding the escalation process is necessary for effective deterrence.[7]

[5] Review Article, Robert Jervis, 'Deterrence Theory Revisited'. In: *World Politics*, 31 (1979) 2, p. 289-324.
[6] Thomas Schelling, *Arms and Influence*. New Haven: Yale University Press, 1966.
[7] Ola Tunander, 'The Logic of Deterrence'. In: *Journal of Peace Research*, 26 (1989) 4, p. 353-365.

The *third* wave came in the 1960s and 1970s as criticism of deterrence theory as it had developed up to that time. Statistical data and case studies were used to empirically test the theory. In addition, deterrence of the second wave was considered to be too apolitical. The third-wave thinkers were of the opinion that deterrence had to be viewed in the political and geopolitical context in which the concept was being applied. According to these experts, second-wave deterrence theory did not adequately examine the underlying problems that had resulted in a crisis and how the crisis might have been prevented. In addition, in their view, not enough attention was devoted to the process of compromising, while most conflicts are ended when the parties involved agree to a compromise. Finally, the third-wave thinkers disputed the assumption that actors act rationally, a core assumption of the second wave. They questioned the extent to which leaders remain rational in the heat of battle.

In the following decades, deterrence thinking initially continued to focus mainly on traditional conflict between states. Gradually, however, a new view on the applicability of deterrence emerged.[8] In contrast to earlier theories, non-traditional threats became a primary focus of the thinking on deterrence. This approach forms part of the fourth wave, which came against the backdrop of the end of the end of the Cold War in 1991 and the 9/11 attacks of 2001. Deterrence was no longer viewed only in the light of nuclear weapons and conventional war. It was considered in relation to a much broader range of threats, including violent non-state actors and asymmetric warfare. The main question was whether deterrence could also be used against non-traditional threats such as terrorism, piracy and cyber attacks.

According to Jeffrey Knopf and other authors of the fourth wave, deterrence is also relevant in this context, though only as just one of the various instruments that are available. Deterrence therefore no longer has the central role that it had during the Cold War. Knopf believes that deterrence must continuously be adapted to the specific threat that it is being used to counter and must be based on a detailed study of the adversary. Strategic cultural awareness of the adversary is essential.

Much of the literature on deterrence and non-traditional threats concerns the United States or the international level more generally. This study explores how deterrence can be relevant against threats in the specific case of the Netherlands.

National security and the international context

Dutch security interests and external threats

This study considers the extent to which deterrence is a relevant instrument for the protection of Dutch security interests. What are these national security interests and to what extent are they actually or potentially at risk because of the external threats discussed in this study? Maintaining the territorial integrity of the Netherlands – that is, guaranteeing its continued existence as an independent state – is a primary or vital security interest. In addition to this primary interest, the Dutch National Security Strategy includes four other vital security interests: economic security, environmental security, physical security and social and political stability.[9] Economic security means the ability to function without disruption as an effective

[8] Jeffrey Knopf, 'The Fourth Wave in Deterrence Research'. In: *Contemporary Security Policy* 31 (2010) 1, p. 1-33.

[9] Ministry of the Interior and Kingdom Relations, *Strategie Nationale Veiligheid*. The Hague, 2007, p. 11. See also Ministry of Foreign Affairs, *Veilige wereld, veilig Nederland: Internationale Veiligheidsstrategie*. The Hague, 21 June 2013; Scientific Council for Government Policy (WRR), *Aan het buitenland gehecht: Over verankering en strategie van Nederlands buitenlandbeleid*. Amsterdam: Amsterdam University Press, 2010.

and efficient economy. Environmental security concerns ensuring a safe natural living environment. Physical security concerns the ability of individuals and groups of individuals to function safely within society. Social and political stability is about maintaining a social climate in which the core values of democracy and the rule of law are observed.

As a relatively small country with an open democratic system and a country that is in many ways, especially financially and economically, strongly intertwined with the European and global system, the Netherlands is by definition vulnerable to external developments and threats. As also shown by previous editions of the Strategic Monitor,[10] the primary threat to the Netherlands is not the risk of a direct attack by another state on Dutch territory. That risk is still considered to be extremely low. Dutch involvement in territorial conflicts elsewhere is a possibility, however, though this involvement would be based on alliance commitments in the context of NATO and the duties to assist within the European Union (EU). The probability of such involvement has increased, particularly as a result of Russian action in the eastern part of Europe. Nevertheless, the threats discussed in this study indicate that the greatest dangers to the Netherlands are not military, or at any rate not directly military in nature. The threats are hybrid and transnational in nature, ranging from returning foreign fighters, crime and cybercrime, the disruptive effects of migration and financial and economic shocks to climate change and the risk of pandemics. Moreover, the Monitor 2015 shows that today's unsettled world order, which is mainly the result of increasing instability in the immediate neighbourhood of the EU and therefore of the Netherlands, has made a number of these threats more acute.

Within this varied range of threats, this study focuses in particular on the threats posed by terrorism, organised crime, vulnerabilities in the cyber domain, economic vulnerability and ambiguous warfare. It is clear that all of these phenomena may threaten the national security interests referred to. Organised criminal activity in the cyber domain can adversely affect Dutch *economic security*, which can likewise be undermined by international tensions, the implementation of economic sanctions and instability in regions and areas of importance to the Netherlands. *Political and social stability* and *physical security* can come under pressure as a result of organised terrorism – due to its polarising effect on society, among other things – and as a result of organised crime. Finally, there is the threat of ambiguous warfare. Although this phenomenon does not directly endanger the territorial security of the Netherlands, it is a potential threat to the territorial security of partners and allies which were referred to earlier. Moreover, where ambiguous warfare involves the use of propaganda, cyber and other tools to undermine the status quo, it can certainly pose a threat to political and social stability.

Protecting national security is primarily a responsibility of the Dutch government. Because of their respective natures and origins, however, threats to national security can in many cases only be effectively countered and neutralised through cooperation with others. In this sense, the security interests of the Netherlands as listed above can be referred to as extended interests in that they are interests that the Netherlands shares with other countries and which the Netherlands can only successfully protect in cooperation with others. This need to cooperate applies to the most fundamental national interest, namely the protection of territorial integrity, for which the Netherlands depends on its allies. However, it also applies to the other security interests referred to in relation to the threats described.

[10] Clingendael Monitor 2012, 2013, 2014.

To protect these interests, the Netherlands must therefore actively cultivate and engage in international cooperation within the EU, NATO, the UN or other international frameworks, preferably within an international legal order that guarantees global security and stability and safeguards the values and principles promoted by the Netherlands. It is only through such active engagement that the Netherlands can also exercise influence.

The global and regional context

Expectations for the coming five to ten years regarding the threats to Dutch society discussed in this study must also be seen in the light of broader regional and global developments in international security, stability and cooperation. As stated in the preceding section, the Netherlands is vulnerable to external developments and events. This means that a stable global system in which cooperation is the rule is of major importance to the Netherlands.

The Clingendael Monitor 2015 'A world without order?' shows that developments that constitute an existing or potential threat to international security and stability and to the functioning of current frameworks for international cooperation are occurring at regional and global levels.[11] Partly as a result of a continuing *global spread of power*, tensions are increasing between the great powers, a process also referred to as 'the return of geopolitics'. This is placing the existing multilateral system of cooperation and the international order associated with it under considerable pressure. At the same time, there is a strong interdependence between the key players, particularly in financial and economic terms.
An important question for the coming period is therefore whether geopolitics will dominate global relations or whether interdependence will have a moderating effect. The most likely scenario for the coming five to ten years is an *fusion* of a more multipolar world with elements of a multilateral system, in other words, a world in which cooperation will be more dependent on relations between the great powers – the US and China in particular – and will be more ad hoc and therefore outside the formal frameworks of current international organisations.
In short, the world order will be characterised by a mix of rivalry and cooperation, the latter to the extent that cooperation serves the interests of the major powers.

Beneath this global level there are signs of a complex *regional* pattern of relations. Three '*hot spots*' are of particular relevance in terms of existing or potential threats. First, in East Asia, China's regional ambitions are clashing with the role of the US as *security provider* for a number of countries in the region (among others, Japan, South Korea and Taiwan) and therefore with the US role of '*balancer*', i.e. as a counterweight to China's political aspirations. The dynamics in this region and the further development of Sino-US relations in particular will to an important extent determine the nature of the *global* system.

Second, future developments in the security and political situations in the MENA region and Sub-Saharan Africa will be important. The serious destabilisation within this region has been amplified by the control gained by the Islamic State of certain parts of Syria and Iraq, Boko Haram's operations in Nigeria and al-Shabaab's operations in the Horn of Africa. In combination with the disintegration of countries such as Yemen, Libya, Mali and the Central African Republic and an international community that is unable to adequately oppose these groups, further destabilisation seems likely as a result of, among other things, the further spread of destabilising and terrorist activities to other countries in the region and

[11] See Jan Rood, Frans-Paul van der Putten and Minke Meijnders, *Een wereld zonder orde? Clingendael Monitor 2015*. The Hague: Clingendael, Netherlands Institute of International Relations, February 2015.

beyond. To the extent that this further destabilisation occurs, the external-internal security nexus means that there will be consequences for the Netherlands and its European partners in the form of terrorist threats, refugee flows, crime and so on.

The third hot spot is the eastern part of Europe, where an ambiguous conflict is taking place. The hostilities between Russia and Ukraine in particular will determine future relations on the European continent. A factor of decisive importance in this context is that Russia is no longer willing to accept the starting points of territorial integrity and recognition of sovereignty that crystallised in post-war Europe during the Cold War and especially in the years following the Cold War. In addition, Russia is turning its back on the West, particularly in terms of the values fostered by the EU, since these values are a potential threat to those in power in Moscow. The current situation as a whole, which includes feelings, whether manipulated or not, of frustration and humiliation and the likelihood of continuing economic decline, suggests a permanent risk of instability in the eastern part of Europe. The scope and intensity of Russian aggression are difficult to predict and will in part depend on the Western/European stance taken. The current form of ambiguous warfare and undermining of stability give Russian leaders ample scope to cause unrest in surrounding territories if they wish to do so. In any case, finding a new *modus vivendi* with Moscow will be one of the great challenges in the coming years for the EU/the West.

The broader context therefore shows an unsettled world order in which the territory of the EU is surrounded by a belt of instability or, in the words of *The Economist*, a 'ring of fire'.[12] Above all, the associated range of threats is diffuse. Threats are often interrelated and frequently reinforce each other. Examples in this regard include criminal activities and abuse of the cyber domain, economic warfare conducted by means of cyber tools and espionage, and the use of the proceeds of crime to fund terrorist activities. These examples underline the fact that effective combating or deterrence requires an integrated approach, in other words, the availability and use of a broad range of assets. In addition, action will in many cases have to be taken in cooperation with other countries within the framework of the EU or NATO. Action must of course also be taken independently as and when possible. International cooperation is required because in many cases threats manifest themselves through the territories of other countries, because the Netherlands has committed itself to the protection of partners on the basis of agreements, and because the Netherlands is and will be too small on its own to act as an effective counterweight to state actors like Russia and China.

The five main areas of threat

There are different direct and indirect threats facing Dutch society. As stated, this study focuses on cyber threats, threats in the economic domain, terrorist threats, the threats posed by organised crime and the threats emanating from ambiguous warfare. Although these threats are not new in and of themselves, the way in which each threat manifests itself has changed. The threats are discussed in detail individually in separate appendices. This section provides an outline of the current situation and expectations for the coming five to ten years in terms of the nature of each threat and the way in which it will manifest itself in the coming

[12] See Jan Rood, *Een wankelende wereldorde: Clingendael Strategische Monitor 2014*. The Hague: Clingendael, Netherlands Institute of International Relations, June 2014; 'Charlemagne: Europe's ring of fire'. In: *The Economist*,20 September 2014.

period. It also discusses expected future developments. Each main area of threat concerns threats that could affect the Netherlands, at least in part, from abroad.

To start, the Netherlands faces *terrorist threats*. As a result of recent events in Paris and elsewhere, the threat of terrorist violence has become more palpable in the Netherlands. For some time already, the Dutch government has held the view that the likelihood of an attack in the Netherlands or on Dutch interests abroad is substantial. At the same time, the nature of the terrorist threat has changed in recent years in that religious extremism has increasingly become a driving force. In addition, terrorism has become considerably more transnational. Growing international and cross-border terrorist networks such as al-Qaeda, the Taliban, Boko Haram, al-Shabaab, al-Nusra and Islamic State (IS) render the threat more acute. The growing number of individuals who travel to unstable areas in the Middle East and North Africa – and the risk of them joining a jihadist group upon arriving there – poses a tangible threat to Dutch security when these *foreign fighters* return to the Netherlands. *Foreign fighters* from across the world are being attracted mainly by the civil war in Syria and the rise of IS. The Dutch National Coordinator for Security and Counterterrorism (NCTV) estimates that around 190 Dutch fighters have travelled to jihad areas. Of this total, approximately 35 have returned and 30 have been killed.[13] The International Centre for the Study of Radicalisation and Political Violence (ICSR) believes the number to be even higher and estimates that there are approximately 200-250 Dutch foreign fighters.[14] The risk of an attack being carried out in the Netherlands by fighters who have returned from conflict zones (either on their own or as a group action) has increased. It must be noted in this regard that, as shown by the attacks in Paris and Canada, among others, sympathisers who remain at home also constitute a threat. Not all of the perpetrators of these attacks were fighters who had returned.

Terrorism is therefore not only a physical threat to individuals in the Netherlands and other countries. The main threat of terrorism lies in its potential to cause wider social unrest, which can in turn lead to further social polarisation between, and the radicalisation of, population groups. Given the permanent instability and ongoing conflicts in the MENA region and the spread of these conflicts to other areas, it is highly likely that there will be a permanent and possibly increasing terrorist threat to the Netherlands and its European partners. The MENA region, including Sub-Saharan Africa, West Africa and the Horn of Africa remain important operational areas for terrorist groups and therefore, in some cases, a breeding ground for terrorist activities on European territory. Combating the threat in the region themselves will remain difficult because of reluctance and a lack of unity within the international community on the one hand and because of the ability of these groups to embed themselves in societies or acquire an organised, quasi-state character (like IS and Boko Haram, for example) on the other. It is uncertain whether the terrorist threat will remain confined to this region. It cannot be ruled out that a further deterioration of the situation in Afghanistan and Pakistan will lead to a resurgence of threats emanating from that region. It is also imaginable that Russia may use terrorism as an instrument of ambiguous warfare.

[13] National Coordinator for Security and Counterterrorism (NCTV), *Beleidsimplicaties Dreigingsbeeld Terrorisme in Nederland 38*, The Hague: NCTV, 7 April 2015.

[14] Peter R. Neumann, 'Foreign fighter total in Syria/Iraq now exceeds 20,000', International Centre for the Study of Radicalisation and Political Violence, 26 January 2015, http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/ (consulted on 23 February 2015).

Two additional risks underline the threat that will in the future emanate mainly from the MENA region: the attractiveness of the movements there to foreign fighters, with the increasing risk of the use of violence by returning jihadis, and, in addition, the mobilising effect that radicalisation and polarisation within Western/European societies can have on foreign fighters and home-grown terrorists. The danger must also be seen in the light of the effective propaganda that terrorist groups transmit through the internet and social media for the purpose of recruiting, undermining the status quo and radicalising.

Second, to an increasing degree, the Netherlands is faced with *threats posed by the cyber domain*. The Dutch General Intelligence and Security Service (AIVD) views digital threats as being among the greatest threats currently facing the Netherlands.[15] Although the intensity and use of information and communication technology (ICT) has increased drastically in all sectors in recent years, security is lagging behind by some margin. The potential impact of a cyber attack is therefore considerable. According to the Dutch National Cyber Security Centre (NCSC), states (cyber espionage) and criminals (cybercrime) currently pose the largest threat.[16] Less of a threat is currently posed by terrorists, cyber vandals, hackers and script kiddies.[17] The purpose of cyber espionage is to obtain sensitive information of companies, citizens or the government about, for example, defence, foreign, economic or energy policy. According to the NCSC, the number of attacks carried out by other states has increased sharply, as well as the intensity and impact of the attacks. Cyber espionage and cybercrime are to an important extent aimed at the business sector and therefore cause considerable economic damage. It remains very difficult, however, to determine the exact amount of losses suffered. At the beginning of this year, for example, it became clear that an international digital bank robbery had taken place. No less than 100 banks in 30 different countries were targeted and the perpetrators managed to steal EUR 260 million.[18] Attacks carried out through the cyber domain can also be directly aimed at sabotaging the social and economic infrastructure. Such attacks can cause serious disruptions if successful. With economic hubs such as the port of Rotterdam and Schiphol airport, and with the Amsterdam Internet Exchange (AMS-IX) being one of the most important internet exchanges in the world, the Netherlands is especially vulnerable to such attacks. These vulnerabilities may be exploited in situations of ambiguous warfare and conflict. The internet has also created new possibilities that could make the threat posed by criminals and terrorists more acute, including possibilities to offer merchandise and recruit sympathisers.

Although diffuse, the threat emanating from the cyber domain and the threat of organised crime will probably become greater for the Netherlands. The increase of cybercrime is primarily caused by the fast pace of developments in ICT, the increasingly easy access to this technology, and the increasing reliance of societies on uninterrupted ICT services. These factors make modern societies like the Netherlands more vulnerable to abuse of the cyber domain. Moreover, such abuse does not necessarily have to take place in the Netherlands to affect the country. Because of the international interconnectedness of all kinds of systems (satellites, financial transactions, etc.), the proper functioning of Dutch institutions could also be undermined by cyber attacks on other countries or non-Dutch agencies.

[15] General Intelligence and Security Service (AIVD), *Jaarverslag 2013*. The Hague: AIVD, April 2014.

[16] National Cyber Security Centre (NCSC), *Cybersecuritybeeld Nederland: CSBN-4*, July 2014, p. 7.

[17] Individuals who misbehave on the internet and use scripts or programs developed by others to do so.

[18] ‘Digitale bankrovers stelen zeker 260 miljoen euro’. In: *NRC Handelsblad*, 16 February 2015.

The two main threats of the cyber domain, cybercrime and cyber espionage, will in all likelihood become more acute in the future. Increasing cybercrime is partly a result of the low probability of getting caught and the easy access to ICT. Instances of cyber espionage will probably occur more frequently, also by friendly nations. On the one hand, this is related to the need to gather intelligence in response to threats like terrorism. On the other hand, it comes naturally in a world that is more strongly defined by geopolitical tensions and economic competition. The use of cyber capabilities will therefore not be limited to traditional industrial espionage. State-sponsored spying will also take place in the economic domain. The use of cyber capabilities in the context of ambiguous warfare will probably likewise increase.

Third, the Netherlands also has to deal with the threats posed by national and international *organised crime*. Organised crime manifests itself in many different ways. In its National Threat Assessment, the Netherlands Police Agency (KLPD) distinguishes between three categories of criminal phenomena: various illegal markets (drug trafficking, human trafficking or child pornography, for example), money laundering and fraud, and property crime (the police use this term to refer to 'middle segment' crimes like burglary and theft).[19] The nature of organised crime is closely linked to the geographic position and physical and digital infrastructure of the Netherlands and can best be described as 'transit crime'.[20] Organised crime focuses on international trade. The Netherlands plays a major role in the international criminal market, particularly in terms of drug trafficking, human trafficking, fraud, money laundering and cybercrime. As stated in the most recent Organised Crime Monitor, however, it is extremely difficult – if not impossible – to determine the total damage that it causes because it also concerns intangible issues such as loss of reputation.[21]

Given its geographic position, the Netherlands will remain attractive to internationally operating criminals in the coming five to ten years. Organised crime will be a threat mainly to social and political stability. It can disrupt the functioning of the market, lead to a loss of confidence in trade and the financial sector, and harm the reputation of important economic hubs like Schiphol airport and the port of Rotterdam as safe points of transit. The more successful criminals are in establishing themselves in legitimate society through bribery and corruption, the greater the effect of organised crime will be. In addition, organised crime could also have negative economic effects through a broad range of activities, including in particular cybercrime, money laundering and all kinds of illegal transactions, that undermine confidence in the economy.

Developments outside the Netherlands are an important catalyst in this regard. Given the instability in the MENA region described above, there is a greater risk that refugee flows will be abused by human traffickers as a channel for the 'export' of terrorist activities. In any case, areas that lose effective forms of government control may become sources of criminal activity and may then serve as springboards from which criminal operations in Europe are launched. In view of the instability in the MENA region, this risk is becoming more acute. It must be

[19] F. Boerman, M. Grapendaal, F. Nieuwenhuis and E. Stoffers, *Nationaal Dreigingsbeeld 2012: Georganiseerde Criminaliteit*. Zoetermeer: Netherlands Police Agency (KLPD), p. 30-31.

[20] E.W. Kruisbergen, H.G. van de Bunt and E.R. Kleemans, *Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. The Hague/Rotterdam: Research and Documentation Centre (WODC)/Erasmus University Rotterdam (EUR), 2012, p. 16.

[21] Idem, p. 34.

noted in this regard that government authorities in parts of Latin America have lost control of certain areas of their respective territories to criminal groups as well.

Fourth, there are also threats to the Netherlands *in the economic domain*. The nature of these threats is closely linked to the Netherlands' open and internationally oriented economy. The threats originate from a variety of actors (states, criminal organisations and terrorists) and also differ in terms of type. First, there is the possibility of explicit or implicit economic pressure. An example in this regard are the sanctions imposed by Russia last summer as a response to the European and US package of sanctions put in place following Russia's annexation of Crimea. Sanctions are being used more frequently as a way of asserting political pressure and are greater in scope and more effective than was the case in the past, mainly because of the high degree to which the Netherlands is interconnected with the international market. Second, the strategic economic policy of other states can, for instance if such policy is part of hybrid warfare, affect Dutch national security by limiting access to raw materials that are important to the Netherlands, for example. Third, instability in areas of importance to the Netherlands can have adverse effects, in terms of, for example, the supply of essential raw materials. . These threats mainly affect the economic security of the Netherlands. Finally, there are threats that emanate from the overlap between the economic and cyber domains. These threats can disrupt core economic processes, including power generation, communications, transport and monetary transactions, and so forth. This might not only have consequences for the Netherlands' economic security, but could also potentially affect social stability in the country.

The expectation is that threats in the economic domain will not decrease in the future, not least because of the broader global context outlined above, which suggests a world that will become less ordered and less stable in the coming years. In cases where the Netherlands has an economic interest in a global system that is open and stable, especially in financial and economic terms, this interest will come under further pressure. In this more volatile world, particularly at regional level, the risk to direct Dutch interests in terms of free access to markets, the unhindered transport of goods by water and air, and the uninterrupted supply of energy and raw materials will be greater as a result of economic competition and political tensions (including sanctions), regional instability and conflicts, and possible domestic political unrest. Especially as regards the supply of raw materials and energy, the Netherlands in cooperation with its European partners depends on countries or regions with which relations are tense (Russia), regions that are unstable (MENA region) or countries whose long-term stability is far from certain (Saudi Arabia). This situation will most likely not improve in the foreseeable future.

Finally, there is a specific phenomenon that has recently garnered quite a bit of attention, namely *ambiguous warfare*. Warfare is ambiguous when one of the parties involved in the armed conflict takes covert action, conceals its identity, pretends to be a different party or wrongly denies that such action is directed against the adversary. Such action is often aimed at causing confusion and uncertainty, in respect of which the ability to deny responsibility is a key element to the perpetrator.[22] Exactly because of the use of advanced, modern technology and the high degree to which countries are interrelated, such warfare is now

[22] Ambiguous warfare is not the same as hybrid warfare. Ambiguous warfare is waged on the basis of being able to deny involvement, whereas hybrid warfare is based on the use of all possible means, including economic and diplomatic, propaganda, cyber attacks and so on. These two types of warfare can occur in combination.

Russian soldiers at the military base in Perevalne, Ukraine, during the annexation of Crimea in March 2014.
Foto: Anton Holoborodko/Wikimedia Commons.

easier to conduct. It is also more effective and its impact is possibly greater. A state that is engaging in ambiguous warfare may make use of anonymised military assets, whether or not in combination with non-military means such as implicit economic pressure and cyber attacks. Large-scale information and propaganda campaigns and the provision of covert support to local *proxy* groups can contribute to the creation of uncertainty regarding the identity of the actor responsible for a certain action. One characteristic of this type of warfare is that the actor in question strives for deniability of its involvement, making it harder to justify counteraction. A current example of ambiguous warfare is Russia's military action in Ukraine (see Box 1). The threat of ambiguous warfare is relevant to the Netherlands in terms of the functioning of the international legal system, the credibility of NATO and the EU as organisations that are crucial to our national security, and the danger of direct or indirect damage to our vital infrastructure as a result of ambiguous warfare.

The threat to the Netherlands and its European allies will in the future emanate mainly from Russia. It seems likely that Russia will maintain its current position and use all of the means at its disposal to try to influence its Near Abroad. This also implies attempts to divide the West by setting countries against each other or turning public opinion in favour of the Russian viewpoint. A variety of activities that form part of this kind of ambiguous warfare must therefore be taken into account. These activities may range from subtle economic sanctions or support, through propaganda, disinformation, political manipulation and influence, to direct activities carried out through the internet and other means aimed at undermining the status quo. For the Netherlands and the EU, the threat for the coming period will emanate primarily from Russia. There is a real chance that other countries will also realise the advantages of this kind of warfare and that it will therefore occur more frequently.

Box 1 The crisis in Ukraine and ambiguous warfare

The hostilities in the eastern part of Ukraine and Russia's annexation of Crimea in March 2014 focused attention on ambiguous warfare. According to Western analysts, Russia is playing a major role in East Ukraine and Crimea. The 'little green men' in Crimea turned out to be members of Russia's special forces and naval infantry units, for example. In addition, an arsenal of weapons was provided to Ukrainian separatists with coordination and support from Moscow. The presence of artillery, tanks and advanced anti-aircraft missile systems in the eastern part of Ukraine seems to confirm the involvement of Russian troops. In the same vein, an increase in the number of violations of EU and NATO airspace by Russian military aircraft,[23] the cyber attacks on and abductions in the Baltic states and the possible presence of a Russian submarine in Swedish waters have increased tensions between Russia and the West.

These military actions and the involvement referred to are part of a broader strategy that includes the use of a broad range of means such as indirect interventions, covert operations, efforts to politically influence the adversary, economic blackmail, cyber attacks, propaganda and deception. Russian action is not limited to its immediate neighbours. It is also aimed at sowing division among EU and NATO member states for the purpose of, among other things, undermining support for heavier sanctions against Russia. Russia is taking action in this context by offering financial support to populist parties on both sides of the political spectrum within the EU, bribing politicians and influential members of the business community, and putting countries that depend on Russia for their energy supply under pressure. In addition, a disinformation campaign is being waged in Russia itself by the Kremlin-controlled Russian media. Some believe that other states may follow Russia's example and conduct this kind of warfare. Asian countries involved in territorial disputes in the South China Sea, for example, may likewise resort to ambiguous warfare, thereby creating new tensions. The same applies to countries in the Middle East. A key question for the West is how to respond to potential and actual ambiguous warfare.

The relevance of deterrence as a security concept

The ways in which deterrence as a security concept is relevant to the five main areas of threat on which this report focuses are discussed below. The discussion is arranged according to the analysis framework introduced in the second section and is based on the exploratory analysis of each main area of threat. These exploratory analyses are included as appendices to this report.

Deterrence in relation to all five main areas of threat

The purpose of deterrence is to discourage potential perpetrators by influencing their assessment of costs relative to potential gains. If the expected costs associated with carrying out an act that is harmful to the Netherlands increase and/or the expected gains decrease, carrying out the act becomes less attractive to the would-be perpetrator. Therefore, where

[23] Lizzie Dearden, 'Full list of incidents involving Russian military and NATO since March 2014'. In: *The Independent*, 10 November 2014.

possible, measures that focus on both the costs side and the gains side constitute the most effective approach.

Regarding the main areas of threat discussed in this report, three forms of deterrence seem to be suitable in many cases. First, on the costs side, there is the threat of retaliation by legal, economic or military means. A harmful act is less attractive to carry out if a would-be perpetrator knows that such an act is highly likely to trigger undesirable retaliatory measures. Second, on the gains side, it is possible to increase society's resilience, for instance by means of crisis management measures or other measures that strengthen the public's confidence. Such measures reduce the effectiveness of attacks aimed at causing social unrest and therefore make them less attractive to the potential attacker. Third, it is possible to take additional security measures by investing in monitoring and in physical or technological barriers. Such measures can influence the assessment of costs relative to potential gains because they increase the investments that perpetrators must make, i.e. increase the costs that perpetrators must incur, and, in addition, reduce the probability of success, i.e. reduce the potential gains. The *perception* of the would-be perpetrator regarding the balance between costs and gains is decisive in all forms of deterrence. An essential part of all deterrence measures is therefore their visibility. In other words, communication about such measures must be very clear, because measures that are unknown to potential perpetrators cannot have a deterrent effect in relation to the specific target group.

Regarding the relevance of deterrence with respect to the different actors, it can be said that improved security applies in all cases. The relevance of retaliation and greater resilience differs per actor, however. As discussed in greater detail below and in the appendices, retaliation is less effective against terrorists and strengthening society's resilience is less effective against criminals. The motives of the actors are the main variable in this regard. Actors who do not fear retaliation, such as terrorists, cannot be deterred by the threat of retaliatory action, just as investments to increase resilience will not have a deterrent effect on actors, such as criminals, who are not seeking to cause social disruption. In the case of state actors, the relevance of deterrence depends on the motives of the actor in question.

Finally, it must be noted that many of the means referred to below can serve several security purposes. In other words, they can also contribute to greater security in ways other than deterrence. This applies to investments in improved security or crisis management, for example. Even if they do not have a deterrent effect, such investments can help to limit the damage caused by attacks. What differs in this regard from the deterrence function is that the emphasis shifts from the perception of would-be perpetrators (*does the visibility of additional security measures have a discouraging effect?*) to the concrete operation of such measures (*is an actual attack more difficult to carry out?*).

TERRORISM

Relevant actors

- Individual terrorists/terrorist organisations;
- Facilitators.

Effect on the perception of costs

The effect of retaliatory threats is in many cases limited, since, due to their religious or political convictions, terrorists tend not to fear retaliation. Taking retaliatory measures can even be counterproductive because they can generate greater support for terrorists in the population groups from which they originate. The observable reinforcement or greater visibility of defence mechanisms such as the physical presence of security personnel or surveillance assets contributes to deterrence against terrorism because it forces perpetrators to make larger investments in preparing an attack.

Effect on the perception of gains

Measures aimed at reducing opportunities to carry out an act of terrorism or the probability of success of such an act constitute a relevant instrument of deterrence. Visible investments in defence mechanisms can therefore be important also on the gains side. In this case, it is not about the greater investment that perpetrators must make, which is the concern on the costs side. It is, rather, about the assessment that the probability of success is decreasing. Capabilities that visibly contribute to the early detection of attempts to launch attacks (intelligence services) can therefore deter terrorists. Convincing terrorists that acts of terrorism do not contribute to the objective that they are trying to achieve likewise has a certain deterrent effect. Counternarratives are a way of doing this or of reducing support for terrorists in their social environment. Another relevant method is visibly increasing resilience within society, for instance, in terms of being well prepared for emergency situations and in terms of public confidence in the functioning of the government. A resilient society is disrupted less quickly and acts of terrorism are therefore less meaningful. A high level of social resistance in terms of not being receptive to extremist or terrorist ideology can also influence terrorists' assessments of potential gains.

Categories of possibly relevant instruments

- Criminal law;
- Physical and digital security;
- Communication;
- Crisis management;
- Deradicalisation policy;
- Counternarratives;
- Improved detection capabilities.

CYBER THREATS

Relevant actors

- States (including hackers directed by states);
- Individual criminals/criminal organisations;
- Individual terrorists/terrorist organisations.[24]

Effect on the perception of costs

The counterthreat of retaliation is limited in terms of effect because it can be difficult to identify the perpetrator of an attack (if the perpetrator wished to remain hidden) or even to detect the attack itself (if it concerns espionage). To identify a perpetrator and take retaliatory measures, it is often important to have the cooperation of the country in which the perpetrator is based. This cooperation will of course not be extended if state actors are carrying out the attacks. Retaliation in the context of cyber threats can include, among other things, prosecution and punishment (in the case of criminal actors) or economic sanctions (in the case of state actors). Moreover, a greater counter threat against state actors can be created using military means (conventional or cyber warfare). In April 2015, for example, the US government announced that it would retaliate, militarily if necessary, in the event of serious cyber attacks by other states on its national security.[25] The difficulty of determining a suitable degree of proportionality complicates retaliation, however. The observable improvement of defence mechanisms contributes to deterrence against cyber threats if this improvement results in higher costs in terms of money or time on the part of the perpetrator.

Effect on the perception of gains

Convincing politically motivated actors (states or terrorists) that they will not reach their objectives through carrying out cyber attacks contributes to deterrence.
A relevant way of doing so is visibly increasing what is referred to as cyber resilience, for instance, by ensuring redundancy. This method may discourage cyber attacks that are carried out by states and aimed at causing disruption. It would be less effective against cyber attacks carried out for the purpose of espionage or the illegal amassing of assets, since any disruptive effects are not directly relevant to the perpetrator in such cases. In addition, visible investments in improved defences such as multi-layered firewalls, advanced encryption and authentication systems and so-called 'honeypots' are relevant if they lead would-be perpetrators to believe that the probability of success is lower.

[24] This does not include 'smaller' actors like script kiddies and hacktivists and the like. *CSBN-4* indicates that states, terrorists and professional criminals pose the greatest threat (National Cyber Security Centre, *Cybersecuritybeeld Nederland: CSBN-4*, July 2014).

[25] US Department of Defence, 'Carter Unveils New DoD Cyber Strategy in Silicon Valley', 23 April 2015, http://preview.defenselink.mil/news/newsarticle.aspx?id=128659; 'Preparing for Warfare in Cyberspace'. In: *The New York Times*, 28 April 2015.

Categories of possibly relevant instruments

- Criminal law;
- Cyber security (encryption and the like);
- The ability to expose perpetrators;
- Increasing cyber resilience.

CRIMINAL ORGANISATIONS

Relevant actors

- Individual criminals/criminal organisations;
- Facilitators.

Effect on the perception of costs

Deterrence by means of the threat of retaliation (prosecution and punishment) is relevant as a security concept against criminals. In addition, the threat of limited retaliation against individuals in the social environment of criminals (facilitators) may be relevant in the context of weakening the support that criminals receive from this environment. This support is often essential to criminals because they base their reputations and status on it. The threat of limited retaliation can include measures aimed at the financial interests of these facilitators, for instance, by seizing the property of the confidants and family members of convicted criminals. Retaliation can also be effective against facilitators who operate behind a legal façade in order to support an illegal objective. They have a reputation to lose and can be deterred by the threat of being openly associated with criminal activity. The application of deterrence by retaliation at international level usually requires the cooperation of the country in which the criminals or their facilitators are based. Strengthening defence mechanisms increases the costs required to perform criminal activities. Doing so is therefore a relevant, additional deterrence measure also with respect to criminals.

Effect on the perception of gains

It is unlikely that criminals can be convinced that the ultimate objective of harmful acts cannot be achieved. Deterrence by means of strengthening resilience therefore seems to be ineffective in this case. On the gains side, only measures aimed at reducing opportunities to carry out criminal activities or the probability of success of such activities constitute a relevant instrument of deterrence. Visible investments in defence mechanisms are a key element of this approach.

Categories of possibly relevant instruments

- Criminal law;
- Physical security;
- Cyber security;
- The ability to expose perpetrators.

THREATS IN THE ECONOMIC DOMAIN

Relevant actors

- States;
- Individual criminals/criminal organisations;
- Individual terrorists/terrorist organisations.

Effect on the perception of costs

Deterrence by means of the threat of retaliation (economic sanctions) is relevant as a security concept against state actors that pose a threat in the economic domain. This form of deterrence is also relevant in the case of criminal organisations that do so. The effectiveness of the threat with sanctions as a means of retaliation is substantially greater if it is made in a multilateral context. Targeted sanctions (smart sanctions) can be more effective or have fewer harmful side effects than broad sanctions. It seems unlikely, however, that the threat of a foreign consumer boycott could be deterred by means of retaliation as a counter threat if the boycott concerned was initiated by social organisations and individuals rather than state actors. As is the case with the other main areas of threat, better defence mechanisms are relevant in the economic domain in the case of attacks by criminals or terrorists. Increasing the likelihood of damage to the perpetrator's reputation can also have a deterrent effect on state actors. For this specific kind of deterrence to work, however, there must be clear standards that are violated by states when they threaten the security of other states such as the Netherlands in the economic domain.

Effect on the perception of gains

If states are seeking to exert pressure by causing economic or social disruption through action in the economic domain, undermining the idea that this objective is achievable can contribute to deterrence. Having alternatives is an example in this regard. A relevant way of doing so is visibly increasing resilience. Visible investments in defence mechanisms, such as better internet security in the case of economic and other cyber threats, can influence perpetrators' perceptions of gains.

Categories of possibly relevant instruments

- Economic policy;
- The policy option of imposing sanctions;
- The ability to expose perpetrators;
- Physical and cyber security.

AMBIGUOUS WARFARE

Relevant actors

- States.

Effect on the perception of costs

The counter threat of retaliation is less effective in this case because ambiguous warfare by definition makes it difficult or even impossible to identify the perpetrator. In the case of covert action, even the ambiguous act itself is difficult to detect. The threat of retaliation can have a deterrent effect if the threat is accompanied by a visible ability to identify the actor that is conducting ambiguous warfare. To be effective, this ability must mean that the identity of the perpetrator can be demonstrated in a convincing manner so that the identification is accepted by third parties (public opinion, the international media and so on). If the foregoing is the case, retaliatory measures can include the use of military means or economic sanctions. Retaliatory action taken in a multilateral context is considerably more effective. In this case, retaliation has the same effect as deterrence against traditional military threats (see Box 2). In addition, retaliation by means of ambiguous counteraction is also possible. The drawback of taking such action, however, is that it would in the long term undermine the effect of the standards in place to prevent ambiguous warfare. Apart from retaliatory measures, better defence mechanisms can also contribute to deterrence against ambiguous warfare if they are combined with a visible ability to convincingly demonstrate the identity of the actor conducting the ambiguous warfare. Increasing the likelihood of damage to the perpetrator's reputation through exposure of the perpetrator's identity in combination with the presence of widely accepted standards against ambiguous warfare can also influence the assessment of costs in that they will be deemed to be higher.

Effect on the perception of gains

If states conduct ambiguous warfare for the purpose of disrupting a society or an international coalition, undermining the idea that this objective is achievable can contribute to deterrence. A relevant way of doing so is visibly increasing the resilience of the society or coalition concerned, for instance by showing that an adequate crisis management system is in place and thereby ensuring that the public's confidence in the functioning of society is not easily undermined. This form of deterrence does not apply in the case of ambiguous warfare that is being carried out to achieve more limited objectives such as territorial gain. Finally, greater defence capacities, in the first place by military means, can also contribute to deterrence if these capacities reduce the probability of success as perceived by the attacker.

Categories of possibly relevant instruments

- The ability to carry out a hybrid counteroffensive;
- Military means;
- Economic means/the policy option of imposing sanctions;
- Diplomacy, physical and digital security;
- The ability to expose perpetrators;
- Crisis management;
- Communication/counternarratives.

Box 2 Deterrence as an instrument against traditional military threats

In this box, the following definition of traditional military threat is used: 'the open threat posed by regular armed forces to a state's territorial integrity or interests that could potentially compromise the threatened state's sovereignty.' In contrast to ambiguous warfare, a traditional military threat is a visible one and the state responsible can be identified.

The territorial integrity of the Netherlands does not appear to be threatened at the present time. Even when considering the Kingdom of the Netherlands as a whole, it can be said that, with the relative normalisation of Venezuela's regional position, there is no direct threat. If we also take NATO-related obligations and participation in military peacekeeping and stabilisation missions into account, however, the probability that the Dutch armed forces will have to deal with traditional military threats is considerably higher. Threats that are not directly aimed at the Netherlands and against which the Dutch armed forces take action in a multinational context are therefore the ones that will probably occur the most for the time being. Historically, deterrence has been used as a security concept against traditional military threats and will therefore remain relevant also to the Netherlands in the context outlined.

A first option in terms of creating deterrence against traditional military threats is having a powerful military. An actor will not use military assets in a traditional sense if that actor believes that the adversary is militarily powerful enough to prevent the achievement of the intended objective by military means. If it is not possible to achieve an adequate level of power for the purpose of deterrence by means of conventional troops and weapons and weapon systems, the aim can perhaps be achieved by means of unconventional military means.[26] However, the Netherlands decided against having nuclear, chemical or biological weapons. A second option, which the Netherlands is indeed making use of, is to become a member of an alliance. Such an alliance can as a whole be capable of maintaining adequate military potential to deter possible adversaries. A third option in terms of creating deterrence is the ability to make decisive use of the state's non-military weapons,[27] particularly economic ones. The ability of the Netherlands to achieve deterrence on its own by means of non-military weapons is limited, however. The fourth option is therefore to establish ties of international cooperation that enable economic pressure to be exerted. This option is available to the Netherlands through its membership of the EU. If used as a non-military weapon as and when necessary, the EU economy as a whole would be a very significant factor and therefore constitutes a kind of deterrence.

The Netherlands has conventional military assets and economic means that can be used for deterrence purposes, preferably in the context of international action. In the case of traditional military threats, both can be divided into deterrence in terms of increasing the costs for the attacker (mainly because of the threat of retaliation) and deterrence in terms of reducing potential gains (mainly because of greater resilience).[28] The Netherlands does not have its own nuclear military capability for the purpose of deterrence. Nuclear military capability was central to the concept of deterrence during the Cold War. Nevertheless, as was the case during the Cold War, the Netherlands is under NATO's 'nuclear umbrella' and deterrence based on nuclear military capability therefore indirectly remains relevant as a form of deterrence against traditional military threats. Although nuclear deterrence receded to the background following the end of the Cold War, partly because of its limited relevance in the context of non-traditional threats,[29] the situation now appears to be changing somewhat. Current geopolitical developments are drawing attention back to the role of nuclear deterrence. This is particularly the case regarding relations between the US, Russia, China and India. As a result, however, many other countries may focus more on the option of nuclear deterrence.

Conclusions

This study explores the possible usefulness to the Dutch government of deterrence as a security concept with respect to the non-traditional security threats of terrorism, crime, threats in the cyber and economic domains, and ambiguous warfare. The starting point in this regard is that deterrence can be achieved by influencing the costs versus gains assessment of potential perpetrators or their facilitators such that it is less attractive or unattractive to perform or support harmful acts.

The ***main conclusions*** of this study are, first, that deterrence as a security concept is relevant to all of the five main areas of threat discussed and, second, that the most effective

[26] CBRN: Chemical, Biological, Radiological/Nuclear, and also cyber, for example.

[27] DIME: Diplomacy, Information, Military and Economy.

[28] Regarding conventional military deterrence, see Jon Solomon, 'Conventional Deterrence Requires Forward Presence'. In: *Information Dissemination*, 14 October 2014; 'Conventional Deterrence in the Second Nuclear Age'. In: *Carnegie Endowment for International Peace*, 17 November 2010; Maren Leed, 'The Role of Conventional Forces in Deterrence'. In: *Global Forecast 2015*, Centre for Strategic and International Studies, 2014.

[29] Adam Lowther, 'Framing Deterrence in the Twenty-First Century: Conference Summary'. In: Anthony C. Cain (ed.), *Deterrence in the Twenty-First Century: Proceedings*. Maxwell Air Force Base: Air University Press, 2010.

kind of deterrence depends on the main area of threat in question and the specific actors in that context. An effective deterrence policy should therefore be tailored to a specific area of threat and, where possible, specific groups and actors. Little is as yet known about the effectiveness of actual deterrence instruments.

The report also presents ***additional conclusions***, which are set out below.

- These additional conclusions are based on the analysis framework used. The most effective form of deterrence is one that addresses both the costs and gains side:
  a. *The costs assessment* of potential perpetrators can be directly influenced by means of the threat of retaliation. This method seems to be most suitable as deterrence against criminal activity (by means of prosecution and punishment, for example) and economic threats posed by state actors (by means of countersanctions, for example). The more difficult it is to identify the perpetrators, the less effective the threat of retaliation. The effectiveness of this method against cyber threats and ambiguous warfare is therefore limited. Moreover, it is difficult in both cases to determine the proportionality of retaliatory measures. The effectiveness of this method is also limited with respect to terrorist threats, particularly in the case of terrorists who do not fear retaliation. Taking retaliatory measures can even be counterproductive in that they can generate greater support for terrorists in the population groups from which they originate. In the case of criminals, the threat of limited retaliation against individuals in their social environment can be relevant in the context of weakening the support that criminals receive from this environment. The costs assessment of perpetrators can be indirectly influenced by convincing them that major investments are necessary. The most important way of achieving this objective is by visibly improving or emphasising defence mechanisms. This applies to all of the five main areas of threat discussed in this study.
  b. *The assessment of potential gains* can be directly influenced by reducing opportunities to carry out harmful acts or the probability of success of such acts, or at any rate by generating the impression that success is less likely. Visible investments in defence mechanisms are important and relevant to all of the five main areas of threat. In the case of ambiguous warfare, investments could be made in, for example, defensive, individual or collective military or cyber capabilities and the visible strengthening of the ability to identify and expose the perpetrator. Capabilities that visibly contribute to the early detection of attempts to launch attacks can deter terrorists. The gains assessment of perpetrators can be indirectly influenced by convincing them that harmful acts do not contribute to the achievement of their respective objectives. Although this probably does not apply in deterrence terms to criminals, it applies to politically motivated actors (terrorists and states). An important measure in this regard is visibly increasing the resilience of society so that it is less easily disrupted by terrorist acts or state threats.

- With respect to all measures discussed, international cooperation considerably strengthens the deterrence capability of the Netherlands. In many cases, effective deterrence is probably not even possible without international cooperation. When taking diplomatic and economic retaliatory measures, the Netherlands is far more effective when acting in concert with international partners. International cooperation is also important in terms of acquiring the intelligence required to identify an actual or potential perpetrator. The ability to identify and expose a perpetrator is a key part of an effective deterrence policy.

- It is also important to note that deterrence aimed at preventing *Dutch* interests from being compromised is less far-reaching and therefore possibly easier to achieve than forms of deterrence that reduce the level of threat posed by *any country whatsoever*. The need for joint action in an international context as a condition for an effective deterrence policy implies, however, that deterrence aimed solely at protecting Dutch national security is inadequate.

- To achieve effective deterrence, in addition to *international* cooperation, there are a few more conditions. The measures taken must be *credible*, the deterrence message must be clearly communicated to the potential perpetrator (*communication*), the threat and the actors from which it emanates must be known (*intelligence*), and the deterrence must be based on actual *capabilities* and an *integrated approach* (it must deal with both the costs and gains side through several policy domains and types of capabilities).

Appendices

Appendix 1

Deterrence as a security concept against terrorism

Bibi van Ginkel

Current situation

Developments in the period 2014 to the beginning of 2015 were in keeping with the trends identified in the recently published 2014 *Global Terrorism Index*. It records a sharp rise in the number of lives lost to terrorist activity in the period 2012-2013 (+61%). Over 80% of the deaths occurred in only five countries: Iraq, Afghanistan, Pakistan, Nigeria and Syria. In 2013, a total of 17,958 people were killed in approximately 10,000 terrorist attacks. It is striking that OECD countries were relatively unaffected. In 2013, 113 people lost their lives in over 300 incidents.

The five most heavily-affected countries also reflect the terrorist organisations and networks that were most active in recent years: al-Qaeda (Iraq/Syria), the Taliban (Afghanistan), Boko Haram (Nigeria) and IS (Iraq/Syria). It must be noted that there is also permanent and in some cases increasing terrorist activity in countries other than the five referred to. This applies in particular to Yemen, Somalia/Kenya, Libya, Mali and the Central African Republic (CAR), where movements affiliated with the organisations referred to are active and sometimes even fight each other.

The current wave of terrorism is characterised by the increased prominence of religious extremism as a motivation for terrorist activity rather than political ideas or national separatism. A distinction is made in this regard between *dawa Salafism* and *jihadi Salafism*. In addition, the 'hot spots' of this terrorist activity are mainly countries or regions that are characterised by ethnic and religious differences, social and economic discrimination against certain groups and arbitrary state violence. Although there is not necessarily a direct causal link, the situation as a whole highlights the fact that regions that are characterised by instability and by fragile, authoritarian and failing states are particularly vulnerable to terrorism or are attractive locations for the organisation of terrorist activity.

Events of recent years have given this general view greater definition. First, Islamic State (IS) emerged as a 'state-based' terrorist organisation that is seeking to establish a caliphate in Syria and Iraq through violence. The organisation also has other objectives, including against the West. This development must be placed in a broader context, particularly, as emphasised in the Clingendael Strategic Monitor 2014, in terms of the MENA region's instability, which threatens to make the region a source of terrorism.

Second, as a result of the violence in Syria and the rise of IS, there has been a sharp increase in the number of foreign fighters who travel from OECD countries, Western European ones in particular, to Syria and Iraq to take part in the fighting. This development is partly the result of, and is accompanied by, the increasing radicalisation of young Muslims in Western countries in recent years. Moreover, it is no longer only young men who travel to Syria and Iraq. Young and older women and in some cases entire families are also going. The Dutch General Intelligence and Security Service (AIVD) refers to the 'swarm dynamics' of jihadism regarding the way in which jihadists organise themselves.

Third, as a result, the risk of returning jihadists posing a threat to Dutch and other Western societies has increased. That this is not only a theoretical threat is evidenced by the recent attacks in Brussels on the Jewish museum (May 2014) and in Paris on the head office of satirical magazine Charlie Hebdo and a Jewish supermarket (beginning of January 2015). These attacks also show that a risk is posed by jihadists who have not previously travelled to conflict zones, but nevertheless carry out attacks in their own countries in the name of jihadist organisations. In keeping with a current trend, police officers and military personnel were also targeted in the attacks in addition to civilians.

Fourth, the foregoing underlines the strong relationship between external and internal security and the vulnerability of open, Western societies. This vulnerability has increased in recent years in the Netherlands and other Western countries as a result of participation in the international coalition that is fighting IS. In addition, many European countries have become more polarised on the matter of Islam and the integration of migrants. This polarisation can make radicalisation more likely and is also increasing the risk of lone wolf terrorism.

Finally, the aim of terrorists is to cause social and political disruption and create fear. They were already making greater use of social media and the internet for recruitment and propaganda purposes, among other things. The rise of IS and the practice of releasing videos of hostage executions appear to have given this tendency a new dimension. To an even greater extent than was previously the case, communication is one of the key arenas in which the battle is being fought.

Expectation for the coming five to ten years

The threat level in the Netherlands has been at 'substantial' since spring 2013. Moreover, the government acknowledges that the level is rising to the upper limit within the bandwidth of this qualification. Today's society is becoming more aware of the risks and can also see that security measures are being tightened. Because of the risks, military personnel are currently not allowed to travel by public transport in uniform. To increase the level of national security, the Royal Netherlands Marechaussee has deployed additional personnel to secure and guard locations deemed to be at high risk. In addition, society is under pressure and the risk of social polarisation as a result of, on the one hand, reaction and resistance from Muslims to the strong language being used by the government and the measures being taken and, on the other, a stronger need within anti-Islamic groups to counter the 'Islamisation of the Netherlands', is very real. Indications of a continuing and possibly increasing terrorist threat to the Netherlands and other Western societies in the coming years mainly concern the MENA region's lasting instability and the spread of terrorist activity from this region to other areas, a possible development discussed in the Clingendael Monitor 2014 and the 2015 update and elsewhere. The MENA region is and will remain unstable and therefore a source of terrorism.

Although the terrorist threat, particularly as posed by foreign fighters, currently seems to be related mainly to the fighting in Iraq and Syria, the threat is real to the Netherlands as well. It must not be forgotten that there are clear links between jihadist, al-Qaeda-like groups in the Middle East, North Africa, East Africa, the Sahel region and South Asia. The risk of terrorist activity spreading to other unstable countries or regions is therefore considerable, also because of the possibility of jihadist fighters travelling to other hot spots from all parts of the world. The situation is further complicated by the rivalry between groups (in Syria, for example) and the use of groups by external powers as proxies to fight their conflicts, which increases the risk of unrest in, and the involvement of, other neighbouring countries.

Given the interests of Europe and the West that are at stake, particularly in terms of the external-internal security nexus, it will be necessary for Western countries, including the Netherlands, to remain involved in the MENA region and its hot spots, in whatever way (ad hoc, EU, UN and so on). This involvement, in combination with domestic radicalisation and polarisation, means that for the coming years the Netherlands will remain a potential target of attacks, either launched and organised from the outside or from within.

As regards the nature of the terrorist threat, trends that have been going on for some time will probably become more pronounced. These trends include the fusion of terrorism and criminal activity as a way of funding terrorist action, the use of social media and the internet for recruitment purposes, among other things, and responding to feelings of frustration and dissatisfaction, particularly among young Muslims in the West and in the region itself. Of particular influence is also the acquisition by an essentially non-state terrorist movement of a more state-like character (IS, Boko Haram) and the control exercised by this movement over large parts of a state's territory. This phenomenon may gain momentum in the future.

Sowing fear remains a key objective of terrorists. The increasing use of communication as a means of conducting the fight must be taken into account. In addition to sowing fear, setting population groups within Western societies against each other will be an important objective. The extent to which these movements succeed in achieving these objectives will depend strongly on the resilience of Western societies and the ability of their political establishments and governments to find adequate responses to such attempts made to undermine society.

The foregoing underlines the conclusions of the analysis in the Strategic Monitor 2014. The terrorist threat is and will remain diffuse and therefore unpredictable. Differences in root causes, motives, methods of communication and operation and the different levels at which this phenomenon manifests itself - national, regional and international - make it difficult to formulate a targeted policy, especially in terms of deterrence measures.

The relevance of deterrence as a security concept

In the literature, most authors do not consider deterrence to be an effective instrument against terrorism. It is asserted that terrorists are not affected by deterrence.[1] As an instrument, deterrence is known primarily in terms of the way in which it worked effectively during the Cold War in that two nuclear power blocs successfully prevented each other from carrying out nuclear strikes by threatening to carry out nuclear counterattacks. The risk of catastrophic destruction was deemed to be so high that neither of the power blocs used

[1] "*After September 11, many observers dismissed the applicability of traditional concepts of deterrence to non-state actors. They pointed to the difficulties of finding effective threats both against individual terrorists who may care more about heavenly than earthly rewards and are willing to commit suicide for their cause, and against terrorist organizations that lack a 'return address' against which to retaliate.*", in Jeffery W. Knopf, 'The Fourth Wave in Deterrence Research', in Contemporary Security Policy, 31 (2010) 1.

nuclear weapons. This traditional interpretation of deterrence clearly does not apply in much the same way to the considerations made by terrorists, and it is indeed possible to argue that deterrence in its entirety is ineffective in the context of terrorism. At the same time, however, it is useful to analyse in greater depth the different aspects of deterrence and the way in which this instrument can be used, and to examine it against the objectives and working methods of terrorists and terrorist organisations. It is important to make a distinction between deterrence as a means of preventing terrorism and deterrence as a means of reducing the probability of success of a terrorist attack or its impact. Especially with respect to the latter category, it can be concluded that certain forms of deterrence can be effective. If one calculates the risk of a terrorist attack as the probability of it happening times the effect that it can achieve, reducing these elements provides a frame of reference for deterrence as an instrument against terrorism.

When carrying out an attack, terrorists, whether operating alone or as part of an organisation, always seek to achieve the greatest possible effect in terms of physical damage (victims and the destruction of buildings and infrastructure), economic damage and the creation of fear and social unrest in a society. Reducing the probability of attacks and the impact of attacks that do occur are key objectives of counterterrorism policy.

Terrorists carry out attacks to draw attention to their political message and consider attacks necessary to achieve their political aims. Furthermore, terrorist activity may be motivated by extremist religious ideology or extreme left or right political ideology, or may be separatist in nature. Unlike most state actors, when forming their battle plans, terrorists do not rationally assess whether the sacrifices required are worth it in relation to the expected results. Extremist jihadist fighters, for example, are more willing to die because they believe that Paradise awaits them. At the same time, the mere threat of an attack or a relatively minor attack is sometimes enough to disrupt a society. In other words, from the terrorist perspective, an optimal result can at times be achieved with very few resources. Based on these characteristics, many authors assert that deterrence is ineffective. It can even have the opposite effect. Deterrence measures aimed at the support environment of terrorist organisations may actually serve to unite the people in that environment against a common enemy, resulting in further radicalisation. This problem is occurring in Pakistan and Yemen, for example, as a result of drone strikes.

Prior to looking at the different deterrence instruments and their effectiveness in countering terrorism, it is important to recognise the different actors and their respective roles within an organisation, as well as their tactics and working methods. Generally speaking, large, global terrorist networks are well organised. Different actors each play a role within the organisation. In addition, these actors each have different motives and convictions with respect to their willingness to die. There is an upper echelon, where strategy is formulated and from where an infrastructure is rolled out, a middle echelon, the foot soldiers and the support network. Moreover, certain terrorist organisations are more *ruthless* than others. The willingness to make what are disproportionate personal sacrifices in the eyes of ordinary civilians or states therefore differs per organisation, but also per category of actor within a network. It is important to recognise these differences when considering the potential effectiveness of the various deterrence instruments available.

These instruments can be aimed at the network that supports a terrorist organisation in a broad sense by supporting its objectives and working methods. Fighters are also recruited from this group of followers. Deterrence instruments can also be aimed at the ‘facilities service providers', the infrastructure and the supply routes for weapons and explosives, and at the technical and financial support provided. The deterrence instruments that can be effective against this group differ from those that can be effective against the first group. A tailored approach to deterrence also applies to the actual fighters and those in the upper echelon.

In addition, the tactics and working methods of terrorist organisations and the targets selected mean that deterrence instruments must be used in a targeted way to be effective. In terms of working methods and types of attacks, there are suicide bombings, the use of improvised explosive devices (possibly carried by vehicles which are driven into buildings or crowds), shootings, hijackings, kidnappings, beheadings, bomb attacks and so on. These methods are often accompanied by social disruption and a sense of threat and fear among the population. Terrorist organisations or individual terrorists use media campaigns and a variety of communications strategies designed to exacerbate the situation and make the threat and fear more acute. Some tactics are used mostly to make political demands or secure payments. To ensure maximum effectiveness, it is not only important to determine which deterrence instruments should be used against which parties, but also when to use them. Clearly, for example, if an individual is already on an aircraft with an explosive and with the intention of blowing up the aircraft, deterrence will no longer have any effect.

Deterrence used against terrorism does not necessarily have to be military or repressive in nature. Glenn Snyder makes a distinction between deterrence on the gains side (*deterrence by denial*) and deterrence on the costs side (*deterrence by punishment*). The priority regarding the latter is to increase the 'costs' of an attack to such a level that they are no longer justified by the potential gains. This classification corresponds in part with the definition of terms as used in the general chapter of this study. Where deterrence on the costs side concerns retaliation or criminal prosecution, for example, one can also refer to a direct form of deterrence on the costs side in accordance with the categorisation used in this study. This is a strategy propagated particularly by Israel, though it is generally not supported in the literature or by policymakers in other countries. The problem is that this kind of deterrence involves retaliating against the families or communities of the terrorists and is based on a need to make the countermeasures taken seem excessive and disproportionate in order to convince the hard-core terrorists that their analysis of costs and gains is misguided.

Deterrence on the gains side concerns measures aimed at discouraging potential perpetrators by reducing the probability of success, i.e. the potential gains, or by convincing them that there are other ways of achieving their political objectives. According to Davis and Jenkins, even the most hardened terrorists tend to want to avoid operational risks, and increasing both the level of uncertainty regarding the success of an attack and the risks of early detection has a deterrent effect. The latest method as introduced by Knopf can also be included in this category of deterrence. This method is aimed at invalidating the justification used by extremist organisations for the use of violence by means of counterpropaganda.

James Smith and Brent Talbot make a distinction between the different levels at which deterrence on the gains side is used. They refer to the tactical level, the operational level and the strategic level. At the tactical level, deterrence is aimed mainly at reducing the opportunity to carry out an attack by increasing security measures and the operational risks that terrorists must contend with prior to an attack. According to the categorisation used in this study, such measures could also be seen as constituting a form of indirect deterrence on the costs side aimed at increasing the prior investment required for an attack.

The category also includes measures aimed at cutting off logistical support and financial flows. Smith and Talbot place these measures in the operational level category, since they are aimed at reducing capabilities. Such measures can be taken together with deterrence measures on the costs side, such as criminal prosecution, for example. In this context, Knopf also refers to indirect deterrence if the measures are aimed at the support group. At strategic level, deterrence is aimed at reducing the intended objective. Dutter and Seliktar believe that this is the most important level for the use of deterrence. Efforts at this level include convincing the target audience that the terrorist methods will never achieve the political objectives, preventing overreaction on the part of governments, increasing societal resilience to prevent panic through, among other methods, fear management and increasing the level of acceptance of danger as a part of life. Deterrence at this level can be considered to have been successful if the community concerned no longer supports the terrorists.

In some cases, deterrence methods overlap. A policy which clearly states that no ransom will be paid for the release of hostages and which is adhered to practice, for example, is a combination of reducing the intended objective and increasing the prior investment required.

In view of the current emphasis on dealing with jihadism and the problem of foreign fighters, it is important to assess deterrence measures, either taken or planned, in terms of the extent to which they can be expected to effectively contribute to a reconsideration on the part of a terrorist who is planning an attack or to reducing the risk of this attack taking place, or to reducing an attack's impact on society.

Sources

National Coordinator for Security and Counterterrorism (NCTV), *Samenvatting Dreigingsbeeld Terrorisme Nederland* 36. 30 June 2014.

National Coordinator for Security and Counterterrorism (NCTV), *Samenvatting Dreigingsbeeld Terrorisme Nederland* 37. 12 November 2014.

'Actieprogramma Integrale Aanpak Jihadisme: Overzicht maatregelen en acties'. TK 29754, no. 253. 29 August 2014.

General Intelligence and Security Service (AIVD), *Transformatie van het jihadisme in Nederland: zwermdynamiek en nieuwe slagkracht*. June 2014.

Benjamin Darnell, *Deterrence in Counter Terrorism*. 19 May 2010. Available at: http://www.e-ir.info/2010/05/19/deterrence-in-counter-terrorism/.

Matthew Kroenig and Barry Pavel, 'How to Deter Terrorism'. In: *The Washington Quarterly*, 35(2012)2.

Jeffrey W. Knopf, 'The Fourth Wave in Deterrence Research'. In: *Contemporary Security Policy*, 31(2010)1.

Glenn Snyder, 'Deterrence by Denial and Punishment'. In: *Research Monograp*. Princeton University Center of International Studies. (1959)1.

Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security*. Princeton, NJ, Princeton University Press, 1961.

Paul K. Davis and Brian Michael Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda*, Santa Monica, CA: RAND, 2002.

James Smith and Brent Talbot, 'Terrorism and Deterrence by Denial'. In: Paul R. Viotti, Michael A. Opheim and Nicholas Bowen (eds.), *Terrorism and Homeland Security: Thinking Strategically about Policy*. Boca Raton, FL: CRC Press, 2008.

Lee E. Dutter and Ofira Seliktar, 'To Martyr or Not to Martyr: Jihad Is the Question, What Policy Is the Answer?'. In: *Studies in Conflict & Terrorism* 30(2007)5.

Gerald M. Steinberg, ‘Rediscovering Deterrence after September 11, 2001’. In: *Jerusalem Letter/ Viewpoints* 467. Jerusalem Center for Public Affairs, 2 December 2001. Available at: www.jcpa.org/jl/vp467.htm.

International Centre for the Study of Radicalism, ICSR Data. ‘ICSR Insight: Up to 11,000 Foreign Fighters in Syria; Steep Rise Among Western Europeans’. Available at: http://icsr.info/2013/12/icsr-insight-11000-foreign- fighters-syria-steep-rise-among-western-europeans/; Govt. Agency Data. ‘Foreign Fighters in Syria’, The Soufan Group. Available at: http://soufangroup.com/wp-content/uploads/2014/06/TSG-Foreign-Fighters-in-Syria.pdf).

Institute for Economics and Peace, Global Terrorism Index 2014. Available at: http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%20Report%202014_0.pdf.

Appendix 2
Deterrence as a security concept against cyber threats

Sico van der Meer

Current situation

Cyber threats, also referred to as digital threats, are among the greatest threats currently facing the Netherlands.[1] Cyber threats encompass a broad spectrum. Examples include digital warfare, digital terrorism, digital espionage, digital activism and digital crime. While the purpose of each type of activity differs, the use of technology is the same in all cases in that weaknesses within the cyber domain are exploited.

It is clear that the number of cyber attacks is increasing sharply. It is very difficult, however, to determine the exact number of attacks, as most attacks are never reported. Indeed, individuals or organisations often remain unaware that they have been attacked, since the purpose of many attacks is precisely to hack into computers or computer networks while avoiding detection. There are so many forms and types of cyber security breaches, and they are committed by such a variety of actors, that it is not reasonable to view such breaches as constituting some kind of uniform whole. Cases literally range from students who hack into other people's computers for relatively harmless fun to large-scale industrial espionage, to digital warfare waged for the purpose of disrupting a society in its entirety. Nevertheless, within the limitations of this publication, a cautious attempt is made to provide a general outline of the current situation.

In its most recent cyber security assessment, the Dutch National Cyber Security Centre (NCSC) identifies cyber espionage and cybercrime as being the greatest cyber threats to the Netherlands at the present time.[2] This is especially the case because these are the two kinds of cyber attacks that, by quite a margin, occur the most frequently in the Netherlands. In addition, the NCSC observes that the continuing digitisation of Dutch society is increasing the risk of more large-scale cyber attacks aimed at disrupting society. In terms of the security of individuals and society, the greater the reliance on digitisation, the greater the impact of malicious acts carried out by parties who abuse digital environments for their own ends. Cyber espionage and cybercrime primarily cause economic damage. In addition to economic consequences, such as weakening the competitive position of the Netherlands, cyber espionage in particular is also a security issue in that it can be used by potential enemies of the Netherlands, whether state or non-state actors, to learn a great deal about the national security situation in the Netherlands and discover potential weaknesses. Stolen information about vital infrastructure or military operations, for example, could be used to do damage by digital or non-digital means.

[1] General Intelligence and Security Service (AIVD), Jaarverslag 2013. The Hague: AIVD, April 2014.

[2] National Cyber Security Centre (NCSC), Cybersecuritybeeld Nederland: CSBN-4, July 2014, p. 7.

Whereas cyber attacks on organisations, companies and individuals are by now fairly common throughout the world, there have so far been only a few cyber attacks aimed at causing large-scale disruption to society. The most well-known examples are the attacks that took place in Estonia in 2007 (attacks on the government, banks and media), the United States in 2012 (attacks on various banks) and South Korea in 2012 (banks and media). There are also examples of large-scale cyber attacks that were carried out for different purposes: Georgia in 2008 (by Russia to support its conventional military operation), Iran in 2010 (aimed at sabotaging the country's nuclear programme), Saudi Arabia in 2012 (attack on state oil company Saudi Aramco, possibly to sabotage oil exports) and the United States in 2014 (attack on Sony Pictures Entertainment, possibly to prevent the release of a movie about North Korean leader Kim Jong-un). Although the economic damage was considerable in a number of these cases, large-scale cyber attacks on a country's truly vital infrastructure, such as power or water purification plants, or, of vital importance in the Netherlands, flood protection and water management systems, have as yet not taken place.

Although alertness to cyber threats has increased considerably in the Netherlands in recent years, technological developments in the cyber domain are occurring at such a rapid rate that cyber security measures must constantly be modernised to keep up in the fight against those who are intent on doing harm. At present in the Netherlands, it is mainly cyber experts of specialist companies and government agencies (the National Cyber Security Centre and the Dutch Ministry of Defence's Cyber Command, for example) who are permanently engaged in battling cyber threats. In spite of increased awareness of risks among users of cyber technology, whether they be organisations or private individuals, such users remain a weak link in the chain in terms of countering cyber threats. To give just one example, the NCSC notes in its most recent assessment that approximately 35 percent of all users have not installed antivirus software on their computers, even though installing such software is the first and most basic step in the context of cyber security.[3]

Expectation for the coming five to ten years

Although there is currently a lack of clarity in terms of the exact number of cyber incidents, the cyber threat to the Netherlands will certainly increase in the near future, mainly because of the further digitisation of Dutch society, also in vital sectors. The number of devices and appliances (medical devices, household appliances and automotive devices, for example) that are connected to each other and to the internet will increase exponentially worldwide to approximately 25 billion in 2020.[4] The greater this dependence, the more vulnerable society will be to cyber threats. Because a growing number of processes are occurring in the digital domain and a growing number of devices and appliances are connected to cyber networks, the risk of these processes, devices and appliances being manipulated by unauthorised parties is increasing correspondingly.[5]

While considerable progress is being made with respect to the security of the cyber domain in terms of, for example, increasing awareness of the risks and the technological level of security of vital cyber infrastructure, other actors are also very much on the move. Many

[3] National Cyber Security Centre (NCSC), Cybersecuritybeeld Nederland: CSBN-4, July 2014, p. 43.

[4] Idem, p. 77.

[5] Idem; Jan Rood, Een wankelende wereldorde: Clingendael Strategische Monitor 2014. The Hague: Clingendael, Netherlands Institute of International Relations, 2014, p. 110-119 and p. 126-128.

countries, including the Netherlands, as well as non-state actors are investing in offensive cyber warfare capabilities; references are regularly made in this context to a cyber arms race.[6] Because cyber attackers immediately look for other weaknesses as soon as a gap in security has been closed, they virtually always have the advantage. This is because it is impossible to close every security gap in cyber infrastructure. Cyber security will therefore always be a competition between attackers who are exploiting or seeking to exploit a newly discovered weakness and defenders who work to close a given security gap as quickly as possible.

Cybercrime and cyber espionage will continue to pose the main threats in the future, and therefore they will remain a threat to national security. Cyber criminals are becoming more professional and cyber attacks are becoming more sophisticated and greater in scope. Cyber espionage carried out by states as well as private organisations (industrial espionage) will likewise increase. It is possible that allies will in the future also engage in espionage through the cyber domain. In addition, a major cyber terrorist attack remains a possible nightmare scenario. A great deal of damage could be caused by cyber terrorists who succeed in sabotaging, for example, the energy supply, flood protection and water management systems, hospitals, chemical plants, air and railway traffic control systems or payment systems. Such an attack would likely lead to social unrest. In this sense, what applies to terrorism in general also applies to cyber terrorism: although the probability of an attack is relatively low in the Netherlands in statistical terms, the impact of such an attack would be considerable.

Actual cyber warfare directed against the Netherlands is unlikely, although a diplomatic conflict between the Netherlands and another state could perhaps also result in the disruption of certain cyber services (see the examples from abroad given above).

It is also important to bear in mind that cyber incidents in other countries can also have consequences for the Netherlands. A disruption to the American Global Positioning System (GPS), for example, could also disrupt traffic in the Netherlands. Equally, if a cyber terrorist caused a nuclear disaster at a nuclear power plant elsewhere in Europe, any radioactive fallout could also be an issue in the Netherlands, just as a cyber attack on the European Central Bank (ECB) could disrupt Dutch payment transactions. Increasing digitisation is therefore also increasing the interconnectedness between the Netherlands and other countries.

The relevance of deterrence as a security concept

Defence and deterrence capabilities against cyber threats are very much a subject of discussion among researchers and policymakers. Although it is probably impossible to prevent all cyber security breaches, deterrence may prevent some cyber attacks.

With regard to the costs side, potential attackers could be deterred by the possibility of, for example, retaliatory measures within the cyber domain itself (a cyber attack on the attacker carried out by the party first attacked), diplomatic and/or economic sanctions, or even conventional military action against the attacker. In 2014, for example, NATO, of which the Netherlands is a member, decided that a cyber attack on one of its member states would

[6] See for example Michael Riley and Ashlee Vance, ‘Cyber Weapons: The New Arms Race’. In: Businessweek, 20 July 2011.

be deemed to be an attack as defined in Article 5 of the North Atlantic Treaty, thus making it possible for the alliance to take military action against cyber attackers.[7] To a certain extent, such deterrence would undoubtedly raise the threshold. Because of various specific characteristics of the cyber domain, however, it is relatively difficult to apply deterrence as an instrument against cyber attackers.

The main obstacle to the effectiveness of such deterrence measures is the attribution problem. It is extremely difficult to conclusively establish the identity of the actor or identities of the actors responsible for an unclaimed cyber attack. Cyber weapons are not like conventional weapons, as the origins of cyber weapons are not clearly visible and traceable. For example, attackers can use a chain of hacked or infected computers without the owners actually being aware of any wrongdoing. Although it is technically possible to locate the source of a cyber attack by means of IP addresses, there is always the possibility that the source identified was merely a link in the chain of the attack and that the owner was not in any way deliberately involved in the attack. In addition, state actors can conceal their involvement by having cyber attacks carried out by non-state actors (hacker groups, for example). Conversely, non-state attackers may claim an association with a given state even if this is not actually the case. Moreover, cyber attackers can strike within a very short period of time and erase their tracks immediately after they have carried out the attack. Identifying the sources of the attack, on the other hand, is a complicated and time-consuming process. It is therefore almost impossible to take retaliatory measures during or immediately after the attack. Because it is virtually impossible to establish the identity of the party responsible for a cyber attack with absolute certainty, especially if the accused denies responsibility, there is also the risk of a retaliatory measure being taken against an innocent party. In practice, few state actors will be willing to take this risk, something that cyber attackers are aware of.[8] It could perhaps be argued that indisputable and conclusive evidence is not required in some cases and that retaliatory measures can be taken if it is virtually certain that a certain state or non-state actor was involved or did not seek to stop the attackers.[9] However, leaving aside whether it is desirable to adopt this route – with the risks it entails of making false accusations – the question remains whether such an approach is actually permitted under international law. This is another area in the cyber domain where developments are still in full swing.[10]

Strong forensic capabilities in the cyber domain are crucial to identifying the party guilty of a cyber attack. A higher probability of being identified will also have a deterrent effect on potential attackers. In this regard, international cooperation, such as exchanging information about cyber weapons and cyber vulnerabilities that have been detected, is likewise essential.

In addition to the difficulty of conclusively identifying the party guilty of a cyber attack, there are other problems associated with deterrence against such attacks. The credibility of deterrence and the risk of escalation are key issues. Deterrence based on the possibility of

[7] David E. Sanger, 'NATO Set to Ratify Pledge on Joint Defense in Case of Major Cyberattack'. In: The New York Times, 31 August 2014.

[8] Emilio Iasiello, 'Is Cyber Deterrence an Illusory Course of Action?'. In: Journal of Strategic Security. 7 (2013) 1, p. 58; Advisory Council on International Affairs (AIV), Digitale Oorlogvoering, 77 (2011), p. 13.

[9] Jason Healy, 'Beyond Attribution: Seeking National Responsibility in Cyberspace'. In: Atlantic Council Issue Brief (2012).

[10] For a discussion on international law and cyber attacks, see Advisory Council on International Affairs (AIV), Digitale Oorlogvoering, p. 19-27.

retaliation only works if the party seeking to deter communicates clearly about the retaliatory measures that may be taken in the event of a cyber attack. What acts are classified as cyber attacks that will trigger retaliation? Will retaliation take place in the cyber domain or is a conventional military strike also a possibility? If communication about possible retaliatory measures is not clear, it is unlikely that a potential attacker will take them into account and they will therefore not have a deterrent effect. After all, deterrence measures are only effective if the opponent is aware which actions will result in their implementation. The difficulty is that drawing 'red lines' in the cyber domain can also have the opposite effect to the one intended. Cyber attackers may deliberately cross a red line to cause escalation, perhaps even while taking advantage of the attribution problem and posing as a different party. To maintain the credibility of deterrence, the party using it as an instrument must retaliate even if doing so at that specific time is not the favoured course of action. Any failure to adhere to the deterrence mechanisms communicated would dilute the deterrent effect, since potential opponents would be encouraged to think that the red lines are not all that red in practice.[11]

A third problem with deterrence based on retaliation in the cyber domain is the proportionality of the retaliatory measures. The effects of retaliation by conventional means can usually be fairly accurately assessed. The consequences of responding to a cyber attack through the cyber domain are more difficult to control, however. This is because a retaliatory cyber attack can easily have unintended consequences precisely because everything in the cyber domain is interconnected. A cyber attack on government networks, for example, may also accidentally affect networks of hospitals, water purification plants and other providers of essential services. A retaliatory attack carried out through the cyber domain may have greater effects than the ones intended and make the retaliating party the black sheep of the international community.[12] The question as to when and the extent to which retaliatory measures may be taken is another problem. In the cyber domain, it is difficult to identify the boundary between acts intended to cause economic damage or disruption and obvious acts of war. There is as yet no clarity whatsoever regarding such issues.

A final key consideration is that the diversity of actors in the cyber domain makes deterrence difficult. State actors usually have interests that would be jeopardised by retaliatory action. However, non-state actors such as hacker or terrorist groups, for example, may not actually have any interests or goods of value against which a retaliatory attack could be directed, a situation which in itself undermines the credibility of retaliation. Moreover, such non-state groups, which are capable of carrying out major cyber attacks in spite of their relatively limited resources, may not always act rationally and may not even be deterred by any kind of possible retaliation.[13]

There are also other, more passive ways of making attacks more costly for potential attackers, not least by improving security in terms of, for example, multi-layered firewalls and advanced encryption and authentication methods. So-called 'honeypots' can also be used to improve security. These appear to be the kind of vulnerable areas in a system that cyber attackers are looking for, but they are in fact deliberately set traps designed to gather information about the

[11] Martin C. Libicki, 'Cyberdeterrence and Cyberwar', RAND Research Report, RAND Corporation (2009), p. 65-73.

[12] Emilio Iasiello, 'Is Cyber Deterrence an Illusory Course of Action?' p. 59-60.

[13] Clorinda Trujillo, 'The Limits of Cyberspace Deterrence'. In: Joint Forces Quarterly, 75 (2014) 4, p. 49; Emilio Iasiello, 'Is Cyber Deterrence an Illusory Course of Action?', p. 64-65.

working methods of cyber attackers. In practice, cyber criminals avoid the Netherlands and Dutch servers because of the use of honeypots. In other words, honeypots have a deterrent effect.[14]

Improving security increases the costs that an attacker must incur to carry out a successful attack and makes it less likely that the attack will have the desired effect and secure the desired gains. To achieve this kind of deterrence, the cyber infrastructure of the potential victim must be secured in such a way as to ensure that any attackers encounter barriers that considerably reduce the likelihood of their attack succeeding. Government authorities, organisations and private individuals can take a major step towards passive deterrence simply by remaining aware of the dangers of cyber attacks and ensuring that the latest security systems are always installed on their computers and computer networks. Networks must also continuously be monitored so that countermeasures can be taken as soon as there is any sign of an attack.

Improving security, or passive deterrence, entails fewer potential pitfalls than active deterrence.[15] The main problem is that this form of deterrence is expensive and complex and requires continuous investment; technological developments occur at such a rapid rate in the cyber domain that stagnation means decline. In addition, it is difficult to raise awareness on the part of all concerned, even though a certain level of awareness is necessary, since cyber attackers always exploit the weakest link in the chain that they can find. In a manner of speaking, this could very well be that one inattentive employee who downloads infected files, thereby creating an opening for the attacker. As stated above, approximately 35 percent of users do not even have antivirus software installed on their computers. There is therefore a lot of room for improvement in terms of awareness. Moreover, cyber attackers always have the advantage in that they have all the time to look for weaknesses in cyber infrastructure, whereas the targeted individual or organisation must respond as soon as a previously unknown weakness is exploited in a cyber attack. In other words, cyber attackers always have the element of surprise.

It is important to realise that the Netherlands is not an isolated entity in the cyber domain. Regardless of the methods used to reduce cyber threats, international cooperation will always be necessary. As a method to decrease the number and danger of cyber threats, deterrence will also usually be used in the context of international alliances such as the EU and NATO. In the cyber domain, deterrence is as yet still a concept that is surrounded by many questions and problems. Nevertheless, it is in any case clear that investing in security has a certain deterrent effect. Good cyber security does not just increase the costs that an attacker must incur to carry out a successful attack, it also makes it less likely that the attack will have the desired effect and secure the desired gains.

[14] KPN (in cooperation with the Netherlands Organisation for Applied Scientific Research, the police and the National Cyber Security Centre), 'European Cyber Security Perspectives 2015', p. 49-51.

[15] David Elliot, 'Deterring Strategic Cyberattack'. In: IEEE Security & Privacy, 9 (2011), p. 38-39.

Appendix 3
Deterrence as a security concept against organised crime

Sander Huisman[1]

Current situation

The nature of so-called organised crime in the Netherlands is inextricably linked to the nature of Dutch society and the Dutch economy, as well as to the country's geographic location and its physical and digital infrastructure. Europol notes for instance that the Netherlands functions as a major transit point for various forms of international crime, such as drug trafficking and smuggling, the illegal cigarette trade and cybercrime.[2] The Netherlands has played a dominant role in various criminal markets for decades, particularly in relation to drugs, fraud, money laundering and cybercrime.[3] The (1) international orientation of the open Dutch economy and (2) the country's highly developed financial system with its specialist service providers foster an environment that is conducive to trade. Moreover (3), the risk, from a criminal's viewpoint, of illegal goods being intercepted is limited because of the volume and sheer diversity of the legal trade. The opportunities are further increased by the open borders with other European countries. The Netherlands also has an (4) excellent road, water, rail and air transport infrastructure. In addition, the country (5) is favourably located relative to several markets and is a European distribution point and logistics hub, as manifested by Schiphol and other airports, the port of Rotterdam and other centres of transhipment. The (6) presence of various migrant communities means that there are many bridgeheads that contain an active or passive network of helpers. Amsterdam (7) is an attractive international meeting place. This applies particularly with regard to foreign criminals, who, according to a number of experienced investigating officers, usually remain under the radar of the police and intelligence services. Lastly, the Netherlands (8) is seen as being soft on crime, as a result of which criminal entrepreneurs like to do their business in the country.

The Dutch Advisory Council on International Affairs[4] (2013) identifies VAT fraud in the EU and cybercrime as the most extensive and rapidly growing forms of international crime in relation to the Netherlands. The National Threat Assessment[5] prepared by police investigators observes that criminal activity is currently influenced most by developments in digital technology and the use of the internet. This applies to different forms of organised crime, in

[1] The author wrote this contribution in a personal capacity.

[2] Europol, 'EU Serious and Organised Crime Threat Assessment (SOCTA) 2013'. The Hague: Europol 2013.

[3] Netherlands Police Agency (KLPD), *Overall-beeld aandachtsgebieden Dienst Nationale Recherche 2010*. Driebergen: KLPD, 2010.

[4] Advisory Council on International Affairs (AIV), *Criminaliteit, corruptie en instabiliteit: een verkennend advies* 85, The Hague, 2013.

[5] F. Boerman and M. Grapendaal, *Nationaal Dreigingsbeeld Georganiseerde Criminaliteit 2012*. Driebergen: KLPD, 2012.

the context of which several people cooperate primarily for the purpose of making money. In terms of characterising the core of criminal organisations,[6] a division into three categories can be made. First, there are the career criminals who hold dominant positions in the global and European drug markets. Second, there are individuals who, with the help of legal entities, enrich themselves through environmental crime, fraud, swindle and money laundering methods (such as the Palm Invest and Easy Life or construction fraud and property fraud cases). Third, there are cyber saboteurs who used advanced digital technology to con private citizens and companies and who often pose a threat to vital infrastructures (such as in the 2012 Bredolab case).

In view of the key position held by the Netherlands in the international drugs market in geographic and logistics terms, the country is a logical base for criminal entrepreneurs from a variety of source and destination countries. The ability of foreign criminals to reside anonymously in the Netherlands is facilitated by, among other things, willing estate agents, the anonymous prepaid telephones that are, for now, still available and the lack of compulsory identification checks in some internet cafés. In recent years, there has been growing awareness of the existence of various foreign individuals and criminal groups. Various groups or subcultures, such as Brits, Colombians, Italians, individuals from the former Yugoslavia and Hong Kong Chinese, have been present in the Netherlands for decades. Numerous investigations have shown that criminal enterprises in the top segment of the drugs market are typically active in many countries. In addition to the geographic scope, the most dominant networks are also firmly embedded in legal sectors and have contacts with government agencies in the Middle East, West Africa and South America.

Career criminals who occupy a dominant position in certain criminal markets usually also have an extensive network of international contacts. This is certainly the case in the international drugs market, which is dominated by the Netherlands and Dutch career criminals. Virtually every major criminal investigation concerning this underworld has revealed international branches. Criminals typically regard Belgium as more of a hinterland rather than as a different country. Countries and regions that tend to feature most heavily in Dutch criminal investigations are Spain, Morocco, Turkey, various countries in South America, Eastern Europe, East Asia and West Africa and the city state of Dubai.[7] This sometimes has to do with the origin of the suspects and sometimes with the role of the country in the smuggling process, as a source country of goods or as a link in financial processes. Various investigations have shown that new relationships are usually forged during periods of detention in the Netherlands or abroad, since it is during such periods that new business opportunities are discovered.

[6] The term 'criminal organisations' is controversial in the academic world because it places an emphasis on the existence of 'organisations', whereas in the opaque world of fighting crime, such entities usually cannot be observed. Moreover, 'organisation' suggests a certain duration, whereas practical experience shows that most partnerships in criminal circles are rather transient (Kleemans et al., 2002). In terms of criminal law, a criminal organisation exists in the case of "participation in an organisation that intends to commit crimes". A conviction virtually always concerns an individual, however, rarely a legal entity. For this reason, the decision was made to approach the subject in terms of an individual who, with or without others, engages in organising profitable crime, in other words, in terms of criminal entrepreneurs (Van Duyne, 1995) who are referred to in popular parlance as 'career criminals' or 'professional criminals' who are active in 'organised crime'.

[7] Netherlands Police Agency (KLPD), *Overall-beeld aandachtsgebieden Dienst Nationale Recherche 2010*.

The use of legal entities plays a crucial role in environmental crime, various forms of large-scale fraud and money laundering operations. These entities offer a veneer of legitimacy and protect the individuals who organise the illegal processes. Accounting items such as assessment reports and false claims create a false reality on paper to create the impression of compliance and adherence to proper procedures. As the analysis of the Netherlands Police Agency states regarding money laundering, the capital must pass the review of regulators in such a way that it receives a stamp of approval and can therefore be used in the legal economy.[8]

With respect to cybercrime, the range of suspects is extremely diverse and ranges from a 16-year-old school whiz kid to a 38-year-old computer science ace from a former Soviet republic. Motives also vary, from hacking for ideological purposes to sabotaging for fun to monetary gain, for example by extorting money from victims. Attacks on vital infrastructure constitute the main threat. Although government agencies appear to be the most capable of carrying out such attacks (think of the destructive power of the Stuxnet computer worm or Regin malware, for example), individuals can also do a great deal of damage. Police investigations reveal that the attacks, which are usually aimed at the financial system, are becoming more technically advanced. Use is often made of botnets, networks that commonly consist of millions of infected computers. The network hides the identity of the perpetrator and makes it possible to carry out powerful attacks. Against this backdrop, it is safe to say that international crime poses a threat primarily to the following national security interests: political and social stability (confidence of citizens in the state and vital infrastructure), economic security (financial damage to the government and private individuals and the functioning of the business sector) and environmental security (environmental damage).

Expectation for the coming five to ten years

The threats emanating from organised crime will probably remain acute in the coming five to ten years. As described in the Clingendael Monitor 2014, among elsewhere, two trends are set to dominate future developments. First, international crime will be characterised by increasing flexibility (in terms of form, composition and sphere of activity) and mobility (people, money and goods). In addition, there will be a further shift towards the virtual world.[9]

As a result of increasing digitisation and the increasing ease with which borders can be crossed, it will become more difficult in the future to combat criminal organisations, especially if they operate internationally. It is not just the case that cybercrime will substantially increase. Even in traditional organised crime cases there is an increase in the use of digital anonymisation and encryption techniques.[10] Furthermore, 'old school' members of the underworld occasionally hire cyber criminals to gain control of increasingly digitised logistics processes, for instance by hacking computer systems in seaports. With regard to financial processes, it is conceivable that greater use will be made of what are commonly referred to as new payment methods, which include prepaid debit cards onto which vast amounts can be loaded without being linked to traceable account holders. In addition, police investigators consider it likely that Trade-Based Money Laundering (TBML) will become more

[8] Netherlands Police Agency (KLPD), *Criminaliteitsbeeldanalyse Witwassen 2012(b)*. Driebergen: KLPD, 2012.

[9] Jan Rood, Frans-Paul van der Putten and Minke Meijnders, *Een wereld zonder orde? Clingendael Monitor 2015*. The Hague: Clingendael, Netherlands Institute of International Relations, February 2015.

[10] Netherlands Police Agency (KLPD), *Criminaliteitsbeeldanalyse Hightech Crime 2012*. Driebergen: KLPD, 2012.

commonplace. In TBML, the proceeds of crime are used to purchase legal goods, after which the goods are traded on the international market. This enables criminals to transfer large amounts of money and illegal profit can be reported as legal profit.[11]

Successful criminal enterprises are also engaged in legitimate business practices that provide them with access to information. This enables them to influence the business community and political representatives in the non-criminal world. Positions can be secured in local communities, for instance in the hotel and catering industry, real estate or retail. These positions make such enterprises a counterpart (discussion partner and legal actor) of the local authorities. The ongoing economic recession may make individuals who are in debt more willing to provide assistance. Such assistance can be provided in many ways. Examples include the services of money mules and the selling of information within public service providers, banks or logistics companies (such as in ports). Logistics and financial links may be corrupted as a result. The protection of identities remains an integral part of the modus operandi of career criminals, financial legal entities and cyber saboteurs. Digital concealment techniques are expected to be used more often and will also become more readily available. In recent years, anonymity networks (The Onion Router, or Tor) and anonymous payments have become more popular in the physical crime world. In addition, career criminals will continue to rely on the loyalty and alertness of their supportive and robust communities (streets in certain neighbourhoods, trailer parks and clubhouses of outlaw motorcycle gangs (OMGs), for example).

In the years ahead, particular attention will need to be paid to the growing ease with which international relations are established in criminal circles. Career criminals who have a dominant position in certain criminal markets usually also have an extensive network of international contacts. The international phenomenon of expanding outlaw motorcycle gangs is relatively new. Until 2009, the Hells Angels were the only international outlaw motorcycle gang in the Netherlands. The next five years saw the emergence of Satudarah, No Surrender and the Bandidos. The number of members and chapters also grew tremendously in the five-year period referred to.[12] Many career criminals are members of an outlaw motorcycle gang. Plausible reasons for joining include the additional contacts and trading opportunities provided by an international outlaw motorcycle gang and the protection that comes with membership. If these gangs continue to grow, tensions between them are likely to increase as they compete for territory and seek to protect their interests. This competition will probably include violent incidents in the Netherlands and in other countries where there are chapters.

In the coming years, the use of the latest technological innovations is likely to be a key element in criminal activity. An increasing number of goods and services will be traded in hidden online markets (through Tor networks). Examples of such markets are the Silkroad 2.0 and Black Market Reloaded sites that were dismantled by the Team Hightech Crime of the Dutch police. Innovations such as the 3D printer and drones are also used in criminal circles, mainly to hide from and to monitor competitors and authorities more effectively. The hardware deployed is becoming smaller (easier to conceal), smarter (remote control, for example) and more powerful. Nanotechnology and robots, for example, will undoubtedly also be used in criminal circles in the future. A 'traditional' crime such as identity fraud

[11] Netherlands Police Agency (KLPD), *Criminaliteitsbeeldanalyse Witwassen 2012*.

[12] Police, *Outlaw Bikers in Nederland*. Woerden: Police Central Unit, 2014.

(the cornerstone of many criminal acts) may also acquire new dimensions as a result of technological innovations. This race is likely to continue.

The relevance of deterrence as a security concept

Deterrence based on retaliation is an important instrument in countering threats emanating from national and international criminal activity. Research has shown that preventive measures have the greatest effect in a broad-based approach aimed at undermining logistic elements of criminal markets.[13] When the authorities have identified suspects, administrative or tax-related interventions can also be highly effective in fighting crime. To be successful, such actions must be based on a multidisciplinary approach in which several parties feel that they own the problem and therefore consult on an approach in which to use all of the capabilities available to them. The Netherlands is a European and international leader in this context.

Apart from the development of a more broad-based approach initiated in recent years, however, it is not clear which approach has a deterrent effect on criminal organisations or individual career criminals. An approach based on criminal law usually results in detention or confiscation, an approach based on administrative law results in an administrative measure (the withdrawal of a licence or closing of a home, for example), and a tax-related approach results in a financial penalty (a tax assessment or an additional tax assessment, for example). A combined, or better, integrated approach is probably the one that is experienced as being the most effective and is therefore the one that probably has the greatest deterrent effect.

Criminal enterprises respond rapidly to changes in their environment. When government interventions occur, activities are temporarily suspended or relocated. When the authorities implement legislative changes, operations are adapted where possible to keep up the appearance of legality. When certain branches change logistics processes, logistic activities are adapted. The fragmentation that characterised criminal investigations in the Netherlands for many years made the country an ideal place for those who wished to advance to the position of 'king of the hill'. Such individuals can thwart, overcome or endure the existing measures (checks, investigations, prosecution, detention and rehabilitation) with relative ease. The climb up the criminal career ladder can be countered more effectively if opportunities to intervene are recognised and acted on at an earlier stage. This means, however, that the threat of an intervention, such as a rapid seizure or a rapid conviction, must also be credible, which is only possible if the authorities have built up a track record in terms of these measures.

The most successful career criminals derive their power from their reputation and status in criminal circles. They cannot sustain this power, however, without a reliable social environment (neighbourhood, family, criminal 'crew'). It is clear that temporary detentions have no effect on heavyweight career criminals. To them, such detentions come with the territory. They are business risks that they have taken into account. Moreover, such periods offer new opportunities, mainly in terms of forging new business relationships. The strategic ties with the social environment are strong and are not undermined by temporary detentions. The robustness of criminal groups is therefore virtually inextricably linked to the presence

[13] See for example H.G. van de Bunt and C.R.A. van der Schroot, *Prevention of Organised Crime: A Situational Approach*. The Hague: Boom, 2003.

of thick crime habitats and community support.[14] A good reputation in the relevant circles is essential to the development of a criminal career. The status of career criminals is partly based on historical success, trust, discipline, useful contacts and business acumen. It also relies on their ability to intimidate, and to ensure that those closest to them remain silent with respect to the authorities.[15] Visible public servants (counter staff of a municipality and community police officers, for example) have the most to fear in this respect. This situation has an added dimension in cases where friends or family members are employed at a government agency and have access to specific information. Criminal networks can thereby gain in robustness and, as a result, benefit from an enhanced capacity to absorb government interventions. Reducing the resilience of criminal circles is by no means easy.

There are examples of government interventions in which a criminal network was dismantled in such a way that those in the more immediate social environment who were also benefiting from the criminal activity were also 'reprimanded'. This kind of dismantling occurred in 2010 in the case of an extremely wealthy drug dealer who had operated under the radar for many years and had built up an excellent reputation in criminal circles. A thorough national and international criminal and financial investigation resulted in long jail terms for those who had been directly involved in the criminal activity as well as the seizure of a range of movable and immovable property that had been registered as belonging to confidants and family members. This intervention therefore sent out a signal that went beyond those who were convicted. For capacity reasons, however, large-scale and comprehensive interventions of this kind will always be the exception rather than the rule. Smart and well-considered choices will therefore need to be made. Ideally, the actual effect of an intervention should also be gauged on the basis of current information. Various studies show that the most effective measures against criminal entrepreneurs and criminal organisations are those that affect the financial situations of such individuals and organisations. Use should be made first and foremost of rapid prejudgment attachment to ensure that the suspect and those in his or her social environment experience the effects immediately.[16] This measure would have a deterrent effect.

A special form of deterrence is the provision of information by former partners in crime to the police and judicial authorities for the purpose of incriminating other criminal entrepreneurs. It should come as no surprise to learn that criminal lawyers who mainly represent individuals who are often a focus of investigations into organised crime are highly critical about the more frequent use of criminal civilian infiltrators. From an investigative perspective, however, obtaining human intelligence from the underworld itself is becoming more important. This is because it is becoming more difficult to obtain information of real evidentiary value through more traditional investigation methods such as surveillance and the interception of communications. Cases often concern close-knit groups, the members of which consistently seek to conceal their activity. For this purpose, they use technical means and front men, and intimidate and threaten potential witnesses or officials. Sources in criminal circles are therefore becoming increasingly important in terms of both the informants and the (threatened) witnesses and, in certain cases, criminal civilian infiltrators.

[14] J. Ayling, 'Criminal Organizations and Resilience'. In: *International Journal of Law, Crime and Justice*, 37 (2009), p. 182-196.

[15] Netherlands Police Agency (KLPD), *Overall beeld aandachtsgebieden Dienst Nationale Recherche 2010*.

[16] E.W. Kruisbergen, H.G. van de Bunt and E.R. Kleemans, *Vierde monitor georganiseerde criminaliteit*. The Hague/ Rotterdam: Research and Documentation Centre (WODC)/Erasmus University Rotterdam (EUR), 2012.

Deterrence can only be effective if the threat of retaliation is credible.[17] Strikingly, this rule also applies in criminal circles as a condition for obtaining a respected and credible status. The risk of discovery, prosecution and detention must be high. This requires a robust government that intervenes swiftly, flexibly and firmly. It requires high-quality and therefore current information and proper cooperation between the partners involved (both public and private). It requires a solid contingent of capable guardians who are able to deal with willing offenders on the basis of current insight. The importance of international cooperation is self-evident in a world in which national borders are becoming less significant as a result of globalisation and the internet. This means that requests for assistance from other countries must be dealt with without delay. Interventions must take place in quick succession in order to secure and execute a judgment so that a clear message is also sent to those close to the criminal in question. This requires close cooperation between authorities as well as rapid action by professionals in their respective spheres of work. Finally, how to communicate with the general public must be properly considered. Media strategy is therefore extremely important, since substantial gains can be made with the correct 'framing'. Experience to date has shown that such communications are meaningful only if a new and unique understanding has been gained through investigation methods. In the right circumstances, deterrence based on retaliation can therefore be an effective instrument against crime, also with respect to criminal activity from abroad. However, other forms of deterrence that are part of the analysis framework of this report, i.e. indirectly increasing the costs that the perpetrator must incur or reducing the gains that the perpetrator can achieve, appear to be less relevant in countering this threat, except in the case of defensive measures in the field of cyber security that substantially increase the costs of engaging in cybercrime against targets in the Netherlands.

[17] K.H. Hicks, 'The Case for Deterrence'. In: C. Cohen and J. Gabel (eds.), *2015 Global Forecast: Crisis and Opportunity*. Washington, DC: Center for Strategic and International Studies, 2014.

Appendix 4
Deterrence as a security concept against threats in the economic domain

Peter van Bergeijk

Current situation

With its open and internationally oriented economy, the Netherlands is potentially vulnerable to external security threats that reach it through the economic domain. Additional attention must be given to this vulnerability because of the increasing geopolitical tensions in the world and the instability in regions close to Europe as outlined in the summary report of the Clingendael Monitor 2015. In this context, the 'economic domain' includes all external economic contacts of the Netherlands. On the one hand, the threat concerns activities that disrupt economic core processes, i.e. processes that are of vital importance to the functioning of the economy (energy production, communication, transport, monetary transactions and so on). The threat may involve a core process being disabled or the undermining of confidence of members of the public and the business community in that core process. A stable supply of energy and other raw materials from abroad is of vital importance to the functioning of economic key processes. A cyber attack on Dutch payment transactions, for example, would be an attack directed against an economic core process that, even if it failed, could undermine confidence in the uninterrupted functioning of the process. In the same sense, a physical attack on the energy supply (on a distribution point, for example, whether or not in the Netherlands itself) or a blockade that prevents the supply of certain raw materials could disrupt economic core processes. On the other hand, in addition to these core processes, the threat also concerns the interest that the Netherlands has in free trade and access to foreign markets, and in attracting foreign investment as a foundation for employment and a dynamic business sector. The disruption of international trade and investment in particular could result in major macroeconomic damage. The more unexpected and prolonged the disruption, the greater its impact. The Netherlands is vulnerable in the economic domain in all these senses. Van Bergeijk and Mennen (2014) discuss numerous economic disruptions that were analysed in the context of the National Risk Assessment.

Deterrence may be relevant in this context with respect to actors who deliberately perform acts that harm the national security of the Netherlands. Three relevant groups of actors are criminals, terrorists and states. Internationally operating criminal organisations that harm the Netherlands usually do so through the economic domain. Drug trafficking, human trafficking, fraud, money laundering and cybercrime are directly linked to economic processes. Terrorism is linked to the economy in terms of the funding of terrorist organisations, or indeed when terrorist attacks are aimed at disrupting economic core processes. The activities of criminal and terrorist organisations and the relevance of these activities to national security are discussed elsewhere in this study.

The actions of states in the economic domain can pose a threat to national security in a number of ways. First, economic vulnerabilities can be exploited by another state by intervening directly in the economy in order to strengthen its own competitive position at the expense of Dutch competitiveness. A government can do so by, for example, favouring national companies in the home market, providing state aid to national companies, carrying out or supporting industrial espionage (through the cyber domain or otherwise) and using political and diplomatic influence to restrict access to markets or raw materials in third countries. A foreign government may also use state-run enterprises or companies that it influences in some other way to effect corporate takeovers and thereby eliminate Dutch competitive advantages and/or create dependencies. Whether or not such measures pose a threat to national and economic security depends on their scale and relevance to economic core processes.

Second, a foreign government may try to exert political pressure by means of carrying out economic sanctions, or by implicitly or explicitly threatening with sanctions. Then there are fuzzy sanctions, which are derivatives of sanctions. These are consumer boycotts that harm Dutch economic interests but are not led and were not initiated by a foreign government. At the international level, the past decade has seen a significant increase in the use of economic sanctions. This trend started in the 1990s, when the collapse of the Soviet Union led to the end of the conflict between the two superpowers, which entailed that UN sanctions were less limited by geopolitical considerations. Figure 1 illustrates the increase in the average number of sanctions in relation to a higher success rate, possibly caused by closer trade links between the side imposing the sanctions and the target of the sanctions.

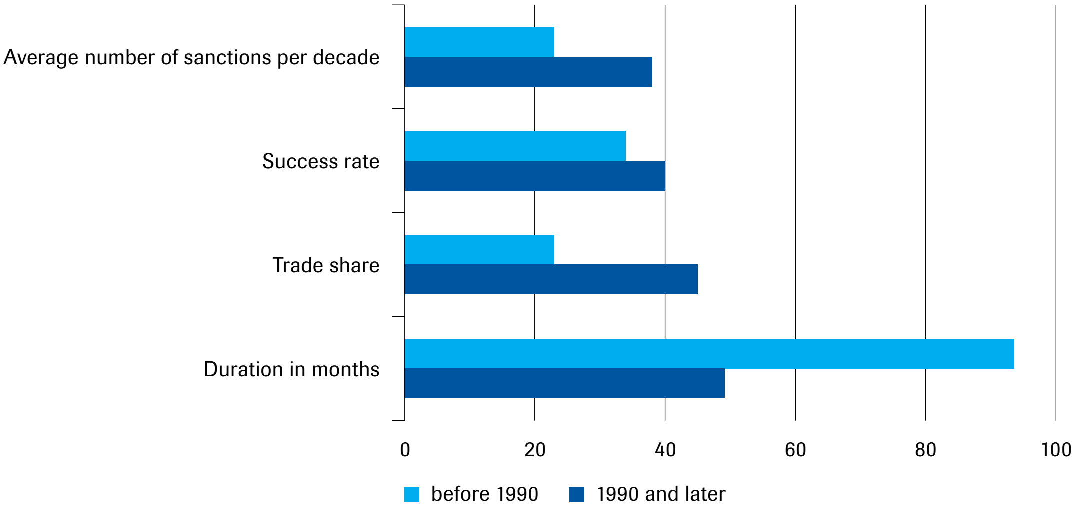


Figure 1 The changing characteristics of economic sanctions (before and after 1990)

Source: calculated from Van Bergeijk, 2009, Table 6.6, p. 134

It is unclear whether the higher success rate is the result of a more judicious use of sanctions or a reflection of the trend towards internationalisation of all economies. Whatever the case, sanctions are used more frequently and the flows concerned are larger than they were in the past. It is therefore reasonable to expect that the Netherlands will be involved in economic sanctions more often, also as a target. In addition, sanctions against countries other than the Netherlands may also indirectly affect important Dutch economic interests. This development is both quantitative and qualitative. Another new type of sanction is the targeted sanction or smart sanction. Smart sanctions target specific decision makers and their associated groups rather than entire populations. Smart sanctions have as yet not been used against the Netherlands.

In summary, security interests possibly harmed by economic influence are mainly economic security, social and political stability and territorial integrity (in the sense of undesired restrictions on the autonomous functioning of the Dutch state). Threats are posed by terrorist organisations, criminal enterprises, consumer boycotts, great powers and governments of countries that have a high degree of influence over specific international production chains, raw materials or technologies, or that have large financial reserves.

Expectation for the coming five to ten years

Economic core processes are becoming more complex, more dependent on technology and are more strongly influenced by the situations in other countries. The extension and branching out of international value chains both increase economic security (international value chains softened the impact of the 2008/9 slump in world trade) and give rise to new risks. The creation of added value in the Netherlands is becoming more dependent on supplies from and sales in other countries. There are risks of disruption in all parts of the value chain. As both a hub of international trade and a participant in the international economic system, the Netherlands is vulnerable, (Van Bergeijk and Mennen, 2014) and will remain so in the coming years. This vulnerability applies to attacks from all relevant groups of actors: criminals, terrorists and states. It is likely that, as discussed elsewhere in this report, the threats posed by criminal and terrorist actors will remain relevant, and will become more acute in the future, also through the cyber domain. As the internet becomes an ever more integral part of society and the economy, state actors will have more opportunities to wage ambiguous warfare on the economies of other states.

Based on events in the past five years, it is more likely that the Netherlands will be a target of sanctions or of sanctions targeted at other countries that nevertheless affect Dutch economic interests. Sanctions or boycotts could be directed against the Netherlands for religious and geopolitical reasons, for example. Religious considerations have already prompted fuzzy sanctions (because of the Dutch short film *Fitna*), cancellations of state visits (because of the Parliamentary Support Agreement concluded with the PVV) and threats to boycott Dutch companies (Saudi Arabia). Sanctions among third parties that may indirectly affect the Netherlands could be initiated for geopolitical reasons – a further exacerbation of the recent trade war between Russia and the West, for instance. But it is also conceivable that frictions between the US and China impact the Netherlands in some way. The risk of geopolitical escalation with respect to trade and investment will become greater as the share of emerging economies increases, on the one hand, because economic power translates into political power, and on the other hand, because these emerging economies are becoming less dependent on OECD countries. Dutch companies have already had to deal with US and European sanctions against countries such as Cuba, Iran and Russia. Possible US sanctions against Chinese targets in the future could have more far-reaching consequences for Dutch business interests.

An important change in the coming five to ten years is that the ability of the Netherlands to use its international influence to limit threats in the economic domain will wane. This key change will take place because the Netherlands' share in gross world product (GWP) will decrease, not because the Netherlands will become poorer, but because the new economic powers are undergoing strong growth (Figure 2). The power base/influence of the Netherlands will halve before 2030 and it is likely that this decrease will start to increasingly affect the policy latitude of the Netherlands already in the near future. The country's relative decline on the international stage means that privileged information and key positions will no longer be a matter of course. Although the decrease in policy latitude cannot accurately be expressed in terms of money, it is clear that there may be macroeconomic costs. In the past, the Netherlands was able to play a key role in shaping institutions that were of vital importance to the country's well-being. It is becoming increasingly unlikely that senior Dutch policymakers will be able to continue playing that key role.

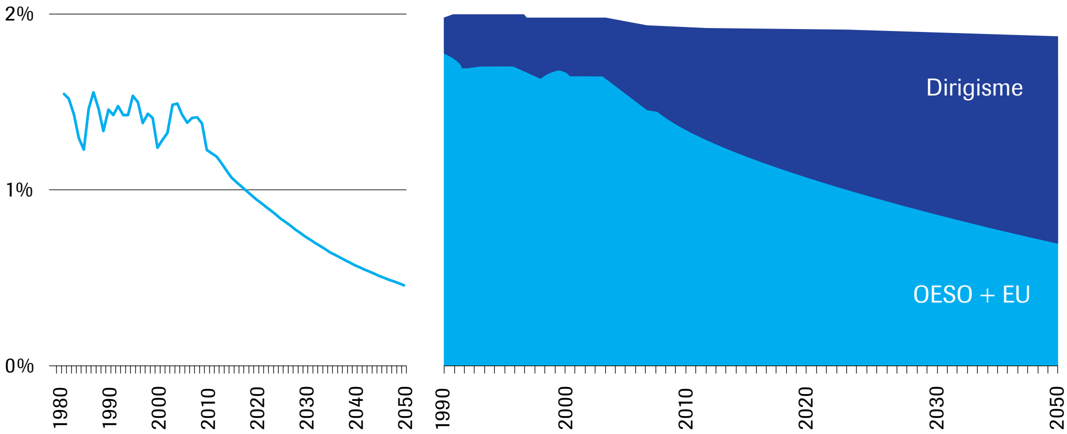


Figure 2 **Decreasing share of the Netherlands (left) and shift of the share according to policy orientation (forecast up to and including 2050)**
Source: calculated from Fouré, J., et al., underlying data set

Nevertheless, the Netherlands remains an important open economy. Schiphol airport and the port of Rotterdam are global hubs and although there is significant international competition, it may be assumed that the Netherlands will maintain its leading position for the medium term. By contrast, the Netherlands will not remain a leader in the financial sector. This is not only due to the banking crisis, but also due to policy choices regarding, for example, development cooperation, including the reduction of the standard for development cooperation relative to GNP. Relative decline is of course not a uniquely Dutch problem. At the global level, the share of the market economies that have supported and developed the multilateral system since the Second World War and that adhere to the OECD's rules is decreasing. The crisis has undermined the credibility of the Washington Consensus. The Chinese development model is effective and offers a clear alternative. The current international situation will inevitably lead to changes in the standards and rules of the international system. The traditional values of the major democratic economies will also lose ground. It is clear that the BRIICS countries (Brazil, Russia, India, Indonesia, China and South Africa) are proactively trying to fill the vacuum (cf. Morse and Keohane, 2014). Steps are being taken to establish an alternative to the World Bank. Unlike the OECD's Development Assistance Committee, the BRIICS countries do not attach any special value to emancipation, reaching the poorest and human rights in bilateral international cooperation. As their economic power grows, the BRIICS countries will probably be less reluctant to place economic relations in general in a geopolitical context that is relevant to them as opposed to a relevance defined exclusively by Western powers.

A complicating factor in all of this is that essential facilities (hard and soft infrastructure that is necessary for international business, such as communications satellites, secure data exchange for commercial credit and international payments, international rules and enforcement options and so on) are increasingly being established in jurisdictions other than the 'traditional' ones. This trend will become more pronounced as the relatively new jurisdictions gain further economic clout and interests. Since this development may have extraterritorial effects, it may pose a threat to national security. The SWIFT sanctions against Iran are an example of hard infrastructure (communications channel for international payment transactions) that was no longer available to Iran. It is not possible to predict where providers of new global essential facilities will be located in exact terms. What is certain, however, is that more of them will be based in BRIICS countries and that it will be more difficult to shape multilateral policy or control global essential facilities in a multilateral way. The multilateral system has traditionally protected small and medium-sized countries. In the current context, regional cooperation is becoming increasingly indispensable as a means for offering the necessary counterweight.

The relevance of deterrence as a security concept

The deterrence concept, as in causing a change in the assessment of expected costs and gains of deliberated actions - plays an important role in the literature on economics. The application of the concept within the framework of rational choice theory is established primarily in analyses pertaining to criminal behaviour and the prevention of such behaviour ('*Law & Economics*'). More recently, as an extension of this, the focus has been on various forms of terrorism (Miller, 2013, Schneider et al., 2014). The analysis of economic sanctions (both positive and negative interaction) has been placed in a similar framework (Dizaji and Van Bergeijk, 2013). In essence, the findings are as follows. Actors who are considering behaviour that could threaten national security may be temporarily or definitively persuaded to refrain from such behaviour by a change in their expected costs and gains or their assessment of them. This effect may be temporary in the event of substitution, modification and innovation. In addition, a shift to other forms of misbehaviour or other, possibly easier targets often occurs.

Deterrence is effective if it increases the *costs* that the attacker must incur, which can be achieved by investing in preventive, protective barriers and more intensive investigation. Making punishments heavier does not have a deterrent effect if the attacker and his property are not on Dutch territory. Because of globalisation, in certain domains economic threats can originate from anywhere in the world (cybercrime is an example). This makes it more difficult to identify the source of the threat. The harder it is to identify the perpetrator, the less effective deterrence becomes as an instrument. Concrete deterrence measures that can be used against criminal or terrorist organisations are: additional protective measures, the threat of smart sanctions, the threat of punitive measures aimed at the environment of the individual that poses a threat and policy designed to influence the milieu from which the threat originates. In addition, increasing the likelihood of being detected is a deterrence measure that can be used against individual criminals or terrorists. The threat of countersanctions and increasing resilience against sanctions may have a deterrent effect on state actors.

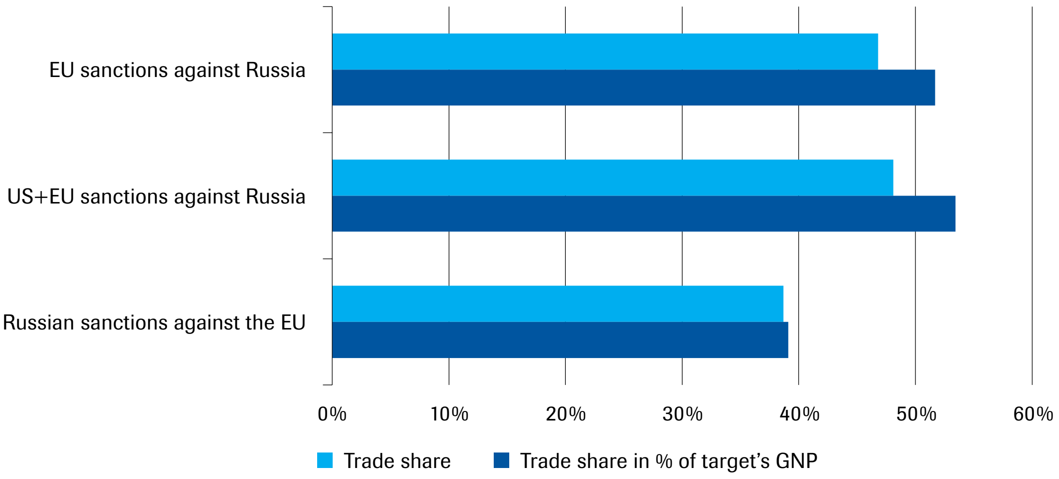


Figure 3 **Success rate of sanctions in the context of the Ukraine crisis**

Source: Voxeu, 25 April 2014

With respect to politically motivated perpetrators, the *gains* can be lowered by reducing the actual or potential impact of a disruption (prioritisation, replacement production capabilities, greater resilience and clear communication of solutions). Excessive dependence on a single area or region in terms of supplies and sales must be prevented to the greatest extent possible, on the one hand in order to ensure that there are alternatives for supply and sales, and on the other hand because a greater spread means that an attack must be carried out against several channels to affect economic core processes or interests. In addition, measures can be taken to increase the resilience of the population and the business community (Frey, 2009) and protective measures can influence a would-be perpetrator's assessment of potential gains.

A complicating factor is the high degree of heterogeneity on both the origin side (the determinants of terrorism, for example; see Kis-Katos et al., 2014) and the target side (the influence of the form of government on the effects of sanctions, for example; see Von Soest and Wahman, 2014). The implication is that findings for a certain domain (religious terrorism, for example) are not necessarily relevant to another domain. In addition, the effectiveness of all deterrence measures is substantially greater if they are taken as part of a bilateral or multilateral alliance (the EU or other alliances). The ability of the Netherlands to use deterrence to counter threats in the economic domain without such cooperation is extremely limited.

Literature

P.A.G. van Bergeijk, *Economic diplomacy and the geography of international trade*. Edward Elgar, 2009.

P.A.G. van Bergeijk and M.G. Mennen, 'De economische betekenis van nationale veiligheidsrisico's'. In: *Tijdschrift voor Veiligheid*, 13(2014)2, p. 35-51.

S.F. Dizaji and P.A.G. van Bergeijk, 'Potential early phase success and ultimate failure of economic sanctions: A VAR approach with an application to Iran'. In: *Journal of Peace Research*. 50(2013)6, p. 721-736.

J. Fouré, A. Bénassy-Quéré and L. Fontagne, '2012, The Great Shift: Macroeconomic projections for the world economy at the 2050 horizon'. In: *CEPII 2012–03*, CEPII: Paris.

B.S. Fresy, ‘How can business cope with terrorism’. In: *Journal of Policy Modelling*, 31(2009), p. 779-787.

A. Hoeffler, ‘Can international interventions secure the peace?’. In: *International Area Studies Review*, 17(2014)1, p. 75-94.

Krisztina Kis-Katos, Helge Liebert and Günther G. Schulze, ‘On the heterogeneity of terror’. In: *European Economic Review* 68(2014), p. 116-136.

K. Kholodilin, D. Ulbricht and G. Wagner. ‘Are the Economic Sanctions against Russia Effective?’. In: *DIW Roundup: Politik im Fokus* 28. DIW Berlin, German Institute for Economic Research, 2014.

Jeffrey W. Knopf, Steven Metz, and James Andrew Lewis, ‘Old Tools, New Century: Deterrence, Containment and Collective Cyberdefense’. In: *World Politics Review*, 2013.

G.D. Miller, ‘Terrorist decision making and the deterrence problem’. In: *Studies in Conflict & Terrorism*, 36(2013), p. 132-151.

J.C. Morse and R.O. Keohane, ‘Contested multilateralism’. In: *The Review of International Organizations*, 2014, p. 1-28.

Friedrich Schneider, Tilman Brück and Daniel Meierrieks, ‘The Economics of Counterterrorism: A Survey’. In: *Journal of Economic Surveys*, 2014.

C. von Soest and M. Wahman, ‘Are democratic sanctions really counterproductive?’. In: *Democratization*, p. 1-24.

A.W. de Vries, C. Portela and B.Guijarro-Usobiaga, ‘Improving the Effectiveness of Sanctions: A Checklist for the EU’. In: *CEPS special report 95*, 2014.

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'étât* 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.