CYBER WARFARE

No 77, AIV/No 22, CAVV December 2011

ADVISORY COUNCIL ON INTERNATIONAL AFFAIRS
ADVIESRAAD INTERNATIONALE VRAAGSTUKKEN

AIV

ADVISORY COMMITTEE ON ISSUES OF PUBLIC INTERNATIONAL LAW
COMMISSIE VAN ADVIES INZAKE VOLKENRECHTELIJKE VRAAGSTUKKEN

CAVV

Members of the Advisory Council on International Affairs

Chair	F. Korthals Altes
Vice-chair	Professor W.J.M. van Genugten
Members	Ms L.Y. Gonçalves-Ho Kang You Professor J. Gupta Dr P.C. Plooij-van Gorsel Professor A. de Ruijter Ms M. Sie Dhian Ho Professor A. van Staden Lt. Gen. M.L.M. Urlings (ret.) Ms H.M. Verrijn Stuart Professor J.J.C. Voorhoeve
Executive Secretary	T.D.J. Oostenbrink

P.O. Box 20061
2500 EB The Hague
The Netherlands

Telephone + 31 70 348 5108/6060
Fax + 31 70 348 6256
aiv@minbuza.nl
www.aiv-advice.nl

Members of the Advisory Committee on Issues of Public International Law

Chair	Professor M.T. Kamminga
Members	Professor K.C.J.M. Arts Dr A. Bos Dr C.M. Brölmann Professor M.M.T.A. Brus Dr A.G. Oude Elferink Professor T.D. Gill Professor L.J. van den Herik Dr N.M.C.P. Jägers Professor J.G. Lammers Professor W.G. Werner Professor R.A. Wessel
Civil service liaison	Professor E. Lijnzaad
Executive Secretaries	Ms W.E.M. van Bladel Ms M.A.J. Hector

Members of the Cyber Security Committee

Chair	Lieutenant General M.L.M. Urlings (ret.)
AIV members	D.J. Barth Dr I. Duyvesteyn Dr P. van Ham Major General C. Homan (ret.) Dr P.C. Plooij-van Gorsel J. Ramaker Ms H.M. Verrijn Stuart
CAVV members	Professor T.D. Gill Professor L.J. van den Herik Professor M.T. Kamminga
External expert	Professor M.J.G. van Eeten
Executive Secretary	A.D. Uilenreef

Contents

Foreword

By letter of 30 August 2011, the Minister of Foreign Affairs and the Minister of Defence, together with the Minister of Security and Justice, asked the Advisory Council on International Affairs (AIV) and the Advisory Committee on Issues of Public International Law (CAVV) to prepare an advisory report on cyber security. They asked the following 12 questions on the central issue of the significance of developments in cyberspace to the Netherlands' foreign, security and defence policies:

1. What are the political and military objectives for which operational cyber capabilities should be developed? How can they be deployed?

2. What is the nature and role of operational cyber capabilities in military operations?

3. Under what circumstances can a cyber threat be regarded as the threat or use of force within the meaning of article 2, paragraph 4 of the UN Charter?

4. Under what circumstances can a cyber attack be regarded as an armed attack against which force may be used for self-defence on the basis of article 51 of the UN Charter?

5. When do the humanitarian laws of war apply to acts performed in the digital domain?

6. Are they the same as those applying to the kinetic use of force?

7. If so, how should we interpret the law-of-war principles of distinction and proportionality and the obligation to take precautionary measures?

8. In the digital domain, how should we interpret the international law concepts of sovereignty and neutrality?

9. To what extent can international standards of conduct for the use of the digital domain contribute effectively to increasing cyber security?

10. Can we learn from experiences with existing codes of conduct, for example in the area of non-proliferation?

11. How can NATO and the EU apply the principles of common defence and deterrence and the solidarity clause to cyber threats?

12. How can NATO and the EU improve information exchange for the purpose of analysing threats?

The first part of this report considers the nature of cyber conflicts and the Dutch armed forces' development of appropriate operational capabilities in this area. The second part looks at relevant aspects of international law, in particular the conditions governing the use of force and the application of international humanitarian law. The third part considers international cooperation, including

agreements on standards of conduct aimed at reducing cyber conflicts and on cooperation within NATO and the EU. The report closes with a summary of the main conclusions and recommendations.

The advisory report was prepared by a joint committee of members of the AIV and CAVV. It was chaired by Lieutenant General M.L.M. Urlings (ret.) and consisted of D.J. Barth, Ms I. Duyvesteyn, Professor T.D. Gill, Professor L.J. van den Herik, Dr P. van Ham, Major General C. Homan (ret.), Professor M. Kamminga, Dr P.C. Plooij-van Gorsel, J. Ramaker and Ms H.M. Verrijn Stuart. Professor M.J.G. van Eeten of Delft University of Technology sat on the committee as external expert. The committee was assisted by civil service liaison officers Ms L.C. den Breems (Ministry of Foreign Affairs, DVB/VD), M.A. Veenendaal (Ministry of Defence, DAB), Ms E. van Beurden (Ministry of Security and Justice) and the executive secretary of the CAVV, Ms M.A.J. Hector. The committee's secretariat was headed by A.D. Uilenreef, assisted by the trainees A.P. Smit and Ms S. de Jong.

The experts the AIV interviewed for this report are listed in annexe IV. The AIV/CAVV is grateful to them for their assistance.

The advisory report was adopted at a meeting of the CAVV on 6 December 2011 and at a meeting of the AIV on 16 December 2011.

Introduction

'Cyber' and the need for demystification

Cyber security is a relatively new phenomenon that has rapidly become a focal point for politicians, policymakers, academics and the media. At the same time, though, cyberspace has been described as *terra nullius,* currently beyond the reach of mature political discourse.[1] It is the AIV and CAVV's aim to contribute to the discourse within the Dutch context. Involvement in cyber conflicts must be tested against political beliefs and the principles of international law. The discourse on this new threat may not be dominated by military and technological responses. As cyberspace inevitably crosses borders, cyber security should be strengthened chiefly through international cooperation. The AIV and CAVV have based this joint report on a sober analysis of the issue, avoiding technical jargon wherever possible and resisting popular parallels in science fiction. Their overriding consideration is that although the phenomenon may be new, we are not facing technological innovation for the first time in history and established principles can help us formulate a response.

Definitions and risk of confusion

Since cyber security is a relatively new phenomenon, we first outline the terminology used in this report. *Cyber security* is defined as *'freedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown, or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information.'*[2]

Apart from failure due to technical weaknesses or natural occurrences, cyber security can be threatened by cyber warfare, cyber espionage, cyber terrorism, cyber activism and cyber crime. These phenomena must be defined not only to ensure the advisory report is understood correctly but also to prevent these different forms of threat creating conceptual confusion at political and policy level. This does not mean the threats are not interrelated. On the contrary, states may use criminal organisations or 'hacktivists', for instance, to engage in espionage. The techniques used are often similar; only the intended objective is different. Identifying the objective is particularly important when deciding on the correct national response to a particular threat, if only to reduce the risk of overreaction. The government needs to adopt clear and uniform definitions. Internationally, too, governments and organisations should agree on uniform interpretations if they are to make international agreements to address cyber threats.

In this report, *cyber warfare* is defined as '*the conduct of military operations to disrupt, mislead, modify or destroy an opponent's computer systems or networks by means of cyber capabilities'*. The key criteria that define cyber warfare are: 1) the presence of a military operation aimed at achieving a political or military advantage, 2) the causing of damage to the opponent's cyber infrastructure; and 3) the use of cyber capabilities (since computer systems can also be destroyed using kinetic capabilities).

Cyber espionage is defined as '*the clandestine gathering of information on networks or information systems by governments or enterprises to further their diplomatic, military or economic interests'.*

1 Chatham House, *On Cyber Warfare*, November 2010.

2 National Cyber Security Strategy, 22 February 2011.

Cyber terrorism is defined as *'the attempt, using cyber capabilities, to seriously disrupt a society or parts of a society in order to achieve a political objective'*.

Cyber activism (also known as *hacktivism*) is defined as: '*an individual or group's penetration and subsequent disruption or modification of networks or information systems in order to raise awareness of a political ideology or social belief'.*

Cyber crime is defined as '*criminal activity involving the use of networks or information systems to obtain a financial or other advantage'*.

In accordance with the request for advice, this report considers cyber security in relation to the Netherlands' foreign, security and defence policies. It thus pays only passing attention to cyber crime. Where necessary, links with cyber crime are considered, as it is not always entirely clear in practice what form of threat is involved.

I The cyber threat and the armed forces' capabilities

I.1 Nature and intensity of cyber conflicts

The cyber threat
The government observes in its request for advice that reliance on the performance of digital networks presents new security risks. The current threat assessment recognises that citizens, public authorities and enterprises are vulnerable to cyber abuse and that cyber crime is becoming more sophisticated, and points to various examples of cyber espionage from abroad.[3] A variety of techniques is used, such as 'botnets' and 'malware'. Similar attacks are also a feature of military operations. Examples include the disruption of internet traffic and military communication systems in Georgia (2008) and the Stuxnet attack on process control systems at a nuclear enrichment facility in Iran (2010). The threat is real, not virtual. Even the report commissioned by the OECD, 'Reducing Systematic Cybersecurity Risk', which questions the impact of the threat, concludes that 'the deployment of cyber weapons is already widespread' and that 'it is a safe prediction that the use of cyberweaponry will shortly become ubiquitous'.[4]

Although the existence of cyber threats as such is not in dispute, there is uncertainty about their extent and influence. The government recognises in the available trend analyses that research into the subject is still in its infancy.[5] The available quantitative studies are in general so statistically unreliable and subjective that no useful conclusions can be drawn from them.[6] The Dutch organisation Bits of Freedom has therefore called for an independent and scientifically-sound baseline study of the nature and extent of cyber security issues.[7] The AIV/CAVV recognises the importance of more systematic and quantitative research into the extent of the threat. Since the problem is transnational and available capabilities can accordingly best be pooled, the AIV/CAVV recommends that the government initiate such an independent study at EU and NATO level.

Using public and classified information from sources including the police, intelligence services and the business community, the Dutch government's Cyber Security and Incident Response Team (GOVCERT.NL) has estimated the threat to our cyber security. It found that cyber crime is becoming more targeted and more sophisticated and now accounts for the majority of all cyber incidents. It also noted that public authorities and enterprises are regularly the victims of cyber espionage and that recent incidents worldwide suggest that

3 Het Nationale Trendrapport Digitale Veiligheid en Cybercrime 2010. Cybersecuritybeeld Nederland (National Trends in Cyber Security and Cyber Crime 2010, Cyber Security Threat Assessment for the Netherlands), December 2011.

4 P. Sommer and I. Brown, *Reducing Systematic Cybersecurity Risk*, OECD/IFP Project on Future Global Shocks, 14 January 2011.

5 Cybersecuritybeeld Nederland, December 2011, GOVCERT.NL, p. 12.

6 D. Florêncio and C. Herley, *Sex, Lies and Cyber-crime Surveys*, Microsoft Research, <http://www.research.microsoft.com/pubs/149886/SexliesandCybercrimeSurveys.pdf>.

7 Bits of Freedom, *Kamerbriefing Nationale Cybersecurity Strategie*, 27 May 2011.

the threat is growing. Terrorists currently initiate very few cyber attacks; they tend to use the internet simply as a propaganda and recruitment tool. With regard to cyber warfare, the existing analyses go no further than stating that this threat is currently the least prevalent but 'its potential impact is probably the greatest'.[8] Some fairly sensationalist publications by foreign trend watchers suggest that wars will in future be fought and won in cyberspace.[9] As explained below, the AIV/CAVV considers a 'cyber war', fought solely in cyberspace, unlikely. The use of such descriptions, moreover, is not conducive to a good understanding of the issue.

A fifth domain for military action

References to cyberspace sometimes suggest that it is a distinct 'space' that has no relationship to time, place or human action. Cyberspace, however, is nothing more or less than the sum of all ICT equipment and services. It consists not only of the internet but also of all the networks and other digital devices that are not connected to the internet.[10] If we put this in the context of military activities, cyberspace can be regarded as a fifth theatre of operations – albeit one with specific characteristics – that interacts with the other four domains of military operation: land, sea, air and space. Operations in the fifth domain can therefore act as a force multiplier in the other domains. Activity in the other domains, incidentally, is now barely even possible without the use of digital equipment. Wars were originally fought only on land and at sea. At the beginning of World War I, aerial warfare added a third domain. A fourth – space – acquired operational significance in the 1980s with the development of anti-satellite missiles and the Strategic Defence Initiative ('Star Wars'). With the development and spread of the internet and the digitisation of society in general, we can also talk of a fifth domain, the only one to have been created by man.

It is now possible to launch cyber attacks as part of a military operation. In essence, this is the use of a military means – cyber capability – to help achieve a political end. In some of the best-known examples, such as those mentioned above, cyber attacks have been conducted in conjunction with conventional operations. In the Stuxnet case the infected programme had to be smuggled into the Iranian enrichment facility by means of a physical human intelligence operation. Of course, a military operation may also consist solely of cyber attacks. It would be technically feasible, using such means only, to disrupt parts of a country's critical infrastructure, at least temporarily. Cyberspace is expected to be an important arena in every future conflict. However, a 'cyber war', fought with devastating consequences solely in cyberspace, is unlikely. The more narrowly defined term 'cyber warfare' is therefore used in this report. Cyber warfare may be regarded as part of a military operation that can include other (non-cyber) dimensions.

I.2 Operational cyber capabilities

Political and military objectives

What are the political and military objectives for which operational cyber capabilities should be developed? Political objectives should precede military objectives. To quote the military theoretician Carl von Clausewitz: 'War is the continuation of politics by other means.' The starting point should therefore be to align with the Netherlands' foreign policy objectives,

8 Het Nationale Trendrapport 2010, p. 37.

9 R.A. Clarke and R.K. Knake, *Cyber War: The next threat to national security and what to do about it*, HarperCollins Publishers Inc, 2010.

10 Het Nationale Trendrapport 2010.

whereby the Dutch government seeks to strengthen three pillars: security, prosperity and freedom. It does so by promoting international stability and security, energy and raw material security, the international legal order – including human rights – and trade and economic interests.[11] The government is aware of the close relationship between internal and external security given the open nature of Dutch society with its strong international ties. This is an important factor in the prosperity of our country but it also makes us vulnerable. The threats of the 21st century are transnational in character and are posed by both state and non-state actors.

The government has set the armed forces three core tasks: defending national and allied territory; protecting and promoting the international legal order and international stability; and supporting the civil authorities.[12] In practice, this means that the Netherlands will use all the resources at its disposal to it to defend national and allied territory. The armed forces carry out the second core task – protecting and promoting the international legal order and international stability – by participating in EU and NATO intervention and stabilisation operations and by taking part in ad hoc coalitions and police missions. The third core task is fulfilled by providing ad hoc assistance to civil authorities (e.g. disaster relief, maintaining public order and security) and performing regular duties such as border control by the Royal Military and Border Police, coastguard management by the Navy and explosive disposal activities.

The deployment of operational cyber capabilities should facilitate these core tasks. A secure and properly functioning digital network is essential to the prosperity of the Netherlands with its strong international logistics and service sector. The Netherlands has one of the highest internet densities in the world. The freedom to exchange thoughts peacefully on the internet anywhere in the world ties in with the importance the Netherlands attaches to respect for human rights and fundamental freedoms. Secure digital services are vital to ensuring public confidence in the government. Combating cyber threats is in the interests of national security. The AIV/CAVV would emphasise that such threats (the extent of which, as noted above, is not known) should be tackled first and foremost using non-military means. In addition to the important contribution that can be made by private parties, diplomatic efforts have a role to play, such as the agreement of international standards of conduct on the management of potential cyber conflicts. We return to this topic in section III.1. In addition to developing operational cyber capabilities, it is also important to invest in coherent ‘cyber diplomacy’ so that a broad pallet of well thought-out measures can be considered in response to concrete threats. These may range from exerting political pressure and imposing economic sanctions to pressing for criminal law measures and – in the final instance – the use of authorised force.

Operational cyber capabilities – part of the military capability – can be a means to achieve a political end. Their use requires a clear political framework. Owing to the transnational character of most security threats (and particularly cyber threats), there is a strong relationship between external and internal security. The Netherlands, however, does not have an integrated strategy on foreign and domestic security policy. The existing national security

11 Coalition Agreement and explanatory memorandum of the Ministry of Foreign Affairs, 2012. The promotion of the international legal order is also laid down in the Constitution (article 90).

12 The Constitution (article 97) provides that the armed forces are for the defence and protection of the interests of the Kingdom and to maintain and promote the international legal order. This is elaborated further in the Defence White Paper (2000) and subsequent government documents.

strategy has a national focus and does not recognise the promotion and enforcement of the international legal order as a vital interest.[13] In the AIV/CAVV's view, operational cyber capabilities and developments in this area should be included in an integrated strategy for domestic and foreign security policy. Such a strategy should provide an insight into the objectives, how they will be achieved and the resources that will be deployed in the process.

Nature of operational cyber capabilities

The specific characteristics of 'cyber weapons'[14] have implications for their operational deployment in cyberspace. Firstly, cyber attacks usually have an *indirect impact*. Since everything on the internet is so closely interrelated, an attack on a military system can have consequences for civil networks. The extent and seriousness of the consequences are not known in advance. It is difficult to distinguish between combatants and non-combatants. *Initial costs are also relatively modest*: it is easier and cheaper to buy the equipment needed for a cyber attack than to buy an aeroplane or tank. This does not mean, however, that every cyber attack can be carried out with easy-to-obtain equipment. Planning and executing a *technically complex attack* requires specialised knowledge. This need is often underestimated but is particularly relevant to the intelligence operations that precede an attack. Cyber weapons also have a *limited shelf life*. Unlike traditional weapons, sophisticated cyber attacks (which actually consist of programming language) can instantly become obsolete and need to be kept secret.[15] The moment a cyber weapon is deployed or otherwise becomes known, the weaknesses it exploits can be identified and rectified. In this respect the traditional arms race has been replaced with a new race in digital expertise and skills. Finally, cyber attacks are *difficult to attribute* to a state, group or individual. The problem of attribution plays a key role in the discussion of the deployment of cyber weapons, and is considered in more detail below.

These characteristics mean that cyber weapons can be deployed *asymmetrically*. Countries without advanced kinetic capabilities, hackers and other non-state actors can obtain the necessary equipment and – if they have no concern for the potential indirect consequences – use it at relatively low cost without needing an extensive military organisation. They are further abetted by the fact that aggressors are difficult to identify. In addition, cyberspace is characterised by *offensive dominance*: it is easier, faster and cheaper to attack a system than it is to defend it. This is partly because an aggressor can prepare an attack anonymously and exploit the element of surprise. In all probability, however, there is no 'first strike' capability that can destroy an opponent's defences and its ability to retaliate using cyber or kinetic weapons. Finally, monitoring the use of cyber weapons is *difficult to regulate*. They are easy to hide and – unlike nuclear weapons – can be developed and tested in secret. Non-proliferation and standard-setting in this area are considered in section III.1.

As noted above, the problem of attribution is a key factor in the discussion of policy on cyber weapons. The perpetrators of espionage or minor attacks are difficult to identify. An attacker can use a chain of hacked computers to conduct espionage or a botnet of infected

13 P.A.L. Ducheine and J.E.D. Voetelink, 'Cyberoperaties: naar een juridisch raamwerk' (Cyber operations: towards a legal framework), *Militaire Spectator,* 180(6).

14 This weapon analogy requires some qualification. 'Cyber weapons' primarily involve technological knowledge and skills.

15 *The New York Times*, 'U.S. Debated Cyberwarfare in Attack Plan on Libya', 17 October 2011. The article names this as one of the reasons for not deploying cyber capabilities in Libya.

computers to cause damage. A government can respond by using non-state actors such as 'patriotic hackers'. Conversely, hackers may declare their support for a state without actually supporting it at all. All these factors can have consequences for the use of offensive action against an aggressor. The inability to identify an aggressor makes launching a counterattack complicated. It is technically possible to identify the source of an attack (a computer's IP address) and direct a counterattack against it by means of trace-back applications. But the computer identified as the source may only be a link in the attack. If the systems involved have been compromised, the perpetrator of the initial attack will not be known. However, it is certainly not impossible to identify an attacker and it is not always necessary to use the internet to do so. Other sources can be used (non-technological attribution), such as intelligence services, political declarations (e.g. claims of responsibility for an attack or previous public threats) and other indications that may point to a potential perpetrator. If the origin of the attack is known with sufficient certainty, exercising the right of self-defence could be justified under certain conditions. These conditions are considered in chapter II.

The role of cyber capabilities in military operations

The Minister of Defence wants the armed forces to develop offensive as well as defensive cyber capabilities. The Knops motion (December 2009) argued that defensive capabilities were not enough.[16] To decide what role operational cyber capabilities should play in military operations, the meaning of defensive and offensive capabilities must first be clear. This is not always the case in the public debate. This also affects the applicable legal framework. The Intelligence and Security Services Act 2002 (WIV 2002), for example, applies to cyber intelligence operations while *jus in bello* applies to the digital destruction of an opponent's air defences. The legal implications are considered in chapter II.

In the table below, the different types of operational cyber activity are grouped into defensive, intelligence and offensive activities and classified as network defence, network exploitation and network attack.

16 Knops, Voordewind and Eijsink motion, House of Representatives, 2009-2010, 32 123 X, no. 66.

Defensive activities	- Securing/monitoring own networks (including weapons systems) **network defence (passive defence)** - Securing defence industry network connection **network defence (passive defence)** - Neutralising counterattack to protect systems *(e.g. disrupting command & control of botnets or taking control of/sabotaging an aggressor's system using malware)* **network attack (active defence)**
Intelligence activities	- Tapping/accessing internet traffic *(interception of IP data or underlying protocols)* **network exploitation** - Monitoring the volume and patterns of data traffic on foreign networks **network exploitation** - Clandestine penetration of systems to download data (*e.g. by means of exploits*) **network exploitation** - Counter-intelligence activities *(e.g. manipulation or disruption of third-party cyber intelligence activities)* **network exploitation**
Offensive activities	- Psychological operations *(e.g. communicating with the public or public authorities via a hacked network)* **network attack** - Eliminating/disrupting the opponent's command, control and communication functions and other defence systems *(distributed denial-of-service (DDoS) attacks)* **network attack** - Destruction of critical infrastructure *(e.g. influencing utility companies' process management systems)* **network attack**

Operational cyber activities

The Ministry of Defence and the armed forces use digital applications for a variety of purposes ranging from command and control to operational management. These applications must be adequately protected. The *security of defence systems* can consist of static defence, such as a firewall or other application that makes it difficult to penetrate a system, and dynamic defence, which monitors for suspect activity within the operator's own networks. A network can also be protected by counterattacking the aggressor's systems.

Cyberspace is becoming more and more important in *intelligence gathering*. An intelligence service's cyber capabilities contribute to the information available on the nature and source of real or potential cyber threats and the ability to penetrate and exploit networks for intelligence operations. A person or organisation can be bugged in cyberspace by intercepting IP data or monitoring activity on third-party networks. Data on other computers or networks can also be copied. A distinction can be made in intelligence gathering between intercepting data traffic on the one hand and penetrating a system on the other. The former involves analysing data patterns (i.e. the volume and direction of data traffic) and listening in to data traffic, possibly with the aid of intercepted encryption codes. The latter involves gaining access to a network by installing malware, exploiting system weaknesses or using *social engineering* techniques.

Offensive cyber capabilities can be deployed in military operations. It is the armed forces' ambition to develop not only defensive cyber capabilities but also offensive capabilities. Cyber attacks are operations to disrupt, damage or destroy computers and networks or the information on them.[17] Many forms of cyber attack are possible, such as disrupting an opponent's command functions by exploiting weaknesses contained in them. Other attacks, for example on critical infrastructure, can result in physical damage and human injury. The same techniques are often used for both attacks and exploitation; only the objective is different. A Trojan horse that surreptitiously downloads data from a penetrated network for intelligence purposes, for example, can later be used to destroy the data on that network.

In addition to the actual use of operational capabilities, an important function of military power is *deterrence*. This raises the question of what role offensive cyber capabilities can play to deter both state and non-state actors. A credible deterrent must be based on a potential opponent's belief that capabilities exist and will be deployed to retaliate for an attack or prevent an imminent attack.[18] There are problems with the application of this principle in cyberspace, however. An adequate cyber deterrent requires a means of early detection. A country's conventional and nuclear capabilities are usually known but cyber weapons can be developed and tested in complete secrecy. The attack itself can take place at the speed of light. Human decisions on countermeasures will always be one step behind. The use of defensive measures with *automatic* retaliation capabilities entails the risk of the wrong targets being hit or of the response being disproportionate. Furthermore, if the motive for an attack is not known it may be difficult to decide on a proportional response. Was the attack conducted with a view to cyber espionage or something more harmful?[19] Finally, as noted above, there is the problem of attribution.

Consequences for the operational deployment of armed forces

Legal parameters. The deployment of cyber weapons, like that of any weapon system, is subject to international legal restrictions. These are considered in the next chapter. The WIV 2002 also places restrictions on the use of cyber capabilities in intelligence work. Firstly, while messages could be intercepted in the past (subject to the necessary ministerial

17 Based on the definition of the National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 2009, pp. 10-11.

18 'UK warns it will strike first against cyber-attackers'. Interview with UK foreign minister William Hague, *The Sun*, 18 October 2011.

19 Under international law, cyber espionage can lead only to diplomatic retaliation, no matter how harmful the loss of information is.

permission) by listening in to satellite traffic, this method can now be used to trace only part of the data that makes up a message. Messages are broken down into data packets and transmitted via different channels using, for example, optical fibre. Under section 27 of the current WIV, only wireless data may be intercepted at random.[20] In the light of technological advances, the AIV/CAVV recommends that a review be conducted of whether the current distinction between wired and wireless data should be retained. Secondly, the AIV/CAVV notes that section 24 of the WIV provides for the exploitation of a network by downloading data from another network by placing an exploit (such as a Trojan horse or virus).[21] However, it rightly prohibits an intelligence service from using a local exploit in a network attack that has a military objective aimed at modifying or damaging a system. Such an attack must be conducted under the responsibility of the Chief of Staff of the Armed Forces with prior political authorisation. Within the armed forces, clear procedural agreements flowing from this segregation of duties must also be made in respect of cyberspace.

Technical restrictions. As noted above, the specific characteristics of cyber weapons also place restrictions on their responsible operational deployment. It cannot always be foreseen how and to what extent the indirect consequences of their deployment will affect civilian systems. The deployment of cyber capabilities in a military operation, for example to eliminate an air defence system, is also technically complex and can require lengthy preparation. If rapid intervention is required and there is no need to keep the operation secret, the use of kinetic forces can be considered. The problem of attribution is also a complicating factor in the deployment of cyber weapons.

Personnel and financial capacity. Despite the sweeping spending cuts in the armed forces, the Ministry of Defence has announced it intends to strengthen the Netherlands' digital defences and to develop greater operational cyber capabilities. An operational *cyber task force* was established on 1 January 2012 and a budget of €50 million allocated for the period up to 2015. It will be spent largely on improving the protection of the Ministry's networks, systems and data and expanding its cyber intelligence capabilities. This is a relatively modest amount in the light of the overall defence budget and the investments being made in cyber capabilities by other countries (especially the US and UK). The Ministry of Defence also needs to build up sufficient expertise in order to deploy its operational cyber capabilities. It will do so by strengthening DefCERT (the Defence Computer Emergency Response Team) and setting up the Defence Cyber Expertise Centre. Some of this specialised expertise will have to be recruited externally. However, public sector terms and conditions of employment make it difficult to recruit high-quality IT specialists and skilled hackers. The corporate culture, moreover, holds little appeal for hackers and seems to form a greater obstacle than financial terms of employment. Using cyber volunteers or cyber 'reservists', as some countries do, is not a cure-all either. There may be insufficient enthusiasm in the Netherlands for individuals to register as qualified volunteers, and the confidential nature of the information concerned means their use would be limited in any event. Cyber reservists could play a role, for example, in training staff at the Ministry of Defence. They could also be used to a limited extent in planned operations. But should the armed forces need additional capacity in the event of an (imminent) attack on Dutch

20 WIV 2002, section 27, subsection 1: 'The services are authorised to intercept and record, with the aid of a technical device, random wireless telecommunications. The powers referred to in the first sentence include the power to decrypt the telecommunications.'

21 Pursuant to this section, the intelligence services may use a technical device to penetrate an automated network and copy the data stored in it.

networks, there is a risk that the companies that employ such IT specialists would need all the expertise at their disposal.

Civil-military cooperation in cyber security

Civil-military cooperation in cyber security touches upon the third core task of the armed forces. Since military and civil networks are closely connected on the internet and one of the armed forces' tasks is to assist civil authorities, cooperation in cyber security seems to be a logical step. We noted at the beginning of this report that it is difficult to make a strict distinction between the various forms of cyber threat. When a system is penetrated, it is not immediately clear which actors are responsible (e.g. hacktivists, criminals or states) and what the motivation for the attack is. The techniques used are largely the same. An appropriate response requires an integrated government strategy. The importance of such a strategy was recently underlined by the DigiNotar incident. The government took a significant step by preparing a National Cyber Security Strategy and setting up the National Cyber Security Centre (NCSC) under the responsibility of the Minister of Security and Justice in January 2012. The Centre's exact ambitions are not yet fully crystallised. The breadth and depth of its tasks will be determined by its growth model. For the time being, the Centre is expected to concentrate on information exchange and crisis management. GOVCERT.NL will become part of the Centre and the Ministry of Defence, like other relevant government organisations, will appoint a liaison officer (probably from the Military Intelligence and Security Service; MIVD) to it. Partly in view of the scarcity of technical knowledge and capability, the AIV/CAVV would advocate an even more integrated approach. The Centre could develop in due course into a kind of national CERT responsible for aggregated monitoring of vital networks, making more use of the capabilities already present at GOVCERT.NL, the MIVD, the General Intelligence and Security Service (AIVD) and the Dutch Police Services Agency (KLPD) and complemented at times by commercial organisations and academic institutions. Pooling this knowledge and skills must not reduce the formal responsibilities of the various client organisations within central government and must not weaken their statutory powers and relationship with foreign partners. The Ministry of Defence, for example, is responsible primarily for protecting its own networks and the networks used to exchange confidential information with allies and the defence industry. Any cyber attack (or counterattack) against a state should also be conducted by the armed forces. Finally, it is worth noting that where intelligence is concerned, there is also scope for more cooperation between the AIVD and the MIVD. The AIV/CAVV recommends combining the available capital- and knowledge-intensive signals intelligence (SIGINT) and cyber capabilities into a joint unit.

II The international legal framework

II.1 Cyber attacks and *jus ad bellum*

Prohibition of the use of force
Article 2, paragraph 4 of the United Nations Charter prohibits the threat or use of force in international relations. This prohibition is often considered a rule of peremptory international law that permits no exceptions except in recognised exceptional cases. The customary interpretation of this provision is that all forms of armed force are prohibited. Purely economic, diplomatic and political pressure or coercion is not defined as force under article 2, paragraph 4. Suspending trade relations or freezing assets, for example, can be very disadvantageous to the state affected but has not to date been considered a prohibited form of force within the meaning of the Charter. Armed force that has a real or potential physical impact on the target state is prohibited. However, such force is not restricted to the kinetic impact of conventional weapons systems. The distinction between armed force and other forms of force depends on whether the force caused or could have caused death, injury or damage to goods or infrastructure. Such force is prohibited if it is more than an isolated, minor incident. Any use or threat of armed force is prohibited under both the UN Charter and customary international law. Armed force is generally seen as force which has the power to inflict casualties or cause physical damage. A use of force which rises to the level of an armed attack is considered further below.

The right of self-defence
Article 51 of the United Nations Charter confirms the right of self-defence against armed attack. It is a temporary right that may be exercised until the Security Council has taken appropriate measures. In its judgment in the Nicaragua case, the International Court of Justice (ICJ) established that the right of self-defence arose from the Charter and customary law. The Charter does not state what forms of force can constitute an armed attack or how it should be decided that such an attack has commenced. This must be determined by the customary law on the exercise of the right to self-defence on which article 51 is based. It is generally thought that an armed attack requires the significant use of armed force that exceeds the level of a minor armed incident or criminal activity. With regard to the time at which an armed attack commences, customary law is generally understood to permit a response to an immediate and unmistakable threat of an armed attack ('imminent threat').[22] It is generally accepted that an armed attack can be carried out directly by a state's armed forces or indirectly by armed groups operating under the authority or control of a state. For the latter to be an armed attack, the ICJ ruled (in the Nicaragua case) that the scale and consequences of an indirect attack must be comparable to those of a direct, conventional armed attack by a state.

There is less agreement on the degree of control a state must exercise over an indirect armed attack. The ICJ's standard is 'effective control', but the International Criminal Tribunal for the former Yugoslavia (ICTY), in its judgment in the *Tadic* case, settled on the slightly broader standard of 'overall control', albeit in the slightly different context of criminal law. Both forms of armed attack are carried out by or under the control of a state. Since the attacks of 11 September 2001, there has been a third possibility not considered in the Nicaragua judgment: that of an organised armed group carrying out an armed attack of

22 See: AIV/CAVV advisory report number 36, *Pre-emptive Action*, July 2004.

its own volition without state control or substantial state influence. The ICJ has not yet adopted a clear position on this matter. In practice, states and the UN Security Council have recognised since 11 September that an organised group can in principle be the author of an armed attack and that a response to such an attack can be qualified as self-defence. It seems reasonable to assume that the attack should be comparable to one carried out either directly by a state or by an armed group under the control or substantial influence of a state. If this third possibility is accepted, it must be asked against whom or what self-defence should be directed and whether it can take place in the territory of a state not directly involved in the attack. These questions are considered separately below in the light of the criteria of necessity and proportionality when the right of self-defence is invoked.

Cyber attack

Can a cyber attack against a computer or information system without the deployment of kinetic weapons qualify as an 'armed attack' within the meaning of article 51 of the UN Charter? Nothing in article 51 or customary international law specifically excludes a particular type of weapon or weapons system. Conventional kinetic weapons are included of course, as are radiological weapons, poison gas, other chemical weapons, biological weapons and laser weapons. There is therefore no reason not to qualify a cyber attack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or unconventional weapons. In other words, if a cyber attack leads to a significant number of fatalities or causes substantial physical damage or destruction to vital infrastructure, military platforms or installations or civil property, it could certainly be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter. The fact that such an attack has not yet taken place does not mean it could not in the foreseeable future. A digital attack against information systems linked to vital infrastructure, military installations and platforms for weapons systems or vital services, such as the emergency services or air traffic control systems, could breach the threshold of an armed attack if it causes significant loss of life or physical destruction.

It is more difficult to conclude whether this is the case if there are no actual or potential fatalities, casualties or physical damage. A serious, organised cyber attack on essential functions of the state could conceivably be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state. In such cases, there must be a disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks for it to be qualified as an armed attack. A disruption of banking transactions or the hindrance of government activity would not qualify as an armed attack. However, a cyber attack that targets the entire financial system or prevents the government from carrying out essential tasks, for example an attack on the entire military communication and command network that makes it impossible to deploy the armed forces, could well be equated with an armed attack.

Organised groups

As in conventional forms of attack, the perpetrator of such a cyber attack could be a state or an organised group acting under the authority or control of a state. It is less clear whether an autonomous group acting of its own volition without the involvement or support of a state can launch a cyber attack of this nature. Neither customary law nor article 51 of the UN Charter excludes the option of self-defence in response to an attack by an organised group that has comparable consequences to a direct or indirect attack by a state. Its exercise in cyberspace, however, entails specific problems. Since computer networks are connected all over the world, the term 'organised group' in this context differs considerably from that used in the physical domain. A cyber attack on vital infrastructure could be conducted by,

for example, people in six different countries working with some measure of coordination but without the degree of cohesion and organisational structure typically associated with an organised armed group located in a specific geographical area. Such a diffuse form of cooperation does not readily lend itself to a military response except in exceptional situations. It is unlikely that an alternative to military action in the form of international judicial cooperation or law enforcement would not be available, allowing the individuals concerned to be apprehended in their respective countries and thus ending the attack. In the great majority of cases in which a state has defended itself against an armed attack by a non-state entity perpetrated without any real involvement by the state in which the entity is located, the armed group behind the attack has been located in a geographical region that the state does not effectively control (e.g. Hezbollah in southern Lebanon, the PKK in northern Iraq and the Taliban/al Qa'ida in the Pakistan/Afghanistan border region).

Attribution

No form of self-defence whatever may be exercised without adequate proof of the origin or source of the attack and without convincing proof that a particular state or states or organised group is responsible for conducting or controlling the attack. International law does not have hard rules on the level of proof required but practice and case law require sufficient certainty on the origin of the attack and the identity of the author of the attack before action can be taken. This requirement can therefore also be an obstacle to self-defence in response to a cyber attack. In cyber warfare, unlike conventional forms of warfare, it will often be difficult to identify the origin and the author of the attack with sufficient certainty to justify a military response. This is also true of other forms of warfare (such as guerrilla wars) but is particularly applicable in cyberspace. In view of the high risk of error and the political, legal and humanitarian consequences, reliable intelligence is required before a military response can be made to a cyber attack. As concluded in chapter I, however, the author of an armed attack can also be identified using non-technological means, especially in the case of a large-scale cyber attack that has a similar impact to a conventional armed attack.

Necessity and proportionality

The legal terms necessity and proportionality have different meanings in different contexts. In the context of self-defence, *necessity* usually refers to the existence of an armed attack or the imminent threat of attack. It also refers to the absence of feasible alternatives, such as law enforcement in the case of an organised group operating in the territory of another state without the direct involvement of that state. In most cases, mutual assistance in a law enforcement context would be a feasible and available alternative, removing the grounds for self-defence. The option of a military response in self-defence is relevant only where a cyber attack is comparable to an armed attack and is conducted by a group of people operating with some measure of coordination but cannot be stopped by a law enforcement agency because the state in which the attack originated is either not willing or not able to take the necessary law enforcement measures. Even then, it is only relevant if there are no alternatives, there is sufficient certainty regarding the identity of the author of the attack (see below) and the self-defence measures can be taken in a targeted and proportional manner.

This has a direct bearing on the position, rights and duties of the state or states in which the group operates. International law is based on a strict prohibition of the use of force and a duty to respect the sovereignty and territorial inviolability of other states. These rights and duties are a two-way street, however. Action on the territory of another state can be justified only on the grounds of a recognised exception to the prohibition of the use of force. A state that allows organised groups to operate and attack other states from its territory breaches a fundamental obligation of international law not to allow its territory to be used to violate the

rights of other states, especially if the violations are comparable in form and seriousness to an armed attack. The 'host' country may be either unwilling or unable to end such activities. In both cases, the necessity of self-defence in response to an armed attack by an organised group operating from another state would be lawful provided it is targeted at the organised group and not at the state in which it is located and the other aspects of the necessity and proportionality criteria are satisfied.[23] If a state is unable to take appropriate action against an organised group operating from its territory, it should allow the target state to take action. It must in any event refrain from taking measures that frustrate or obstruct the target state's lawful exercise of self-defence.

Proportionality in the context of self-defence has both a quantitative and a qualitative dimension. In effect, proportionality means the action must be directed at ending the attack and preventing further attacks in the near future. Moreover, it must be in proportion to the scale of the attack. Proportionality does not presume a specific response to an attack nor does it require the response to be of the same nature as the attack. A cyber attack that has comparable consequences to an armed attack (fatalities, damage and destruction) can justify a response with cyber weapons or conventional weapons provided the intention is to end the attack, the measures do not exceed that objective and there are no viable alternatives. The proportionality requirement rules out measures that harbour the risk of escalation and that are not strictly necessary to end the attack or prevent attacks in the near future.

II.2 Cyber attacks and *jus in bello*

The application of international humanitarian law depends on whether an armed conflict exists, either of an international or non-international character.. If there is no armed conflict, international humanitarian law does not apply (with the exception of certain elements of it that create obligations and/or prohibitions in times of both peace and armed conflict, such as the obligation not to develop certain kinds of weapons). An *international armed conflict* is a military encounter between two or more states or one state's occupation of all or part of another state's territory, regardless of whether or not the occupation encountered armed resistance. This applies to all encounters in which force is used that exceed the threshold of minor or isolated armed incidents such as border skirmishes or isolated incidents in the air or at sea. In other words, the hostilities must reach a sufficient level of intensity.[24] If this threshold is exceeded the humanitarian law of war applies. A *non-international armed conflict* consists of prolonged hostilities that exceed the threshold of purely internal unrest, between a government and an armed group that is organised to some extent or between two or more such groups within a state.

The entire corpus of international humanitarian law, including all treaties binding on one or more of the parties, and the entire corpus of customary humanitarian law apply to international armed conflicts. Common article 3 of the Geneva Conventions in any event applies to a non-international armed conflict, as do the customary law rules of international humanitarian law that are deemed to apply to non-international armed conflicts. In fully-fledged civil wars, Additional Protocol II to the Geneva Conventions applies if the state in question is a signatory to it.

23 Under international law, the host country has a duty of due diligence to ensure that persons in its territory do not violate international legal obligations.

24 Greenwood, Scope of Application of Humanitarian Law, in Fleck (ed), *The Handbook of International Humanitarian Law*, 2nd ed. (2008) p. 48.

Regarding the application of international humanitarian law to cyber operations, a distinction can be made between those that are carried out in conjunction with conventional forms of warfare and those that are not. In the first case, international humanitarian law applies *ipso facto*. If the cyber operations precede or coincide with kinetic operations to disrupt the opponent's communication, command and control systems or to weaken or eliminate its weapons systems, the rules of international humanitarian law apply to both the cyber and the kinetic aspects of the operations. In such a situation, the cyber operations can be considered a means and a method of warfare that are subject to all relevant rules of international humanitarian law. It is a means of warfare as such operations can damage an opponent and disrupt its operations. It is a method of warfare that does not differ in principle from other forms of electronic or information-based warfare. There can therefore be no doubt about the application of international humanitarian law to hostilities in which the belligerents use cyber weapons and techniques as well as kinetic means and methods of warfare.

The application of international humanitarian law to cyber operations that are not carried out in conjunction with conventional forms of warfare is more complicated. A cyber attack that impacts civil or military computer systems and only results in the modification or destruction of non-essential data would not rise to the threshold of an armed conflict. Even if an attack has clear political, financial or economic consequences, such as the DDoS attack on Estonia in 2007, it would not be sufficient to breach the threshold of an armed conflict. Acts that have such consequences in the physical world are not subject to international humanitarian law either. However, if an organised cyber attack (or series of attacks) leads to the destruction of or substantial or long-lasting damage to computer systems managing critical military or civil infrastructure, it could conceivably be considered an armed conflict and international humanitarian law would apply. The same is true of a cyber attack that seriously damages the state's ability to perform essential tasks, causing serious and lasting harm to the economic or financial stability of that state and its people. An example would be a coordinated and organised attack on the entire computer network of the financial system (or a major part of it) leading to prolonged and large-scale disruption and instability that cannot easily be averted or alleviated by normal computer security systems.

Hostilities and precautionary measures in connection with cyber operations
If international humanitarian law applies to an international or non-international armed conflict, it applies to all hostilities, including those in cyberspace. Other branches of law remain relevant to hostilities in such an armed conflict but international humanitarian law is the principal legal instrument and every attack[25] must respect its principles, including those of *distinction, proportionality* and *taking precautionary measures.* In accordance with this regulatory framework, attacks must be directed solely at enemy forces/direct participants in the hostilities or at military targets or objects that contribute to military operations on account of their nature, use, location or purpose. Attacks on civilians or civilian objects are strictly prohibited. Force, including intensive and prolonged force, may be used to eliminate an opponent but it must be applied within the legal framework of international humanitarian law. Continuous measures must also be taken to ensure that individual civilians, the civilian population in general and civilian objects suffer as little damage as possible from operations against legitimate military targets. Attacks on military targets are prohibited if it may be presumed that the civilian casualties and damage to civilian objects they cause will be disproportionate to the expected concrete and direct military advantage. Weapons

25 'Attack' here means an act of violence against an adversary within the meaning of article 49 of Additional Protocol I to the Geneva Conventions (not to be confused with an armed attack within the meaning of article 51 of the UN Charter, in response to which the right of self-defence may be invoked).

or methods of combat are also prohibited if they make no distinction between civilian and military objects or cause unnecessary suffering or needless damage to armed forces relative to the concrete military advantage expected in the circumstances. In this respect, certain weapons (such as chemical and biological weapons) are completely prohibited whereas others (such as cluster munitions) are subject to restrictions.

International humanitarian law also provides that objects or persons with a protected status may not be attacked unless they have lost that status owing to their direct participation in hostilities or their use for military purposes (for example, the use of an ambulance as an army truck or of a church tower or minaret as an observation post). Attacks on objects that enjoy special protection (such as cultural objects of special importance) or that could release dangerous forces (e.g. dams, dykes and nuclear power stations) are permitted only if they make a direct and significant contribution to military operations and there is a compelling military need for the attack. International humanitarian law also prohibits the use of means and methods of war that lead to starvation or threaten the survival of the civilian population (for example attacks against water treatment plants or the electricity grid as a whole). It also prohibits acts intended to spread terror among the civilian population. Finally, international humanitarian law prohibits the feigning of protected status or the use of protected emblems to kill, wound or capture an opponent, or attempt to do so, or to make misleading use of recognised symbols (for example the use of the distinctive emblems of the Geneva Conventions, the feigning of wounds or the misuse of recognised symbols such as a flag of truce or surrender). In this connection and in accordance with the principle of distinction, armed forces and other persons who conduct attacks are in any event obliged to distinguish themselves from the civilian population when taking military positions, before, during and after an attack and they may not use civilians or protected persons and objects as shields in military operations.

The application of this regulatory framework in cyberspace is technically feasible and legally necessary since it applies to all hostilities regardless of the weapons or combat methods used. Every technical advance made in the field of warfare over the centuries has been incorporated into international humanitarian law and there are no grounds, either technical or legal, to assume that cyber warfare will be an exception. It is technically possible to identify military and military-related information systems with reasonable certainty and necessary precautions can be taken to limit the consequences for civil systems. A combined cyber-kinetic attack on military communication, command and control systems, for example, need not lead to excessive damage to civil systems if precautionary measures to prevent external consequences (such as the dissemination of malware) are taken when planning and executing the operation. International humanitarian law prohibits attacks if there is an absence of reasonable certainty concerning the expected collateral effects. In certain situations this would make a cyber attack unlawful. Critical information systems for vulnerable installations such as nuclear power plants, chemical plants and flood protection systems must be adequately protected and secured against attack, except in the exceptional situations in which international humanitarian law permits an attack. This can be achieved by ensuring that they are not targeted and are not affected by attacks against other systems. Attacks against legitimate targets can have negative consequences for civil information systems but they need not be excessive in relation to the military advantage expected from the attack; proportionality should be assessed in the same way as for other forms of warfare.

Digital warfare against civil systems or systems serving protected persons or objects, such as medical files, fire alarm systems in museums or ambulance or fire brigade alarm systems, is subject to the same prohibitions and restrictions as kinetic warfare. Except within the narrow exceptions provided for by international humanitarian law, attacks on

computer systems are prohibited if those systems monitor, for example, dykes, dams and nuclear power stations and/or are necessary for the survival and basic welfare of the civilian population, such as irrigation and drinking water systems. Use of the internet and other means of digital communication to cause terror in the civilian population, for example by spreading rumours that create large-scale panic and mass hysteria, certainly falls within the prohibition on terrorising the civilian population. Finally, the concept of distinctive emblems and the prohibition of perfidy apply by analogy to cyber warfare. Misusing the IP addresses of protected organisations such as the Red Cross or feigning a protected or neutral status to carry out an attack are as prohibited in cyberspace as they are in the real world.

In brief, the existing framework for hostilities provided for by international humanitarian law has legal application and can be technically applied to operations in the digital domain and to the phenomenon of cyber warfare. Some rules, such as the wearing of a uniform during operations, may not be relevant in cyberspace but many if not most are, and the argument that this type of warfare is 'different' and falls outside the legal domain is not convincing. It ignores the fact that international humanitarian law applies to all forms of warfare and to all types of weapons and weapons systems, as it has done throughout its long history.

Neutrality in the context of cyber warfare

Although formal declarations of neutrality in an armed conflict are nearly as rare today as formal declarations of war, it is generally accepted that the right of neutrality still applies in armed conflicts between states except where limited by decisions of the UN Security Council. In essence, this means that the territory, vehicles and aircraft of a non-belligerent state may not be attacked or captured so long as it remains neutral. A belligerent party may not violate neutral territory so long as the neutral state hinders, and does everything necessary to prevent, military operations by parties to the conflict carried out either from or via its territory.

In a digital context, cyber attacks on objects or information systems in neutral territory are therefore prohibited. Where possible, neutral states can take measures to prevent the transmission of military data in their territory and scan or delete data in the internet domain they control using software to identify certain data files containing malware or other cyber weapons of one of the belligerent parties. If an attack uses computer systems in the territory of a neutral state, that state can protect its neutrality by taking measures to identify the origin of the attack and take corrective action provided it does not breach other legal obligations related to respect for human rights. If a neutral state cannot reasonably prevent the transmission of malicious data through the part of the internet in its jurisdiction, its neutrality is not violated or lost. The situation is comparable to that of a radio or telephone message transmitted through part of the global communication network located in neutral territory, which is not considered a violation of neutrality by either the belligerent party or the neutral state.

III International cooperation

III.1 International standards of conduct

Agreements on the organisation of the internet
The government asked to what extent international standards of conduct could contribute effectively to increasing cyber security and what lessons could be learnt from existing codes of conduct, including those on non-proliferation. There are various ways to regulate conduct by means of international agreements. Codes of conduct containing normative rules can be agreed or legal obligations laid down in a binding treaty. The AIV/CAVV thinks it may be useful to develop further agreements on the use of cyberspace. Such agreements are already being made in a number of areas. The standards need not necessarily be anchored in a treaty. Codes of conduct can also be an appropriate means to lay down, apply and internalise agreements on appropriate conduct.

Cyber security can be facilitated firstly by making more far-reaching agreements on use of the internet. In its current form the internet is sometimes described as the 'Wild West' or as a Hobbesian jungle where might is right. An apparent contradiction is often created by counter posing freedom and regulation. Yet in a free society it is necessary to have agreements in the form of rules and standards. The countries participating in the Deauville G8 summit in May 2011 declared that they strongly believed that 'freedom and security, transparency and respect for confidentiality as well as the exercise of individual rights and responsibility have to be achieved simultaneously'.[26] The greatest challenge is to retain the right balance: sufficient security to exercise our freedoms but not so much as to endanger them.

Standards of conduct for conflict management
Since the request for advice places an emphasis on foreign, security and defence policy, this section considers international agreements that can help manage conflicts in the digital domain. The issue is being debated in many bodies, such as the UN, the EU, NATO, the Council of Europe, the OSCE, the International Telecommunication Union (ITU) and the OECD. Although the Dutch government is – rightly – a very active proponent of freedom of expression on the internet, the Netherlands has not yet been as active in global talks to agree standards on conflict management in cyberspace. We recommend that the Netherlands participate in initiatives to agree standards in this area. The 15-country Group of Governmental Experts established by the UN Secretary-General presented its recommendations last year.[27] The Netherlands could participate in the new group of experts that will be established in 2012 to follow up on the original group's report. The participation of Dutch organisations in the ITU's Global Cybersecurity Agenda could also be considered. This forum consists of a variety of interest groups. The Netherlands is already active in the UN-mandated Internet Governance Forum, an important vehicle to exchange thoughts with the private sector and civil society organisations.

26 G8 Declaration, *Renewed Commitment for Freedom and Democracy,* Deauville, 26-27 May 2011.

27 The group was established in 2009 in accordance with Resolution 60/45 of the General Assembly. Its full title is the Group of Governmental Experts on Development in the Field of Information and Telecommunications in the context of International Security. The report can be found at <http://www.unidir.org/pdf/activites/pdf5-act483.pdf>.

Standards of conduct can relate to the protection of networks, cooperation in criminal matters, the application of international law and the exchange of information. With regard to the *minimum quality of networks*, the UN General Assembly has underlined the importance of countries increasing the protection of their national systems.[28] In the EU, there has been some harmonisation of legislation. For example, article 13a of Directive 2009/140/EC (amending *inter alia* Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services) requires member states to ensure that their communication networks are protected, are prepared for potential threats and guarantee a minimum level of service.[29] In general, the private sector could assume more responsibility for the protection of the critical infrastructure it operates. This could be encouraged through better regulation of companies' responsibilities and liabilities in this area. Assurances must also be given on the provision of a minimum level of service if part of the critical infrastructure fails. NATO adopted the Policy on Cyber Defence in June 2011. It includes agreements to strengthen the resilience of national systems. It is now a matter of implementing them. It is in the interests of the countries that have made most progress to help those that have not come as far. A chain is only as strong as its weakest link: states that fail to protect their digital networks may be used as bases for cyber attacks.

The scope of existing agreements on *cooperation in criminal matters* in the Council of Europe Convention on Cybercrime needs to be extended.[30] Although the Convention plays an important role setting standards that extend further than the participating countries, more states than the 47 that have already signed it and the 32 that have ratified it (including the Netherlands) must be encouraged to sign up to this binding international instrument. The Convention provides guidelines on the development of national legislation on computer crimes and offers a framework for international cooperation. Significantly, the Convention states that countries must prosecute or extradite groups or individuals accused of committing cyber crimes in third countries while in the territory of the state in question. This makes it easier to combat such illegal activities as large-scale illegal trade in malware and identity data. The attack on Estonia in 2007 demonstrates that cooperation to identify the source of an attack cannot yet be guaranteed. Although there were strong indications that the attack came from computers in Russian territory, Russia refused to cooperate with the investigation.[31]

The previous chapter concluded that existing *international law* applies to the use of force, the laws of war and the principles of sovereignty and neutrality in cyberspace. It is therefore not necessary to agree a special 'cyber treaty' for these purposes. Although there is growing international consensus in the legal community on the application of existing legal instruments, there is no such consensus at political level. The application of international law would be significantly strengthened if states were to elaborate upon these principles in an

28 Resolution 58/199 of the General Assembly of the United Nations, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, 23 December 2003.

29 See: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF>.

30 Council of Europe Convention on Cybercrime, available at <http://conventions.coe.int/Treaty/EN/projects/FinalCybercrime.htm>.

31 Such an attitude can also be taken as an indication of the attribution. E. Tikk (2011), Ten Rules for Cyber Security, *Survival*, vol. 53 (3), pp. 119-132.

international code of conduct or declaration.

Finally, standards could be agreed on *sharing information* and *settling disputes* to prevent the escalation of conflicts. Standards on the provision of information, including cooperation between CERTs, must evolve in practice. It is encouraging that Vice President Biden said during the London Conference on Cyberspace in early November 2011 that the US was working with Russia to reach an agreement on direct communication channels between the two countries' CERTs and nuclear risk reduction centres in the event of an alarming incident.[32] It may even be worth considering setting up an international centre to monitor serious cyber attacks and issue early warnings. Disputes could be settled by such institutions as the Permanent Court of Arbitration and the International Court of Justice, though investment would need to be made in judges' knowledge of 'cyber justice'.

Standards of conduct in the area of non-proliferation

Before answering the question on the practicability of a non-proliferation regime, we would first consider the existing regimes. The current non-proliferation regime for weapons of mass destruction consists of a body of global and regional multilateral treaties, export control regimes and codes of conduct. Important multilateral treaties are the 1968 Nuclear Non-Proliferation Treaty (NPT), the 1972 Biological Weapons Convention (BWC), the 1993 Chemical Weapons Convention (CWC) and the 1996 Comprehensive Nuclear Test-Ban Treaty (CTBT).[33] Existing codes of conduct include The Hague Code of Conduct Against Ballistic Missile Proliferation (HCOC), which calls for restraint in the production, testing and export of ballistic missiles. The NPT makes a distinction between the nuclear haves and the nuclear have-nots. The non-nuclear-weapon states have undertaken not to develop nuclear weapons and the nuclear-weapon states have agreed to reduce their nuclear arsenals and not block other states' peaceful use of nuclear energy. Compliance with these agreements is monitored by the International Atomic Energy Agency (IAEA). The CTBT prohibits nuclear explosions. The significant differences between cyber weapons and the weapons systems subject to the treaties above would make it difficult to agree a cyber non-proliferation regime. In practice, a distinction cannot be made between cyber haves and have-nots. A non-proliferation regime for cyber 'weapons' would also be difficult to monitor since their possession is difficult to confirm – such weapons actually consist of programming language – and they can be tested in secret on a non-explosive basis. One country therefore cannot be entirely confident that another will observe the agreements.

Besides the above comments on the *feasibility* of a non-proliferation regime, the very *need* for such a regime is open to question. Some of the literature evokes images of 'Cyber Armageddon' or a 'Cyber Pearl Harbor' with apocalyptic consequences. Yet as noted in the first part of this advisory report, a true 'cyber war' – fought exclusively in cyberspace with devastating consequences – is unlikely.

For these reasons, the AIV/CAVV is of the opinion that there is neither the means nor the need to agree a worldwide non-proliferation regime such as those in place for nuclear, chemical and biological weapons. Nor are there sufficient opportunities to introduce and enforce controls on the export of certain digital technologies and software to protect military and civil digital infrastructure. There are also practical objections since the technology in

32 See: <http://www.whitehouse.gov/photos-and-video/video/2011/11/01/vice-president-biden-delivers-remarks-london-conference-cyberspace#transcript>.

33 The Comprehensive Nuclear Test-Ban Treaty (CTBT) has not yet entered into force.

question is dual use and can be found in many applications. Some export control regimes can even be counterproductive if they restrict the public's access to the internet in certain countries.[34]

III.2 International cooperation in the framework of NATO and the EU

Common defence

The government asked the AIV/CAVV to examine the role of NATO and the EU regarding cyber threats in the context of foreign, security and defence policy. In June 2011, the North Atlantic Council (NAC) adopted the NATO Policy on Cyber Defence and related action points.[35] This policy plan is an elaboration of the cyber security goals presented in the NATO Strategic Concept.[36] The ambition level is low. The agreements relate chiefly to protection of NATO's own systems and minimum requirements on the protection of national networks that are connected to NATO systems or process NATO information. The member states remain responsible for the security of all other national systems, including those relating to critical infrastructure. Even though some may be disappointed about the absence of a grand design for a truly common cyber defence policy, the current proposal displays a sense of realism and places responsibility at the right level (principle of subsidiarity). It is also in line with practice in the Netherlands and elsewhere in Europe and North America, where networks are largely in private hands. NATO is considering whether security requirements should be imposed in respect of national infrastructure that is critical to the Alliance and extends beyond the systems connected to NATO, for example private optical fibre connections that NATO relies on for data traffic or national infrastructure that is essential for troop deployments. Even if agreement is reached, it is emphatically not the intention to make NATO directly responsible for such protection.

In the coming years NATO will therefore concentrate on improving the protection of its own systems. On request, it will also help its members develop appropriate protection for national systems that are connected to the NATO network. With some countries clearly further ahead than others, NATO expertise can help the less advanced reach the necessary level of protection and so reduce the Alliance's vulnerability to cyber attacks. NATO can help its members implement national cyber defence strategies by sharing best practices and holding joint training programmes and exercises. Assistance can be provided by, for example, the Cooperative Cyber Defence Centre of Excellence (CCD CoE), the NATO Consultation, Command and Control Agency (NC3A) and the NATO Communications and Information Systems (CIS) School. It is also essential that the exchange of intelligence on cyber threats be improved. Since the Alliance does not have its own intelligence service, individual countries must provide the information required to make an accurate threat assessment. In practice, this is problematic because the countries prefer to share intelligence in a small circle rather

34 See: Jillian C. York, 'Syrian surveillance project raises concerns about effectiveness of export controls', November 2011, at <https://www.eff.org/deeplinks/2011/11/sanctions-fail-stop-syrian-regime-still-harm-citizens>.

35 NATO Policy on Cyber Defence and Cyber Defence Action Plan, 7 June 2011 (classified). Public version at <http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf>.

36 NATO's Strategic Concept states (in point 19) that the Alliance: *'*[will] develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralised cyber protection, and better integrating NATO cyber awareness, warning and response with member nations'.

than make it available to NATO as a whole. As long as this is the case, it will be difficult to pursue an active defence policy that encompasses more than passive defence against cyber attacks. NATO's capabilities in this area are still fairly limited, as illustrated by Cyber Threat Assessment Cell (CTAC) which is staffed by only a handful of people, in contrast to the 50 or so staff at the expanding NATO Computer Incident Response Capability (NCIRC), which is responsible for the technical security of NATO systems and providing support at the request of the member states.

Common defence against cyber threats must be organised differently from conventional defence. The protection of vital non-governmental infrastructure will remain in private hands wherever possible. Although private operators are primarily responsible for the systems' security, the protection of this infrastructure requires the participation of a wider variety of government services and private parties than the protection of conventional systems. In addition to national actors, the European Network and Information Security Agency (ENISA) has an important role to play in this area at European level. The first joint cyber security exercise between the EU and the US was held with the support of ENISA and the American Department of Homeland Security in Brussels on 3 November 2011. It is also vital that the EU institutions improve the protection of their own systems. The Council's secretariat seems particularly prone to cyber espionage.[37] With the establishment of the European External Action Service (EEAS) and the EU delegations that report to it, appropriate network security has become an even higher priority.

The EU currently does not have a cyber security strategy as part of its Common Foreign and Security Policy (CFSP). The EU should present coordinated efforts in this area within the UN and other international bodies, for example regarding required standards of conduct. There is also uncertainty about the role the PSC (Political and Security Committee), COSI (Standing Committee on Operational Cooperation on Internal Security) and the CSC (Council Security Committee) would play in the event of a serious cyber attack. The way in which COREPER (the Permanent Representatives Committee) would be informed requires particularly urgent clarification.[38] As noted elsewhere in this advisory report, the EU is actively engaged in other areas, such as criminal law, network quality standards and privacy legislation. In these areas, too, however, the European Commission's Directorates-General – in particular Home Affairs (HOME), Information Society and Media (INFSO), Justice (JUST) and Internal Market and Services (MARKT) – and the European External Action Service (EEAS) need to implement a joint strategy that will increase the coherence of their activities.

Deterrence

The principle of *deterrence* against cyber attacks, like that against kinetic attacks, is based on the likelihood of minimising an attack on the one hand and the capability and willingness to retaliate on the other (see section I.2). The first chiefly requires investment in common security as described above, with the EU cast in a leading role alongside NATO. The second requires an investment in offensive capabilities and agreements on their deployment. A complicating factor with cyber weapons is the problem of attribution, which is not addressed in NATO's latest policy plan. As noted in section I.2, it is certainly not impossible to identify the perpetrators of particularly violent attacks using non-technological means. However, this

37 BBC News, 'Serious' cyber attack on EU bodies before summit', 23 March 2011. See: <http://www.bbc.co.uk/news/world-europe-12840941>.

38 European Parliament, Directorate-General for External Policies, 'Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU', 2011.

requires a good intelligence capability and NATO must rely on its individual member states for intelligence. Moreover, NATO does not have true offensive cyber capabilities and the Policy on Cyber Defence does not include agreements on their development. Cooperation in this area is frustrated by countries' unwillingness to provide other NATO members with an insight into their capabilities. As noted in section I.2, unlike a gun or armoured vehicle, a cyber weapon is less effective when others know how it works.

In the opinion of the AIV/CAVV, NATO could develop modest offensive cyber capabilities to protect its own systems and networks, i.e. for active defence. Investing in large-scale offensive cyber capabilities that NATO could deploy in a cyber conflict would have far-reaching consequences. It would require NATO to establish its own intelligence organisation. Regardless of whether NATO's own capabilities could make a meaningful contribution to the defence of NATO territory or operations in third countries, the individual member states' conventional and nuclear capabilities already act as deterrents. And it is not only in cyberspace that cyber attacks need to be deterred. As noted in chapter II, NATO can also decide on the proportional use of kinetic weapons to deter or retaliate for cyber attacks. The individual member states' offensive cyber capabilities also act as deterrents. They could be used in future NATO operations, for example as an enabler, supporting the deployment of kinetic weapons.

Solidarity clause

In an emergency, the Cyber Defence Management Board (CDMB), which consists entirely of NATO personnel with no national representatives, can respond independently to attacks on NATO's own networks. In such an event it will inform the NAC of the situation as quickly as possible and request political guidance. If an attack against a member state is imminent or under way, the country concerned can – if the threat is serious – invoke article 4 or 5 of the NATO Treaty. As the AIV/CAVV sees it, both articles may be invoked in respect of cyber attacks. This is consistent with the philosophy of NATO's Strategic Concept that NATO will defend itself against 'any threat of aggression, and against emerging security challenges'.[39] Article 5 is worded so generally that it can cover all forms of armed force. It deliberately provides for a great deal of flexibility, including with respect to the response required from the allies. It does not lay down how they should provide individual or collective assistance by invoking article 51 of the UN Charter. Article 4 is not as extensive in scope, providing that the member states will consult together whenever the 'security of any of the Parties is threatened'. It can be reserved for cyber attacks that compromise national security but do not breach the threshold of an armed attack. In the event of a purely digital attack, article 4 is more likely to be invoked than article 5 since, as noted previously, it is difficult to conclude in such a case that the threshold of an 'armed attack' has been breached. The AIV/CAVV concludes that the wording of the two articles does not need amending but that further agreements could be made on the role of the various NATO organisations and NATO member states in the event of an armed cyber attack. The CDMB could play a leading role as initiator in this matter. Training courses that simulate such an attack should also be organised.

The EU also has a mutual assistance clause (article 42, paragraph 7 of the TEU). If a member state is attacked, the other member states will offer assistance in accordance with article 51 of the UN Charter. In addition, the EU's solidarity clause (article 222 of the TFEU) can be invoked in the event of a terrorist attack or a natural or man-made disaster. NATO is expected to remain the most important instrument for collective defence in the foreseeable future. It is therefore realistic to assume that the EU will restrict itself to expressions of political support. The EU could however play a leading role in promoting cyber security in the private sector in member states.

39 NATO Strategic Concept, point 4a.

Information exchange between the EU and NATO with a view to threat analysis
The EU and NATO's cooperation in threat analysis could be improved. But there is no simple remedy. The exchange of information on cyber security between the EU and NATO runs into the same familiar institutional obstacles as their cooperation in other areas (e.g. the Turkey/Cyprus issue). The problem of information exchange is unlikely to be resolved in the near future. The issue's sensitivity is illustrated by the fact that the NATO Policy on Cyber Defence has never formally been submitted to the EU. Nevertheless the first cautious steps seem to have been taken in regard to sharing information on cyber security strategy design and policy implementation. The problem is that any exchange of information in the near future will be chiefly one way only, given the EU's limited policymaking and capabilities in the fields of CFSP and cyberspace. More systematic use could be made of the information available to ENISA, however.

The exchange of intelligence that can contribute to an accurate threat assessment is even more sensitive. Most NATO and EU members are exceptionally reluctant to share information gathered by their intelligence services with the two organisations. Many countries prefer to work in a smaller circle with like-minded countries in which they have full confidence. The EU and NATO therefore have only limited intelligence information, the formal exchange of which also runs into the institutional problems referred to above. National intelligence organisations might be more willing to share information when the EU and NATO have increased their own stock of intelligence, for example within the EEAS or through the CTAC's analyses of attacks on NATO data traffic.

If formal or institutional obstacles prevent the exchange of information between NATO and the EU, informal contacts between the two organisations' senior officials seem to be the only remaining option. The question is whether this *organisation-to-organisation model* provides an adequate platform for fruitful cooperation on threat analysis. Such contacts do not seem to be widespread at present and without formal agreements and assurances there is a risk of inadequate account being taken of potential violations of privacy rules (due to, for example, differences between EU and US legislation). In the interests of the member states and with due regard for privacy rules, however, the AIV/CAVV is of the opinion that as much use as possible should be made of informal channels for the time being.

IV Conclusions and recommendations

The problem of definition

1. Cyber security can be threatened by cyber warfare, cyber espionage, cyber terrorism, cyber activism and cyber crime. These phenomena need to be defined to prevent them being confused with each other conceptually. This does not mean the threats are not interrelated. The techniques used are often similar; only the intended objective is different. Identifying the objective is particularly important when deciding upon the correct national response to a particular threat, if only to reduce the risk of overreaction.

2. The AIV/CAVV therefore recommends that the government adopt clear and uniform definitions. Internationally, too, governments and organisations need to agree on uniform interpretations if they are to make international agreements to address cyber threats.

The cyber threat

3. The government observes that reliance on digital networks presents new security risks. In addition to cyber crime, which is largely outside the scope of this report, cyber espionage seems to be on the increase. However, more systematic and quantitative study is required of the extent of the various forms of cyber threat. Since the problem is transnational and available capabilities can accordingly best be pooled, the AIV/CAVV recommends that the government initiate such an independent study at EU and NATO level.

After land, air, sea and space, cyberspace is regarded as the fifth domain of military operations. What are the political and military objectives for which operational cyber capabilities should be developed, and how can they be deployed? What is the nature and role of operational cyber capabilities in military operations?

4. Cyberspace is expected to be an important arena in every future conflict. However, a 'cyber war', fought with devastating consequences solely in cyberspace, is unlikely. The more clearly defined term 'cyber warfare' is therefore used in this report. Cyber warfare can be regarded as part of a military operation that includes other (non-cyber) dimensions.

5. Operational cyber capabilities – part of the military capability – can be a means to achieve a political end. Their use requires a clear political framework. The existing national security strategy has a national focus. The AIV/CAVV recommends that operational cyber capabilities and developments in this area be included in an integrated strategy for domestic and foreign security policy.

6. In addition to developing operational cyber capabilities, it is also important to invest in coherent 'cyber diplomacy' so that a broad pallet of well thought-out measures can be considered in response to concrete threats. These may range from exerting political pressure and imposing economic sanctions to pressing for criminal law measures and – in the final instance – the use of authorised force.

7. The deployment of cyber capabilities must be conducive to the armed forces' main objectives, for instance protecting national defence systems, gathering intelligence and disrupting, damaging or destroying an opponent's computers and networks.

8. Although cyber weapons are initially relatively inexpensive, planning a technologically complex attack requires specialised knowledge. Cyber weapons have a limited shelf life, their deployment often has indirect consequences and the aggressor is difficult to trace. But it is certainly possible to identify the aggressor with the aid of non-technological means.

9. In the light of technological advances, the AIV/CAVV recommends that a review be conducted of whether the current distinction between wired and wireless data should be retained in the Intelligence and Security Services Act (WIV).

10. The WIV rightly prohibits an intelligence service from using a local exploit in a military network attack aimed at changing or damaging a system. Any such attack must be conducted under the responsibility of the Chief of Staff of the Armed Forces with prior political authorisation. Further to this segregation of duties, clear procedural agreements must also be made within the armed forces in respect of cyberspace.

11. It may be decided to use cyber attacks in military operations. In essence, this is the use of a military means – cyber capability – to achieve a political end. The operational deployment of cyber capabilities in conformity with applicable legal frameworks is limited by the technical characteristics of cyber weapons and the knowledge available within the armed forces. The AIV/CAVV therefore recommends that, for the time being, scarce defence resources be used to develop offensive capabilities on only a limited scale and that priority be given to improving the protection of defence networks and gaining an adequate intelligence capability in respect of the digital domain.

12. Partly in view of the scarcity of technical knowledge and capability, the AIV would advocate an even more integrated approach at the National Cyber Security Centre. The Centre, operational as of January 2012, could develop in due course into a kind of national Computer Emergency Response Team (CERT) responsible for aggregated monitoring of vital networks, making more use of the capabilities already present at GOVCERT.NL, the Military Intelligence and Security Service (MIVD), the General Intelligence and Security Service (AIVD) and the Dutch Police Services Agency (KLPD), and complemented at times by commercial organisations and academic institutions. Where intelligence is concerned, there is also scope for more cooperation between the AIVD and the MIVD. The AIV/CAVV recommends combining the available capital- and knowledge-intensive signals intelligence (SIGINT) and cyber capabilities into a joint unit.

Under what circumstances can a cyber threat be regarded as the threat or use of force within the meaning of article 2, paragraph 4 of the UN Charter? Under what circumstances can a cyber attack be regarded as an armed attack against which force may be used for self-defence on the basis of article 51 of the UN Charter?

13. Article 2, paragraph 4 of the United Nations Charter prohibits the threat or use of force in international relations. The prohibition includes armed force that has a real or potential physical effect on the target state. It also covers other forms of force that have led or could have led to death, injury or damage to goods or infrastructure.

14. Under international law, the use of force in self-defence pursuant to article 51 of the UN Charter is an exceptional measure that is justified in armed cyber attacks only when the threshold of cyber crime or espionage is breached. For a cyber attack to justify the right of self-defence, its consequences must be comparable with those of a conventional armed attack. If a cyber attack leads to a considerable number of fatalities or large-scale

destruction of or damage to vital infrastructure, military platforms and installations or civil property, it must be equated with an 'armed attack'.

15. An organised cyber attack on essential state functions must be regarded as an 'armed attack' within the meaning of article 51 of the UN Charter if it causes (or has the potential to cause) serious disruption to the functioning of the state or serious or prolonged consequences for the stability of the state, even if there is no physical damage or injury. In such cases, there must be a disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks.

16. When exercising the right of self-defence in response to a cyber attack, the use of force must comply with the requirements of necessity and proportionality. The measures must be directed at ending the attack and preventing its repetition in the near future and there must be no viable alternatives.

17. The principle of proportionality does not require a response to be of the same nature as the attack itself. A cyber attack that meets the criteria of an armed attack can justify a response with conventional arms.

18. Taking measures against cyber aggression is lawful only if there is a sufficient degree of certainty regarding the origin and source of the attack.

When do the humanitarian laws of war apply to acts performed in the digital domain? Are they the same as those applying to the kinetic use of force? If so, how should we interpret the law-of-war principles of distinction and proportionality and the obligation to take precautionary measures?

19. The humanitarian law of war applies only to armed conflict, international or otherwise. Cyber operations that do not breach the threshold of an armed conflict do not fall within the scope of the humanitarian law of war.

20. Cyber attacks that are more than sporadic, isolated armed incidents and that (could) result in loss of life, injury, destruction or prolonged damage to physical objects may be qualified as armed conflict within the meaning of the humanitarian law of war. This is primarily the case where cyber attacks are conducted in conjunction with a kinetic attack. But it is also the case where a cyber attack – without the deployment of kinetic capabilities – causes destruction or prolonged and serious damage to computer systems that manage critical military or civil infrastructure, or seriously compromises the state's ability to perform essential public functions and hence causes serious and long-lasting damage to the economic or financial stability of the state and its population.

21. In every armed conflict, international or otherwise, the rules on the conduct of hostilities apply to the deployment of all types, capabilities and methods of warfare, including those of a digital nature. These rules include the principles of distinction, proportionality and the taking of precautionary measures. Moreover, feigning a protected or neutral status with a view to conducting an attack, and misusing such a status (including an IP identity) as a shield against an attack are also prohibited.

In the digital domain, how should we interpret the international law concepts of sovereignty and neutrality?

22. The right of neutrality applies in respect of the deployment of cyber weapons and capabilities. Where possible, it prevents belligerent parties from using computers or computer systems located in neutral territory and from attacking computer networks or information systems in neutral territory. A neutral state may prevent a belligerent party from using computers and information systems located in its territory or jurisdiction. The mere transmission of data through part of the internet located in neutral territory, however, does not constitute a violation or loss of neutrality.

To what extent can international standards of conduct for the use of the digital domain contribute effectively to increasing cyber security? Can we learn from experiences with existing codes of conduct, for example in the area of non-proliferation?

23. Standards of conduct can apply to the protection of networks, cooperation in criminal matters, the application of international law and the exchange of information. The scope of existing agreements laid down in the Council of Europe Convention on Cybercrime needs to be extended. Significantly, the Convention states that countries must prosecute or extradite groups or individuals accused of committing cyber crime in third countries while in the territory of the state in question. This makes it easier to combat such illegal activities as large-scale illegal trade in malware and identity data. As concluded above, current international law applies to the digital domain as regards the use of force, the law of war and the principles of sovereignty and neutrality. It is therefore not necessary to agree a special 'cyber treaty'. The AIV/CAVV thinks, however, that the application of international law would be significantly strengthened if states were to elaborate on these principles in an international code of conduct or declaration.

24. In general, the private sector could assume more responsibility for protecting the critical infrastructure it operates. This could be achieved through better regulation of enterprises' responsibilities and liabilities in this area. Assurances must also be given on the provision of a minimum level of service if part of the critical infrastructure fails.

25. The AIV/CAVV would note that although the Dutch government is rightly an active proponent of freedom of expression on the internet, the Netherlands has not yet been as active in global talks to agree standards on conflict management in the digital domain. The AIV/CAVV recommends that the Netherlands participate in initiatives to agree standards in this area, such as a Group of Governmental Experts to be re-established by the UN Secretary-General.

26. There is neither the opportunity nor the need to reach agreement on a global non-proliferation regime. There are significant differences between weapons of mass destruction and cyber 'weapons'. Nor is there sufficient reason to impose and enforce export restrictions on certain digital technologies and software in order to protect national military and civil cyber infrastructure.

How can NATO and the EU apply the principles of common defence and deterrence and the solidarity clause to cyber threats? How can NATO and the EU improve information exchange for the purpose of analysing threats?

27. NATO will likely be able to develop only modest offensive cyber capabilities to protect its systems and networks, i.e. for active defence. The conventional and nuclear capabilities of individual NATO members already act as deterrents, but their respective offensive cyber capabilities could be used in future NATO operations.

28. The European Commission's Directorates-General – in particular Home Affairs (HOME), Information Society and Media (INFSO), Justice (JUST) and Internal Market and Services (MARKT) – and the European External Action Service (EEAS) need to implement a joint strategy that will increase the coherence of their cyber security activities.

29. Articles 4 and 5 of the NATO Treaty may be applied to attacks in cyberspace. Article 5 is worded so generally that it can cover all forms of armed force. Article 4 is not as extensive in scope and may be applied to cyber attacks that endanger national security but do not breach the threshold of an armed attack. In the event of a cyber attack, article 4 is the more likely of the two to be invoked.

30. The EU's mutual assistance clause (article 42, paragraph 7 of the TEU) will probably be invoked chiefly to express political support. The EU can however play a leading role in promoting cyber security in the private sector in the member states.

31. The EU and NATO's exchange of information on cyber security runs into the same familiar institutional obstacles as their cooperation in other areas. An additional problem is that any exchange in the near future will be chiefly one way given the EU's limited policymaking and capabilities in the fields of common foreign and security policy and cyberspace. For the time being, the EU and NATO will have to exchange as much intelligence as possible through informal channels, with due regard for privacy rules.

Annexes

Request for advice

Mr F. Korthals Altes and Professor M.T. Kamminga
Chairs of the Advisory Council on International Affairs and the
Advisory Committee on Issues of Public International Law
Postbus 20061
2500 EB The Hague

Re Request for advice on digital security

Dear Mr Korthals Altes and Professor Kamminga,

Our dependence on digital networks has given rise to new security risks, as is recognised in NATO's new Strategic Concept and the Netherlands' Cyber Security Assessment.

In February 2011, the Government presented the National Cyber Security Strategy. In accordance with the policy letter 'Defence after the credit crisis' of 8 April 2011, we have been investing additional resources in digital resilience at the Ministry of Defence and the development of operational cyber capabilities.

Against this background, we, the Minister of Foreign Affairs and the Minister of Security and Justice, wish to ask the Advisory Council and the Advisory Committee to answer two general questions: *What do developments in the digital domain mean for Dutch foreign policy as well as security and defence policy? And how can international cooperation contribute to effective protection against cyber threats?*

We would also ask you to address the following specific questions:

1. After land, air, sea and space, the digital domain is regarded as the fifth domain of military operations. What are the political and military objectives for which operational cyber capabilities should be developed? And how can they be deployed? What is the nature and role of operational cyber capabilities in military operations?

2. To what extent and in what ways is the existing international law framework relevant to acts performed in the digital domain, especially cyber violence?
    - Under what circumstances can a cyber threat be regarded as the threat or use of force within the meaning of article 2, paragraph 4, of the UN Charter? Under what circumstances can a cyber attack be regarded as an armed attack against which force may be used for self-defence on the basis of article 51 of the UN Charter?
    - When do the humanitarian laws of war apply to acts performed in the digital domain? Are they the same as those applying to the kinetic use of force? If so, how should we interpret distinction and proportionality (two important principles of humanitarian law governing warfare) and the obligation to take precautions?
    - In the digital domain, how should we interpret the international law concepts of sovereignty and neutrality?

3. International cooperation is indispensable to cyber security.
    - To what extent can international standards of conduct for the use of the digital domain contribute effectively to increasing cyber security? Can we learn from experiences with existing codes of conduct, for example in the area of non-proliferation?
    - How can NATO and the EU apply the principles of common defence and deterrence and the solidarity clause to cyber threats? How can NATO and the EU improve information exchange for the purpose of analysing threats?

Given the speed of change in cyber security, we would appreciate receiving a concise advisory report as soon as possible.

Yours sincerely,

[signed]

Uri Rosenthal
Minister of Foreign Affairs

[signed]

Hans Hillen
Minister of Defence

Abbreviations

AIV	Advisory Council on International Affairs
AIVD	General Intelligence and Security Service
BWC	Biological Weapons Convention
CAVV	Advisory Committee on Issues of Public International Law
CCD CoE	Cooperative Cyber Defence Centre of Excellence
CDMB	Cyber Defence Management Board
CDS	Chief of Staff of the Armed Forces
CERT	Computer Emergency Response Team
CFSP	Common Foreign and Security Policy
COREPER	Permanent Representatives Committee
COSI	Standing Committee on Operational Cooperation on Internal Security
CTAC	Cyber Threat Assessment Cell
CTBT	Comprehensive Test-Ban Treaty
CWC	Chemical Weapons Convention
DDoS	Distributed Denial of Service
DefCERT	Computer Emergency Response Team of the Ministry of Defence
EEAS	European External Action Service
ENISA	European Network and Information Security Agency
GOVCERT.NL	Computer Emergency Response Team of the Dutch government
HCOC	The Hague Code of Conduct against Ballistic Missile Proliferation
IAEA	International Atomic Energy Agency
ICT	Information and Communications Technology
ICTY	International Criminal Tribunal for the former Yugoslavia
IP	Internet Protocol
ITU	International Telecommunication Union
KLPD	Dutch Police Services Agency
MIVD	Military Intelligence and Security Service
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation, Command and Control Agency
NCIRC	NATO Computer Incident Response Capability
NCSC	National Cyber Security Centre
NPT	Non-Proliferation Treaty
OECD	Organisation for Economic Cooperation and Development
OSCE	Organisation for Security and Cooperation in Europe
PSC	Political and Security Committee
WIV	Intelligence and Security Services Act

Terms and definitions

Attribution	The identification of the perpetrators of a cyber attack.
Botnet	A collection of infected computers controlled remotely from a central location.
Cyber activism	An individual or group's penetration and subsequent disruption or modification of networks or information systems in order to raise awareness of a political ideology or social belief.
Cyber attack	An operation to disrupt, damage or destroy computers and networks or the information on them.
Cyber crime	A criminal activity to obtain a financial or other advantage by using networks or information systems.
Cyber espionage	The clandestine gathering of information on networks or information systems by governments or enterprises to further their diplomatic, military or economic interests.
Cyber exploitation	Digitally copying data on other computers or networks.
Cyber security	Freedom from danger or damage caused by the disruption or failure of information and communications technology (ICT) or by the misuse of ICT. The danger or damage caused by misuse, disruption or failure can comprise the restricted availability and reliability of ICT, violation of the confidentiality of information stored in ICT systems or damage to the integrity of that information.
Cyberspace	The sum of all ICT equipment and services, including all networks and other digital devices not connected to the internet.
Cyber terrorism	The use of cyber capabilities to seriously disrupt a society or parts of a society in order to achieve a political objective.
Cyber warfare	The conduct of military operations to disrupt, mislead, modify or destroy an opponent's computer systems or networks by means of cyber capabilities.
DDoS attack	Distributed Denial of Service, an attack in which a particular service (e.g. a website) cannot be accessed by its customary users. A DDoS attack against a website is often carried out by saturating the website with network traffic so that it is unavailable.
Exploit	Software, data or a succession of commands that exploit weaknesses in software or hardware to cause unintended or unexpected activity.
Hacktivism	See cyber activism.
Human intelligence	The gathering of intelligence through interpersonal contact.
Kinetic weapons	Weapons such as handguns, tanks and artillery.
Malware	Malicious software.
SIGINT	Signals intelligence, the gathering and processing of intelligence from satellite and radio communications.
Social engineering	A method of attack using human traits such as curiosity, trust and greed to obtain confidential information or carry out certain actions.
Trojan horse	A file that appears harmless but has a malicious function.
Virus	A means of transmitting malicious software. It is spread by an action performed by the user, for example sending email.
Worm	A means of transmitting malicious software. It uses an infected network or device to spread itself further.
Zero day	A weakness in a piece of software that the maker or operator is not yet aware of.

Interviewees

Name	Position/Organisation
F. Asbeck	Principal Adviser for Space and Security Policy, EEAS
Rear Admiral P.J. Bindt	Director, Military Intelligence and Security Service
D.J. le Clercq	Legal and Administrative Adviser, Administrative Staff, Directorate of Legal Affairs, International and Legal Policy Affairs Division, Ministry of Defence
Dr P.A. Ducheine	Colonel of the Military Legal Corps, Professor of Military Law, Netherlands Defence Academy
R.V. Duiven	Project planner, National Cyber Security Strategy
Col. H. Folmer	Cyber programme manager, Ministry of Defence
Maj. Gen. K. Gijsbers	Reorganisation Project Coordinator, Ministry of Defence
E.E. Gillissen	Senior legal adviser, WIV 2002, Directorate of Legal Affairs, Legislation Division, Ministry of Defence
N. Groeneveld	Information Security Engineer, Confidential
Ms E.C. van den Heuvel	General Manager GOVCERT.NL
M.J. Kuipers	Deputy Head, AIVD
E. Luiijf	Consultant/adviser, Centre for Protection of National Infrastructure and the Netherlands Organisation for Applied Scientific Research (TNO)
F. Peters	Senior policy officer, MIVD, Policy Division, Ministry of Defence
R. Prins	CEO and Co-Founder, Fox-IT
Col. W. Sleurink	Emerging Security Challenges Division, NATO
M.A. Stibbe	Deputy Director, Security Policy Department, Ministry of Foreign Affairs
A. Suleyman	Head of Cyber Defence Section, Emerging Security Challenges Division, NATO Cyber Defence Coordination & Support Centre
Dr E. Tikk	Legal adviser, NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD CoE)
P. Zandstra	Policy officer, Permanent Delegation to NATO

Previous reports published by the Advisory Council on International Affairs

1 AN INCLUSIVE EUROPE, *October 1997*
2 CONVENTIONAL ARMS CONTROL: urgent need, limited opportunities, *April 1998*
3 CAPITAL PUNISHMENT AND HUMAN RIGHTS: recent developments, *April 1998*
4 UNIVERSALITY OF HUMAN RIGHTS AND CULTURAL DIVERSITY, *June 1998*
5 AN INCLUSIVE EUROPE II, *November 1998*
6 HUMANITARIAN AID: redefining the limits, *November 1998*
7 COMMENTS ON THE CRITERIA FOR STRUCTURAL BILATERAL AID, *November 1998*
8 ASYLUM INFORMATION AND THE EUROPEAN UNION, *July 1999*
9 TOWARDS CALMER WATERS: a report on relations between Turkey and the European Union, *July 1999*
10 DEVELOPMENTS IN THE INTERNATIONAL SECURITY SITUATION IN THE 1990s: from unsafe security to unsecured safety, *September 1999*
11 THE FUNCTIONING OF THE UNITED NATIONS COMMISSION ON HUMAN RIGHTS, *September 1999*
12 THE IGC AND BEYOND: towards a European Union of thirty Member States, *January 2000*
13 HUMANITARIAN INTERVENTION, *April 2000**
14 KEY LESSONS FROM THE FINANCIAL CRISES OF 1997 AND 1998, *April 2000*
15 A EUROPEAN CHARTER OF FUNDAMENTAL RIGHTS?, *May 2000*
16 DEFENCE RESEARCH AND PARLIAMENTARY SCRUTINY, *December 2000*
17 AFRICA'S STRUGGLE: security, stability and development, *January 2001*
18 VIOLENCE AGAINST WOMEN: legal developments, *February 2001*
19 A MULTI-TIERED EUROPE: the relationship between the European Union and subnational authorities, *May 2001*
20 EUROPEAN MILITARY-INDUSTRIAL COOPERATION, *May 2001*
21 REGISTRATION OF COMMUNITIES BASED ON RELIGION OR BELIEF, *June 2001*
22 THE WORLD CONFERENCE AGAINST RACISM AND THE RIGHT TO REPARATION, *June 2001*
23 COMMENTARY ON THE 2001 MEMORANDUM ON HUMAN RIGHTS POLICY, *September 2001*
24 A CONVENTION, OR CONVENTIONAL PREPARATIONS? The European Union and the ICG 2004, *November 2001*
25 INTEGRATION OF GENDER EQUALITY: a matter of responsibility, commitment and quality, *January 2002*
26 THE NETHERLANDS AND THE ORGANISATION FOR SECURITY AND COOPERATION IN EUROPE IN 2003: role and direction, *May 2002*
27 BRIDGING THE GAP BETWEEN CITIZENS AND BRUSSELS: towards greater legitimacy and effectiveness for the European Union, *May 2002*
28 AN ANALYSIS OF THE US MISSILE DEFENCE PLANS: pros and cons of striving for invulnerability, *August 2002*
29 PRO-POOR GROWTH IN THE BILATERAL PARTNER COUNTRIES IN SUB-SAHARAN AFRICA: an analysis of poverty reduction strategies, *January 2003*
30 A HUMAN RIGHTS BASED APPROACH TO DEVELOPMENT COOPERATION, *April 2003*
31 MILITARY COOPERATION IN EUROPE: possibilities and limitations, *April 2003*
32 BRIDGING THE GAP BETWEEN CITIZENS AND BRUSSELS: towards greater legitimacy and effectiveness for the European Union, *April 2003*
33 THE COUNCIL OF EUROPE: less can be more, *October 2003*
34 THE NETHERLANDS AND CRISIS MANAGEMENT: three issues of current interest, *March 2004*
35 FAILING STATES: a global responsibility, *May 2004**

36 PRE-EMPTIVE ACTION, *July 2004**
37 TURKEY: towards membership of the European Union, *July 2004*
38 THE UNITED NATIONS AND HUMAN RIGHTS, *September 2004*
39 SERVICES LIBERALISATION AND DEVELOPING COUNTRIES: does liberalisation produce deprivation?, *September 2004*
40 THE PARLIAMENTARY ASSEMBLY OF THE COUNCIL OF EUROPE, *February 2005*
41 REFORMING THE UNITED NATIONS: A closer look at the Annan report, *May 2005*
42 THE INFLUENCE OF CULTURE AND RELIGION ON DEVELOPMENT: Stimulus or stagnation?, *June 2005*
43 MIGRATION AND DEVELOPMENT COOPERATION: coherence between two policy areas, *June 2005*
44 THE EUROPEAN UNION'S NEW EASTERN NEIGHBOURS: *July 2005*
45 THE NETHERLANDS IN A CHANGING EU, NATO AND UN, *July 2005*
46 ENERGISED FOREIGN POLICY: security of energy supply as a new key objective, *December 2005***
47 THE NUCLEAR NON-PROLIFERATION REGIME: The importance of an integrated and multilateral approach, *January 2006*
48 SOCIETY AND THE ARMED FORCES, *April 2006*
49 COUNTERTERRORISM FROM AN INTERNATIONAL AND EUROPEAN PERSPECTIVE, *September 2006*
50 PRIVATE SECTOR DEVELOPMENT AND POVERTY REDUCTION, *October 2006*
51 THE ROLE OF NGOS AND THE PRIVATE SECTOR IN INTERNATIONAL RELATIONS, *October 2006*
52 EUROPE A PRIORITY!, *November 2006*
53 THE BENELUX: the benefits and necessity of enchanced cooperation, *February 2007*
54 THE OECD OF THE FUTURE, *March 2007*
55 CHINA IN THE BALANCE: towards a mature relationship, *April 2007*
56 DEPLOYMENT OF THE ARMED FORCES: interaction between national and international decision-making, *May 2007*
57 THE UN HUMAN RIGHTS TREATY SYSTEM: strengthening the system step by step in a politically charged context, *July 2007*
58 THE FINANCES OF THE EUROPEAN UNION, *December 2007*
59 EMPLOYING PRIVATE MILITARY COMPANIES: a question of responsibility, *December 2007*
60 THE NETHERLANDS AND EUROPEAN DEVELOPMENT POLICY, *May 2008*
61 COOPERATION BETWEEN THE EUROPEAN UNION AND RUSSIA: a matter of mutual interest, *July 2008*
62 CLIMATE, ENERGY AND POVERTY REDUCTION, *November 2008*
63 UNIVERSALITY OF HUMAN RIGHTS: principles, practice and prospects, *November 2008*
64 CRISIS MANAGEMENT OPERATIONS IN FRAGILE STATES: the need for a coherent approach, *March 2009*
65 TRANSITIONAL JUSTICE: justice and peace in situations of transition, *April 2009**
66 DEMOGRAPHIC CHANGES AND DEVELOPMENT COOPERATION, *July 2009*
67 NATO'S NEW STRATEGIC CONCEPT, *January 2010*
68 THE EU AND THE CRISIS: lessons learned, *January 2010*
69 COHESION IN INTERNATIONAL COOPERATION: Response to the WRR (Advisory Council on Government Policy) Report '*Less Pretension, More Ambition', May 2010*
70 THE NETHERLANDS AND THE RESPONSIBILITY TO PROTECT: the responsibility to protect people from mass atrocities, *June 2010*
71 THE EU'S CAPACITY FOR FURTHER ENLARGEMENT, *July 2010*
72 COMBATING PIRACY AT SEA: a reassessment of public and private responsibilities, *December 2010*
73 THE HUMAN RIGHTS OF THE DUTCH GOVERNMENT: identifying constants in a changing world, *February 2011*
74 THE POST-2015 DEVELOPMENT AGENDA: the millennium development goals in perspective, *April 2011*

75 REFORMS IN THE ARAB REGION: prospects for democracy and the rule of law?, *May 2011*
76 THE HUMAN RIGHTS POLICY OF THE EUROPEAN UNION: between ambition and ambivalence, *July 2011*

Advisory letters issued by the Advisory Council on International Affairs

1 Advisory letter THE ENLARGEMENT OF THE EUROPEAN UNION, *December 1997*
2 Advisory letter THE UN COMMITTEE AGAINST TORTURE, *July 1999*
3 Advisory letter THE CHARTER OF FUNDAMENTAL RIGHTS, *November 2000*
4 Advisory letter ON THE FUTURE OF THE EUROPEAN UNION, *November 2001*
5 Advisory letter THE DUTCH PRESIDENCY OF THE EU IN 2004, *May 2003****
6 Advisory letter THE RESULTS OF THE CONVENTION ON THE FUTURE OF EUROPE, *August 2003*
7 Advisory letter FROM INTERNAL TO EXTERNAL BORDERS. Recommendations for developing a common European asylum and immigration policy by 2009, *March 2004*
8 Advisory letter THE DRAFT DECLARATION ON THE RIGHTS OF INDIGENOUS PEOPLES: from Deadlock to Breakthrough?, *September 2004*
9 Advisory letter OBSERVATIONS ON THE SACHS REPORT: How do we attain the Millennium Development Goals?, *April 2005*
10 Advisory letter THE EUROPEAN UNION AND ITS RELATIONS WITH THE DUTCH CITIZENS, *December 2005*
11 Advisory letter COUNTERTERRORISM IN A EUROPEAN AND INTERNATIONAL PERSPECTIVE: interim report on the prohibition of torture, *December 2005*
12 Advisory letter RESPONSE TO THE 2007 HUMAN RIGHTS STRATEGY, *November 2007*
13 Advisory letter AN OMBUDSMAN FOR DEVELOPMENT COOPERATION, *December 2007*
14 Advisory letter CLIMATE CHANGE AND SECURITY, *January 2009*
15 Advisory letter THE EASTERN PARTNERSHIP, *February 2009*
16 Advisory letter DEVELOPMENT COOPERATION, The benefit of and need for public support, *May 2009*
17 Advisory letter OPEN LETTER TO A NEW DUTCH GOVERNMENT, *June 2010*
18 Advisory letter THE EUROPEAN COURT OF HUMAN RIGHTS: protector of civil rights and liberties, *November 2011*

* Issued jointly by the Advisory Council on International Affairs (AIV) and the Advisory Committee on Issues of Public International Law (CAVV).

** Joint report by the Advisory Council on International Affairs (AIV) and the General Energy Council.

*** Joint report by the Advisory Council on International Affairs (AIV) and the Advisory Committee on Aliens Affairs (ACVZ).