Government response to the AIV/CAVV report on cyber warfare

On 17 January 2012 a joint committee of members of the Advisory Council on International Affairs (AIV) and the Advisory Committee on Issues of Public International Law (CAVV) presented an advisory report on cyber warfare. The government is grateful to the AIV/CAVV for its in-depth study of this issue. It is a valuable contribution in the debate on cyber security and will aid the government in clarifying and consolidating policy in this field. The report supplements the National Cyber Security Strategy which focuses on protecting national security and tackling cybercrime (Parliamentary papers 26643, no. 174). It also supplements the Cyber Security Legal Framework sent to the House of Representatives on 23 December (Parliamentary papers 26643, no. 220).

1. Summary

The main points of the government's response are as follows.

- The cyber threat we face demands a comprehensive strategy. The advisory report is supplementary to the national approach. In light of this, the existing national crisis management structure will have to be reviewed.
- Cyberspace is an operational domain for the armed forces. The Ministry of Defence is investing in measures to greatly strengthen existing capabilities and develop new (including offensive) capabilities.
- The right to use force in self-defence may apply in relation to cyber attacks.
- The government sees no need for a new global 'cyber treaty', although it will promote a practical framework for the application of international law in cyberspace.
- Though NATO cyber policy is defensive, discussion of the use of offensive capabilities will become necessary at some point. Article 5 of the NATO Treaty also applies to cyber attacks.
- A comprehensive EU approach is required.

2. The cyber threat

The government sees the growing threat in cyberspace to national interests and the increase in technologically advanced cyber attacks as cause for concern. Espionage, sabotage, crime and terrorism in cyberspace constitute a direct threat to national security. This was one of the conclusions of the first National Cyber Security Assessment (CSBN) completed in December 2011 (Parliamentary papers 26 643, no. 220). Without diminishing the seriousness of the threat, the government endorses the AIV/CAVV's conclusion that further study is needed. The CSBN,

coordinated by the National Cyber Security Centre (NCSC), is a valuable instrument for this purpose. It will be further refined in the coming years, with specific emphasis on improving the quality and quantity of the data it contains.

A secure and properly functioning digital network is essential to the Netherlands, with its open and internationally oriented economy and strong service sector. The comprehensive approach set out in the National Cyber Security Strategy will continue to be the general principle underlying government policy. This was the basis for the establishment of the NCSC, which is a public-private partnership. A joint, public-private and civil-military approach is required because neither the nature, extent and level of complexity of an attack will always be clear, nor the ultimate aim (criminal, ideological, military or political) of the attacker. This makes it difficult to determine the legal basis of the response and the resources required. In organising a joint approach it is important for roles, tasks and responsibilities to be clearly defined. On the initiative of the National Coordinator for Counterterrorism and Security (NCTV), the existing crisis management structure will be reviewed to see whether it is capable of dealing swiftly and effectively with large-scale digital disruption. As the AIV/CAVV rightly points out, it is also important to invest in coherent ‘cyber diplomacy’.

3. The armed forces – operational domain

The large-scale use of ICT has enabled the armed forces to perform their tasks more effectively and efficiently, but it has also increased its vulnerability. The digital domain is therefore of critical importance to the armed forces. Without a functioning ICT infrastructure the armed forces simply cannot carry out their duties. Virtually all weapons and sensor systems have ICT components, while both command and control and logistical support are dependent on digital systems. Disruption of the armed forces’ ICT infrastructure will thus jeopardise its effectiveness and the ability to continue operations. The priority is therefore to safeguard the reliability of military networks, weapons systems, intelligence and command and control systems, and to prevent the theft of information.

At the same time, cyberspace provides an operational domain for the armed forces which, as the AIV/CAVV rightly notes, is expected to play an important role in every future conflict. As the networks of potential opponents are vulnerable like our own, cyberspace can also be exploited to enhance our intelligence position and to carry out military operations. The rise of cyberspace as an operational domain strengthens the current trend whereby traditional warfare is giving way to a more hybrid and multifaceted model of conflict, in which the use of ICT plays an ever-growing role. This picture is further complicated by the fact that it is difficult to establish where cyber attacks originate and who is behind them. In addition, the AIV/CAVV rightly concludes that a ‘cyber war’, fought solely in cyberspace, is currently an unlikely prospect. What is probable, however, is that operational cyber capabilities will be deployed frequently in the near future, either independently or

in support of regular military actions. To this end, offensive operational cyber capabilities will have to become part of the total military capability of the Dutch armed forces. In this regard, the armed forces must have sufficient capability to be able to respond adequately and effectively in all circumstances and against every opponent.

Intelligence capability

An excellent intelligence capability is a basic necessity for the defence organisation in order to function and operate in cyberspace. With regard to the issue of attribution, the AIV/CAVV correctly concludes that the intelligence and security services have an important role to play. Intelligence and counter-intelligence activities conducted by the Defence Intelligence and Security Service (MIVD) do not constitute offensive activities. These activities concern the gathering of information from closed sources within the constraints of the Intelligence and Security Services Act 2002 (WIV 2002).

The AIV/CAVV is of the opinion that in the light of technological advances a review should be conducted of the WIV 2002 to see whether the current distinction between cable-access and satellite interception should be retained. This view is supported by the conclusions of the Intelligence and Security Services Review Committee (CTIVD) in its recent supervisory report (no. 28) on the use of signals intelligence (SIGINT). The government is of the opinion that this distinction cannot be maintained. It is therefore preparing an amendment to the WIV 2002 which will have to make a careful assessment of privacy issues and take account of the effects on providers of electronic communications networks. The House of Representatives will be informed on progress regarding the amendment in the course of 2012.

Strengthening the cyber capabilities of the armed forces

Following the parliamentary debate on matériel on 7 November 2011, in answer to a question from MP Marcial Hernandez, the Minister of Defence promised to give an overview of the cyber activities of the armed forces in this response. This promise is fulfilled here. The degree to which the activities described can in fact be performed depends on the financial resources available. For policy development purposes, a defence strategy for cyber operations is being drawn up in close consultation with national and international partners. The strategy will be finalised and presented to the House before the summer.

A cyber programme manager has been appointed and Cyber Task Force set up under the authority of the Chief of Defence (CHOD). The programme manager is responsible for coordinating all cyber-related activities within the defence organisation. In the short term, priority is given to strengthening defensive and intelligence capabilities. In the medium term, the focus is on establishing a Defence Cyber Expertise Centre (DCEC) by the end of 2013 and a Defence Cyber Command Centre (DCC)

by the end of 2014. The DCC will coordinate cyber operations within the defence organisation and will be responsible for the connection between the various cyber capabilities within the defence organisation. The Royal Netherlands Army (CLAS) will play a major executive role in the operational arena.

The AIV/CAVV also notes that recruitment and retaining sufficient numbers of properly qualified staff will present a major challenge. In view of the need for qualified specialists in other sectors, here too the Ministry of Defence will have to work closely with other public and private parties so as to make the most effective joint use of scarce human resources. Consultations are already taking place between ministries and with companies and universities. The possibilities for creating a pool of ‘cyber reservists’ are also being explored.

Defensive measures focus on enhancing protection of networks and weapons and control systems. The Ministry’s Computer Emergency Response Team (DefCERT) holds joint responsibility for the security of these networks and systems and must be fully operational by mid-2013 to protect the most sensitive defence networks around the clock. Capacity will be expanded further in the period leading up to 2016 to include other networks and weapons and control systems. DefCERT is due to conclude a voluntary agreement with the NCSC establishing a framework for intensive cooperation (information exchange and support) in the event of a disaster.

At the same time, the Cyber Task Force will be developing an offensive capability and drafting a cyber doctrine for the armed forces. The AIV/CAVV also concludes that for offensive operations in the digital domain often the same technology is used as for intelligence purposes. Achieving an offensive capability therefore requires the efficient use of the scarce cyber capacity (including intelligence capacity) within the defence organisation. In developing this offensive capability, the AIV/CAVV’s considerations on the distinction between the duties of the CHOD and the director of the MIVD will be taken into account.

In the period from 2012 to 2015 the MIVD will increase its cyber intelligence capacity. The first step was taken with the addition of nine FTEs as of 1 January 2012. What is more, the MIVD and the General Intelligence and Security Service (AIVD) are stepping up cooperation in the field of cyber and signals intelligence, which should culminate in the establishment of a joint unit for gathering SIGINT and cyber intelligence.

Within the defence organisation, developing and retaining knowledge regarding the cyber threat is the primary responsibility of the DCEC. The first priority is to increase awareness of the threat among personnel. An interactive environment consisting of e-learning modules, a simulation and a knowledge base will soon be available for training purposes.

Investment will also be made in research. In 2012 a senior lecturer in Cyber Studies will be appointed and a research group set up at the Netherlands Defence Academy (NLDA), while on 1 January 2014 a chair in cyber defence studies will be established. A wide-ranging cyber research programme was launched at the Netherlands Organisation for Applied Scientific Research (TNO) in January 2012. The defence research programme is part of a national cyber security research agenda that aims to make the most effective use of the available research budgets.

4. The international legal framework

Use of force and the right of self-defence (jus ad bellum)

The findings of the AIV/CAVV with regard to the use of force and the right of self-defence are largely in line with the government's position. Particularly relevant is its conclusion that cyber attacks are subject to the same rules as the use of force in the physical domain. In the advisory report the existing rules of international law on the use of force are strictly applied to cyber attacks, fully echoing the government's views. The AIV/CAVV concludes that both state and non-state actors can carry out an armed attack within the meaning of the UN Charter against which the use of force for the purposes of self-defence is permissible. The government endorses this conclusion and emphasises that it constitutes a significant legal development.

The government also endorses the AIV/CAVV's conclusion that attribution presents a substantial challenge where cyber attacks are concerned. It concurs with the AIV/CAVV's view that force may be used in self-defence only if the origin of the attack and the identity of those responsible are sufficiently certain. It also concurs with the view that the use of force in response to an armed cyber attack must comply with the international law requirements of necessity and proportionality.

International humanitarian law (jus in bello)

The government shares the AIV/CAVV's conclusion that applying the rules of international humanitarian law (*jus in bello*) to hostilities in cyberspace is 'technically feasible and legally necessary'. However, it also agrees with the AIV/CAVV's view that armed attacks in cyberspace only fall under international humanitarian law if they are carried out in the context of an armed conflict by the parties to that conflict. This constitutes an important distinction with regard to other cyber attacks. The advisory report examines the issue of armed conflict initiated by a cyber attack and gives some useful examples of the practical application of the basic principles of international humanitarian law to cyber warfare.

Neutrality

The government regards the AIV/CAVV's elaboration of the concept of neutrality in relation to the deployment of cyber weapons as a useful starting point for further thinking on this subject. In an armed conflict involving third parties, the Netherlands can protect its neutrality by impeding the use by such parties of infrastructure and systems (e.g. botnets) on Dutch territory. Constant vigilance, as well as sound intelligence and a permanent scanning capability, are required here.

Cyber treaty

Like the AIV/CAVV the government sees at present no need for a new, global cyber treaty. It believes that existing rules of European and international law suffice with regard to cyber attacks. It does however support the recommendation in the report to give more political weight and practical effect to the application of international law in the digital domain through the introduction of a code of conduct.

5. International cooperation

The interconnected and interdependent nature of ICT systems worldwide makes international civil-military and public-private partnerships indispensable. Close, bilateral consultations to this end are being held with the United States, the United Kingdom, Germany, Australia and the other Benelux countries. The potential for closer cooperation with Canada, France and the Scandinavian countries is being explored.

As the AIV/CAVV observed, the Netherlands plays an active role in discussions on standards of conduct in cyberspace, mainly in order to preserve a free and open internet and offer a counterweight to countries wishing to restrict the free use of internet and media in the name of security and combating cyber crime. At the same time, the government acknowledges the importance of avoiding potential conflicts between countries resulting from cyber incidents. The Netherlands will pursue these aims in the appropriate forums. It also believes it is essential for businesses to shoulder their responsibilities when it comes to the export of technologies that could be used by governments for repressive purposes. In the interests of protecting human rights, the Netherlands considers it important for businesses not only to engage in self-regulation but also to have a framework in which to take decisions on the export of their products. It is therefore pressing for an expansion of the EU Dual-Use Regulation. This would make it possible to impose an ad-hoc licensing obligation for individual cases if there are indications that items will be used, partly or solely, for the commission of human rights violations.

NATO

NATO's new Strategic Concept was followed up by a cyber defence policy, adopted in June 2011. As the AIV/CAVV notes, where cyber threats are concerned NATO is focusing primarily on strengthening its defensive capability. Partly owing to pressure from the Netherlands, the policy now addresses the need for more intensive information exchange, the development of a joint threat assessment and the importance of EU-NATO cooperation. The government also believes that in the longer term, NATO will have to develop a doctrine on the deployment of an offensive cyber capability. The decision on any collective response to a cyber attack would be taken according to the existing procedures. In the digital domain, as elsewhere, it is not always easy to establish when article 5 would come into operation. That is always a question that must be tackled at political level.

European Union

The government shares the AIV/CAVV's view that the EU would benefit from a comprehensive, coordinated approach to cyber security. Last year the European Commission launched its internal security strategy, which identifies raising levels of security for citizens and businesses in cyberspace as one of five priorities. The House of Representatives was informed of this on 19 January 2011 (Parliamentary papers 32317 no. 32). At the beginning of this year, European Commissioner Neelie Kroes announced plans for a European internet security strategy. The Netherlands supports these developments and will put its expertise, for example in the areas of threat assessment and public-private partnerships, at the Commission's disposal. In addition, the Netherlands is urging the Commission to give external, geopolitical considerations a clearly defined place in the EU approach to cyber security.