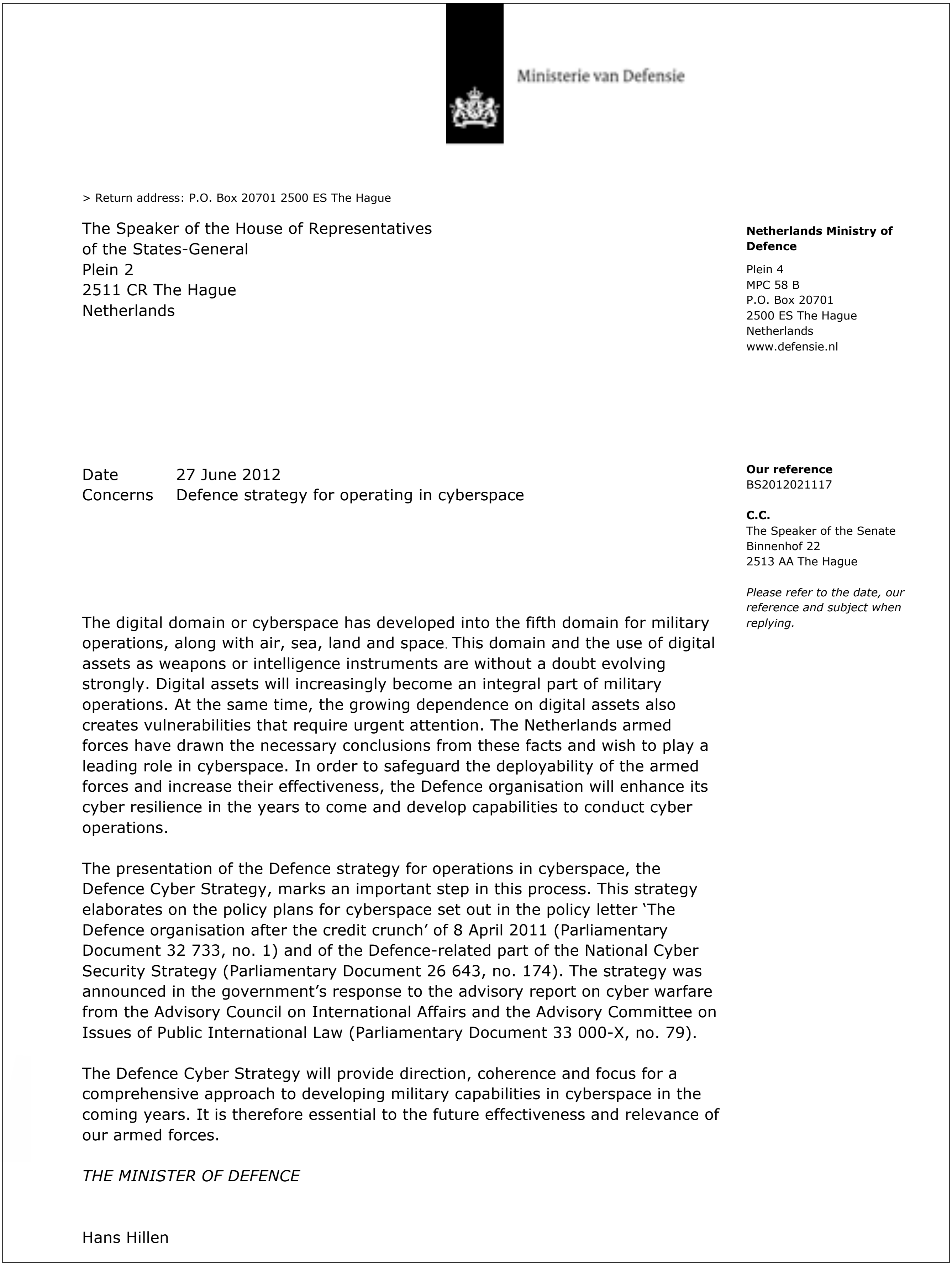
Ministry of Defence

THE DEFENCE CYBER STRATEGY



Ministerie van Defensie

> Return address: P.O. Box 20701 2500 ES The Hague

The Speaker of the House of Representatives
of the States-General
Plein 2
2511 CR The Hague
Netherlands

Netherlands Ministry of Defence

Plein 4
MPC 58 B
P.O. Box 20701
2500 ES The Hague
Netherlands
www.defensie.nl

Date 27 June 2012
Concerns Defence strategy for operating in cyberspace

Our reference
BS2012021117

C.C.
The Speaker of the Senate
Binnenhof 22
2513 AA The Hague

Please refer to the date, our reference and subject when replying.

The digital domain or cyberspace has developed into the fifth domain for military operations, along with air, sea, land and space. This domain and the use of digital assets as weapons or intelligence instruments are without a doubt evolving strongly. Digital assets will increasingly become an integral part of military operations. At the same time, the growing dependence on digital assets also creates vulnerabilities that require urgent attention. The Netherlands armed forces have drawn the necessary conclusions from these facts and wish to play a leading role in cyberspace. In order to safeguard the deployability of the armed forces and increase their effectiveness, the Defence organisation will enhance its cyber resilience in the years to come and develop capabilities to conduct cyber operations.

The presentation of the Defence strategy for operations in cyberspace, the Defence Cyber Strategy, marks an important step in this process. This strategy elaborates on the policy plans for cyberspace set out in the policy letter ‘The Defence organisation after the credit crunch’ of 8 April 2011 (Parliamentary Document 32 733, no. 1) and of the Defence-related part of the National Cyber Security Strategy (Parliamentary Document 26 643, no. 174). The strategy was announced in the government’s response to the advisory report on cyber warfare from the Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law (Parliamentary Document 33 000-X, no. 79).

The Defence Cyber Strategy will provide direction, coherence and focus for a comprehensive approach to developing military capabilities in cyberspace in the coming years. It is therefore essential to the future effectiveness and relevance of our armed forces.

THE MINISTER OF DEFENCE

Hans Hillen

Introduction

The digital domain or cyberspace[1] is the fifth domain for military operations, along with air, sea, land and space. This domain and the use of digital assets as weapons or intelligence instruments are without a doubt evolving rapidly. Digital assets will increasingly become an integral part of military operations and lead to modernisation. At the same time, the growing dependency on digital assets also creates vulnerabilities which require urgent attention. A large-scale cyber attack could have an enormous impact on society. As is the case with terror attacks, cyber attacks can cause great upheaval and widespread social disruption. Within the military domain, the infrastructure and weapon systems can be affected in such a way that an effective defence is no longer possible. The Netherlands armed forces have drawn the necessary conclusions from this and aspire to fulfil their military role in cyberspace, too.

The three core tasks of the Defence organisation are leading for the armed forces' efforts in cyberspace.[2] The armed forces must therefore be capable of taking action against digital threats to our society or to the international rule of law. There is an increasing overlap between the first and the third core tasks. However, because the principles and the procedures for the deployment of the armed forces differ for each of the core tasks, the distinction between them continues to be important. Political-constitutional relations apply equally in cyberspace. Deployment of the armed forces for international operations therefore takes place on the basis of a government mandate, while deployment for national operations occurs, in principle, in response to a request for assistance to civil authorities (usually by the Minister of Security and Justice).

In order to safeguard the deployability of the Netherlands armed forces and increase their effectiveness, the Defence organisation will enhance its cyber resilience and develop capabilities to conduct cyber operations. The Defence Cyber Strategy will provide direction, coherence and focus for a comprehensive approach to developing military capabilities in cyberspace in the coming years. This strategy elaborates on the policy plans for cyberspace set out in the policy letter 'The Defence organisation after the credit crunch' (Parliamentary Document 32 733, no. 1) and of the Defence-related part of the National Cyber Security Strategy (Parliamentary Document 26 643, no. 174).

The armed forces wish to make optimal use of the possibilities afforded by developments in cyber technology. This technology is already being used on a large scale in the Defence organisation and enables the armed forces to perform their tasks more effectively and more efficiently. For instance, virtually all weapon systems depend to a large degree on the use of IT components. Command & control systems and logistic support also rely heavily on digital systems. In addition, the armed forces' information position and situational awareness are significantly enhanced by the use of digital assets. Digital networks and systems, including weapon systems and measurement and control systems, as well as the information contained by these systems, have become of vital importance to the armed forces.

[1] There is currently no international agreement on the definition of the term "cyberspace". For the purposes of this strategy, "cyberspace" is understood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases relates in some way to the data (source code, information, etc) present in this domain.

[2] The Defence organisation's three core tasks are:
- Protecting the integrity of national and Alliance territory, including the Caribbean part of the Kingdom;
- Promoting stability and the international rule of law;
- Supporting civil authorities in upholding the law, providing disaster relief and humanitarian assistance, both nationally and internationally. Reliability is understood to mean availability, integrity and exclusivity.

The dependence of the armed forces on digital technology, however, also makes them vulnerable. It is crucial for the Defence organisation to safeguard the reliability[3] of its own networks, systems and information and to take measures to prevent the theft of information. The Defence organisation must remain vigilant and invest in high-quality assets and knowledge to keep the protection against cyber attacks at the required level. It is also essential that the Defence organisation develop a clear understanding of the threats it faces in cyberspace in order to protect itself effectively.

Since the digital systems of our (potential) opponents are also vulnerable, cyberspace can also be used for military operations against opponents or for strengthening our own intelligence position. The Defence organisation therefore explicitly considers digital assets as operational capabilities, i.e. as weapons or as intelligence assets, which must be incorporated in the operational capabilities of the armed forces as a whole. This concerns the protection of our own networks, systems and information during deployment, the deployment of offensive capabilities and the gathering of mission-related intelligence using digital technology. Since intensive use is made of IT assets throughout the Defence organisation, far-reaching joint cooperation is required.

Given the multifaceted and complex character of cyberspace and in order to utilise the Defence organisation's scarce assets optimally, all activities connected with military operations in cyberspace should be centrally controlled and coordinated. The speed at which developments in cyberspace occur places high demands on the Defence organisation's adaptability and innovative strength. It must be able to rapidly implement new technologies and complete short innovation cycles in cyberspace. The dynamics and complexity of cyberspace require constant development of knowledge, expertise, skills and techniques, as well as constant adjustment of modi operandi in cyberspace.

Given the interconnectivity within cyberspace and the dependence on similar technology, a comprehensive approach is called for at both the national and international level. The traditional divisions between military and civilian, public and private, and national and international actors are less clear-cut in cyberspace. National security can, for instance, be jeopardised by a large-scale attack on a private organisation. To defend against such attacks, cooperation between different parties is necessary, including the affected organisation itself, the National Cyber Security Centre (NCSC), the intelligence services, the criminal investigation services and, in certain cases, also the armed forces.

[3] Reliability is understood to mean availability, integrity and exclusivity.

Focal Points

Given all of the above, the Defence Cyber Strategy has six focal points on the basis of which the Defence organisation will endeavour to realise its objectives in cyberspace:

1. adopting a comprehensive approach;
2. strengthening the cyber defence of the Defence organisation (defensive element);
3. developing the military capability to conduct cyber operations (offensive element);
4. strengthening the intelligence position in cyberspace(intelligence element);
5. strengthening the knowledge position and the innovative strength of the Defence organisation in cyberspace, including the recruitment and retention of qualified personnel (adaptive and innovative elements);
6. intensifying cooperation, both nationally and internationally (cooperation element).

The development of the cyber threat to the Defence organisation

As a result of its intensive use of high-quality (satellite) communication, information, sensor, navigation, logistics and weapon systems, the Netherlands Defence organisation is dependent on reliable internal and external networks and on digital technology. It is therefore vulnerable to digital attacks.

Various countries now have offensive cyber capabilities for military use at their disposal or are in the process of developing such capabilities. But non-state actors can also pose a threat to our armed forces, by disrupting our systems and our information management systems. In modern conflicts, the distinction between combatants and non-combatants is becoming blurred and areas of operations are increasingly less clearly defined. The actions of opponents will frequently take a digital form and will probably more often extend to the homefront.

The biggest threat to Defence in cyberspace in the medium term is presented by sophisticated and complex digital offensive capabilities directed against a specific military target. Such an attack could potentially severely limit the armed forces' freedom of action. A lack of knowledge about and insight into the possibilities for conducting cyber attacks constitutes a real risk to the armed forces.

Already, armed forces and industry involved in the development and production of sophisticated military technology are incessantly confronted with – attempted – digital attacks and espionage activities. The strategic and economic value of information in this field is great. Furthermore, the Defence organisation will have to be alert from an early stage to clandestine introduction of vulnerable spots ("backdoors") in information and communication systems. This risk is growing due to the complexity of systems and the quantity of their components. Intelligence services will probably not shrink from tampering with equipment to be supplied to potential opponents.

Focal point 1: a comprehensive approach

The point of departure is that Defence cyber capabilities form an important and viable addition to existing military capabilities. The strength of cyber assets lies in the possibilities they offer in supporting and reinforcing operational capabilities in all domains. Cyber assets strengthen the armed forces' actions for all military functions: logistics, command & control, intelligence, force protection, manoeuvre and firepower. The Defence Cyber Strategy is therefore based on a comprehensive approach, both in terms of the supporting processes (force generation, operational support, sustainment) and in terms of operational deployment (both independent and as part of operations of other units, possibly under civilian command).

Military operations will increasingly involve the use of operational cyber capabilities, mainly in support of the armed forces' regular operations, but also as a weapon in its own right. Operational cyber capabilities must become an integral part of the overall military capability of the Netherlands armed forces. The Defence organisation must therefore invest substantially in strengthening its cyber capabilities. The Defence organisation will not, however, establish a separate Service for operations in cyberspace. In 2014, the relevant cyber capabilities will be incorporated within the joint Defence Cyber Command which will come under the single-service management of the Royal Netherlands Army.

An operational cyber capability encompasses all knowledge and assets necessary to predict, influence or obstruct the actions of opponents during operational deployment using digital technology, and to protect against similar operations conducted by opponents. This is done by infiltrating computers, computer networks, weapon and sensor systems and software in order to collect information and intelligence and to influence systems. An operational cyber capability thus encompasses deployable defensive, offensive and intelligence elements.

In planning and preparing for operations, all aspects relevant to cyberspace are taken into account. Cyberspace thus forms an integral element of the joint operational planning process. In this process, attention is given to the potential influence of cyberspace on the mission as well as to the effects that can be achieved by deploying cyber capabilities. The operational commander therefore has his own capabilities at his disposal and can call upon the intelligence capability to gather and process cyber information and make it available for the decision-making process in a timely fashion. This relates to both the threat against friendly networks and systems and the possibilities for exploiting vulnerabilities of the opponent. Good situational awareness in cyberspace is part of the commander's total situational awareness.

It is essential for operations in cyberspace that the mandate allow for this, and the Rules of Engagement must therefore stipulate how offensive cyber capabilities may be deployed.

Focal point 2: Defensive

Networks and systems are vulnerable to attacks and disruptions, both from outside and from within. Defence against these threats entails the protection of networks, monitoring and analysing data traffic, detecting digital attacks, and responding to them.

The Defence organisation is, of course, responsible for protecting its own networks and systems. It must be prepared for and capable of protecting itself against cyber threats so as to guarantee the deployability of the armed forces. The Defence organisation must therefore be familiar with potential threats in cyberspace and the vulnerabilities of its own networks and systems. The Defence organisation will therefore conduct a risk analysis on the basis of which the necessary minimum protection measures will be determined. There must be a balance between the measures to be taken and their practicability, and a comprehensive set of security measures must be implemented (including in the personnel, physical and information security domains). For networks and systems in which highly classified information is processed and stored, a more stringent security regime will be required. Unauthorised access to these networks and systems could cause – very – serious harm to the Defence organisation, to the Netherlands government and its services and to our Allies. For networks and systems containing only unclassified information or information with a low level of classification, a set of more limited security measures will suffice.

It must be assumed that a persistent and technologically sophisticated opponent will nonetheless be capable of compromising networks and systems or parts thereof. Setting up an all-encompassing cyber defence is virtually impossible and, what is more, unaffordable. As much flexibility as possible must therefore be built into both the (passive) protection of our own cyber infrastructure and the active response to any attack. The priority must lie with the protection of information and information exchange. In addition, systems must be resilient by being able to respond quickly to attacks and to adapt themselves in order to keep functioning.

The most important vulnerability leading to the (potential) loss or compromise of information is caused by inadvertent actions by personnel, such as incompetent or careless use of IT assets. All Defence personnel must therefore be aware of the risks associated with the use of digital assets. Cyber security awareness will therefore become an integrated part of all Defence training courses. Defence personnel must also be trained in working under conditions where they temporarily have no access to (all) functions of networks and systems.

The Defence organisation will continuously improve the security of its networks and systems. This policy is to be implemented by the Joint Information Management Command which is expected to be operational by early 2013. The Joint Information Management Command will develop and implement adequate and high-quality security measures and ensure the protection of all networks and systems. Illegal and non-standard use will be detected. The Defence Computer Emergency Response Team (DefCERT) monitors the security of systems and networks, taking account of current threat levels. DefCERT, which is to become part of the Joint Information Management Command, is tasked with identifying and analysing risks to and vulnerabilities of the main Defence networks, 24 hours a day, seven days a week, and with advising the Defence organisation on the security measures that should be taken. DefCERT must also have good cyber situational awareness at its disposal. To this end, DefCERT will work together closely with the other components of the Joint Information Management Command and with the Defence Intelligence and Security Service. Outside the Defence organisation, there will be cooperation with the National Cyber Security Centre (NCSC), NATO, other CERTs and with companies possessing specific knowledge or resources. This cooperation may concern the exchange of information as well as personnel support and other types of assistance in the event of emergencies.

The available defensive cyber capabilities must be capable of protecting the Defence organisation's IT infrastructure as well as the weapon and sensor systems it uses. Those capabilities will be used by the Joint Information Management Command to protect the Defence organisation's generic networks and systems, and by the Defence Cyber Command to protect operational networks and systems during deployment. The Defence organisation will also enhance the reliability of weapon and sensor systems by improving insight into digital vulnerabilities and by tightening supervision of the development, supply chain and use of IT components. Special attention will be paid to cyber defence in the procurement of both software and hardware. When procuring or developing new systems, potential risks pertaining to the reliability of those systems must be taken into account right from the outset. These risks must then be mitigated, if possible, with the help of security requirements and/or security measures.

Focal point 3: Offensive

Offensive cyber capabilities are capabilities aimed at influencing or disabling the actions of an opponent. The Defence organisation must have sufficient knowledge and capabilities at its disposal to be able to conduct offensive operations in cyberspace, with a view to conducting an effective defence and to support operations.

This concerns the development of complex and high-tech assets and methods, including the relevant expertise, that are specifically aimed at increasing our own military capability. A cyber attack on an air defence system may thus increase the effectiveness of an air attack while reducing the risk of collateral damage.

An offensive cyber capability can be a force multiplier and thus increase the armed forces' effectiveness. By developing a robust cyber capability, the Netherlands can play an important role within NATO in this respect.

Internationally, the development of offensive operational cyber capabilities is still in its infancy. A great deal is still unclear about the nature of these capabilities, the possibilities they may offer and the effects they can achieve. Offensive cyber capabilities are distinguished from conventional military capabilities in that they can often be used only once and generally have a limited service life. High-quality cyber capabilities hardly bear comparison with generally known, relatively easy-to-use and widespread methods of attack. They are complex assets and developing them requires a high level of knowledge, making them costly and time-consuming. The fact that the opponent may at any time discover his own vulnerabilities and address them means that achievement of the desired effects cannot be guaranteed.

In developing offensive operational capabilities, optimal use will be made of the expertise and assets of the Defence Intelligence & Security Service (DISS). Given the scarcity of qualified personnel, both the expertise and the assets must be deployed as efficiently as possible and duplication of efforts in asset development in the Defence organisation must be avoided. Optimal use must therefore be made of the expertise, assets and contacts of the DISS to enable the development and deployment of offensive assets by the Chief of Defence (CHOD). The CHOD may deploy these offensive assets in a military operation on the basis of a mandate from the government, leaving intact, as required by law, the division between the tasks and responsibilities of the CHOD and the DISS. In addition, offensive assets can be deployed to prevent or stop a cyber attack and to guarantee our own freedom of action in military operations in cyberspace ('active defence'). The Defence Cyber Command will ensure the deployment readiness of offensive cyber capabilities. The Cyber Task Force will formulate a doctrine for operations in cyberspace, develop deployment scenarios, and describe the effects and consequences of offensive assets in more detail. This will be done with the help of tests, training and exercises.

Focal point 4: Intelligence

The rapidly increasing influence of cyberspace and the increased intertwinement of systems have greatly expanded the possibilities for information-gathering. Having a high-quality intelligence position in cyberspace is a precondition both to protecting our own infrastructure and to conducting operations. The Defence organisation needs to have a clear insight into the cyber threats it may be exposed to in order to be able to protect itself effectively against those threats. This requires knowledge of the technical threat itself as well as insight into the possibilities and intentions of – potential – opponents and attackers. The DISS therefore needs to have the intelligence capabilities to acquire and analyse this information and to report on it in a timely fashion. Furthermore, the DISS must have the capability to disrupt and stop the intelligence activities of others. The DISS' intelligence activities in cyberspace are, of course, conducted within the parameters of the law.

In the coming years, the DISS will expand its capability for the covert gathering of information in cyberspace. This includes infiltration of computers and networks to acquire data, mapping out relevant sections of cyberspace, monitoring vital networks, and gaining a profound understanding of the functioning of and technology behind offensive cyber assets. The gathered information will be used for early-warning intelligence products, the composition of a cyber threat picture, enhancing the intelligence production in general, and conducting counterintelligence activities. Cyber intelligence capabilities cannot be regarded in isolation from intelligence capabilities such as signals intelligence (SIGINT), human intelligence (HUMINT) and the DISS' existing counterintelligence capability. A decisive factor for the effectiveness of operations is the combined deployment of scarce expertise and assets. With that in mind, the DISS and the GISS (General Intelligence and Security Service) are intensifying their cooperation in the areas of cyber and SIGINT by establishing a joint SIGINT-Cyber Unit. The establishment of this unit should further improve the effectiveness of the national cyber intelligence capability. The DISS will also contribute to the further development of the National Cyber Security Assessment which is being formulated under the responsibility of the National Coordinator for Counterterrorism and Security of the Ministry of Security and Justice.

A complex challenge in the cyber context is the attribution of attacks and attempted attacks. If it is not possible to identify the origin, perpetrator and objective of an attack, the possibilities for responding effectively are limited. By using all intelligence sources at its disposal as well as forensic investigation, the DISS will improve the possibilities for attribution and cooperate closely with the Joint Information Management Command, the GISS, the Netherlands Forensic Institute and the criminal investigation services (the National Police Services Agency and the Royal Netherlands Marechaussee). In addition, intensive confidential international cooperation is often essential for being able to eventually establish the identity of the attacker and take effective protective measures.

Focal point 5: Adaptive and Innovative

The speed at which developments in cyberspace occur places high demands on the Defence organisation's adaptability and innovative strength. It must be able to rapidly implement new technologies and complete short innovation cycles in cyberspace. The dynamics and complexity of cyberspace require constant adaptation of the initial requirements for knowledge, expertise, skills and techniques, and the modi operandi.

The Defence organisation must possess the necessary knowledge to follow relevant developments and to respond to them quickly and effectively. It invests in people, technology, research and development so as to be able to procure or develop and implement the necessary cyber capabilities in a timely fashion. The Defence Cyber Expertise Centre (DCEC) is to become the central entity for the promotion of knowledge development, knowledge retention and knowledge dissemination. The DCEC must bring the knowledge of the Defence organisation in the field of cyber operations up to a high level and maintain that level. It is aimed at both knowledge development (including research & development and concept development and experimentation) and the transfer of knowledge (exercise, training and instruction) within the Defence organisation. The DCEC will cooperate closely with knowledge institutes, such as the Netherlands Organisation of Applied Scientific Research (TNO).

In order to permanently improve the security of networks and systems, the Defence organisation must be able to respond quickly and effectively to new developments, to test new techniques at an early stage and to work together closely with the business and science communities. Tendering and procurement procedures for cyber-related materiel and services are to be set up in such a way that the hybrid and changeable character of this domain can be tackled proactively while, at the same time, guaranteeing the reliability of assets and operating processes. In cyberspace, the private sector is the driver of innovation, including in the areas of security and protection of the IT infrastructure. The Defence organisation should therefore make optimal use of this innovative strength. The Defence organisation's sourcing policy can make a contribution in this regard.

For the benefit of research and development, but also for the purposes of training and exercise, the Defence organisation will obtain a cyber laboratory and testing environment. This cyber lab will be available for use by the various elements of the Defence organisation and also by partners. These elements can be situated at various physical locations and connected from a distance.

A particular challenge for the Defence organisation is to recruit and retain qualified personnel who are also able to perform in a military environment. The required military personnel capacity will be realised partly through the recruitment of cyber reserve personnel. In order to acquire and retain the required knowledge, competence and skills for the organisation, particular attention will be given to personnel policy and training. For example, specific career patterns will be developed to embed and further develop the knowledge and expertise of Defence personnel in the field of cyber. Exchange of personnel may be promoted by cooperating with the NCSC, criminal investigation services and the business community. This ensures that personnel can gain the required experience and at the same time provides them with an interesting career perspective.

Additional research is required into the impact of cyber assets as an operational capability and the threat they pose to the armed forces - technically, legally and in terms of the potential disruption of processes. The Defence organisation will seek to link up with research being carried out in the Netherlands and internationally. It will also carry out research independently. In 2014, a chair in cyber defence and cyber operations will be established at the Netherlands Defence Academy.

Focal point 6: Cooperation

Cyber security depends on the ability of countries and organisations to protect cyberspace, individually and collectively. Cyberspace is by definition an area where both public and private, civilian and military, and national and international actors act simultaneously and are mutually dependent. In addition, the techniques used by attackers are largely similar and designed to exploit generic vulnerabilities of networks and systems. A joint approach to cyber threats is therefore required in order to increase cyber security in a sustainable manner.

At home

As part of the National Cyber Security Strategy (NCSS), the Defence organisation needs to work closely together with both public and private parties. To this end, the Defence organisation is represented in the Cyber Security Council and participates in the NCSC.

As manager of high-grade digital networks and systems, the Defence organisation is an important partner with specific knowledge and capabilities. On the basis of the Defence organisation's third core task, it can make this knowledge and these capabilities available to civil authorities on request. Following a formal request and approval in accordance with the legal basis for assistance or the regulations for providing support, measures can be taken under the authority of the party making the request. The manner in which capabilities are to be made available for cyber operations is being worked out in greater detail. Furthermore, there are grounds to consider whether cyber assets of the Defence organisation can be brought into the interdepartmental administrative agreements concerning specific guaranteed availability of the armed forces as part of the Intensification of Civil-Military Cooperation policy. The capabilities of the Defence organisation will have to contribute to improving the security and reliability of the entire Dutch cyberspace.

When organising a comprehensive approach, it is important for roles, tasks and responsibilities to be clear. It is essential to be able to bring large-scale digital disruptions under control rapidly and effectively, in joint consultation. In this context, at the initiative of the National Coordinator for Counterterrorism and Security, the current national crisis management structure will be reviewed. The Defence organisation will contribute to this review.

Cooperation with public-sector partners, universities and the private sector is also needed in the areas of research and development, training and personnel. Different parties are confronted with the same challenges, such as limited budgets and scarcity of qualified personnel. New possibilities for strategic cooperation must be investigated. The Defence organisation contributes to the National Cyber Security Research Agenda and, as part of the government's policy regarding the private sector, to the priority status given to cyber security by the high-tech industry. Within the same framework, the Defence organisation will work together closely with other ministries, knowledge institutes and the private sector. With regard to the development of resources and capabilities, alliances will be sought with the private sector.

Abroad

At the international level, the Defence organisation seeks cooperation with countries that aspire to a similar level of ambition and approach and operate at a similar level as the Netherlands. The initial purpose of cooperation is the exchange of knowledge. At a later stage, the possibilities for the joint development of assets and techniques and the collective establishment of capabilities will be looked into.

For the Netherlands Defence organisation, NATO is the primary partner for cooperation in strengthening cyber defence. In that context, the Defence organisation contributes actively to the development and implementation of NATO policy. As was emphasised during the Chicago summit of May 2012, NATO will improve the protection of its own networks and systems, as well as those of allies that are crucial to the functioning of NATO. The Netherlands also endorses NATO's ambition to strengthen its members' combined capabilities for intelligence analysis. It is unlikely that collective cyber capabilities will be developed under the aegis of NATO. The Alliance will, however, have to develop a vision on the deployment of cyber capabilities in NATO operations.

The Defence organisation also supports the EU's efforts to put in place a comprehensive Internet security strategy. It is important for the Defence organisation that the EU and NATO keep working together intensively to enhance member states' abilities to defend themselves. To this end, the exchange of information in this field between the two organisations must be increased.

In conclusion

The focal points in the strategy set out in this document must ensure that the armed forces will be able to operate effectively and efficiently in cyberspace. By investing in cyber defence and operational capabilities, the Netherlands will be able to maintain high-quality and high-tech armed forces that can be deployed flexibly and perform their tasks in every domain. The House of Representatives will be informed of the progress made in implementing this strategy in the Defence budget and the annual report. In 2016, a policy assessment will be carried out.

This brochure is a publication of:
The ministry of Defense
Central Staff

September 2012