Cyber Security Strategy for Defence

		Tel
Edited by	ACOS STRAT	9-2400-6455
Approved by	CHOD	
Published by	ACOS STRAT	9-2400-6455

1. TABLE OF CONTENTS

2. GENERAL

a. Purpose

The purpose of this document is to describe the Cyber Security Strategy for Defence in order to obtain a horizontal concept for the establishment of a cyber capability for Defence. This is thus a vision document.

b. Document structure

(1) Upper applicable directive(s)

(a) “Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace” Brussels, 8 February 2013

(b) National Cyber Security Strategy 21 Dec 12

(c) “Defence Mission Statement and Strategic Framework for the Preparedness” CHOD-MISSION Ed 1 version Mar 14

(d) CHOD Policy Handbook Ed 1 version Mar 14

(2) Lower applicable directive(s)

(a) Several concepts with regard to the cyber domain to be established (later)

c. Reference documents

(1) Act of 30 November 1998 governing the intelligence and security service

(2) Regulations IF 5 “Instruction on military security”

(3) ACOT-ODP-ICOMDOC-CCSC-001, Intercomponent Doctrine, 09 Jun 10

(4) Cyber Security Strategy Belgium; 21 Dec 12

(5) ITU National Cybersecurity Strategy Guide, Sep 11

(6) AC/322-N(2014)0072, Report on Cyber Defence Taxonomy and Definitions, 30 May 14

(7) Technical Report 2012/SPW008416/03 CIS Security Capability Breakdown, NCIA, Rev 4, Aug 13

(8) National Cyber Security Framework Manual, CCDCOE, Alexander KLIMBURG, Jun 12

(9) Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, 07 Feb 13

(10) National Cyber Security Strategies – Practical guide on development and execution, ENISA, Ed Dec 12

3. DEFINITIONS

As a result of the fact that actions in cyberspace are created by humans in an increasingly complex, constantly changing and demanding environment, there are no standardised definitions of “cyber”.

Each country, each organisation has established its own definitions based on the legal framework, its needs, the political and historical context, its structure, its processes, its interpretations, and its mentality.

The definitions that apply to Defence are mentioned in annex B.

4. SITUATION

a. Introduction

(1) The internet and new computer technologies have brought about an unprecedented shift in power centres and lead to new forms of warfare.

(2) Existing security strategies and military doctrines have to be adjusted to this evolution, and the required enhancement of protection capabilities needs to be realised very quickly.

(3) Because of the constant evolution of threats and technologies, the strategy will be revised every 5 years.

b. Time horizon of the strategy

The time horizon for this strategy is ± 2020.

c. Scope

The scope of this document is the following:

(1) Defining a strategic framework for the Belgian Defence approach of cyber security consisting of three pillars: Cyber Defence, Cyber Intelligence and Cyber Counter-Offensive[1].

(2) Defining a clear vision in the cyber security domain in order to be able to further develop and improve Defence’s cyber security capabilities in a coherent and implementable way.

(3) Creating a cyber security culture, starting with the acknowledgement of the increased cyber risks.

5. GENERAL FRAMEWORK

a. Description of the (military) environmental elements

(1) Dependence

(a) Our society and, to a very large extent, Defence as well, have become dependent on communication and information systems (CIS).

(b) Command & Control (C^2) systems, logistic systems as well as weapon systems (incl. sensors and navigation systems) are critical and are daily in use, both during planning on the homeland territory and during the execution of operations, but also as a means of supporting military diplomacy.

[1] See definitions in annex B

(2) Due to the simplicity, availability and the low cost of modern CIS, the alternative communication tools are gradually disappearing. Without available and reliable CIS we have no other means and processes at our disposal anymore to guarantee a minimum performance and operationality of our military capabilities.Vulnerability

(1) Military CIS are currently strongly integrated within the internet and are based on standard commercial technology (COTS, Commercial off the Shelf), mainly because of economic reasons. This tendency is increasing, which makes these CIS even more vulnerable. Every month, dozens of new vulnerabilities are discovered in standard commercial products and made public. Most computer and network components come from regions that form a potential threat to our military security.

(2) Internet-connected means of communication are omnipresent. As a result, our staff members, including those in operations, are permanently carrying sensors with them (smartphones, microphones, cameras, GPS, etc.). Because of the irreversible need to consult and share information quickly and widely, all staff members can access a lot of sensitive information anywhere and at anytime. The availability of cheap and mobile high-capacity storage media increases the risk that information could be consciously or unconsciously disseminated without any control.

(3) Big and fast evolution

(a) One of the security challenges that we will be facing is the proliferation of cyber technology. Conventional rules of law, but also defaulting and unstable states, terrorist and criminal organisations will make eager use of cheap (or free) and effective cyber weapons in hybrid or irregular conflicts to cause a strategic shock or to undermine credibility and/or legitimacy.

(b) Some military entities adopt the technical knowledge of criminal hacker groups. There are indications that such groups put their capabilities at the disposal of authorities and of military entities in exchange for sponsoring, protection or tolerance.

(c) Because of the internet revolution, small organised groups (such as countries that are militarily weaker and terrorist groups) on the one hand and non-organised masses or even individuals on the other hand get huge amounts of power. Digital connectivity leads to global social movements having a seriously underestimated strategic importance. “Hacktivists” or movements such as WikiLeaks will become better organised and cause even more problems for authorities.

(d) The intentions remain unchanged (money, knowledge, power, operational advantage, etc.) but the possibilities have greatly increased. With very limited means, the internet revolution is facilitating espionage, sabotage, terrorism, subversion, crime, command & control, propaganda and military cyber operations. In the cyber domain it is actually simpler, cheaper and faster to attack than to defend.

(e) Currently the internet offers terrorist organisations a platform for efficient communication, propaganda, financing, radicalisation, documentation, command & control, intelligence, encryption and recruitment. New small groups are experimenting with computer hacking techniques, in order to take soon control of the cyberspace for launching their attacks.

(f) The internet and the know-how to launch cyber-attacks are becoming generally available. Authorities and non-governmental organisations have to develop efficient and professional Cyber Security capabilities.

b. Constraints and general terms/ framework conditions

(1) Anonymity and attribution

(a) Cyberspace does not have any physical borders, and potential perpetrators of cyber-attacks are widely divergent (from individual hackers through organised crime groups, up to nations).

(b) Anonymity facilitates cyber-attacks significantly. For instance, hackers and cyber criminals would make increasing use of advanced methods for carrying out attacks that are untraceable and difficult to eliminate.

(2) Asymmetric warfare

(a) In about 300 milliseconds, one keystroke can travel twice around the world but the forensic research required for identifying an attacker in cyberspace can take weeks, months, or even years.

(b) This is why in cyberspace, defence is always structurally running after the attacker: countermeasures are always too late and skilful hackers always find new vulnerabilities for them to exploit.

(3) Budgetary constraints

Budgetary constraints are possibly the biggest challenge. In most countries as well as in large international organisations (e.g. NATO, EU) cyber security is becoming a priority. These priorities[2] are described in the respective cyber security strategies and concepts. The investments in “cyber” need to be brought to a level that corresponds to the current risks.

(4) Legal framework

(a) Cyber-specific context

(i) It remains a challenge to have a cyber-attack internationally recognised as an armed attack, and as a result external support cannot simply be relied on. As far as security is concerned, the role of international organisations remains very limited, and the alliances for Cyber Security need to be redefined.

(ii) Cyber-attacks can easily be denied (‘deniability’) and are difficult to punish (‘punishability’). Most of the time, it is not clear to know by whom the attacks were organised.

(iii) Since it is difficult to identify the attacks (in time), it is most of the time not possible to take specific countermeasures which are governed by national and international law.

(b) Right to self-defence

(i) The Charter of the United Nations describes both the prohibition of the use of force and the right to self-defence in response to an armed attack. This right to self-defence is subject to a number of conditions related to the initial attacker, the location, the necessity to respond, the principle of proportionality, etc.

[2] For Belgium: see reference document 4 – “Cyber Security Strategy Belgium”.

(ii) The application of the right to self-defence in the digital domain involves specific challenges. An attack on national critical infrastructure can be initiated from various countries and by persons who do not belong to an officially recognised organisation.

(iii) Exercising the right to self-defence requires sufficient evidence that the initial attack was carried out under the authority of at least one State or group. In cyberspace it is not always easy to identify the individual and the group or State behind the attack.

(iv) A far as the impact is concerned, a cyber-attack should be compared to an armed attack. No alternative responses should be possible, no matter the economic, diplomatic or political pressure. The reaction must be in proportion to the extent of the attack and must be aimed at stopping it (proportionality).

(c) The digital "armed attack"

(i) An armed attack can be carried out by the regular armed forces of a State or by armed groups under the authority of a State. Since the September 11 attacks, self-defence is also accepted in response to the armed attack of an organised group.

(ii) The Charter of the United Nations (article 51) does not describe any specific weapons of which impact or damages are significant enough for the attack to be described as armed. However, this is the case when there are fatalities or when vital or military infrastructure has been destroyed or severely damaged.

(iii) Under specific circumstances a digital attack can be considered as an armed attack and can give rise to a legitimate response (military or not).

(iv) Since the approval of the NATO Strategic Concept (Lisbon, 2010) a cyber-attack can lead to the invocation of Article 5, after a decision by the NAC. It does not take place automatically. This principle was confirmed in September 2014 in the Wales Summit Declaration.

(d) Legal powers

A legal basis (from national law or international law such as the Jus Ad Bellum) is required for conducting cyber operations, and the legal regime must be established[3]. Important elements are the mandate under which the operations are conducted and the Rules of Engagement (ROE).

6. RISK MANAGEMENT

a. Threats

(1) A cyber threat arises from the possibilities and intentions of an adversary to launch a cyber-attack on the CIS and weapon systems (incl. sensors and navigation systems).

(2) There are two kinds of cyber-attack:

(a) Sabotage: Cyber-attacks disrupting the normal functioning of CIS (+…)(Denial Of Service Attack).

[3] For more details on the "legal framework for Cybersecurity": see the Tallinn Manual: http://www.ccdcoe.org/tallinn-manual.html

(b) Espionage: Cyber-attacks involving unnoticed intrusion of a third party into a CIS to read, change, delete or even add information (intrusion). Such intrusions can also be used to make improper use of the CIS attacked to, for instance, attack other systems.

(3) In the future, in operations as well as for its diplomacy, Defence will be facing adversaries having offensive and intelligence cyber capabilities. These create a real risk for the confidentiality and the integrity of the information, and for the availability of military CIS and weapon systems (incl. sensors and navigation systems).

b. Vulnerabilities

(1) Complete security and protection does not exist in the cyber domain. However, the chance of a cyber-attack is much greater than that of a physical attack. The authorities and Defence have already been the victim of a cyber-attack, and will certainly be facing cyber-attacks in the near future, with limited success.

(2) Both on the national territory and in operation, Defence personnel uses cloud computing and social media technologies as well as portable memory devices (e.g. thumb drives, USB flash drives). The biggest challenge lies in raising awareness among personnel. Most cyber incidents are caused by human error. Therefore, the “internal” threat is real as well.

(3) Lack of knowledge and understanding of the digital attack possibilities, poses a real risk to Defence.

(4) As a federal organisation, Defence also symbolises the authority of our State. The Defence critical information infrastructures are more frequently becoming the target of increasingly complex cyber-attacks. Such attacks are specifically aimed at one particular target.
As such, Defence forms a “target of opportunity” for terrorists and hackers looking for sensitive information.

(5) Despite the limited direct impact, the risks related to cyber-attacks should certainly not be underestimated.

c. Impact

(1) An analysis of the threat and vulnerabilities will reveal potential risks for which the impact and the probability could be within the military environment.

(2) Consequently, a cyber-attack affecting the availability, confidentiality or integrity of Defence’s CIS can have a great impact on the functioning of our organisation and on the military operations as well as on our national credibility and on our diplomacy.

(3) The command takes the final decision on which action plan has to be followed, taking into account the legal framework. The commander can then choose from following options:

(a) **Tolerate**. The risk is accepted, and no additional protective measures are taken. Some protective measures are incorporated in legal obligations, resulting in legal action when these measures are not provided.

(b) **Interrupt**. Ceasing the activity that is creating the risk.

(c) **Threat control**. Taking additional technical/procedural measures (incl. back-up plans and Disaster Recovery Plans) to reduce the risk/impact.

(4) This implies the effective application of risk management. Objectives in the cyber domain can only be achieved when the threats, vulnerabilities and impact can be estimated and limited to an acceptable level. Obviously, the risk should remain proportional to the necessity to carry out the mission successfully with the available resources.

7. DESIRED END STATE

a. Vision

> Defence will develop its own cyber security capability, which will be efficient and focused on daily activities, territorial and expeditionary at all levels (strategic, operational and tactic), taking into account the national interdepartmental cooperation and coordination. This capability will also take into account the international opportunities that will possibly present themselves in the future.

b. Strategic objectives

(1) Defence will make sure that its members can live and work in a safe and protected cyberspace.

(2) By 2020, these capabilities will support all of Defence's missions and operations on land, on sea and in the air as well as the military diplomacy, both territorial and expeditionary, with 24/7 service in order to be able to immediately respond to any crisis / cyber incident.

(3) Defence will also be able to support other federal entities on the basis of the available resources.

(4) In order to deal with the problems of security risks in cyberspace, Defence will cooperate with international actors, such as the EU, NATO, BENELUX, UN and other partners, in accordance with the concluded agreements.

c. Effects to be achieved

(1) Keeping the "cyber risks" below an acceptable level to guarantee a good execution of our military mission(s) by a continuous analysis of the cyber threats, a solid management of cyber vulnerabilities completed with efficient detection means enabling early detection of a cyber-attack.

(2) Contributing to safeguarding freedom of action, more specifically the preservation of information dominance, to be able to execute the military mission(s) successfully and to fulfil the legal obligations (e.g. guaranteeing the protection of classified data and personal data).

Defence should be able to protect its communication and information systems as well as its weapon systems (incl. sensors and navigation systems) from cyber-attacks.
The objectives of this protection are described in the CIA triad:

- Confidentiality: the measures to protect information against unauthorised consultation and the protection of the confidentiality and privacy of sensitive data in accordance with current policy.
- Integrity: protecting data against unauthorised modification and ensuring the correct functioning of information systems.
- Availability: ensuring access to the information system and the information itself when desired by the service.

(3) Improving communication to inform and convince the users of the threat and the measures against cyber-attacks.

(4) Developing an operational cyber capability in support of the actions of the armed forces. This will allow to reinforce the effectiveness in operations, and to protect the operational networks and weapon systems against, for instance, a digital attack.

(5) Ensuring a good cooperation with the national and international cyber entities as well as with the industry and the academic world.

8. MEASURES

a. Transformation from strategic objectives to capabilities

(1) Taking into account the specific nature of Cyber Security, Defence will further develop its own capability. It remains a challenge to have a cyber-attack internationally recognised as an armed attack, and as a result external support cannot simply be counted on. As far as security is concerned, the role of international organisations remains very limited, and the alliances for Cyber Security need to be redefined.

(2) Having its own Cyber Security capability allows Defence to pursue an independent security policy and to respond to security incidents. The cyberspace requires a specific strategic approach and specific doctrines. Defence will develop special concepts, processes and procedures for recruitment, awareness enhancement, education and training, procurement of equipment, deployability, etc.

(3) The ambition level described above is directed at the improvement and development of the three pillars of the cyber security capability: Cyber Defence, Cyber Intelligence and Cyber Counter-Offensive[4]. This cyber security capability will be developed with realistic priorities, taking into account the political guidance of the Minister of Defence.

(4) The capabilities in the cyber security domain will be developed according to the “Transformation” process, described per development line (DOTMLPF-I).

b. Requirements in all areas of responsibility

(1) Doctrine

(a) Cyberspace is a new dimension. Cyber security has to be integrated into all areas of responsibility.

(b) Because of its specific nature the evolution of the national and international legal framework should be observed and respected.

(c) Further concepts and doctrines should also be drawn up. They need to describe, among other things, the role and the responsibilities of all “stakeholders” (for each pillar).

(d) These documents will be drawn up in accordance with the national and international legislation and directives as well as with the Defence rules and military regulations.

(e) In order to be able to prioritise Defence’s response, risk analyses, gap analyses, audits (leading to “assessments”) and lessons learned processes with regard to cyber security aspects will be carried out as well. Additionally, a permanent analysis of the threat will be executed (Cyber Intelligence).

(f) Therefore, the doctrinal aspects in the “life cycle” need to be managed, including a fast “change configuration” process.

(g) The existing security procedures will be revised and possibly adapted to new threats. If necessary, additional procedures will be developed: best practices, TTPs, mechanisms for incident handling, etc.

[4]Act of 30 November 1998 “Within the framework of cyber-attacks on military computer and communications systems or systems managed by the Minister of Defence, neutralise the attack and identify its perpetrators, without prejudice to the right to respond immediately with a counter cyber-attack in accordance with the provisions of the law of armed conflict.”

(h) In order to actually implement the objectives described in the “Cyber Security Strategy for Defence” an action plan will be developed by a centralised managing body (“Governance”).

(2) Organisation

(a) The role and responsibilities of the Defence services involved will be explained allowing a coherent development of cyber capabilities. Cooperation between the Defence departments and services is required.

(b) Defence will extend its Cyber Security capability under the authority of ACOS IS and DGMR, and on the basis of their existing capabilities.

(c) **Governance**. In order to effectively develop the Strategy for Defence in an integrated and holistic way and to monitor its execution, a central “Governance” higher body is necessary. This central management needs to be carried out while respecting the competences of all stakeholders (e.g. ACOS IS, DGMR, ACOS O&T, etc.) at every level (Strategic, Operational, Tactical). This body will be based on the existing “Intelligence and Security Steering Committee” (in limited sessions). “Terms of Reference” will have to describe the role and responsibilities of this body.

(d) **Management**. In case of internal, national or even international incidents, Defence has to be able to respond quickly and coherently. This requires an appropriate structure for the management and the required coordination both internally and externally. This will also be used to improve the detection and response capability. This is, for instance, possible through a “*Cyber Security Operations Centre” (CSOC)*, with participation of all parties involved (ad hoc or permanent according to the means available).

(e) The managers of the Defence CIS (incl. “functional authorities”) and of the weapon systems are responsible for the implementation of the required and planned security measures. They verify the compliance of the security guidelines and report security incidents as provided in special directives.

(f) Defence as an organisation must be able to observe its national commitments and the concluded agreements: either for coordination/contact with the national centralised coordination body “Belgian Cyber Security Centre” or for support to other federal entities or for cooperation with other national and international partners.

(g) Due to the evolution of the technology and threats the existing personnel organisation will be revised and adapted regularly, in accordance with the overall HR resources available.

(3) (Education and) Training

(a) Management of expertise and knowledge in the cyber domain. Flexible adjustment of necessary training in relation to a fast and constantly changing threat.

(b) Participation in national and international exercises, training events (workshops, courses, etc.).

(c) **Awareness** tools (e.g. e-learning) and information campaigns have to be set up for all users of Defence systems (CIS and weapon systems).

(d) Adequate courses for all stakeholders (as needed, in time): in-house, outsourced, in national and international partnership (e.g. by participation in NATO Smart Defence Project Education and Training).

(e) It is also important that the executives in the organisation have sufficient understanding of the cyber domain. Therefore, cyber aspects have to be integrated into the existing curricula of the Defence schools.

(4) Material

(a) Improving the detection and response capability. Defence must be able to early detect intrusion or sabotage of CIS, and to immediately respond with **appropriate means**. Sophisticated attacks can have a paralysing and devastating effect on Defence's CIS in operations. They are undetectable by the standard commercial and security systems. Consequently, Defence will invest in more advanced detection and response technologies.

(b) Through cyber coalitions the response capability of Defence will be reinforced or even deployed jointly.

(c) The security of Defence's CIS and weapon systems is a shared responsibility. The functional and operational authorities have to set up sufficient safe systems, and will take appropriate measures to limit the security risks to an acceptable level.

(d) Cyber aspects will also be integrated into the equipment life cycle from the start of the process (expression of needs).

(5) Leadership

(a) The Defence leadership has to be aware of the cyber threat at every level, especially at the Strategic and Operational levels.

(b) **Situational awareness** tools and permanent reporting procedures have to be set up to keep a global and clear overview of the situation in case of an incident. These services will also be provided to the operational commanders as well.

(c) In every domain (Strat, HR, MR, training, etc.) the right priorities and proper processes need to be established for realising the Defence Cyber Security capability. These priorities have to be determined on the basis of a comprehensive risk assessment.

(d) The leadership will constitute the "Governance" level.

(6) Personnel

(a) All Defence staff members must be aware of the cyber threat (**Information Awareness**).

(i) A cyber-attack is often a combination of technical possibilities and of social engineering exploiting the habits and credulity of the victim. Defence staff members must be aware of the cyber threat and of the possible abuses of CIS. They shall be vigilant and report suspicious activities to their CIS or security officer.

(ii) In the domain of Cyber Security Defence shall not just aim at compliance but especially at responsibility.

(iii) Coordination between all stakeholders is required to avoid duplication.

(b) Managing expertise and knowledge in the cyber domain

(i) In the cyber domain knowledge is the main weapon.

(ii) For developing the Cyber Security capability, Defence needs a limited number of specialised staff. This requires a separate study that will be further specified in various concepts later on. An appropriate personnel and training policy has to be developed in order to obtain and maintain sufficient technical expertise.

(iii) Defence shall acquire knowledge about the legal framework for cyber operations, and will keep abreast of national and international initiatives.

(iv) Other possibilities for using expertise will be analysed, such as using reservists and trainees from the civilian ICT world.

(v) In order to be able to offer a response to sophisticated attacks, Defence will have the necessary means ("human and technical") at its disposal to stop the attack, identify, locate and allocate the cause, and to reduce the risk of recurrence.

(7) Facilities

(a) Appropriate infrastructure to keep the risks as low as possible (incl. contingency plans).

(b) Experimentation (test bed), if possible in cooperation with existing national and international R&D facilities (e.g. the Royal Higher Institute for Defence, the Royal Military Academy).

(c) A cyber security capability requires specific infrastructure. This will be described further in the concepts.

(8) Interoperability (and cooperation)

(a) General

(i) The cyberspace does not know any borders. The traditional separation between military and civilian, public and private, and national and international actors is less strict in the digital domain.

(ii) For the extension of the Cyber Security capability internal as well as national, international and even public-private partnerships are necessary. However, this is not easy to accomplish because of the risk of compromising, divulging one's own vulnerabilities or damaging one's own research.

(iii) The intended purpose always has to be weighed against the interests.

(iv) Consequently, the fellow parties in these partnerships have to be chosen carefully, and each party shall permanently assess the added value of the cooperation.

(v) The development of an effective Cyber Security capability is essential to remain a valuable and reliable partner.

(b) National

(i) At the end of December 2012, the national Cyber Security Strategy was presented to the Council of Ministers. The Prime Minister is in charge of coordinating the execution of this strategy.

(ii) At the national level, Defence plays a supportive role. In case of major national cyber incidents Defence will provide the requested technical support as far as resources are available. In order to execute this task[5], Defence will also be able to count on additional resources and on an interdepartmental budget.

(iii) The protection of the scientific and economic potential is an important mission[6] of the General Intelligence and Security Service of Defence (GISS), which will cooperate closely with the actors involved (supportive role for the protection of the national critical infrastructure). If possible, the GISS will share information with them regarding Cyber Security threats, vulnerabilities and incidents.

(iv) Several federal public services are involved and meet in the common platform BELNIS ("Belgian Network for Information Security"). By participating in that platform, Defence recognises the need for interdepartmental cooperation and coordination. The same goes for the national "Cyber Security Centre Belgium".

(v) Furthermore, the speed at which developments in the digital domain take place requires an intense cooperation with the industry and academia.

[5] Measure for the execution of the national strategy (Reference Document 4)
[6] Act of 30 November 1998 (Reference Document 1)

(vi) Research and Development Capabilities will be developed within Defence through existing structures (e.g. the Royal Higher Institute for Defence and the Royal Military Academy). They will also be used for the participation in national and international projects according to the resources available.

(vii) Considering the importance of "knowledge" in the cyber domain Defence will enhance its efficiency in this domain by establishing well-considered partnerships with companies and academic institutions. These collaborations can lead to outsourcing if possible and appropriate, and to clearing the military Cyber Security capability for Defence's core activities.

(c) International

(i) Within the framework of international cooperation the development of an efficient Cyber Security capability is essential to remain a valuable partner.

(ii) However, international cooperation is rarely a matter of course: "information sharing" always requires a balancing of interests. Sharing information implies a risk of compromising, of divulging one's own vulnerabilities or damaging one's own research. There is a general fear for proliferation of cyber weapons. The principal component of such weapons is knowledge, which makes controlling and retaining them much more difficult than conventional weapons. Staff members with considerable technical expertise also have a great deal of freedom to put their knowledge at the disposal of other parties. Therefore, special bilateral relations are important: military, academic, industrial.

(iii) BENELUX

- Historically the Belgian Defence has very good cooperative relations with the Netherlands and Luxembourg.
- In April 2012 the Defence ministers of the BENELUX signed a declaration of intent regarding defence cooperation. This declaration is an important step towards the application of the "Pooling & Sharing" principle within the BENELUX and constitutes the basis for potential extensive cooperation in the Cyber Security domain.

(iv) NATO

- NATO has a clear Cyber Defence Concept and Cyber Defence Policy, and since 2001 it has a "Computer Incident Response Capability" (NCIRC). Because of its pragmatic approach so far NATO has been the benchmark on how to tackle this problem. Cyber Security capabilities will be included in the "NATO Defence Planning Process" as capabilities that need to be acquired and developed.
- Emphasis at NATO is on the cyber defence aspect of its own CIS. At the moment cyber intelligence and cyber offensive are not being considered within NATO.
- NATO supports the "Cooperative Cyber Defence Centre of Excellence" (CCDCOE) in Tallinn, Estonia. With the support of this CCDCOE NATO annually organises cyber defence exercises and trainings (Cyber Coalition).
- Thanks to a "Memorandum Of Understanding (MOU) for Cyber Defence Co-operation" Defence can share and receive specific technical information with and from NATO. This MOU also allows asking support of NATO in case of serious cyber incidents.

- In the cyber defence domain Defence will cooperate further with NATO both on the policy and on the technical level, including through the participation in “Smart Defence” projects. The Multinational Malware Information Sharing Platform (MISP) Smart Defence project led by Belgium is an example of this.
  Initially Defence will not permanently participate in the CCDCOE but it will maintain sufficient contact with it and follow up on the proposed projects. Once Defence has a full Cyber Security capability (Full Operational Capability, see below) a permanent cooperation will be re-evaluated.

(v) European Union

- The EU especially emphasises the Cyber Security of national critical infrastructures. The “European Network and Information Security Agency” (ENISA) aims at a better network and information security within the European Union. The European Commission has established a “European Computer Emergency Response Team” (CERT–EU).
- The “European Defence Agency” (EDA) has a project team for cyber aspects. The EDA also sponsors military important research projects in the cyber defence domain.
- Defence will monitor the evolution in the various entities and agencies of the European Union, and will evaluate the opportunities to set up research projects with the EDA.

c. Top 5-priorities

1. Defence Cyber Security Governance and Management Structure
2. Invest in People, Education and Training
3. Information and Situational Awareness
4. Adequate Material and Infrastructure
5. Collaboration and Partnership

9. ROADMAP

a. A modular and phased realisation

(1) Defence’s resources and cyber expertise in particular are very scarce and expensive. An efficient use of this expertise is thus essential. Defence urgently needs a modular approach leading to versatile expert cells.

(2) In order to be able to respond to the fast evolution of the cyber threat, Defence opts for a phased approach.

(3) The cyber capabilities are developed in three phases: a “quick start”, an initial operational capability (IOC) and a full operational capability (FOC).

b. Guidelines

In order to be able to realise the objectives mentioned above, a pragmatic and realistic approach is required that allows the development of the necessary capability.

In the Cyber Security domain the following is envisaged:

(1) As it is very aware of the current risks to certain systems, Defence has to have a minimum response capability by the end of 2014 ("**Quick Start**"). This will be realised by bringing in additional cyber experts (internal recruitment within Defence).

(2) The **initial operational capability (IOC)** will offer basic services without redundancy and within office hours by the end of 2016. The top 5-priorities mentioned above will be used as a guiding principle, with special focus on the implementation of a "Governance" and a Cyber Security Operations Centre (CSOC), based on existing entities.

(3) By the end of 2020 Defence needs to have a full operational capability (**FOC**) for Cyber Security: extensive services in the various functional cyber domains, duplicated expertise to offer services 24/7 where necessary.

All details on the required resources are described in the "Cyber Security Concept for Defence".

ANNEX A: LIST OF ABBREVIATIONS

GISS	General Intelligence and Security Service
AJP	Allied Joint Publication
BELNIS	Belgian Network for Information Security Platform
CCDCOE	(NATO) Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CIS	Communication and Information Systems
COTS	Commercial off the Shelf
DOS	Denial of Service
EDA	European Defence Agency
ENISA	European Network and Information Security Agency
FCCU	Federal Computer Crime Unit
MoU	Memorandum of Understanding
NCIRC	NATO Computer Incident Response Capability

ANNEX B: DEFINITIONS

Cyberspace

The global environment that is created through the interconnection of communication and information systems. The cyberspace includes the physical and virtual computer networks, computer systems, digital media and data.

CIS Security

(NATO definition) “The application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation”.
[NAC C-M(2013)0004, 2013].
At Defence, CIS Security is located below the general security structure, next to Cyber Security, with a focus on preventive measures.

Cyber Security

The desired situation in which the protection of cyberspace is proportionate to the cyber threat and the possible consequences of cyber-attacks. At Defence Cyber Security comprises three pillars: Cyber Defence, Cyber Intelligence and cyber counter-offensive.

Cyber Security Capability

All material and immaterial resources (Lines of Development) to guarantee information integrity, confidentiality and availability and to protect the network capacity, with the purpose of ensuring freedom of action in cyberspace.

Cyber Defence

The application of effective protective measures to obtain an appropriate level of Cyber Security in order to guarantee Defence’s operation and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level.
Cyber Defence consists of following duties: Protect, Detect, Respond, and Recover.

Cyber Intelligence

Activities using all “intelligence” sources in support of Cyber Security to map out the general cyber threat, to collect cyber intentions and possibilities of potential adversaries, to analyse and communicate, and to identify, locate, and allocate the source of cyber-attacks.

Cyber Offensive

The offensive capacity includes the manipulation or disruption of networks and systems with the purpose of limiting or eliminating the adversary’s operational capability.
This capability can be required to guarantee one’s freedom of action in the cyber domain. Cyber-attacks can be launched to repel an attack (active defence) or to support the operational action.

Cyber Counter-Offensive

(Reference document: act of 30 November 1998) “Within the framework of cyber-attacks on military computer and communications systems or systems managed by the Minister of Defence, neutralise the attack and identify its perpetrators, without prejudice to the right to respond immediately with a counter cyber-attack in accordance with the provisions of the law of armed conflict.”