CYBER STRATEGY FOR DEFENCE

Belgian Defence

Since our society and economy are being digitised and become increasingly interconnected, they need to be able to rely on the availability and integrity of digitised information, and of the underlying enabling systems and infrastructures. Belgian Defence is also increasingly dependent on new technologies. No modern armed forces can function without networked weapon systems, integrated logistics and command and control chains. Recent evolutions such as the definition of cyberspace as a new operational domain, or the more assertive attitude of many cyber actors require us to update the cyber strategy of Belgian Defence.

Didier REYNDERS
Minister of Defence

General Marc COMPERNOL
Chief of Defence

Kingdom of Belgium
May 2019

Table of contents

INTRODUCTION

Defence is highly dependent on the proper functioning of its critical network and weapon systems. At the same time, easy access to sophisticated cyber tools implies that our opponents are given the means to directly or indirectly compromise our critical military systems. Therefore the main task of the military cyber capability consists of protecting military information and guaranteeing the reliability, integrity and availability of its communication, information and weapon systems.

When presenting the strategic plan in 2016, the Minister of Defence explicitly referred to the cyber threat in his analysis of the security environment. The expansion of military cyber capabilities is thus one of the spearheads of this new plan. The objective is twofold: a better understanding of protection against the cyber threat, but also a better understanding of opportunities. In line with the definition of cyberspace as a new operational domain, the military cyber capability mandate also includes an offensive cyber capability. Defence will therefore develop its own cyber effects to support conventional operations or to carry out its own cyber operations.

At the defensive level, each network or weapon system administrator will implement a maximum of security measures with commercial means during the implementation and employment of his systems. The centralised cyber expertise then increases the level of protection with a combination of specific and often in-house optimised toolsets. In addition, the cyber capability has the means to respond immediately and appropriately to a cyber incident.

The intelligence capability provides a coherent picture of the cyber threat to our military network and weapon systems, and gives indications necessary for the investigation into the attribution of a cyberattack. The same capability is also used to map out the vulnerabilities of our opponents, and to obtain maximum intelligence about their espionage and sabotage activities.

Meanwhile, rhetoric in cyberspace is increasing, which leads to more tensions in the diplomatic field. Indeed, technological developments in cyberspace provide nations with a new set of tools to actively pursue their foreign policy without having to rely on conventional military actions. At first sight, cyber actions seem easier to accept and more proportionate. The cyber weapon may well become the preferred weapon of choice.

The research and development of offensive cyber weapons can be completely hidden from the curious gaze of the intelligence services. Large, easily traceable infrastructures and equipment are not necessary to develop these capabilities.

The cyber weapon is an asymmetric weapon. The traditional superpowers invest in high-tech and continuously interconnected weapon systems. A much less wealthy nation and even non-state actors present in cyberspace can take over the initiative from these superpowers by using cyber effects that require only a fraction of the investments necessary for conventional weapon systems. Traditional operational capabilities in the land, air and maritime domain are at risk of becoming less relevant due to a technological breakthrough in the cyberspace domain.

The cyber weapon is multipurpose. It can be used for defensive as well as offensive operations and for espionage as well as sabotage actions. Cyber actions can generate both kinetic and non-kinetic effects, which can be similar or even greater than those that can be created with conventional weapons. The type of effect can vary from influencing and undermining the opponent's trust in his own systems to making the systems temporarily or permanently unavailable. The cyber capability can be used tactically and operationally, but also strategically against, for example, the critical infrastructure of a country.

Cyber effects can be generated via proxies[1] so that suspicion initially falls on someone else. As the actual actor behind a cyber effect is very difficult to find, attribution is almost always based on (sometimes strong) suspicions and only rarely on concrete facts. The cyber weapon is therefore ideally suited for use in all levels of conflict, ranging from peacetime to war.

The effective use of a cyber weapon does not require any prepositioning. A cyber effect can be initiated from any geographical position with data connectivity to any other location in the world. The cyberspace domain is de facto a domain with strategic reach. The opponent does not get a warning time, the result of a cyber effect is immediate.

In order to better frame the risks and opportunities, we have chosen to streamline Defence's cyber strategy and the further development of military cyber capability based on a number of major policy lines. In our new strategy, the efforts have been regrouped into five strategic objectives.

[1] Proxies are real or virtual entities in cyberspace that a cyber actor uses to hide his real intentions or affiliation.

Strategic Objectives

SO_I: Optimum protection of military communication, information and weapon systems

Defence should protect all its communication, information and weapon systems against cyber threats in order to guarantee freedom of action for its military operations. Maximising the security and resilience of all systems requires a coordinated approach at different levels. End users, system administrators, system managers and cyber experts are each responsible at their respective levels for the correct implementation and follow-up of cyber security measures.

SO_II: Strengthening the cyber culture

Cyberattacks are not necessarily sophisticated or inevitable, and are often the result of vulnerabilities in the networks and weapon systems. In many cases, the decisive factor in the success of a cyberattack is not the inventiveness of the attacker but rather the vulnerability of the victim. Therefore additional efforts are necessary to implement a culture of cyber hygiene and cyber threat awareness for all Defence personnel.

SO_III: Responding appropriately to cyber incidents and attacks

A successful cyberattack can never be ruled out, not even with the most advanced cyber security technology. Defence must have a solid set of measures at its disposal to respond adequately to cyber incidents, and thus guarantee continuity in the execution of operations. The capabilities in the domains of detection, analysis and remediation, as well as attribution and communication need to be further developed.

SO_IV: Integrating cyberspace as a new operational domain

Our potential opponents are increasingly using cyberspace. Therefore Defence must also integrate cyber operations, both defensive and offensive, into the operational planning process. At the last NATO summit in Warsaw, the member states adopted cyberspace as a new operational domain. This places the cyber dimension on the same level as the traditional, conventional operational dimensions. The structures of the organisation, processes and doctrines must be adapted to this new reality.

SO_V: Further developing robust national and international cooperation

Cyberattacks rarely or never have a purely local impact but in most cases have cross-organisational or cross-border implications. In order to respond adequately to cyberattacks, Defence must maximise cooperation with other government services, sectoral organisations, foreign partners and international organisations such as NATO and the EU.

Implementation of Strategic Objectives

SO_I: Optimum protection of military communication, information and weapon systems

The functional authorities and system administrators of the communication, information and weapon systems of Defence will use the Defence Cyber Security Framework to structure their cyber security measures. The Cyber Security Framework consists of various functions that organise cyber security activities at the highest level. They are aligned with existing incident management methodologies and help visualise the impact of investments in cyber security.

All Defence communication, information and weapon systems that contain classified information are now accredited. An accreditation is not an end situation. Permanent focus must be given to the cyber security of these systems in order to guarantee the confidentiality, integrity and availability of the classified information.

Moreover, all Defence communication, information and weapon systems will be actively tested and audited on a regular basis in order to evaluate and improve the security of these systems where necessary. New technologies that actively contribute to improving the cyber security of communication, information and weapon systems will be evaluated and implemented, if necessary.

Defence will intensify its contacts with its system suppliers. Guidelines will be issued to integrate cyber security measures into the procurement or development process. Vulnerabilities in the supply chain of these systems, and in the systems themselves will thus be identified more quickly and will also be mitigated in cooperation with the supplier.

The purchasing cycle for cyber systems will be adapted to the ever faster evolving technologies. The most efficient systems and toolsets will be available to the military cyber capability to guarantee optimum protection of our communication, information and weapon systems against the latest cyber threats.

Adapted cyber security measures will be implemented for the Defence deployed communication, information and weapon systems. In accordance with the specific threat environment, stricter guidelines can be imposed. At the same time, a fair balance must be found between the operational importance of the use of the deployed systems, the adjusted acceptance level of residual risks, and the specification of the cyber security guidelines to be implemented.

A maximum number of Defence communication, information and weapon systems will be permanently (24/7) monitored in order to guarantee the integrity and proper functioning of these systems.

SO_II: Strengthening the cyber culture

Since the human factor plays at least as important a role in cyberspace as the technological factor, Defence will ensure that a correct level of cyber expertise becomes established in all ranks. Defence personnel must understand the global cyber landscape including the threats, vulnerabilities and dependencies associated with it at the strategic, operational, tactical and technical levels.

Cyber security awareness campaigns will be regularly programmed to indicate to Defence personnel that they are an attractive target for potential cyberattacks given the specific nature of their work. The campaigns will focus on disseminating information about the general cyber threat and risks, on the specific dangers of careless use of social media, and on providing best practices to counter cyberattacks as a whole.

The cyber education plan will not be limited to cyber experts. It will be expanded and continuously adapted to the changing cyber threat and technological developments. Education and training opportunities will be offered to all end users of Defence's communication, information and weapon systems, as well as to policy makers, planning officers, instructors, and system administrators.

Part of the cyber education plan will be integrated into the mandatory annual Joint Individual Common Core Skills (J-ICCS). Specific cyber modules will also be included in the basic and continuing education curricula. In cooperation with the Royal Military Academy, training programs will be developed that will increase the pool of future cyber experts. As a result, qualified officers will be ready for immediate operational engagement in the military cyber capability.

The units of the various components must participate in cyber security and incident response exercises to test their procedures and communication mechanisms under stress conditions. Prior to deployment abroad, each team or unit will receive additional training with special attention to both specific cyber threats in the area of operations and appropriate protection measures.

The number of cyber experts on the labour market has become very scarce, and competition with the private industry is very high. Once selected and recruited, Defence's new military and civilian experts will therefore enjoy permanent high-tech education and on-the-job training. In addition, initiatives will be launched for these experts to develop specific, challenging career paths and opportunities.

SO_III: Responding appropriately to cyber incidents and attacks

The configuration of Defence's communication, information and weapon systems will be mapped in detail. Information on possible cyber threats against these systems will be collected and evaluated, on the basis of which corrective actions will be proposed.

Business continuity plans will be drawn up for all critical systems to guarantee a minimum continuity of service in degraded cyberspace conditions. Contingency and disaster recovery mechanisms will be put in place and regularly tested. Defence must be prepared for large-scale cyber incidents. The scale-up of the cyber incident response capability with additional temporary resources will be further studied and evaluated.

New advanced and high-performance intrusion prevention and detection systems will be deployed to detect cyber incidents in time, and to better analyse them. Detected cyber incidents will be communicated as soon as possible to the system administrators in charge. Speed of action is important in order to limit possible contamination within the impacted network.

The results of the analysis of cyber incidents and attacks will be used to improve existing security systems, develop new detection systems and provide military and political policymakers with technical intelligence for attributing cyberattacks to a cyber actor. The same intelligence can also be used to initiate mitigating actions aimed at disrupting active cyberattacks or preventing new attacks.

An internal and external strategic communication plan will be drawn up to provide immediate and correct interpretation during major cyber incidents and crises. This plan will take into account the impact of compromised or unavailable critical information and/or systems on the correct functioning of the organisation.

The efficiency of military cyber capability is not so much based on large investments in equipment as on the expertise and professionalism of the specialised personnel. The selection and recruitment of motivated and technically competent personnel will be intensified. Regular recruitment campaigns will be organised both within and outside Defence to recruit the right cyber experts in good time.

SO_IV: Integrating cyberspace as a new operational domain

The cyberspace domain needs a correct legal and procedural framework for conducting cyber actions. The Tallinn Manual of the Cooperative Cyber Defence Centre of Excellence (CCDCoE) provides a non-binding legal basis for national and international legal advisors. The starting point of this manual is that the existing international treaties, rules of law and regulations also apply to cyberspace. Defence supports this statement.

The intelligence position in the cyberspace domain will be expanded with a focus on the capabilities and intentions of cyber actors relevant to the regions where Defence is present abroad. The cyber capability will rely on specific intelligence methods to obtain a maximum of intelligence with regard to the espionage and sabotage activities of our opponents. The intelligence capability will of course also be used as an enabler and facilitator for the offensive cyber pillar by acquiring knowledge about the vulnerabilities of our opponents' communication, information and weapon systems.

Defensive and offensive cyber capabilities will expand the range of operational capabilities for Defence. Freedom of action will be guaranteed by optimum protection of the deployed critical military systems from direct or indirect compromise. Cyber effects aimed at supporting and executing military operations will be integrated into the targeting and operational planning process. Clear concepts, doctrines and lexicons will be defined, and the limits and opportunities of the new medium will be correctly translated to the operational commanders. In the operational staffs, additional functions will be defined for planning officers to ensure the integration of the cyber effects.

The cyber capability will support most of the military operations from reachback. However, some very specific operations will require an embedded presence of cyber experts. The support from the cyber capability will be described in detail for each operation in a separate annex to the operation order.

Cyber capability will remain centralised in the coming years. This capability is still under construction and requires a very high level of expertise to function correctly and to continue to grow. It also needs specific processes and direct control to respond to the very fast evolving technological challenges, and to the continuous interaction between the different subcapabilities and national/international partners. Such niche capability with major challenges for the completion of Human and Material Resources will therefore be kept centralised at least until the full operational capability phase. After that, a possible restructuration of the military cyber capability can be evaluated. However, many international partners have choosen to remain centralised, or to evolve towards a centralised structure if they have started in a different way.

SO_V: Further developing robust national and international cooperation

The structural cooperation with the various national cyber actors must be strengthened and consolidated. Defence will optimally fulfil its national responsibilities, as defined in the national cyber security strategy, and will actively participate in interdepartmental and sectoral consultation bodies for the coordination of cyber security guidelines, processes and incidents. As a loyal partner, Defence endorses the commitments laid down in the national cyber emergency plan. If necessary, the military cyber capabilities can also be deployed as technical experts to support specific legal files.

Military cyber experts will participate as much as possible in national and international cyber exercises for a better understanding of cross-sectoral and cross-border dependencies. These exercises are also essential for increasing the level of trust between different services and nations. Priority will be given to promoting, establishing and maintaining mechanisms for the exchange of information with national and international partners. Formal and informal exchange of contact, incident and threat information will lead to more effective coordination and communication during cyber incidents and crises. Through in-depth and timely knowledge of partners' experiences, we can better identify our own vulnerabilities and improve the resilience of our own communication, information and weapon systems.

Strategic partnerships with sectoral organisations will be evaluated to integrate best practices from the private sector for the protection of critical infrastructures into the protection of military weapon systems. In collaboration with the academic world, initiatives will be launched in the field of cyber security innovation, research and development. In these areas, Defence will cooperate with the Royal Military Academy as a first priority.

Defence will actively participate in the implementation of the cyber projects as planned for in the National Pact for Strategic Investments. This pact foresees investments in the cyber domain for a total amount of 15 billion EUR for the period up to 2030. The focus is on a massive expansion of cyber expertise in police, military and intelligence services, on strengthening and officialising the Cyber Security Coalition to which Defence already belongs as well as drawing up a Cyber Resilience Plan for SMEs, developing a national Cyber Security Coordination Centre and a Cyber Security Council, and on investments in skills and education.

International forums and cooperation initiatives in which Defence will actively participate must be determined. Priority will be given to NATO and EU projects that generate immediate added value for the further development of national military cyber capabilities. Focus will be placed on initiatives in the areas of information exchange, operational cooperation, cyber diplomacy and legal regulations. Cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) will be strengthened.

CONCLUSIONS

The nature of the cyber threat may not have changed recently, but the rapid growth of the Internet-of-Things will give rise to a whole new set of vulnerabilities. Nations are also much less hesitant than before, and are now publicly announcing that they are developing offensive cyber capabilities and will also deploy them if necessary. Diplomatic rhetoric having become much more aggressive, it is clear that the next armed conflict will partly be fought in cyberspace.

Defence must adapt to the new cyber reality to safeguard its freedom of action in this new domain. The decentralised network and weapon system administrators must be supported to maximise their systems' resistance to cyberattacks. The situational awareness in cyberspace must be built up and integrated into the common operational picture. Advanced detection systems must be installed to allow us to detect malware or intrusion attempts in time. Sufficient expertise must be built up and permanently available to allow Defence to respond adequately to major cyber incidents and attacks. Finally, proprietary cyber effects must be created, validated and integrated into the operational planning process, and contingency procedures must be implemented so that Defence can continue to conduct its operations, even in degraded cyberspace conditions.

With this publication, Defence recognises the growing cyber dimension of the global strategic security context, reaffirms the importance of a coordinated approach to cyber threats, and lists the priority strategic objectives, concerns and development paths in the cyberspace domain for the coming years. This update of the cyber strategy creates the necessary conditions to allow the military cyber capability to evolve in line with the changing cyber landscape. In this way, Defence reduces the vulnerabilities of its communication, information and weapon systems to an acceptable level, increases its resilience, maximises its capabilities to counter cyber incidents and attacks, and integrates cyber as an additional operational domain.
