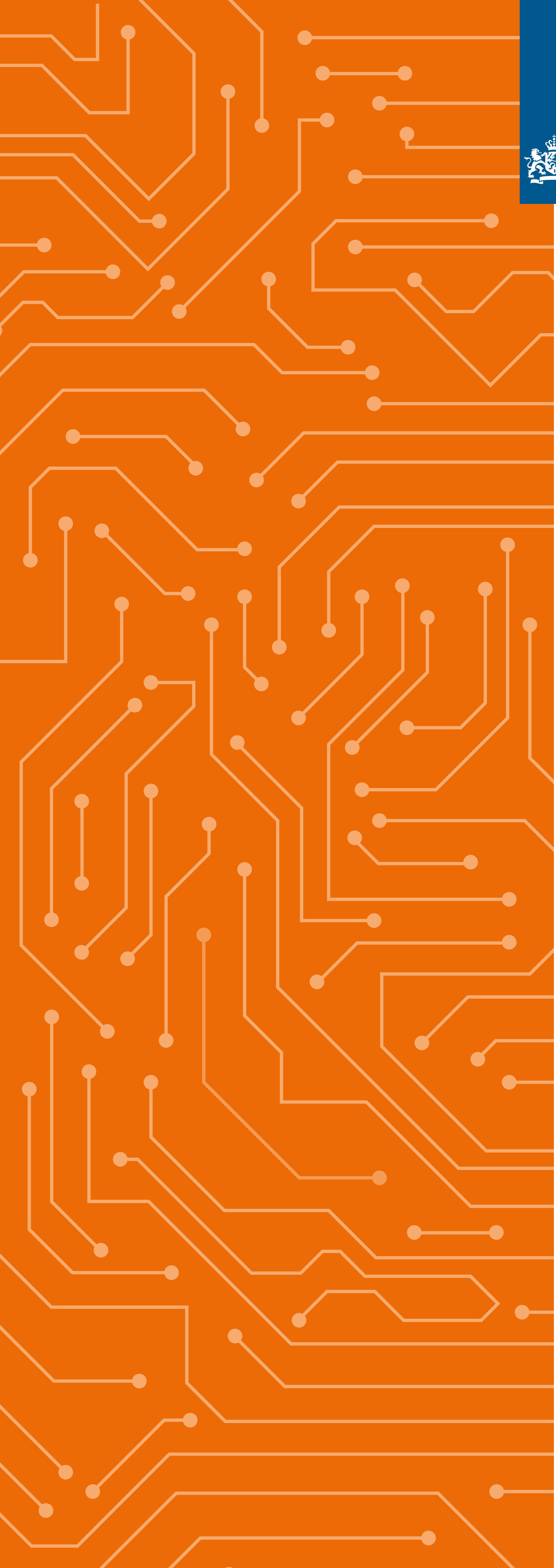
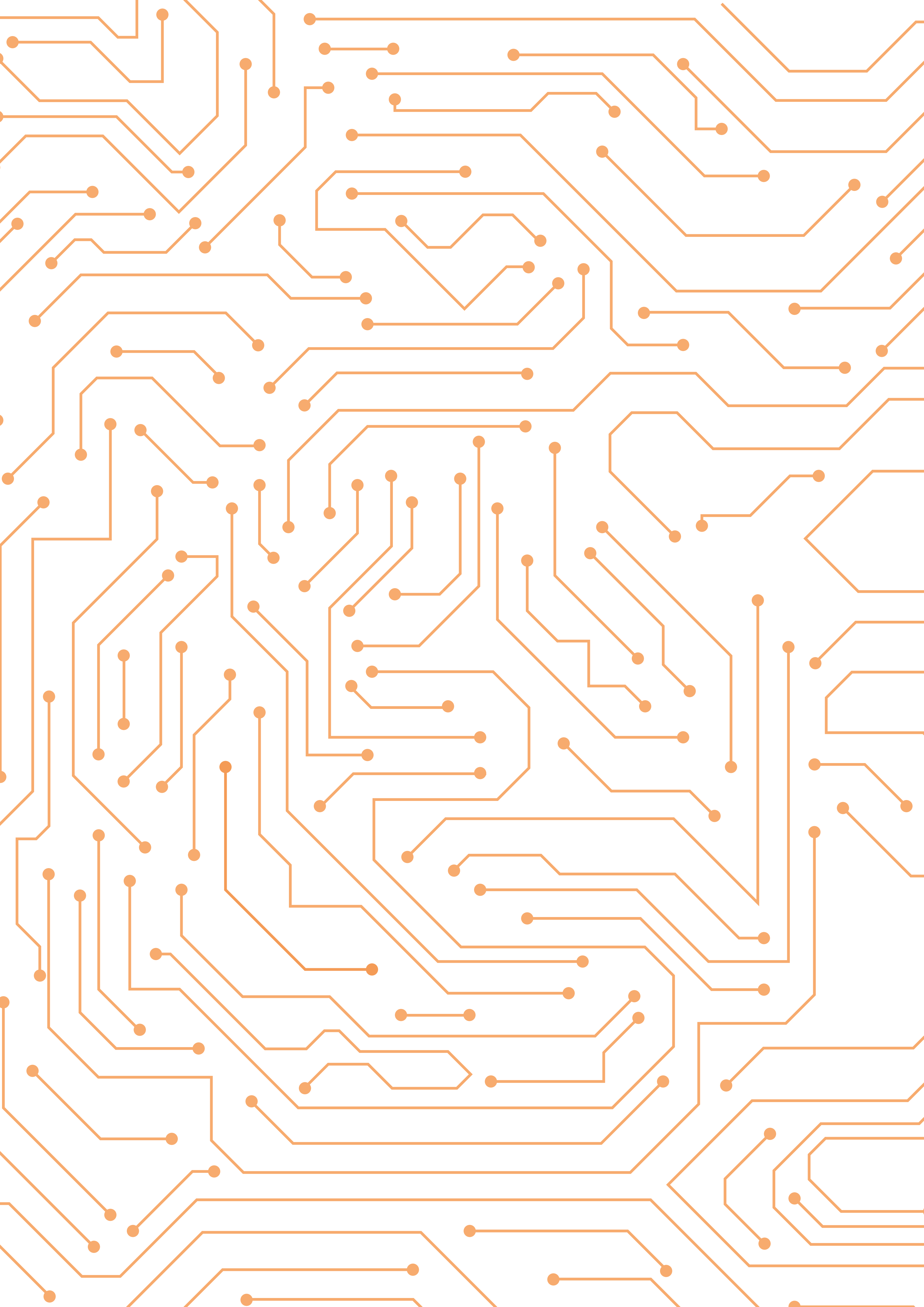


Ministry of Defence

Defence Cyber Strategy 2018

Investing in cyber striking power for the Netherlands



Contents

Introduction

Because of its constitutional tasks, the Netherlands Ministry of Defence (hereinafter referred to as Defence) is the fighting force of the state of the Netherlands. Our country must be able to count on Defence when the need arises. Taking action against serious cyber threats to our security in the national and international context is part of that.

The importance of the contribution that Defence makes to our cyber security has increased with the deterioration of the international security situation and the intensification of geopolitical conflicts of interest. The Cyber Security Assessment Netherlands 2018 (*Cyber Security Beeld Nederland 2018*) makes clear that the greatest cyber threat to our national security is state-based. This has indisputable consequences for the contribution that Defence is expected to make to counter that threat. Furthermore, our increasingly digitised country must be prepared for sophisticated cyber threats in the unfortunate event of military conflict. Defence has a responsibility in this regard, both to the Netherlands and to NATO.

This document, the Defence Cyber Strategy, has been drawn up within the framework of the 2018 Defence White Paper, the Integrated International Security Strategy 2018-2022 (GBVS) and the National Cyber Security Agenda (NCSA) and contributes to the implementation of these strategies. Following the publication of the first Defence Cyber Strategy in 2012, it builds on the foundation that was laid with the setting up of the Defence Cyber Command (DCC) and the Joint Sigint Cyber Unit (JSCU) of the General Intelligence & Security Service (GISS) and the Defence Intelligence and Security Service (DISS) and the reinforcement of the Defence Computer Emergency Response Team (DefCERT) and the Royal Netherlands Marechaussee (RNLM). Many steps have been taken since 2012. Now it is time to accelerate and connect. The cyber intensification in the Coalition Agreement, rising to a structural allocation of 20 million from 2021, makes this possible.

On the basis of this Strategy, Defence is investing in cyber capabilities in order to:

- be in control of its own IT and weapon systems at all times and to safeguard its cyber resilience. This will continue to be an important area of focus over the coming years;
- further improve our intelligence regarding who poses a threat to our national security in the cyber domain. Together with that of the GISS, the role of the DISS is indispensable in this regard;
- have more capabilities at our disposable for the disruption and deterrence of cyber attacks;
- safeguard, together with civil partners, the security of the Netherlands and of our vital infrastructure and processes in the unfortunate event of a military conflict in which offensive cyber assets are deployed;
- deploy cyber assets effectively in order to gain and retain superiority in military operations.

Cyber striking power for the Netherlands is an ambitious aim. But in view of Defence's main tasks, namely to protect our own and NATO territory, promote the international rule of law and support civil authorities, this ambition is a necessity.

Chapter I
The contribution of Defence to the cyber security of the Netherlands and NATO

State actors and criminal groups are becoming increasingly bolder in the cyber domain. Cyber attacks and cyber incidents have become the order of the day. They can no longer be treated as isolated incidents. More and more frequently, they are connected events which together form a campaign by state actors and their proxies, intended to undermine a country's economic revenue model, vital infrastructure, military capabilities or democratic order. Account must also be taken of the fact that certain states purposely place malware in industrial control systems in vital sectors in preparation for a potential military conflict. These are activities or operations that are designed to create the preconditions for a military operation (shaping the battlefield). It is Defence's responsibility to take action, in close consultation with civil partners, to combat this. Nonetheless, it is clear that if a (manifestly imminent) cyber attack is of such a scale that it can be considered a (manifestly imminent) armed attack under Article 51 of the Charter of the United Nations, every state has the right to self-defence.

Proper defence and security alone are not, however, sufficient to prevent malicious parties from carrying out cyber attacks. An increasing number of allies are therefore taking a more active approach in the cyber domain (active defence). In the context of the first and third constitutional tasks (defending our territory and that of NATO allies, and assisting civil authorities) , a more active contribution from Defence within the existing structures is required. With a view to strengthening this contribution, Defence will invest in the following capabilities and concepts over the coming years:

1. intelligence: capability to act and attribution;
2. contribution to deterrence by means of military capabilities in the cyber domain;
3. cyber defence and protection of own networks and systems;
4. research into national fallback options;
5. military aid and support for civil authorities;
6. law enforcement (Royal Netherlands Marechaussee).

1 Intelligence:

Capability to act:
while the vast majority of cyber attacks can be deterred by the IT or CERT department of the affected party, combating persistent covert cyber attacks by state actors (advanced persistent threats; APTs) also requires intelligence or counterintelligence investigations. Such investigations provide unique intelligence, enabling effective defensive measures to be taken. The DISS provides intelligence about threats in the cyber domain to relevant actors within and beyond Defence, such as DefCERT, the Public Prosecution Service, the National Cyber Security Centre (NCSC) and the private sector, so that they can take measures on the basis of that intelligence. Technical properties of cyber attacks garnered by the DISS and the GISS can be registered in the National Detection Network (NDN) for the purpose of detecting cyber espionage and sabotage. The NDN is a collaborative for a better and faster detection of cyber threats to vital sectors and the national government, so that damage can be prevented or limited. The DISS's contribution to the NDN will be extended. New defence assets will be deployed with which an active defence against cyber attacks can be developed. In addition, the number of sensors will be increased so that it is possible to detect and investigate cyber attacks more quickly and effectively and take action to counter the threat. As announced in the NCSA, in addition to participation in the NDN, the DISS will also participate in the collaboration platform with the NCSC, AIVD and the National Police Services Agency (KLPD), with a view to sharing relevant information, technical or otherwise, about cyber threats. Intelligence forms the foundation for military capability in the cyber domain. The availability of intelligence is the starting point for offensive cyber capabilities, and intelligence provided by the DISS enables the Defence Cyber Command to shape the military capability. Furthermore, under the Intelligence and Security Services Act 2017 (Wiv), intelligence enables the DISS to take action itself to disrupt acute threats in the cyber domain.

Attribution:
the increasing cyber threat calls for a vigorous international response based on by international agreements. That response is not vigorous enough at present. It is the government's intention to reprimand perpetrators of cyber attacks for their behaviour more often, in some cases publicly. First of all, this requires detection, followed by political and possible legal attribution. Establishing who the actor is behind a cyber operation (technical attribution) is a vital and complex stage of this process, and requires intensive investigations. In collaboration with partners such as the AIVD and the KLPD, the DISS carries out sophisticated knowledge-intensive intelligence investigations to uncover the actor behind the cyber attack and the actor's intentions, so that the government can proceed with political attribution and take targeted countermeasures. An active political attribution policy contributes to the deterrence capability and to making the Netherlands a less attractive target for cyber attacks. A state actor that is reprimanded, publicly or otherwise, for its actions will think differently than an attacker that can operate in full anonymity. In this way, the Netherlands is helping to counter impunity in the cyber domain.

2. Contributing to deterrence through military capability in the cyber domain:

deterrence means that an opponent decides not to carry out or repeat an attack because he believes that the costs will not outweigh the benefits. Deterrence is not confined to a specific domain. In other words: attacks from a different domain can be deterred with cyber assets, and cyberattack deterrence can also be provided from other domains. The operational capabilities of the Defence Cyber Command contribute to the arsenal of deterrence means available to the government. Deterrence makes the Netherlands a less attractive target for cyber and other attacks and is thus above all a means for conflict prevention. Deterrence requires not only the capability to attribute attacks, but also credible offensive capabilities. By integrating them into future and current missions and operations, Defence will improve the visibility and credibility of its cyber military capabilities.

For the government, NATO is the cornerstone of Dutch security policy. Together with other allies, the Netherlands made a case for Allied recognition of cyberspace as a military domain. The Alliance granted this recognition during the NATO Warsaw Summit in 2016. Since then, much hard work has been put into the operationalisation of the cyber domain, for example by establishing a mechanism whereby cyber capabilities can be integrated into NATO missions. This will contribute to the task of collective defence and deterrence. During the NATO Brussels Summit in July 2018, the Netherlands also declared its willingness to contribute cyber capabilities to Allied missions and operations.

3. Cyber resilience and protection of own networks and systems:

if a contribution is to be made to the cyber security of the Netherlands and if the secure and effective deployment of the armed forces is to be safeguarded, it is vital that the cyber resilience of Defence grows at the same pace as the threat. Accordingly, the deployment of Defence is considered a vital process within the system of vital infrastructure. The IT systems of Defence are fully integrated with organisational management and command and with sensor and weapon systems, and Defence is dependent on these IT systems and the information available on them to function. Cyber attacks targeting IT, sensor, weapon and command systems can thus undermine the deployment and effectiveness of the armed forces. A high level of security awareness and effective protection of systems and networks therefore require constant effort. Preventive measures form the necessary basis for cyber resilience – a combination of awareness, prevention, detection and capability to act. If the Defence systems are to be protected, these measures must be implemented throughout the IT chain, from software development to network protection. This places heavy demands on the personnel who work on the design, security, use and maintenance of IT systems. The knowledge among personnel must be up to date and personnel must have access to the latest techniques.

All the Defence elements involved must make every effort to protect the organisation from cyber threats. The Defence cyber chain consists of several layers, spread across the entire organisation. *Cyber governance and policy* provide direction, focus and frameworks for the efforts in the cyber domain. *Security by design* means that security measures are already implemented in IT systems during the development phase. *Security assessments* analyse and assess systems for residual risks, and *compliance and supervision* are concerned with the observance of policy and the regulatory framework. *Protection and surveillance* focuses on the links between Defence networks and the outside world. *Incident response* ensures the mitigation of cyber incidents.

4. Development of national fallback options:

investigations will be made into which Defence facilities could be deployed, in collaboration with which parties, to keep critical processes running in the event of socially disruptive ICT failure as a result of a cyber attack. Facilities such as the physically separated and secure fibre-optics network of Defence (the Netherlands Armed Forces Integrated Network, NAFIN), for example, could play a role in this respect.

5. Military aid and support for the civil authorities:

with the aim of contributing to national security, Defence will further its execution of its third main task in the cyber domain by providing a greater contribution to existing civil structures. In view of the nature of the threats, Defence is focusing on the vital infrastructure through closer collaboration with the responsible security partners, in particular the NCSC. The supply and demand of Defence's cyber capabilities will be brought into focus in consultation with the civil authorities and the relevant public and private-sector partners. Involvement in sector-specific developments and threats from an early phase will enable Defence to provide aid and support more effectively when required. To this end, Defence wants to provide a greater and more concrete contribution to existing civil structures for information sharing and response.

Information sharing:
Information Sharing and Analysis Centres (ISACs) have been established to create a trusted environment in which organisations from the same sector can share sector-specific and other information at tactical level regarding cyber threats, incidents, past experiences and mitigating measures, with the aim of increasing cyber resilience. Participants in an ISAC have a pivotal role in their organisation regarding information security, and ICT security and policy. The NCSC, the AIVD and the KLPD are affiliated with most ISACs. The RNLM is a permanent partner of the Airport IASC. The permanent network that an ISAC provides and the information that is shared are of great added value for all participants. Their nature and composition make ISACs an ideal platform for furthering knowledge about sector-specific cyber threats and the possibilities for Defence to contribute to mitigating measures when necessary. In consultation with the NCSC and ISAC members, Defence will investigate whether Defence's involvement in the ISACs can be intensified.

Response.

The National Response Network (NRN) is a network of CERT organisations coordinated by the NCSC. Its aim is to strengthen the technical response to cyber security incidents by sharing knowledge, experiences and personnel. In this way, cohesion is organised and existing capabilities are strengthened. In addition to the NCSC, the current NRN partners include DefCERT, the Tax and Customs Administration, the Directorate-General for Public Works and Water Management, SURF, and the Information Security Service for Municipalities. Defence will actively contribute to the NRN and will strive to extend the network. Defence will also commit to using NRN as a platform for exercises with vital sectors and the NCSC. Joint exercises enable organisations to become familiar with each other's procedures, interests and working methods, so that they can collaborate more effectively should there be an actual emergency.

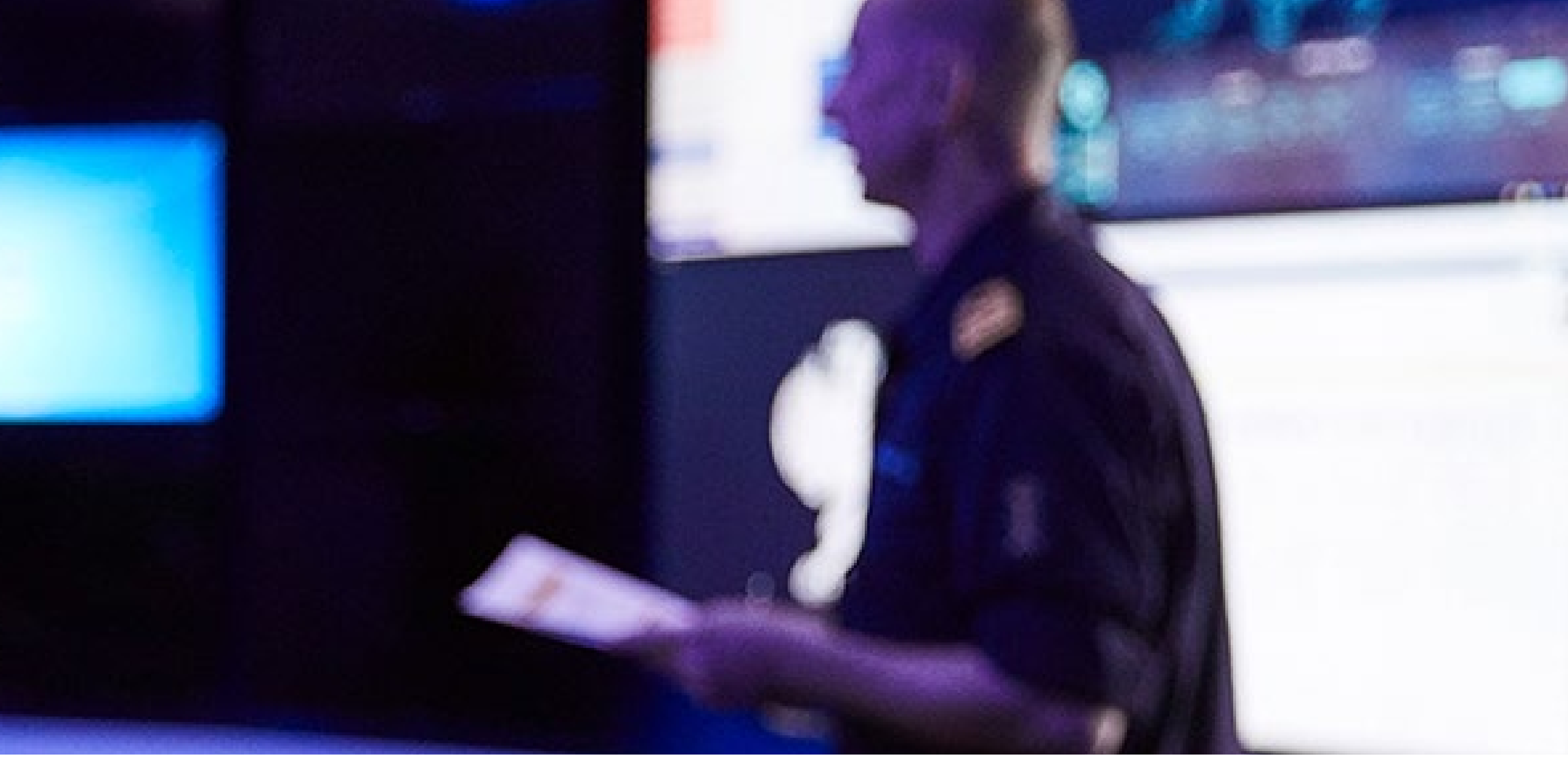
6. Law enforcement (Royal Netherlands Marechaussee)

Defence has a controlling responsibility for the execution of the RNLM's policing tasks. The RNLM, too, must be equipped for the growing cyber threat. The digitisation of border processes and the increase in cyber identity fraud carry particular risks. Risks that need to be managed by both better defence and by investigation. To this end, the RNLM will enter into collaboration with other parties, including the KLPD and the Fiscal Intelligence and Investigation Service.

Part II
Cyber victory in military operations

Article 97 of the Constitution states that there shall be armed forces to, inter alia, "maintain and promote the international legal order." The reference in that article to the international rule of law is closely related to Article 90, which stipulates that the government shall promote the development of the international legal order. In part due to the increasing instability in countries bordering Europe, this, the second main task of Defence, will make great demands of the organisation over the coming years. The undermining of the international legal order also jeopardises open and free international trade flows. Keeping land, sea, air and cyber lines of communications secure is crucial to the international community, to which the government is committed. The Netherlands is committed to the promotion of the international legal order, conflict prevention and stabilisation. One of the ways it achieves this is by taking a comprehensive approach to participation in military missions and operations in an allied context.

The cyber domain will play an important role in all future conflicts. The government recognises that the further development of cyber capabilities is necessary for the effective implementation of the second main task of the armed forces. With a view to establishing greater superiority in the cyber domain when deploying the armed forces for the purpose of promoting the international legal order, Defence will further invest in the following capabilities and concepts in the coming years.

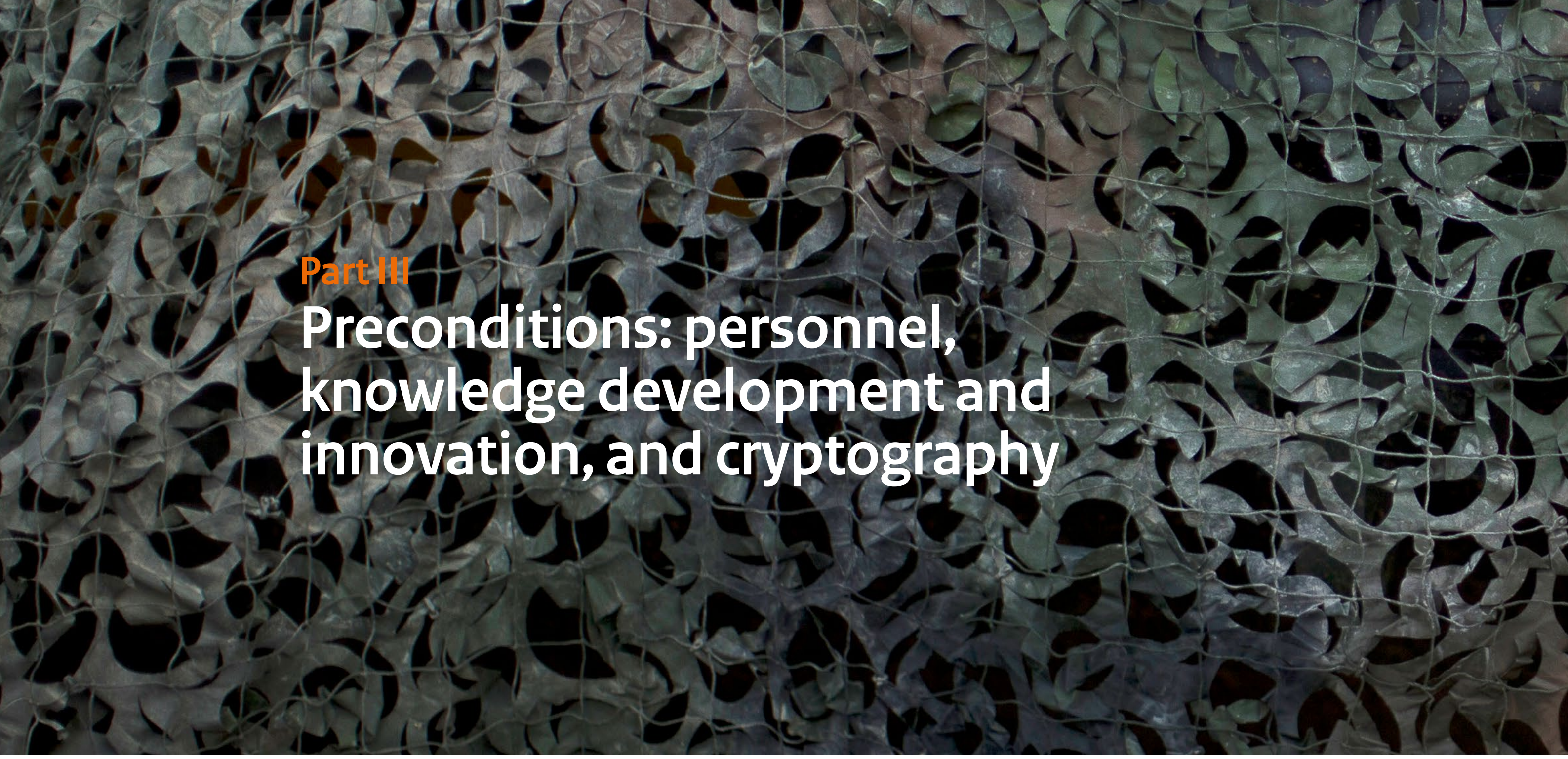


1. Establishing joint cyber mission teams:

as part of the military capability, cyber capabilities can contribute to military missions and operations. With a view to making military capability possible in the cyber domain, in-depth knowledge about vulnerabilities in the systems of potential opponents must be acquired at an early stage. By virtue of its constitutional tasks, the DISS supports the DCC with intelligence that is necessary for effective military deployment in the cyber domain. The knowledge and skills necessary for intelligence operations and military operations in the cyber domain are similar. Following the example given by other countries, cyber mission teams will therefore be formed from DISS personnel and personnel from the armed forces. The designated personnel will operate within the regulatory framework of the Wiv. When the armed forces are deployed, they will be placed under the command of the Chief of Defence within the relevant mandate. If necessary, components from DefCERT and the operational commands will also be added to these teams. The RNLM will invest in acquiring the relevant knowledge to test the legitimacy of military deployment in the cyber domain.

2. Cyber capabilities as a fixed feature of military planning:

the cyber aspect will be taken into consideration at an early stage of the planning phase of every (potential) mission. This will be expressed in recommendations, military and otherwise, and analyses by the Directorate of Operations, and in subsequent (operational) plans. In the event that the armed forces are actually deployed to maintain and promote the international legal order, Article 100 of the Constitution applies to the provision of information to the States General. Article 100 of the Constitution obliges the government to inform the States General in advance “if the armed forces are to be deployed or made available to maintain or promote the international legal order”. In future, Article-100 letters relating to a mission to which cyber is relevant will include a paragraph on cyber, which describes – within the confines of what can be publicly disclosed – the contribution that military cyber capabilities will make to the mission or operation in question. In this way, Defence will be promoting awareness within and outside the organisation of the increasing importance of the cyber domain as a fully-fledged domain of military operation.



Part III
Preconditions: personnel, knowledge development and innovation, and cryptography

This Strategy has outlined the developments and priorities that are intended to ensure that, in due course, Defence can also perform its three main tasks effectively in the cyber domain. This will not be possible without the preconditions for all these measures: personnel, knowledge development and innovation, and cryptography.

Personnel

To be successful in the cyber domain, in-depth knowledge of the domain is indispensable. Cyber and IT professionals have the relevant knowledge and experience; however, the shortage of specialists on the labour market means that it is not a matter of course that Defence will always have this knowledge at its disposal. In the coming period, Defence will investigate possible solutions for more effectively recruiting and retaining military and civilian cyber professionals. As part of this, attention will be focused on bringing together cyber and IT professionals. Career paths will be determined to gain more insight into human cyber potential as a whole and to make it possible to manage recruitment, retention and career development in a more targeted manner. In addition, opportunities for exchange will be exploited within and outside Defence (including market operators), so Defence can ensure that the knowledge of cyber professionals remains up to date, that employees are more satisfied, and that the network of cyber professionals is enhanced. Job roles will also be categorised to give cyber and IT professionals opportunities for development within the domain. Defence is committed to standard job descriptions and equal recognition for cyber and IT professionals to prevent competition within the government and to promote interoperability.

Knowledge development and innovation

Knowledge development and innovation in the field of cyber security is essential to keeping one step ahead of opponents and to combatting new digital threats. Furthermore, if Defence has a high-standing autonomous centre of expertise, it will be less dependent on the cyber-security expertise and solutions of third parties. Knowledge development is therefore one of the NCSA's seven ambitions in the field of cyber security for the coming years. This concerns both fundamental and applied cyber security research, which means multidisciplinary research throughout the knowledge chain with regard to long-term and short-term solutions. To this end, Defence has become a member of the Dutch Cyber Security Platform for Higher Education and Research (Dcypher). This platform's responsibilities include setting the agenda for and coordinating cyber-security research and higher education.

The third edition of the National Cyber Security Research Agenda (NCSRA), which was published recently, provides a determining framework for knowledge development in the Netherlands. Defence actively contributed to the development of this agenda. From 2019, Defence will increase the budget available for research in the field of cyber. From just under 4 million euros over the past few years, Defence will increase the annual budget for cyber research to almost 6.5 million euros from 2019 onwards. Where possible, this will be carried out with other ministries, as announced in the Dutch Digitalisation Strategy.

Together with a number of other parties, Defence is currently conducting a study into the setup, structure and organisation of a Cyber Innovation Hub to be established in 2019, in which ministries, research institutes and companies will work together on shared high-priority security issues in the cyber and cyber-security domain. The purpose of the Cyber Innovation Hub is to strengthen cyber knowledge and skills in the Netherlands, to facilitate innovations and experiments, and to establish an ecosystem of partners, in order to contribute to the reduction of cyber threats.

In 2018, the Digital Trust Center (DTC) of the Ministry of Economic Affairs and Climate Policy granted a subsidy to the Netherlands Industries for Defence and Security Foundation (NIDV) for the realisation of a National Cyber Register for companies working under the General Security Requirements for Defence Contracts (ABDO) and technology suppliers. The purpose of the Register is to improve the cyber resilience of companies that currently process confidential or state secret information under the ABDO or will do in the future. There will be close collaboration to this end with the DISS, the authority that determines the ABDO and grants authorisation in that regard, as well as with the AIVD, the NCSC and the DTC.

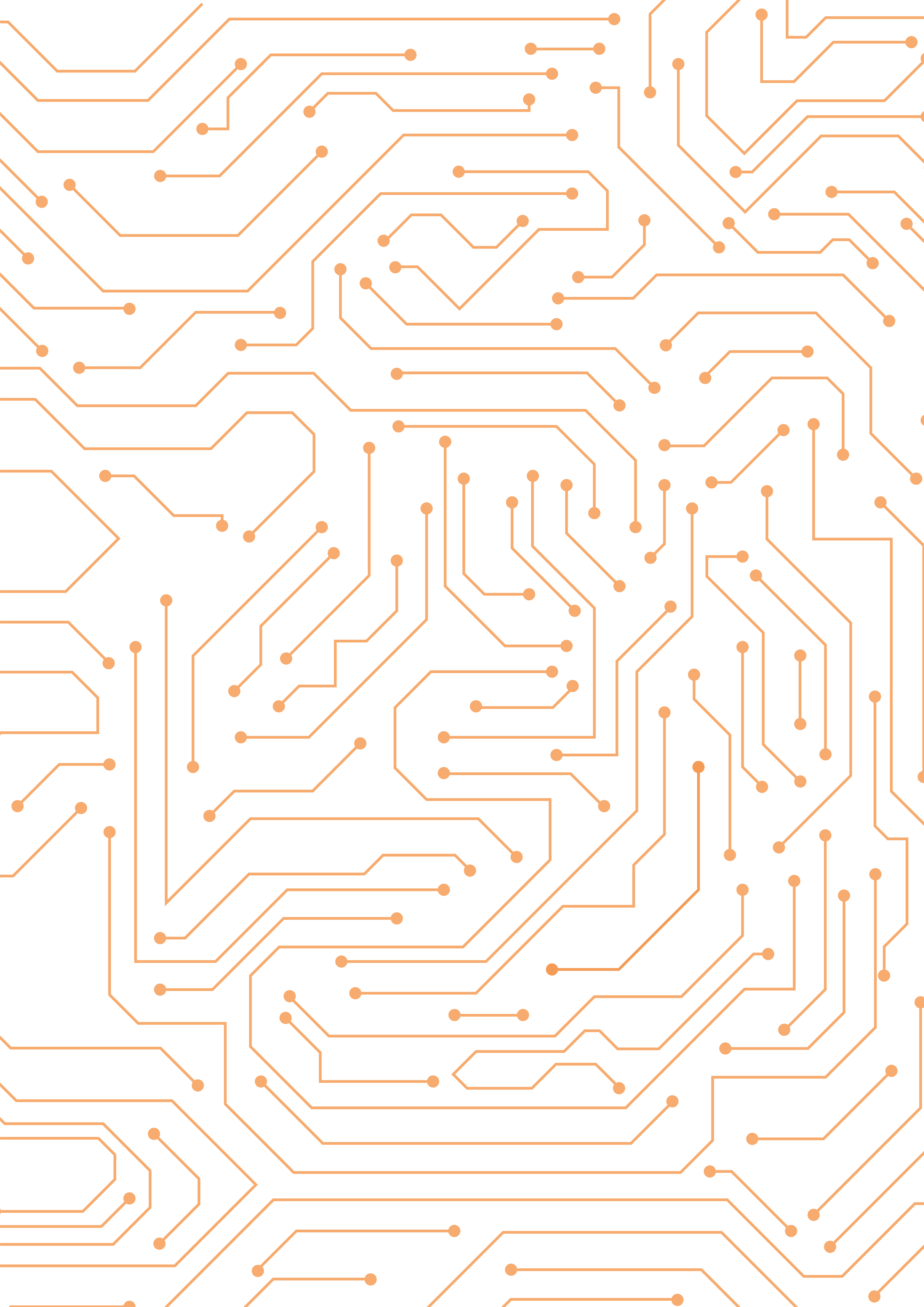
Cryptography

In operational and non-operational circumstances, during regular office automation and in sensor, weapon and command systems, Defence deals with highly classified information (HCI) on a daily basis. Not only does this highly secure HCI concern operational interests, it also falls under the Protection of State Secrets Act and must be handled in compliance with regulations such as the Civil Service Information Security Decree . Advanced cryptographic products are required for the secure storage and distribution of HCI. As cryptography continues to develop, so does code breaking, which means that cryptographic products must be adapted in line with these developments throughout their life cycle.

Cryptographic applications for the secure processing of HCI are primarily used by the national government, a small market in which Defence is the largest customer. Defence will enter into a strategic partnership with Fox-IT to ensure security regarding the development and continued availability of cryptographic products in the long term.

In conclusion

Defence cannot invest in cyber striking power for the Netherlands overnight. In light of the current cyber threat assessment, however, inaction is not an option. Developing offensive cyber capabilities, increasing cyber resilience and ensuring a solid intelligence position relies above all on the human input, for which continued effort and investment are required. Where possible, Defence will therefore have to open its doors. Alone, we cannot combat the threats and challenges that the cyber domain presents. Together, however, with other ministries, knowledge institutes, companies, the defence and security industry, and international partners, we can increase the cyber security of the Netherlands. Each on the basis of their own role and expertise, but with combined strength and a clear shared interest.



Publication
Ministery of Defence
Revised edition, November 2018

Layout
Mediacenter Ministery of Defence | The Hague

Text
Ministery of Defence

Photos
Mediacenter Ministery of Defence | The Hague