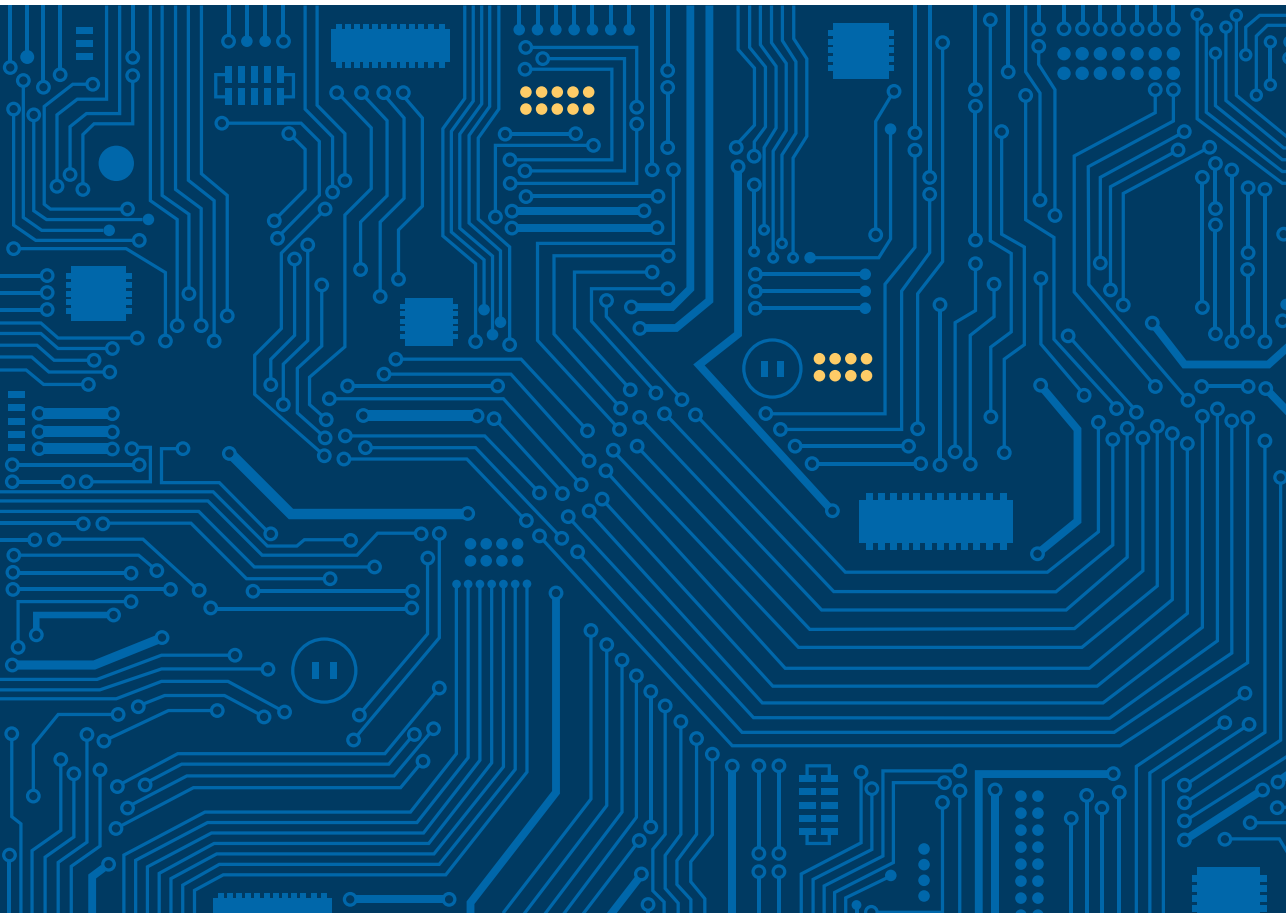
General Intelligence and
Security Service
*Ministry of the Interior and
Kingdom Relations*

# Offensive cyber-programmes

## An ideal business model for states



# Introduction

It is common knowledge that the cyberthreat against the Netherlands has grown significantly in recent years. This is also confirmed by the AIVD in its investigations. Within the field of cyber the AIVD concentrates on the threat posed by state-sponsored cyberattacks. In its investigations into state-sponsored cyberthreats the AIVD has noted that an increasing number of states are developing and implementing offensive cyber-programmes.

An offensive cyber-programme is aimed at using digital means to spy on other states, to influence these states or, in a worst case scenario, to sabotage a state's vital infrastructure, all with the purpose of obtaining one's own political, economic and financial goals. Russia, China, and Iran are examples of states with an offensive cyber-programme. Furthermore various other states are also enhancing their cyber-capabilities. As more and more states use cyber-attacks which directly or indirectly target the Netherlands, the cyberthreat against the Netherlands has grown in recent years. This publication, intended for a wide audience, will take a closer look at why offensive cyber-programmes are so attractive to states.

An offensive cyber-programme has become an ideal business model for states: the costs and risks are low, whereas the range and results are huge. The result is that states increasingly use cyberattacks to obtain their (covert) political, economic, and financial goals. This publication will conclude with the assessment that this cyberthreat will persist for the near future. This conclusion is based on the fact that cyber-attacks are becoming increasingly anonymous, which makes it more difficult to trace them back to the actual attackers; states are also more willing to use cyber-attacks.

A state-sponsored cyber-attack is the unauthorised and often covert penetration of the digital systems of another state. These attacks can be divided into three categories: cyber-espionage, cyber-influencing, and cyber-sabotage.
The AIVD defines cyber-espionage as the use of digital means to obtain the sensitive or confidential information of another state for one's own strategic aims. Think of obtaining important political or economic information, for example. Cyber-espionage can also be a first step in a scheme to influence or sabotage.

Cyber-influencing is the use of digital means to interfere with another state's interests. This can be in the form of spreading incriminating information (i.e. information that has not been manipulated but whose public exposure would be undesirable), or disinformation (fabricated or manipulated information). This information could put certain persons, governments, or countries in a bad light, or create unrest.
Cyber-sabotage is the use of digital means to damage, disrupt, or destroy (vital) systems and processes in another country.

## Offensive cyber-programme directed against Dutch interests

States with offensive cyber-programmes are a threat to our national security. They can be a threat to the Netherlands either directly or indirectly. Directly, because their cyber-attacks target the Netherlands. Indirectly, because the Netherlands could suffer collateral damage in case of an attack on another state, or because the attacks exploit Dutch internet infrastructure.

Our national internet infrastructure is held in high regard, because it is very fast, cheap, and reliable. Abuse of this infrastructure means the Netherlands could inadvertently become involved in cyber-attacks which violate the interests of other countries.

The Netherlands is an attractive target for state-sponsored cyber-attacks. The Netherlands has a high-quality knowledge economy with excellent (digital) infrastructure, and it participates in several international organisations, such as NATO, the UN, and the EU. It is also host to many international companies and organisations.

State-sponsored cyberthreats mainly target Dutch companies and government agencies. These targets could be, for example, individuals with access to valuable information who work for companies, the government, or international organisations based in the Netherlands. State-sponsored cyberthreats to a lesser extent also target individual Dutch citizens. This could be because they have a particular back ground (ethnic and religious minorities) or particular political views (dissidents, activists).

## Offensive cyber-programmes as the ideal business model

Offensive cyber-programmes offer states an ideal 'business model'. The far-reaching digitalisation of our society offers states a choice of new options for espionage, influencing, and sabotage. Here's what this business model looks like:

### Cost

The costs of setting up and carrying out an intelligence cyber-operation are relatively low when compared to the other intelligence means that a state has access to. A limited budget, a few computers with internet access, and a handful of hackers are basically all that is needed for a successful cyber-operation. This means that the threshold for offensive cyber-operations is quite low for states.

### Time and effort

The time and effort needed for setting up and carrying out an intelligence cyber-operation are also much lower when compared to other intelligence-gathering means. Whereas the recruitment process of a single human source can take up to several years, it takes mere hours or days and the talents of only one or a few hackers to infiltrate a computer network.
In addition, the use of malware (malicious software) opens up a range of possibilities for the (partial) automation of intelligence-gathering activities. The expectation is that in the future the use of artificial intelligence will result in an even further reduction of time and effort needed for intelligence cyber-operations.

Once inside a network, the attackers can then set up all kinds of digital 'backdoors' that are difficult to discover and remove. Thanks to these backdoors the

attackers are able to maintain their covert access to these networks.

Several AIVD investigations have revealed that this access can remain in place for several years. Such long-term access pays off because it enables attackers to obtain sensitive information over a longer period of time. It is for good reason that the term Advanced Persistent Threat (APT)[1] is often used for these state-sponsored cyber-attack groups.

## Results

As a result of expanding digitalisation, important and sensitive information is increasingly made available only in digital form, accessible via the internet. Public and private communications via digital means are also still on the rise; more and more production, transportation, and household systems are connected to the internet (the so-called Internet of Things); data is stored in the cloud; and internal business processes are outsourced to digital service providers. All of these mean there has been a huge increase in the possibilities for and profits of cyber-enhanced espionage, sabotage, and influencing.

## Range

In theory, any digital internet-connected system anywhere in the world is vulnerable to attack. Physical proximity to the target is thus no longer a requirement for success in intelligence cyber-operations. This has greatly boosted the range of espionage, sabotage, and influencing. With the arrival of the Internet of Things more and more systems are brought within the range of cyber-attacks.

## Accessibility

The digital means for cyber-attacks are relatively easy to obtain. The hacking tools of various states have been exposed and released to the public in recent years. Zero-days[2] and other attack tools can be bought online. Information security companies regularly publish very detailed analyses of these tools and vulnerabilities, with the aim of promoting resilience against such cyber-attacks. This information, however, can also be used to carry out cyber-attacks. Because all this knowledge on cyber-attack means is (freely) accessible, states can develop their own offensive cyber-programme quickly and easily.

## Scalability

State-sponsored cyber-attacks not only target the individual user of a digital system, but increasingly also those who make these systems. Think, for example, of hardware and software developers. Cyber-attacks also increasingly target digital service providers which play a crucial role in processing, storing, and transferring digital information. Examples of such service providers are internet service providers, telecommunications providers, and managed service providers. Because of the services they provide, these companies often have extensive, substantial, and structural access to their customers (and their digital networks).

These manufacturers and service providers are an attractive target for state-sponsored cyber-attacks, because they often offer their products and services globally, which will benefit the scalability of intelligence operations. This threat becomes more prominent when these manufacturers or service providers come from countries running an offensive cyber-programme against the Netherlands. The authorities in countries such as these can force manufacturers and service providers to collaborate

[1] An Advanced Persistent Threat is a group of actors that is responsible for advanced and long-term cyber-attacks, in wich the group remains hidden as it infiltrates a computer network.

[2] Zero-day exploits, or zero-days, are unknown vulnerabilities in hardware or software that can be used to gain unauthorised access to that hardware or software.

with the intelligence services, to create hidden digital 'backdoors', for example. This would enable these states to increase the scale of their cyber-attacks even more.

### Reusability

The tools and methods used in cyber-attacks can often be reused. This reusability not only applies to the attacker, but also to the target. The attacker can use the same tools and methods on several different targets. States that are or have been targeted in these cyber-attacks can then study the tools and methods used, reproduce and refine them, and then add them to their own arsenal of cyber-attack weapons. This encourages proliferation and with that the availability of these tools and methods.

### Anonymity

Many states carry out their cyber-attacks under cover of a false flag operation. Some states use companies for intelligence cyber-operations in order to hide government involvement. This makes it more difficult to establish who is behind an attack and what purpose the attack served. Cyber-attacks can be carried out in near-complete anonymity. Digital traces are easily deleted or hidden so that their origins cannot be retraced — think, for example, of encryption and TOR.[3] All of these things taken together make it more difficult to attribute a state-sponsored attack (i.e. establish or determine which state actor is behind an attack).

### Low risk

Because of the anonymity available to attackers, it is not easy to expose and bring to justice the hackers and states responsible for these attacks. An international strategy of sanctions to fight attacks of this kind is still under development. At the moment only a few measures are available. These include sabotaging cyber-attack networks (notice and take down), criminal charges, and diplomatic steps. The effect of these measures is generally fairly limited, however. Consequently the risks for attackers are relatively low, and states are more willing to resort to these methods.

### High success rate

Potential victims often invest in cybersecurity in order to withstand state-sponsored cyber-attacks. Often these security measures are not sufficient enough to prevent state-sponsored hackers from gaining access to computer systems, however. New vulnerabilities in hardware and software continue to be discovered, for example. The AIVD also regularly observes that state-sponsored cyber-attacks exploit known vulnerabilities in hardware and software. The speediness at which vulnerabilities of this kind can be used in an attack is usually much greater than the potential victim's ability to take timely counter-measures. The result is that the rate of success of state-sponsored cyber-attacks is high.

## Offensive cyber-programmes contribute to (covert) goals

The result of this ideal business model is that cyber-attacks are used more and more by states in the pursuit of their goals. Some of these goals are public knowledge, others are kept secret. On the whole, these goals can roughly be divided into political, economic, and financial goals. Each of these goals will be illustrated by practical examples which the AIVD has come across in its investigations. The examples illustrate how cyber-attacks contribute to the realisation of (covert) government goals.

### Political goals

Cyber-attacks are often carried out for political reasons. AIVD investigations have revealed, for example, that a certain state attempts to remain

[3] With OR (The Onion Router) it is possible to cover up the source and destination of network traffic.

informed of an international forum's policy making regarding that state. By using cyber-attacks this state has gained entry to the poorly secured government network of one of the member states of this international forum. The attacking state then infiltrates the international communications between the member states of this forum. This strategic position provides the attacking state with insight into the policy viewpoints of all the member states of this forum, including the Netherlands.

In another example, a certain state tries to use digital means to spy on and silence emigrated (former) co-nationals in the Netherlands. The victims feel unsafe in the Netherlands, and they adapt their behaviour because they perceive the spying as restrictive. The AIVD sees this as undesirable foreign interference and a violation of the victims' fundamental rights.

The AIVD has also observed how various states obtain expertise or make preparations for cyber-sabotage operations, in some cases actually carrying out such operations. For example, the AIVD has observed how a state can infiltrate and hide out inside vital European infrastructure, possibly for the purpose of sabotage. Internet-connected operating and control systems for vital technology, e.g. water supply or the electricity grid, can thus be disrupted.

### Economic goals

Cyber-attacks can also be carried out for economic reasons. One of the things revealed by AIVD investigations is that some states want to accelerate the modernisation of their economies, to that end going so far as to steal innovative technologies from Western countries, including the Netherlands, covertly and sometimes on an almost industrial scale. With the use of this stolen knowledge these states intend to integrate these technologies into their own economies or begin manufacturing these technologies at lower market prices. This is a threat to the Netherlands' capacity for economic innovation and employment.

Another example is the discovery of a state using a state company for the takeover of an international business. At the same time as this takeover, the state in question carries out covert cyber-attacks on the law firm that is in charge of the legal aspects of this takeover, with the aim of obtaining confidential information. As a result this state is completely up to date on the company's profits and risks. This provides the state with insight into competitors and their conditions and offers in the takeover process. Consequently this state is able to adapt its takeover strategy and fine-tune its takeover bid with exactly the right set of conditions. Such practices are a threat to the level playing field of the Dutch business world.

### Financial goals

Cyber-attacks can also be carried out for financial reasons. In its investigations the AIVD has come across a state with limited foreign currencies at its disposal which carries out very successful cyber-attacks aimed at financial gain. These attacks use rented Dutch servers. The tens of millions of euros in revenue earned in these state-sponsored attacks end up directly with the national exchequer.
Although their scope and impact are as yet fairly limited, these attacks could become a serious threat to the accessibility and continuity of international money transfers.

## State-sponsored cyberthreat will increase in the near future

It is assessed that in the near future the number of states with an offensive cyber-programme will grow. In its investigations the AIVD discerns two trends that corroborate this assessment.

## Anonymous attacks, difficult attribution

Cyber-attacks are increasingly anonymous, and this anonymity promotes the use of cyber-attacks. Many states not only invest in their cyber-capabilities quantitatively (i.e. more hackers and other ICT specialists) but also qualitatively. There is a noticeable specialisation in various areas related to hacking, and increasingly sophisticated techniques are used to ensure that attacks are untraceable. This makes the attribution of an attack much more difficult. Attribution is also hindered by the fact that states often 'recycle' one another's tools and methods. Successful parts of malware code by one state are developed further and used by another. The AIVD has also noted cross-pollination with criminal means of attack; ransomware[4] , for instance, is also used in state-sponsored cyber-sabotage attacks. This global proliferation of cyber-attack means is a hindrance to attribution.

There is another development that promotes anonymity for states engaged in cyber-attacks. In recent years the AIVD has seen a notable increase in the number of supply chain attacks by state-sponsored actors. In attacks of this kind, external providers of digital services (internet service providers, telecommunications providers, managed service providers) are used as a springboard to infiltrate a target organisation. First the network of the service provider is penetrated, and from there the victim's network is infiltrated. Indirect attacks of this kind using trusted service providers are extremely difficult to detect, prevent and attribute to any particular state. Other types of supply chain attacks are attacks that exploit digital 'backdoors' in hardware or software. These attacks can be carried out entirely anonymously.

## Increased readiness for use of cyber-attacks

More and more states consider cyber-attacks to be part of the government's 'standard' means, to be deployed at a large scale. This applies particularly to cyber-espionage. More and more states see this as a valid intelligence tool that they can use without limitation, practically anonymously, and generally with impunity. In the case of some state-sponsored actors, traditional espionage and cyber-espionage are becoming increasingly intertwined. Traditional (human) espionage operations are thus preceded by (exploratory) cyber-espionage operations. Besides cyber-espionage attacks, states also turn to cyber-influencing and sabotage more often, frequently quite successfully.

Consequently, when two states get into a conflict, more and more often there is an aspect involving cyber. The readiness to use cyber-attacks and the selection of targets for such attacks thus in part depend on geopolitical developments. Strongly shifting global positions of geopolitical power result in a more diffuse threat picture. The AIVD has established that the Netherlands could quite suddenly become a cyber-target after becoming involved – either directly or indirectly – in an international diplomatic conflict.

[4] Ransomware is malicous software used by a cyber-attacker to encrypt a computer or the data on that computer. Ransom money must be paid to have the data decrypted and released again.

## Conclusion

The AIVD concludes that more and more states are developing and using an offensive cyber-programme. The proliferation of such cyber-programmes can be explained by the fact that they offer an ideal business model for states looking to realise their (covert) political, economic, and financial goals. Because the number of states with such programmes is growing, the cyberthreat faced by the Netherlands has increased in recent years. The Netherlands is an attractive target to these states for mainly political and economic reasons.

The AIVD estimates that in the near future this state-sponsored cyberthreat will persist, because cyber-attacks are increasingly anonymous, which makes the attackers more difficult to trace, and states are increasingly willing to use cyber-attacks.

The cyberthreat faced by the Netherlands is even greater when ICT products and services from states that have been shown to run an offensive cyber programme are used for the exchange of sensitive information or for vital processes. This increases the threat, because many of these states legally oblige companies in their country to cooperate with the intelligence services. ICT products and services from these states could have been equipped with digital 'backdoors'. These illegal backdoors could be used to obtain access to sensitive information or vital processes in the Netherlands, easily and anonymously. For these reasons the AIVD considers it undesirable if the Netherlands were to become dependent on ICT products and services from states that run an offensive cyber-programme against the Netherlands.

## How does the AIVD deal with this cyberthreat?

Cybersecurity is essential to the functioning of our society. The AIVD uses its investigatory capabilities to identify, analyse, and where possible eliminate threats coming from states with an offensive cyber-programme at an early stage. The AIVD also assists in the detection and mitigation of attacks on companies and government organisations; the AIVD informs victims of cyber-attacks and promotes awareness by organising informative sessions for potential targets. The AIVD provides tailored information security advice to the Dutch government and other interested parties, such as companies in vital sectors. The purpose of this advice is to increase resilience against state-sponsored cyber-attacks and reduce or prevent the damage caused by such attacks. Because of its access to secret information, the AIVD is in a unique position to provide thorough security advice, enabling others to act.

Close cooperation with the MIVD is crucial here. The AIVD also works closely with other national partners, such as the National Cyber Security Centre (NCSC), the Dutch Cyber Security Council, and international partners. The AIVD, the MIVD, and the NCSC work together in close cooperation in the National Detection Network (NDN) to improve the cybersecurity of government agencies and companies in vital sectors. Relevant threat information is shared regularly within the NDN, enabling member organisations to take targeted measures against cyberthreats. However, the AIVD and these partners cannot deal with these state-sponsored cyberthreats on their own; they require a structural investment from all parts of Dutch society.

This brochure is published by:

General Intelligence and Security Service
aivd.nl

P.O. Box 20010
2500 EA The Hague

February 2020