Letter of 20 April 2018 to the President of the House of Representatives of the States General from the Minister of Justice and Security, Ferdinand Grapperhaus, concerning the integrated approach to cybercrime

Cybercrime has many faces, and its impact can be far-reaching. The number of victims is large and continues to rise. Criminals are turning to computer hacking in order to commit new types of theft or to extort people and businesses, shut down websites, commit corporate espionage and trade goods via the dark web. Such a multi-faceted phenomenon requires an integrated approach that ranges from prevention, investigation and prosecution to reducing the rate of reoffending. The government plays various roles in this regard; it acts as an initiator, supporter, enforcer and, if necessary, creator of policy and legislation. Tackling cybercrime has a significant effect on strengthening cybersecurity, particularly when it comes to activities aimed at preventing cybercrime.[1] The government's approaches to tackling cybercrime and strengthening cybersecurity are being formulated in a cohesive manner. The House will be informed separately about the broad-based National Cybersecurity Agenda.

In December 2016 the House of Representatives adopted the motion submitted by MP Jeroen Recourt. This motion called on the government to work with the private sector to draw up an integrated action plan for cybercrime, with a focus on prevention and prosecution (Parliamentary Paper 34550 VI, no. 87). I am writing both in my own capacity and on behalf of the Minister for Legal Protection and the State Secretary for Economic Affairs and Climate Policy to inform the House about the integrated approach to cybercrime, in accordance with the request made by the House in this regard.

Cybercrime

The digital revolution offers major economies of scale and the possibility of connecting with people quickly and easily, no matter where they are in the world. The downside of this is that criminals also use the internet to significantly expand their activities. As a result, one in nine people were victims of cybercrime in 2017.[2] Nowadays, more people are victims of hacking than of bicycle theft, and while crime in general is falling, cybercrime is not.

The term 'cybercrime' covers a wide range of different types of crime; including traditional offences in digital form as well as new forms of crime. Examples of cybercrime include hacking computers in order to transfer money to criminals' bank accounts and remotely activating devices' cameras and microphones in order to spy on people. For several years, professional criminals and state actors have posed the most serious threat to digital security. Moreover, it is these parties that inflict the most damage. Professional criminals focus primarily on stealing data from private organisations and members of the public. This data can then be sold on to third parties or published.[3] In 2016 20% of businesses with 10 or more employees were affected by cybercrime.[4] For small businesses in particular, the risk can be considerable. A ransomware attack can render customer data inaccessible, for instance, and make operational management impossible, with significant financial consequences. The internet has given rise to a market for 'cybercrime as a service'. This means it is no longer necessary for cybercriminals to have detailed technical knowledge in order to carry out their

[1] Dutch cybersecurity policy aims to keep the Netherlands digitally secure and focuses on the full spectrum of measures to prevent damage through the disruption, failure or misuse of IT systems and to repair such damage if it does occur, with a particular emphasis on the Netherlands' vital interests. The approach to cybercrime focuses on preventing and combating criminal offences and limiting the number of victims, perpetrators and repeat offences. This approach covers both high-tech crime as well as more common forms of crime.

[2] Safety and Security Monitor (*Veiligheidsmonitor*) 2017

[3] Cyber Security Assessment Netherlands (CSBN) 2017.

[4] CBS.nl 25 September 2017.

crimes using IT. For example, a single individual with malicious intent could carry out a distributed denial of service (DDoS) attack and block access to the services offered by a company or a public body. The distinctions between high-tech cybercrime, advanced persistent threats and other types of common crime are therefore becoming blurred.[5]

Several types of perpetrators

Several types of perpetrators appear to be active. Some are motivated more by the 'kick' of carrying out an advanced hack than by financial gain. The question is whether normal interventions can be used across the board when it comes to dealing with perpetrators of cybercrime.[6] People involved in cybercrime, including offences that have a serious impact, are often younger than those who commit traditional crimes. So-called 'script kiddies' are one example. There is a risk that they will carve out careers in crime and turn into hardened cybercriminals.

Victims - a never-ending supply of potential targets everywhere

The fact that people are continuously connected to the internet means that, at any given moment, there is a large pool of potential victims. Most people always have their phones turned on, meaning they are always within reach of criminals. Given the enormous quantity of – sometimes very personal – information on a person's phone (or which can be illicitly obtained through a person's phone), the impact of cybercrime on victims can be considerable. A person's phone could be hacked in order to obtain private photos, for example, which could then be used to extort the victim. Many companies' internet pages are accessible 24/7, meaning they are always vulnerable to hacking and DDoS attacks. The internet offers criminals opportunities to exploit economies of scale. Spreading ransomware, for instance, enables them to find victims around the world to extort. Data held in different types of databases is a valuable target in terms of developing new types of criminal activities. For specific, high-value targets, more advanced criminal methods are used. It often turns out that victims were unaware of the dangers and the relatively simple measures they could have taken to protect themselves. For instance, they didn't have the latest security updates installed or were unconcerned about potential threats.[7]

Difficult to investigate

The anonymous and fast-paced nature of digital developments make investigating cybercrime particularly difficult. Communication via the internet is often anonymous and encrypted. Technology aimed at protecting users' privacy is also used by criminals to effectively mask their own identity. The dark web hosts a diverse array of criminal marketplaces which facilitate the trade in items such as arms and narcotics. In addition, new digital products and services are being continuously developed, including ones that can be used for criminal purposes.

What sets the internet apart is the fact that it is has no territorial boundaries. When it comes to organised cybercrime in particular, many of the perpetrators who target Dutch victims or use Dutch digital infrastructure for criminal purposes are not actually located in the Netherlands. There is usually no personal interaction between perpetrators and victims. Crimes can be carried out at several physical locations simultaneously, often across several different countries. International procedures for investigating such crimes are not sufficiently tailored to respond to this reality.

The law enforcement powers and capabilities currently available are not sufficient to have a real impact in the fight against cybercrime. Thanks to the hard work of many parties, major steps forward are being taken, but too many criminals

[5] Internet Organised Crime Threat Assessment (IOCTA), Europol 2016.
[6] Parliamentary Paper 28741, no. 33, 11 April 2017.
[7] IOCTA 2016.

remain active nonetheless. This needs to change. The internet must not become a safe haven for criminals and crime must not be allowed to pay.

Guiding principles

Given the speed at which cybercrime is developing, the lack of ties to a particular locality and the vital role played by private parties, the guiding principles of the government's approach will be flexibility, cohesion and cooperation.

Flexibility and cohesion

The methods used by criminals continue to develop at a rapid pace. In addition, innovative and technologically complex criminal methods are becoming quickly known and available to less tech-savvy criminals in the form of 'cybercrime as a service'. This means that flexibility must be a key feature of any approach. A schedule of long-term measures that is too specific or rigid will have little effect. The ability to react quickly to changing methods is vital. To combat cybercrime it is necessary to gain an understanding of new criminal methods quickly, develop interventions and, if these are successful, quickly promulgate this response within the police and the Public Prosecution Service, and share it with other partners. In addition, an integrated approach to cybercrime involves examining which actions (prevention, investigation, prosecution, disruption or a combination of these) can be most effective in disrupting criminal revenue models. For example, flexible public information campaigns through channels such as social media can help inform the public of new methods in use, so that people can take steps to make it harder for criminals to target them.

Cooperation

From a societal perspective, the government's task is to reduce cybercrime, minimise its impact and deal with offenders. However, the government cannot do this without the cooperation of the private sector, civil society organisations and the public. In an integrated approach, government bodies, companies, the public and civil society organisations each have their own responsibilities to fulfil. The internet – and services provided via the internet – are, for the most part, not controlled by the government. The fight against cybercrime therefore requires close cooperation with private parties that provide essential internet services. It is primarily private parties that have the knowledge and opportunities to quickly recognise and prevent cybercrime, as well as to erect barriers and disrupt it. What is more, private parties often hold the data needed to conduct investigations.

The Ministry of Justice and Security is actively seeking to collaborate with other ministries and with subnational authorities. The Ministry of Economic Affairs and Climate Policy is responsible for establishing a Digital Trust Center for non-vital businesses in the Netherlands and, together with the National Coordinator for Security and Counterterrorism and the ECP (the Electronic Commerce Platform), has established the information portal *veiliginternetten.nl*. Local authorities can also play an important role in combating cybercrime, as they are often better placed to work with local private organisations.

Furthermore, the cross-border nature of the internet means that international police and judicial cooperation is indispensable. In practice, the normal forms of international cooperation often prove too slow and laborious for effective cybercrime investigations. In addition, criminals also make use of anonymising technologies such as VPN[8], TOR[9] and encryption. Often, this means it is not easy to determine where (i.e. on what servers in which country) data is located and, as a result, which country should be approached for the purposes of cooperation and investigation. This represents a threat to law enforcement on the internet. The

[8] A Virtual Private Network (VPN) is an isolated, encrypted connection between
a device and a specific internet server.

[9] An open network for anonymous communication which makes it difficult for third parties to establish the origin and destination of messages.

Netherlands is actively seeking to strengthen cooperation and find new ways to improve the effectiveness of international investigations. Amending international legal frameworks could support such cooperation.

Four focus areas

The current approach to cybercrime focuses first and foremost on investigating, prosecuting and disrupting criminal offences, preventing people falling victim to such offences (primarily through raising awareness) and strengthening legislation. This approach will be continued and intensified. In addition, new elements will be added, such as preventive measures aimed at potential perpetrators and victims, a possible alternative form of victim support and steps to prevent reoffending. Lastly, more knowledge is needed for policy formulation in the longer term. The integrated approach to cybercrime comprises four focus areas:

1. Investment in prevention
2. Strengthening investigation, disrupting criminal activities and dealing with perpetrators
3. Tailoring support for victims of cybercrime
4. Enhancing academic research on cybercrime

Prevention

In principle, individuals and organisations themselves are responsible for taking measures to increase their own security. This also applies to the digital domain. The government helps by, for instance, making basic information about cybersecurity widely available and promoting hardware and software security. The government is also aware of the fact that people have different needs and capabilities. What they themselves can do in terms of cybersecurity and where they are vulnerable varies and sometimes requires specific attention. This is where the need to work with a range of partners both inside and outside government clearly comes into play. Companies are often best placed to strengthen their cybersecurity and help the public (their customers) do the same. Municipalities, in their turn, are often well placed to actively engage with the public and small and medium-sized enterprises (SMEs).

In order to limit cybercrime, it is vital that potential victims know how to better protect themselves. Many IT professionals and large organisations are familiar with the preventive measures that can be taken, thanks in part to cybersecurity-awareness activities undertaken by both the government and the private sector. However, individuals and SMEs are often insufficiently aware of the risks associated with cybercrime and the relatively simple steps they can take to better protect themselves. The Ministry of Justice and Security is working with the Ministry of Economic Affairs and Climate Policy and private-sector parties to take steps to support consumers and SMEs. It is essential to focus extra attention on reaching reach specific groups effectively. Steps are also being taken to improve hardware and software security.

Investigation, prosecution, sanctions and disruption

Criminal enforcement is one of the government’s core tasks, including in the digital domain. Improvements in criminal enforcement remain necessary in order to protect victims (and potential victims) and to ensure that crime doesn’t pay. The High-Tech Crime Unit of the Central Unit of the National Police now has 120 members of staff. The police are also working to strengthen cybercrime teams in their Regional Units. The Public Prosecution Service has specialised capacity for investigating and prosecuting cybercrime at both the National Public Prosecutors’ Office and the Regional Public Prosecutors’ Offices. However, the current nature and scope of cybercrime, as well as its expected impact, require additional capacity and strengthening of criminal justice expertise, as well as appropriate powers. Where identifying and apprehending cybercriminals proves difficult, criminal activities will be disrupted – including through the application of new statutory powers set out in the Computer Crime III Act. This includes infiltrating servers and taking them offline. Disrupting activities is not only a case-specific response; it is also part of the wider strategy to combat cybercrime. Where necessary, proposals will be developed to adapt national and international legal frameworks. In addition, private parties will be consulted to make it harder for criminals to carry out their activities via legitimate service providers. To limit repeat offending, it is also vital that interventions targeting perpetrators of cybercrime be adapted to the risk factors that are relevant to them.

Focus on victims
Unfortunately, it is impossible to entirely prevent people from falling victim to cybercrime. However, the government can offer support and help ensure that people aren't targeted repeatedly. Steps are being taken to provide support that minimises the impact of cybercrime. When it comes to many forms of cybercrime, people and organisations are often not aware that their systems have been compromised by criminals or are being used for criminal activities. It is therefore important to have proper notification procedures in place, both to inform the victims of cybercrime and to prevent future victims. Notifying victims quickly can help limit the damage. It can also have a disruptive effect on the criminal activities themselves. Furthermore, improving the procedure for reporting cybercrime will make it simpler for victims to contact the police.

Academic research
Cybercrime has been around for some time now, and is the subject of research studies. However, more academic insight into the topic is needed, particularly with regard to the perpetrators and victims of the many common forms of cybercrime. As a result, a wide-ranging research programme has been launched, with the Ministry of Justice and Security commissioning various studies in this area.

Financial matters
The 2018 central government budget includes a structural €6 million increase for policing. This money will be used for a limited expansion of capacity and to improve IT resources for digital investigative activities. The Public Prosecution Service will receive a €1 million structural spending increase, which will be used for a limited expansion of capacity. In addition, €3.5 million will be set aside for the establishment of a Digital Trust Center. The government's coalition agreement, 'Confidence in the Future', sets out investments in cybersecurity across various ministries. For the Ministry of Justice and Security this will mean a structural investment of up to €16 million. This includes a €10 million structural investment for the implementation of the Computer Crime III Act. The remainder will be invested in measures to enhance cybersecurity, which will also have a preventive impact on cybercrime. In addition to these specific budget items, investments will be made in relevant organisations. The coalition agreement sets out investments in the police force and the criminal justice system, for instance. The amounts set aside for this will be used in part to strengthen the approach to combating cybercrime and its knock-on effects.

Conclusion
The internet continues to develop at a rapid pace, often in a haphazard manner. As a result, it is difficult to predict how cybercrime will evolve. In addition, private parties are vital to any effective approach. Flexibility, cohesion and cooperation are our guiding principles in this regard. In the period ahead, measures will be developed with private parties. Frequent modifications will be needed to keep pace with changes in the forms cybercrime takes, and to incorporate research findings and the outcomes of consultations with public and private partners. The public task of combating cybercrime is an ongoing one. In the years ahead it can be expected that new measures will prove necessary, or that the practices we employ will need to be adjusted. The Ministry of Justice and Security will continue to consult with various public and private parties about their vision on cybercrime and the best ways of jointly tackling it. Only a flexible, joint approach will ensure that we can continue to deal with cybercrime effectively in the future.

Annexe – measures by focus area

Prevention

Flexible prevention campaigns that can be introduced quickly
When criminals develop new methods, it is important to disseminate information about potential countermeasures widely and rapidly.. Depending on the specific criminal methods in question, countermeasures and communications may need to be adapted. Together with private parties, insights based on research and behavioural science can be used to assess which core messages are most effective for a wide audience, or where a campaign targeting a specific group is more appropriate. This also requires core messages to be closely coordinated and streamlined.

Supporting SME security
The private sector is being subjected to digital attacks more and more often, and tailored support is required. The motion submitted by MP Maarten Hijink[10] calls for the establishment of a Digital Trust Center (DTC) to increase the private sector's resilience. The aim of the DTC is to enable Dutch businesses to increase their resilience to cyberattacks. In addition, in 2016 the National Crime Prevention Platform commissioned sector-specific studies, and businesses were offered free security checks.

Support provided by municipalities and regional Business Security Platforms
Municipalities often have insight into how prevalent crime is locally and the options available to tackle it. The Ministry of Justice and Security is supporting pilot initiatives by municipalities and Business Security Platforms (PVOs) which are expected to be used in other regions and municipalities, in a form that is adapted to the local situation.

Digital hardware and software security
It is important for products to be digitally secure. The Ministry of Economic Affairs and Climate Policy is working with the Ministry of Justice and Security to draw up a roadmap for digital hard- and software security. The roadmap is expected to be presented to the House of Representatives in spring 2018.[11]

Investigation, prosecution, sanctions and disruption

Strengthening the approach taken by the police and in the criminal justice system
During the previous government's term, the police began creating cybercrime teams within its Regional Units. The current government is increasing this investment in the police and in other partners in the criminal justice system. This involves expanding capacity and expertise in the areas of information provision, preventing and disrupting cybercrime, and strengthening cooperation with private parties. Investment in capacity goes hand in hand with enhancing IT support.

Increasing awareness among web hosting services
In consultation with the Ministry of Economic Affairs and Climate Policy, the private sector has launched the Abuse 2.0 project. It focuses on establishing links with market parties so they recognise different types of cybercrime more quickly and share this information with one another, enabling private parties to introduce measures themselves. Through their involvement in the project, businesses reduce their risk of facilitating cybercrime.

Disrupting criminal revenue models
Efforts to disrupt criminal revenue models – even in cases where prosecution is unlikely – help ensure that crime doesn't pay. In order to do this, emerging criminal methods are analysed, often through public-private cooperation, and

[10] Parliamentary Paper 26643, no. 473, 13 June 2017.
[11] Parliamentary Paper 26643, no. 507, 7 December 2017.

studies are carried out to see what interventions will make life as difficult as possible for criminals.

Strengthening national legislation
The Computer Crime III Bill is currently being considered by the Senate of the States General. From 2019, €10 million will be made available annually for its implementation. The new act will be evaluated two years after it enters into force. In addition, in the coming period an assessment will be made as to whether additional statutory measures are required.

International cooperation
When investigating cybercrime, international cooperation is essential. Within the European Union and the Council of Europe, steps are being taken to improve the procedures underpinning international cooperation, including legal assistance.

Strengthening international legal frameworks
In recent years, the Netherlands has led the way in improving international frameworks for online investigation and will continue these efforts, both in the EU and the Council of Europe. These frameworks should help make gaining access to electronic data faster and more efficient.

Tackling young perpetrators/potential perpetrators and limiting reoffending
Together with organisations including the police, HALT and the Child Protection Board, steps are being taken to explore which interventions can be used to put young offenders and young people at risk of offending back on the right track – and keep them there. Furthermore, the government is working with the Dutch Probation Service and others to determine whether a different approach is needed to reduce the risk of cybercriminals reoffending. Examples include different forms of supervision.

Improving the reporting procedure
Victims are less willing to report cybercrime than traditional types of crime. The police plan to make it possible to report certain types of cybercrime online, in order to make it easier for victims to report offences.

Focus on victims
Notifying victims and limiting damage
Measures to strengthen the organisations in the criminal justice system include a focus on improving communication with victims, who may be individual members of the public or organisations. Actively notifying victims and recommending courses of action can limit the damage and, at the same time, help disrupt criminal activities. Victims targeted by botnets or ransomware, for instance, can respond by disinfecting their own systems and ensuring that they cannot be used to target new victims. The website www.nomoreransom.org is a good example of a source of helpful information about a common form of cybercrime.

Academic research
In order to strengthen academic knowledge of cybercrime and improve future policymaking, studies will be carried out in the following areas:

- the nature and scope of cyber (and cyber-enabled) crime
- victims of cyber (and cyber-enabled) crime
- disruption of cyber (and cyber-enabled) crime
- a criminal-law approach to cyber (and cyber-enabled) crime.