Ministry of Security and Justice

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Our reference
708641

To the President of the House of Representatives
of the States General
Postbus 20018
2500 EA DEN HAAG

Date 4 January 2016
Subject Cabinet's view on encryption

Cabinet's view on encryption

Please find below the cabinet's view on encryption. This is in line with promises made during the debate of the standing committee on Economic Affairs on the Telecommunications Council of10 June 2015 (TK 2014-2015, 21501-33, no. 552) and the debate of standing committee on Security and Justice on the JHA Council of 7 October 2015.

Introduction

Encryption is increasingly easy to obtain and use and is thus more often part of regular data transactions. Encryption is increasingly applied by the government, companies and citizens to protect the confidentiality and integrity of their communication and stored data. This is important for people's confidence in digital products and services and for the Dutch economy in the light of a fast developing digital society. At the same time, encryption inhibits the acquisition of information required for investigation, intelligence and security services when malicious actors (such as criminals and terrorists) use it. The recent attacks in Paris, where encrypted communication may have been used by the terrorists, lead to the justified question what investigation, intelligence and security services need to have and retain good insight into the planning of attacks.

The ambiguity described in the preceding paragraph was also heard in the public debate of the last few months about the dilemmas of the use of encryption. The topic was also discussed in your House. During the debate of the standing committee on Economic Affairs on the Telecommunications Council the question was asked what the cabinet is planning to do to encourage the use of strong encryption. Additionally, the House of Representatives requested the cabinet to adopt a view on encryption.

The importance of encryption for the system and information security of the government and companies and for the constitutional protection of privacy and the confidentiality of communication is discussed below. The importance of detection of serious crimes and protection of national security are also included. Finally, a conclusion is reached after all interests have been assessed.

The situation in the Netherlands cannot be seen separately from its international context. Strong encryption software is increasingly available worldwide or an integral part of products or services. Considering the wide availability and application of advanced encryption techniques and the cross-border nature of data transaction, room for national action is limited.

The importance of encryption for the government, companies and citizens

Cryptography plays a key role in the technical security in the digital domain. Many cybersecurity measures in organisations are strongly based on the application of encryption. The secure storage of passwords, the protection of laptops against loss or theft and the secure storage of backups are more difficult without the use of encryption. The protection of data sent via the internet, for instance in internet banking, is only possible with the use of encryption. Due to the interconnectedness of networks, worldwide branching and the different routes communication can take, the risk of interception, infringement, perusal or modification of information and communication is always present.

The government increasingly communicates digitally with citizens and provides services whereby confidential information is exchanged, such as the use of a digital ID (DigiD) or filing a tax return. As formulated in the Coalition Agreement, citizens and companies must be able to arrange and settle their government affairs fully digitally from 2017 onwards. It is the duty of the government in that respect to make sure that this information is protected against third party examination; encryption is indispensable in that respect. The protection of the internal communication of the government also depends on encryption, for example with regard to the security of diplomatic and military communication.

Encryption is essential for companies to securely store and send company information. Being able to use encryption strengthens the international competitive position of the Netherlands and contributes to an attractive business and innovation climate for, for example, start-ups, data centres and cloud computing. Confidence in secure communication and data storage is essential for the (future) growth potential of the Dutch economy, which is mainly in the digital economy.

Encryption supports the respect of personal privacy and confidential communication of citizens because it offers them a means to protect the confidentiality and integrity of personal data and communication. This is also important for exercising the freedom of expression. It enables citizens, but also professions with an important democratic function such as journalists, to communicate confidentially.

Encryption therefore enables all parties involved to ensure the confidentiality and integrity of communication and to better defend themselves against espionage and cybercrime. Fundamental rights and freedoms, security and economic interests benefit from this.

Encryption and the investigation, intelligence and security services

The powers and resources available to the services must be suited for the current and future digital reality. The investigation, intelligence and security services support the security of the digital and physical world with effective, lawful access to information. Where encryption is applied by malicious actors, it hinders the access to that information for the investigation, intelligence and security services.

They experience this for instance when they investigate the distribution and storage of child pornography, support military missions abroad, counter cyberattacks or when they want to gain and retain insight into the preparation of terrorist attacks. Criminals, terrorists and opponents in armed conflict are often aware that they might attract the attention of the services at some point in time and nowadays also have access to advanced encryption methods which are difficult to circumvent or break. The use of such methods requires little technical knowledge, as encryption is often an integral part of the internet services which they can use. That complicates, delays or renders it impossible to (timely) gain insight into the communication for the benefit of protecting national security and investigating criminal offences. Additionally, the investigative hearing at the trial and the case for a conviction can be seriously obstructed.

The right to respect for personal privacy and privacy of correspondence of citizens

As noted before, the use of encryption helps citizens secure their personal privacy and the confidentiality of their communication. The aforementioned lawful access to information and communication by the investigation, intelligence and security services however infringes on the confidential communication of citizens.

Privacy of communication relates to the constitutional respect for personal privacy and the right to protection of the privacy of correspondence, telephone and telegraph (hereinafter: 'privacy of correspondence'). These fundamental rights are rooted in Sections 10 and 13 respectively of the Constitution. These fundamental rights have also been laid down in Article 8 ECHR and Articles 7 and 8 of the EU Charter (to the extent it touches on EU Law).

The protection of fundamental rights applies to the digital world. The aforementioned constitutional and international law provisions together are the parameters for preventing illegal infringement. The rights mentioned are not absolute, which means that restrictions are allowed as long as they meet the requirements of the Constitution and the ECHR (and the EU Charter where EU law is concerned). An infringement is allowed if it serves a legitimate purpose, if it is regulated by law and if the restriction is foreseeable and known. The restriction must also be necessary in a democratic society. Finally, the infringement must be proportional, which means that the objective sought by the government must be proportionate to the infringement of the personal privacy and/or the privacy of communication.

These requirements are the parameters within which the balance can be decided between the interests at stake with encryption, such as the right to personal privacy and privacy of correspondence, public and national security and the prevention of criminal offences. To the extent it concerns the special powers of the intelligence and security services, the preceding assessment parameters have also been laid down in the Intelligence and Security Services Act 2002 (Sections 18 and 31). The obligations to cooperate regarding decryption that are included in the Intelligence and Security Services Act 2002 (Articles 24 (3) and 25 (7)) and in the Dutch Criminal Code (Article 126m (6)), may be invoked if associated special powers are exercised after an assessment as previously specified.

Assessment and conclusion

Nowadays the possibility to break encryption is decreasing. The possibility to obtain unencrypted information from a service provider is less often available.

Service providers increasingly process information that has already been encrypted through modern applications of encryption when it reaches them. Considering the importance of the investigation and prosecution of criminal offences and the interests involved in national security, these developments require a search for new solutions.

There are currently no options in a general sense, e.g. via standards, to weaken encryption products without compromising the security of digital systems that use encryption. For instance, introducing technical access into an encryption product would make it possible for investigation services to inspect encrypted files, digital systems can become vulnerable to, for instance, criminals, terrorists and foreign intelligence services. This would have undesirable consequences for the security of communicated and stored information and the integrity of IT systems, which are increasingly important for the functioning of society.

For the performance of their statutory tasks, the investigation, intelligence and security services partly depend on cooperation with providers of IT products and services. Given this dependency, consultation with providers is needed about effectively providing information when their services are used by malicious actors, while taking into account to everyone's role and responsibilities and the statutory parameters.

Given the preceding assessment, the following conclusion is reached:

It is the responsibility of the cabinet to guarantee the security of the Netherlands and to investigate criminal offences. The cabinet underlines the necessity of lawful access to information and communication in this respect. Additionally, government authorities, companies, and citizens benefit from maximum security of digital systems. The cabinet endorses the importance of strong encryption for internet security to support the protection of personal privacy of citizens, for confidential communication of the government and companies and for the Dutch economy.

The cabinet is therefore of the opinion that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands. The Netherlands will disseminate this conclusion and the underlying assessment internationally. As regards the stimulation of strong encryption, the Minister of Economic Affairs will follow up on the purport of the amendment (TK 2015-2016, 34300 XIII, no.10) on the budget of the Ministry of Economic Affairs.

Minister of Security and Justice,

G.A. Van der Steur

Minister of Economic Affairs

H.G.J. Kamp