Letter of 1 July 2019 from Minister of Justice and Security Ferdinand Grapperhaus and State Secretary for Economic Affairs and Climate Policy Mona Keijzer to the House of Representatives on measures to protect telecom networks and 5G

Introduction

We are writing to the House in our own capacity and on behalf of the Minister of the Interior and Kingdom Relations. In today's society, digital connectivity is vital. We are making increasing use of the internet, on both desktop and mobile devices. The Netherlands has high-quality telecommunications infrastructure,[1] including several mobile 4G networks and two fixed-line networks. These networks, which have been designated 'vital processes', contribute significantly to the favourable enterprise and business climate in the Netherlands. It is important that we retain this strong position in the future. This is in keeping with the current government's ambition to become the European leader in the digital domain. To achieve this, the rollout of 5G networks is required. Telecom companies are preparing for new applications that make use of 5G. These include self-driving cars, medical procedures carried out remotely, and the further optimisation of production processes. These 5G networks will have higher top speeds and quicker response times than the 4G networks. 5G networks do not operate in isolation; rather, they build on existing networks.[2]

Some concerns exist, in parliament and elsewhere, regarding the risks relating to the rollout of 5G and, in particular, the suppliers of the technology driving these telecommunications networks. The House has submitted several motions on this topic, which stress the urgency of tackling the issues in question and the need for a coordinated approach at EU level.[3] The House also asked the government to respond to the articles *'Experts: angst voor gluurgevaar uit Asia is terecht'* ('Experts say we're right to be worried about spy threat from Asia') and '*VS waarschuwt providers in andere landen voor Huawei*' ('US warns providers in other countries about Huawei').[4] In addition, during a debate on the business of the House on 3 April 2019 (Proceedings of the House of Representatives, 2018-19, no. 70), MP Jesse Klaver (Green Left Alliance) requested a debate on a range of issues, including the rollout of 5G, before any irreversible decisions are made.

This letter provides more information on these motions and requests from the House and informs the House about the outcomes of the work performed by the Economic Security Task Force, in line with commitments made to the House.[5]

National security and 5G

As the House has previously been informed, the government shares the House's concerns with regard to the increasing risks and threats presented by state actors.[6] In their most recent annual reports, the intelligence and security services also referred to the threats posed by espionage and sabotage on the part of state actors. In recent years, the General Intelligence and Security Service (AIVD) and the Defence Intelligence and Security Service (MIVD) have noticed an increase in the number of supply chain attacks by state actors. In various publications, both public and classified, the AIVD and the MIVD have responded, on the basis of the information they have obtained, to the threats posed by state actors. These publications have looked specifically at the telecom sector, with a particular focus on the potential risks that the introduction of 5G poses to national security. Supply chain attacks involve using service providers, such as ISPs, telecom providers and managed service providers, as springboards in order to infiltrate organisations, which are the real

[1] European Commission (2018), The Digital Economy and Society Index (DESI).

[2] European Commission (2019), Recommendation on Cybersecurity of 5G networks.

[3] Motion submitted by MP Arne Weverling et al. (Parliamentary Paper 21 501-33, no. 734) and motion submitted by MP Joba van den Berg et al. (Parliamentary Paper 21501-33, no. 747), Motion submitted by MP Arne Weverling et al. (Parliamentary Paper 24 095, no. 471) and motion submitted by MP Sjoerd Sjoerdsma et al. (Parliamentary Paper 24 095, no. 476).

[4] 28-11-2018, ref. 2018Z22045/2018D57007.

[5] Letter to the House of Representatives of 1 April 2019, Response to reports that KPN is working with Huawei to build 5G networks.

[6] Letter to the House of Representatives on state threats (Parliamentary Paper 30 821, no. 72) and the National Cybersecurity Assessment 2019.

targets of the attack. The providers' hardware and software is then used to gain access to the organisations' networks. Using providers' hardware and software in this way is an attractive option for state actors, because it provides wide-ranging, in-depth, regular access to data and data streams held within the organisations' networks. This presents opportunities for espionage, in the form of gathering personal, technical, scientific, financial, economic, military, political and administrative data on a large scale from public, military and private organisations.

The AIVD and MIVD have observed that espionage by state actors is being facilitated by the infiltration of service providers. There is an associated risk that malicious actors could become ensconced in the Netherlands' critical infrastructure. This could enable the disruption of critical infrastructure management and control systems that are connected to the internet, such as those governing the water supply, electricity distribution and financial transactions. In addition, various countries have legislation in effect that compels service providers to cooperate with intelligence activities. In such cases, state actors make use of the service provider's legitimate ability to access the networks of the organisations being targeted, which makes preventing and detecting such abuses more difficult. The risks to national security increase significantly if these service providers also happen to be from countries that have an offensive cyber programme that targets Dutch interests.

5G is expected to facilitate a significant increase in the amount of hardware and software that is connected to the internet, not only in people's personal lives, but also in the commercial, defence, government and critical infrastructure sectors. This means that the smooth functioning of Dutch society will become increasingly dependent on 5G. As a result of this dependence, Dutch society, as a whole, will become increasingly vulnerable to digital espionage and sabotage. The introduction of 5G thus poses substantial risks to individual privacy and the confidentiality of sensitive information held by businesses and governments. In addition, the continuity and availability of the private sector and critical infrastructure, and of both local and central government service provision, are at stake. This could potentially lead to large segments of the Dutch population being 'cut off'.

Economic Security Task Force: methodology and findings

Because of this threat, the National Coordinator for Security and Counterterrorism (NCTV) established an interministerial Economic Security Task Force comprising representatives of the Ministries of Justice and Security (NCTV); Economic Affairs and Climate Policy; the Interior and Kingdom Relations; Foreign Affairs (including foreign trade and development cooperation staff); Defence; and Finance, as well as the AIVD and MIVD to advise on this issue.[7] In terms of its composition and activities, the Task Force is set up in such a way as to allow balanced decision-making that takes account of security-related and economic interests. The advice of the Task Force is based in part on AIVD and MIVD analyses (including threat analyses). The measures proposed by the Task Force, which are supported by all parties, provide an appropriate response to the threat in question.

In collaboration with the Netherlands' three main telecom service providers (KPN, T-Mobile and VodafoneZiggo), the Task Force has carried out a risk analysis to establish how vulnerable Dutch telecommunications networks are to infiltration through technology service providers. Telecom providers are already taking a range of steps to combat such infiltration. On the basis of this analysis, telecom providers will be obliged to put additional security measures in place in order to increase resilience to the aforementioned threat.

One of the measures to be put in place will be extra stringent requirements for providers of products and services in critical parts of the telecom network. These critical parts have been identified on the basis of the risk analysis. These measures will further reduce telecom networks' vulnerability to abuse via providers of technology. The more stringent security and integrity requirements that mobile telecommunications networks must meet will be set out in a general order in council, to be published this autumn. Due to risks to national security, the House will be informed of the Task Force's findings in more detail in a confidential setting.

[7] Letter to the House of Representatives of 1 April 2019, Response to reports of that KPN is working with Huawei to build 5G networks.

5G networks will build on current networks. This means that risk analysis concerning current networks is also of significance for future 5G networks. A system-wide approach is needed for a variety of reasons: the threat situation is constantly changing; technological advances within the telecom sector are proceeding at rapid pace; and there is a need for solid insight into the technical and other aspects of telecom networks in order to identify where measures are needed. In cooperation with telecom providers, a formal procedure is being established whereby technical and threat-related developments will be considered in conjunction with one another, in line with current roles and responsibilities. Due account will be taken of economic considerations, in so far as they do not jeopardise national security.

The government supports a joint European response

The security of 5G telecommunications networks is on the European agenda. A European approach can contribute to the effectiveness of the measures. As indicated in the National Cybersecurity Agenda (NCSA),[8] the cross-border nature of cybersecurity means that international cooperation is necessary, whether in the form of legislation, coalitions or the establishment of standards. As a result, in accordance with the motions submitted by MPs Arne Weverling and Joba van den Berg,[9] the government is pushing for greater European cooperation in the area of 5G security. The government is therefore pleased that the European Commission is tackling this issue in a number of ways, including its Recommendation on Cybersecurity of 5G networks of 26 March 2019.[10]

The government therefore also supports a joint European approach, which will be fleshed out by way of this recommendation. The added value of such an approach lies mainly in the fact that it allows for the sharing of risk analyses and potential solutions between member states. The Netherlands will actively contribute to the European programme that results from this recommendation and share its experiences in this regard. The recommendation proposes that, by the end of 2019, the EU programme should result in a set of instruments that contains measures to tackle risks identified at both European and national level. The BNC file (drawn up by the Working Group for the Assessment of New Commission Proposals) which sets out the government position in detail, will be sent to the House separately.

Conclusion

As the House has been informed, addressing the concerns surrounding vulnerabilities in the telecom sector is part of a wider approach to tackling threats from state actors and promoting cybersecurity.[11] In addition to the telecom sector, there are also concerns that state actors may represent a threat to other vital services and processes. When it comes to assessing national security risks in relation to critical infrastructure, the government feels strongly about using consistent, technically up-to-date, threat-based criteria and, in light of the need to anticipate new developments as soon as possible, having a clear sense of how the Netherlands' critical infrastructure is developing from a technical and organisational perspective. As set out in the National Security Strategy, the government will therefore, in conjunction with all these parties, enhance its approach to protecting critical infrastructure. This involves creating a framework that brings together knowledge, know-how and expertise in order to suitably address national security risks to critical infrastructure, both now and in the future.[12]

[8] National Cybersecurity Agenda (Parliamentary Paper, 26 643, no. 536).

[9] Motion submitted by Arne Weverling MP et al. (Parliamentary Papers 21501-33, no. 734) and motion submitted by Joba van den Berg MP et al. (Parliamentary Paper 21501-33, no. 747).

[10] European Commission (2019), Recommendation on Cybersecurity of 5G networks.

[11] Letter to House of Representatives on state threats (Parliamentary Paper 30 821, no. 72) and the National Cybersecurity Agenda (Parliamentary Paper 26 643, no. 536).

[12] National Security Strategy 2019, submitted to the House of Representatives on 7 June 2019.