Ministerie van Economische Zaken

> Retouradres Postbus 20401 2500 EK Den Haag

De voorzitter van de Tweede Kamer der Staten-Generaal
Binnenhof 4
2513 AA 's-GRAVENHAGE

Datum
Betreft Verwerven van overwegende zeggenschap in een telecommunicatiebedrijf dat beschikt over vitale telecommunicatie-infrastructuur

Dear Madam President,

With this letter, on behalf of myself and the Minister of Security and Justice, I am meeting a commitment to consider whether supplementary provisions are necessary to effectively safeguard public interests in general, and national security in particular, in the event of a takeover of a telecommunications company like KPN. This commitment arises from a Letter to Parliament (TK 2012-2013, 24095, no. 356) and answers to parliamentary questions (TK 2013-2014, nos. 534 and 535) set around the time of the attempted buy-out of KPN by América Móvil in 2013 and the parliamentary committee meeting on telecommunications on 30 January 2014.

1. Introduction
Dutch telecommunication resources are among the best in the world. The high quality of the facilities is to a large extent attributable to the smooth operation of the Dutch telecommunications market. Foreign investment plays an important role in this market. Without foreign investment it would not be the competitive market we have today. For example, two of the current three large companies in the field of mobile communications are part of a foreign concern and the majority of KPN shares are in foreign hands. The same applies to the large cable companies.

Thanks in part to the broad availability of good telecommunication facilities people now rely heavily on the smooth operation of the telecommunications infrastructure and associated service provision. In view of this reliance, the question logically arises as to what a takeover of a telecommunications company, particularly such an important infrastructure player as KPN, would mean in terms of safeguarding public interests. The House was informed in September 2013 of the attempted buy-out of KPN by América Móvil (TK 2012-2013, 24095, no. 356). In that letter the Government concluded that in general public interests are adequately protected by existing legislation. Public interests such as freedom of choice, value for money and innovation, including investment in the continuity and quality of networks, are best guaranteed by a fully functioning and competitive telecoms market. To ensure the smooth operation of the telecoms market, the Consumer

and Market Authority (ACM) monitors compliance with the Telecommunications and Competitive Trading Acts. Monitoring of mergers by the ACM under the Competitive Trading Act safeguards competition in the market following any takeover of KPN or another company. In this way sufficient incentives remain for investment in sustainable high-quality networks and services at competitive prices.

As well as the above concerns, there are interests of national security at stake in the telecommunications sector. This refers primarily to the potential failure and/or misuse of telecommunications infrastructure. For legal reasons telecoms companies are also provide information to the Dutch intelligence and investigation services, while networks are used to send confidential information. These national security aspects are broadly addressed by the Telecommunications Act, the 2002 Intelligence and Security Services Act and the Security Screening Act. The aforementioned letter on the attempted buy-out of KPN also indicated that, in the specific case of a takeover of KPN by a party exercising undue influence, there might be implications for national security. This letter looks in more detail at such a specific case.

In the context of this letter it is good to be aware that agencies acting on behalf of states seeking improper access to information, in addition to acquiring control of telecoms companies, can also use the resources of the intelligence services (for example in influencing hardware suppliers) to facilitate digital espionage. This also applies to bringing in cybercriminals to access to certain information by exploiting security gaps in hardware and software. This underlines the importance of policy already initiated to reinforce the reliability and integrity of networks and services, as set out in the National Cybersecurity Strategy (TK 2013-2014, 26643, no. 291) and the Vision on Telecommunications, Media and the Internet (TK 2013-2014, 26643, no. 300). An important aspect of this policy is the management of risks arising from the infiltration of networks via compromised hardware. We are working with the sector to obtain greater insight into risks associated with hardware or software tools and possible countermeasures.

2. Developments

As already mentioned, foreign investment plays an important role in the Dutch telecommunications sector. Until now this investment has come largely from European and North American players who invest for commercial reasons. However, with the shifting balance of economic power in the world there are now more takeovers that are geopolitically motivated[1]. In those specific cases current legislation and regulations, or their enforcement, may be inadequate, as players are acting not out of commercial interests but more on geopolitical or ideological

[1] AIV (2013), *Azië in opmars. Strategische betekenis en gevolgen* (Asia on the rise. Strategic significance and implications)

grounds[2]. This can apply to foreign state-run companies or parties attached to foreign governments or to political-ideological organisations. This can present risks to the operation of vital telecommunications infrastructure and so to national security in the Netherlands. Due to the heavy reliance of the current information society on ICT, large-scale failure of telecoms networks has consequences not only for the operation of the telecommunications sector, but also for other potentially vital sectors in Dutch society. It is against this background that telecommunications resources have taken on vital significance. Changing geopolitical trends, and greater political attention [3] to a broader consideration of public interest (including national security) have caused us to reconsider whether current safeguards are adequate to protect national security if parties operating partly out of geopolitical motives gain overriding control of vital telecommunications infrastructure.

3. Potential risks

To answer the question of whether current safeguards are adequate to protect national security if parties operating partly out of geopolitical motives gain overriding control of vital telecommunications infrastructure, and pursuant to the letter on *Staatsfondsen* (Government securities), (TK 2007-2008, 31350, no. 1), two types of risk are considered: geopolitical and security risks.

(1) Geopolitical risk: hostile action with risk to continuity

It is possible that a party operating out of geopolitical motives could use its controlling interest in a company as a political instrument. The company in which the interest is taken is relevant, because of the possibility of control of vital telecommunications infrastructure being used to exert pressure on the Dutch government. This can be done, for example, by (a threat of) hostile action, such as shutting down all or vital parts of the telecommunications infrastructure. Control in this case acts as an instrument of power. This risk arises mainly when there are insufficient means of substitution of vital telecommunications infrastructure in the short term, and there is also the possibility of gaining a controlling influence in a company that does possess such non substitutable infrastructure. That is specifically the case for KPN. KPN owns a significant proportion of the telecommunications networks in the Netherlands. The operations of other telecoms providers and vital government services are partly dependent on these same networks.

(2) Security risk: access to knowledge and information

The first security risk is the potential breach of confidentiality of the content of the communication on telecommunications networks. The second security risk concerns potential breach of confidentiality of the methodology of the security and investigation services with regard to data retrieval and authorised tapping of

---

[2] SER (2012), *Verschuivende Economische Machtsverhoudingen* (The shifting economic balance of power)

[3] Including the Parliamentary Committee on privatisation of government services

telecommunications traffic. This confidentiality of information can come under pressure if a party acting out of geopolitical motives obtains a controlling influence in important infrastructure. This form of control can make it easier to access sensitive knowledge and information. This affects national security specifically where confidential State information is concerned. KPN holds a special position when it comes to the delivery of vital government services.

Continuity of provision of vital government services by KPN
KPN has a special position with regard to a number of services that are important for the proper functioning of government and for national security. This point also came to the fore in relation to the América Móvil takeover bid for KPN (TK 2012-2013, 24095, no. 356). Examples include current service provision for C2000 and services such as emergency communications service provision (NCV) and communications service provision to the Ministry of Defence, including the Netherlands Armed Forces Integrated Network (NAFIN). KPN also provides the Diginetwerk[4]. Many of these services are supplied by KPN itself. In most cases where services are contracted to other parties, they use the KPN network. This reliance on the network could threaten the continuity of the service provision referred to above if KPN decided to stop providing the service. It is therefore important to ensure that KPN, irrespective of the identity of its shareholders, continues to provide the services concerned or in any case until other parties can, if necessary, take over the service provision in due course.

4. Current regulations
This paragraph considers the extent to which the risks referred to in §3 are covered by existing legislation and regulation. We start with the continuity risks as outlined in §3 (1), and more specifically the continuity of provision of vital government services. Next we discuss the two security risks outlined under (2).

Geopolitical risk and continuity of service provision by KPN
Based on chapter 9 (universal service) of the Telecommunications Act (TW) consumers are guaranteed a minimum range of telecommunications services. Chapter 11a of the Act requires suppliers of public electronic communication networks and services to take measures to control the security and integrity of their networks and services. Breaches of security and integrity are seen within the framework of chapter 11a as risks to the continuity of service. Based on chapter 11a the Minister of Economic Affairs can require a supplier of networks and services to take technical and organisational measures within a specified time in relation to the security and integrity of the network and the services offered. With regard to geopolitical risks, chapters 9 and 11a cannot prevent a malicious party who has gained overriding control from using the issue of continuity or lack of continuity of the service provision to put pressure on the government. If the

[4] Network for communication between authorities which plays a central role in information exchange between government and citizens and government and companies

requirement to provide certain basic services under chapter 9 is not met, a penalty can be imposed, but that is not enough to scare off a party with malicious intent. The options for intervention by the Minister of Economic Affairs under chapter 11a do not extend to preventing the supplier from ceasing to provide certain services. For example, it is not possible under chapter 11a to force KPN to continue to provide vital services to the government. In the event that disruption of continuity leads to very serious social disruption – known as extraordinary circumstances, the Minister of Economic Affairs can issue instructions to the telecommunications supplier under section 14.2 of the Telecommunications Act. Here too such instructions may have a limited effect if the party concerned acts with evil intent.

Confidentiality of communication
Sections 11.2 and 11.2a of the Telecommunications Act concern the protection of confidentiality of communication via electronic communications networks. Section 11.2 imposes a duty of care on suppliers of electronic communications networks and services. Such suppliers must ensure that personal data and the personal life of their subscribers and users of their network and service are protected. Section 11.2a, in brief, prohibits tapping, storing, listening in or otherwise intercepting the communications via the networks or services. In the event of a breach of the duty of care or of the above prohibition, the ACM may impose a penalty. A party whose intention is to breach the confidentiality of communication would be able to use its influence to cover up any violations as far as possible. Furthermore, it cannot be ruled out that in such a case the penalties will not be an adequate disincentive, since normal commercial economic interests (damage to one's reputation) play a subordinate role.

Confidentiality of methodology of the security and investigation services
To prevent structural access to state secrets, it is possible to designate certain posts as confidential posts based on the Security Screening Act. Under this Act only people with the necessary security clearance can be appointed to these posts. The system of confidential posts, as the endpiece to the organisational and physical security measures, contributes to the confidentiality of the methods of the security and investigation services.

5. Policy response

In general public interests are adequately protected by existing legislation. As discussed, the specific case of parties with improper motives obtaining control of vital telecommunications infrastructure present certain risks to the continuity of networks and services and the security of information. A supplementary instrument is required to limit those risks whereby the acquisition of overriding control is assessed for its implications for national security. This instrument must adequately safeguard national security, without scaring off commercially motivated investment. This type of investment is necessary to maintaining a competitive and innovative telecommunications market in the Netherlands.

The envisaged instrument grants powers to the Minister of Economic Affairs enabling him, partly on the basis of security advice from the Ministers of Security and Justice (V&J), the Interior and Kingdom Relations (BZK) and Defence[5], to evaluate the national security implications of a party gaining controlling influence in vital telecommunications infrastructure. The powers are as follows:

- The option to designate as such (Dutch) legal entities that have control of vital telecommunications infrastructure. Currently KPN is eligible for this designation;
- To issue a declaration of non-opposition to acquiring a controlling interest in a designated legal entity. The Minister can revoke a previously issued declaration if there is a threat to national security; then the party concerned may no longer exercise their control. The Minister will issue a non-opposition declaration unless he has good reason to suppose that the acquisition of control by the party concerned threatens the security and continuity of the vital infrastructure concerned, and could thus pose a risk to national security;
- To issue a declaration of non-opposition in respect of a possible sale or resale of vital infrastructure of a designated company;
- To issue a declaration of non-opposition (based on an integrity test) in respect of the nomination of the management and supervisory board of a designated company and the option to revoke the declaration if there is a threat to national security. Control of the day-to-day operations of a company is exercised by the management. The supervisory board can also play an important role. Its role is all the greater if the legal entity to be designated is a "structured" (two-tier) company; in that case a large number of important decisions can only be taken with the prior agreement of the supervisory board. Under the full structural regime the supervisory board also has the power to appoint and dismiss directors.

Why have these powers been chosen? In the financial sector a declaration of non-opposition from the Minister of Finance or the Nederlandse Bank is already required for the acquisition for a certain degree of control in certain financial institutions and for the appointment of directors and supervisory boards of such institutions. In addition, some neighbouring countries, such as Germany and the UK, already have instruments for evaluating the national security implications of a takeover of telecommunications and other companies.
In other vital network sectors in the Netherlands, such as drinking water, gas, electricity and railways, the government is the owner the network via an wholly-owned subsidiary. This is because of the importance of these networks and the fact that the networks form monopolies (a single network). The reason that the telecommunications networks in the Netherlands are entirely in private hands, is that the telecommunications sector, unlike the other network sectors, does not have a monopoly on (the) infrastructure. In places there can be several infrastructures belonging to different providers working in parallel; in other words,

[5] This advice will in turn be based in part on an analysis carried out by the Intelligence and Security (I&V) Services

there is infrastructure competition. However, this is certainly not the case across the board: KPN is still the major network provider in the Netherlands and there are significant areas in which no alternative network is directly available. To prevent an undesirable controlling influence, one option would be for the government to reinvest in KPN. However, the Government is not considering this option. It would turn back the liberalisation of the telecommunications market and can distort the even playing field on that market. It would also require heavy investment by the State, while the envisaged legislation and regulations can adequately protect public interests. The option of linking far-reaching State control to a limited percentage of the shares (a so-called "golden share") is not in line with current Dutch legislation and there is too much uncertainty as to whether a golden share would be recognised in European law.
The chosen policy response in this context is in line with a sectoral elaboration of the conclusions and recommendations of the final report of the Working Group on Economic Security. The Minister of Security and Justice, also on behalf of the Minister for Foreign Trade and Development Cooperation and the undersigned, will inform the House on this matter concurrently with this letter.

Continuity of vital public service provision by KPN
The other point to be considered is safeguarding the continuity of a number of services procured by the government which are of vital importance for the proper functioning of the State, such as the provision of emergency communications (NCV) and services to the Ministry of Defence. The Government is making further contractual agreements on vital public services in consultation with KPN, making use of government-wide experience with the relevant (legal) provisions. The Government will also consider what legal guarantees are required to prevent stoppages in vital service provision before an alternative is available.

6. Follow-up

In elaborating the measures much attention will paid to testing them against the framework of European law, since the above measures have a bearing on the provisions on the internal market and the competition rules of the European Union. In the case of the internal market, this means that concrete measures must at all times be justifiable by reference to an applicable treaty exception (public order and public security) or to one or more compelling reasons of general interest.

The elaboration of the measures will also take account of the obligations of the Netherlands under the General Agreement on Trade in Services *(*GATS*)* and the principles, such as non-discrimination, transparency, proportionality and accountability, as referred to in the OECD guidelines for recipient country investment policies relating to national security.

I recognise the importance of providing clarity in the proposed Bill about the criteria and process surrounding the issue and revocation of non-opposition declarations so that market players know where they stand. This is also important for parties intending, even prior to the entry into force of the Act, to acquire such

Directoraat-generaal
Energie, Telecom &
Mededinging
Directie Telecommarkt

a large interest in a company to be designated that they will fall within the scope of the Act. After all, this instrument must strike a balance between safeguarding national security and continuing to attract commercial investment. It must therefore be clear to potential investors that the requirements and restrictions attached to shareholding in a designated company will not only apply to shareholders who obtain a certain interest after the Act enters into force. Market players will therefore be closely involved in the further elaboration [of the measures]. The Government intends to formalise the policy outlined in this letter in a Bill to be presented to the House in the Spring 2015.

Yours sincerely

Henk Kamp,
Minister of Economic Affairs