Appendix: key elements countering state threats

As discussed in the accompanying letter, our approach to countering state threats consists of a number of generic measures. Given the threat, the interests requiring protection and various recent incidents, the government will focus on the following elements in the period ahead:
(1) countering foreign interference targeting diaspora communities,
(2) protecting democratic processes and institutions, and
(3) economic security.
Some major steps have already been taken, and new issues have been identified that require an enhanced approach. This document outlines our approach to these issues, including the results of ex-ante analyses on economic security.

1. Countering foreign interference targeting diaspora communities

'Countering foreign interference targeting diaspora communities' refers to deliberate, often systematic and clandestine activities by state actors (or parties connected to state actors) in the Netherlands or aimed at Dutch interests, which could undermine the political and social system as a result of the goals being pursued, the means employed or the eventual effects.

Within our democracy, Dutch people – regardless of their ethnical or cultural background – must be free to make their own choices about how to live their lives, express their political preferences and maintain ties with their country of origin or that of their parents. Contacts between state actors and Dutch nationals should be transparent and voluntary in nature and should not lead to the export of tensions to Dutch territory or to a negative influence on social integration or a person's connection with Dutch society.

In the past year there have been various examples of foreign interference in diaspora communities about which the House of Representatives has already been informed.[1] The government's approach to foreign interference, about which the House has also been informed, is generic (i.e. country-agnostic) in nature.

On the basis of a shared, structured procedure, the relevant ministries and agencies maintain close contact, with a view to staying abreast of the problem. If necessary, they can decide to take coordinated action or scale up their efforts. A variety of tools are used to deal with incidents or impending incidents. These include monitoring the situation, exchanging information and taking measures related to public order and security. The government also has a variety of diplomatic measures at its disposal to counter foreign interference, including maintaining a dialogue with countries of concern or declaring a diplomatic representative to the Netherlands persona non grata.

The government is also taking measures to boost the resilience of certain municipalities and communities when it comes to foreign interference. These measures are intended to raise awareness and support municipalities and communities in developing plans of action to counter foreign interference that could impede integration.

Countering foreign interference remains a topical issue (as shown by the motion submitted by MP Bente Becker,[2] which you will be informed about before the summer, and financing as a modus operandi of state actors[3]). This is due in part to developments in other countries and changes in

[1] In the following instances, for example:
- The government's response to questions from MPs about reports that President Erdoğan of Turkey was seeking to campaign abroad for Turkish presidential and parliamentary elections in June (House of Representatives, 2017-2018, 2591).
- The government's response to questions from MPs about the news story 'Russische trollen ook actief in Nederland' (Russian trolls also active in the Netherlands) (Parliamentary Paper, no. 14250, submitted 7 September 2018).
- Letter on Iran sanctions, 8 January 2019, House of Representatives, 2018-2019, 35 000 V, no. 56.
- House of Representatives, 2018-2019, 32 735, no. 209.
- The government's response to questions from MPs about the news story 'So werden Erdogan-Kritiker in Deutschland per App denunziert' (This is how Erdoğan critics are being denounced by app) (House of Representatives, 2018–2019, Appendix).

[2] Motion submitted by MP Bente Becker et al., House of Representatives, 30 821, no. 56.

[3] Letter to parliament on a comprehensive approach to problematic conduct and undesirable foreign financing of religious and civil society organisations, House of Representatives, 2018-2019, 29 614,

migration flows. This warrants an ongoing commitment to this issue.

2. Protecting democratic processes and institutions

The second key element of the approach is countering efforts by state actors to undermine democracy and the rule of law. A number of steps are being taken to this end:

Countering political influencing by states

With regard to countering foreign interference, the government previously announced that it would be seeking to boost the resilience of political office-holders, particularly at local level. To that end we will be adopting a two-track approach: (1) protecting political office-holders (i.e. ensuring their safety and integrity) and (2) equipping them to effectively prevent efforts to undermine the democratic legal order (by increasing their knowledge, know-how and capacity to act). With a view to increasing the capacity to act and transparency in the political and governance domain, we will be exploring the scope for and desirability of introducing a policy of mandatory registration for lobbyists. A similar policy is already in place in the United States, Australia and Canada.

Safe and secure elections

Actions by state actors can damage the integrity of our political and governmental system if it compromises the independence of parliament, decision-making processes or the judiciary, or when doubts arise about the freedom, fairness or confidentiality of elections. A democratic society finds itself under pressure when interference engenders a lack of acceptance of the legitimacy of the government or fosters polarisation, the formation of enclaves or a lack of solidarity in society, or when intolerance is spread and freedoms are restricted. Under the coordination of the Minister of the Interior and Kingdom Relations, various ministries and operational and local partners bear joint responsibility for ensuring safe and secure elections. EU member states and institutions share their expertise within the European election network. In this connection the government is particularly interested in identifying signs and evidence of undesirable influencing and disinformation.

Countering disinformation

The dissemination of disinformation for the purpose of undermining the democratic legal order and destabilising society is a real threat. This threat mainly manifests itself online. In the government's view, addressing the issue of disinformation requires multiple parties in society (e.g. private individuals, the media and academia) to shoulder their responsibility.[4] The government's efforts in this regard are mainly focused on countering covert efforts by state actors (or parties connected to state actors) to influence public opinion. In deciding on an appropriate response, the government's top priority is safeguarding freedom of expression and a free press, democracy and the rule of law, and focusing on wider campaigns, rather than individual news reports. However, when there is a threat to economic or political stability or national security as a result of interference by state actors or related parties, a response by the government is justified.

Our multifaceted approach[5] involves taking measures that will ensure that we are prepared for disinformation, that we can recognise and interpret certain signals, that we can formulate options for a proportionate response and, if desired, carry them out without infringing on the above-mentioned freedoms.

Because disinformation is mainly an online phenomenon, it does not stop at the border. The Netherlands therefore attaches great value to international cooperation and knowledge-sharing in this area. In that regard, the Netherlands welcomes the European Action Plan on disinformation, as also discussed in the BNC assessment of 25 January 2019. In line with the Action Plan, the Netherlands is taking part in the European election network and the Rapid Alert System (RAS). In the European election network, member states and the EU institutions share knowledge and discuss the overarching approach to disinformation and protecting elections. The RAS brings together analysts and policymakers from EU member states and the StratCom Taskforces of the European External Action Service to share real time information on disinformation campaigns. The National Crisis Centre of the National Coordinator for Security and Counterterrorism (NCTV) serves as the national point of contact for the RAS; the Ministry of the Interior and Kingdom Relations plays a similar role for the European election network, to which all relevant ministries are connected.

---

no. 108.

[4] Letter to parliament from the Minister of the Interior and Kingdom Relations on disinformation and attempts to influence elections (13 December 2018).

[5] House of Representatives, 2018-2019, 30 821, no. 51.

The Netherlands is also a member of the informal International Partnership to Counter State-Sponsored Disinformation, which also includes the US, the UK, the Baltic states and the Nordic states. The purpose of the partnership is to share analyses and reports about the spread of disinformation and to facilitate cooperation with tech companies.

3. Approach to economic security

A third key element of the approach relates to economic security. Below are the results of the analysis of vulnerabilities in critical sectors and the additional administrative measures needed to further mitigate risks to national security in relation to economic security.

Sector-based ex-ante analyses

In the coalition agreement the government announced its aim of protecting critical sectors, after careful analysis of risks to national security. Such analyses pay particular attention to risks related to changes to corporate control.[6] Our goal is to identify potential risks to national security in individual vital sectors and to determine, on that basis, the extent to which the government's current set of instruments offers sufficient safeguards. Below I have set out the outcome of the sector-based ex-ante analyses with the House, thereby addressing the motions submitted by MP Joba van den Berg et al.[7] and by MP Dion Graus.[8]

It is clear from the analyses that virtually all critical sectors are in some way protected from hostile takeovers. The nature and extent of this protection does vary from sector to sector, however. A number of sectors fall under the control of the government. The Dutch authorities can therefore determine (to some extent) to whom and under what conditions a company may be sold, with due regard for national security interests. A number of sectors are protected by special legislation. The analysis of the telecommunications sector showed the existence of unaddressed risks in this sector with regard to changes in control. At a previous stage the government decided to take direct action on this front and has since submitted a bill on hostile takeover bids in the telecom sectors to the House for consultation.[9] Conclusions of the sector-based ex-ante analyses:

- The critical sectors, the police, the armed forces, the nuclear sector, public drinking water facilities, water defences and water management installations, and Schiphol Airport and the Port of Rotterdam are entirely or largely under state control. For the most part these are core tasks of the state, and the government will retain control over them. The risks to national security due to a change in control are therefore not relevant here.
- Where transport and distribution networks are concerned, the vital sector of energy is in the hands of the government. Multiple companies are involved in supplying energy, which reduces the risks involved. In addition, the Minister of Economic Affairs and Climate Policy is required and authorised to assess any changes in corporate control related to gas and energy production.[10] The potential risks to national security as a result of changes in corporate control are therefore adequately managed.
- There are certain national security risks associated with the critical sector of telecommunication as a result of changes to control, which cannot as yet be adequately offset by statutory norms. The risks to national security as a result of corporate takeovers will therefore be safeguarded with additional legislation.
- There are strict standards and public oversight procedures in place with regard to the vital sectors of payment transactions and chemicals. This helps ensure the integrity of data and physical security, respectively, which pose the biggest risks to national security. These standards and procedures adequately address the risks within these sectors.

The analyses show that the continuity and availability of (virtually) all critical processes, whether controlled by the public or private sector, depend greatly on private companies that supply goods, services or technology. This could give rise to vulnerabilities when it comes to contracting procedures and deliveries. The government will therefore be taking the following action:

Measures

A. Establishing an Economic Security Task Force

An Economic Security Task Force, led by the NCTV, has been set up to further explore the balance between national security interests and economic interests, discuss real-world cases, and

[6] Coalition agreement 'Confidence in the Future', section 2.4.
[7] House of Representatives, 2016-2017, 29 826, no. 84.
[8] House of Representatives, 2017-2018, 34 775 XIII, no. 116.
[9] House of Representatives, 2018-2019, 35 153, no. 5.
[10] See the Electricity Act 1998 and the Gas Act.

comprehensively weigh up the interests concerned. The Task Force is currently looking into vulnerabilities associated with the future 5G telecommunications network and the measures needed to manage the associated risks.

B. Making better use of and tightening up current legislation on national security
The Netherlands has a number of instruments that can help address national security risks within private companies. These relate to anti-takeover laws for the private sector, sector-based legislation, contractual agreements, the Enterprise Division and the designation of confidential positions. The government is evaluating and tightening up current legislation to enhance its utility.

C. Protecting national security in relation to procurement and contract award procedures
The government will continue identifying the national security risks that can arise as a result of the dependences involved and consider how these potential risks can be managed in relation to procurement, contracting procedures and in other areas. In 2018 the government developed and introduced a set of instruments for ensuring safe procurement and contracting practices. We are currently looking into how these instruments can be used in components of critical infrastructure and by local and regional authorities. In addition, the government will apply national security guidelines more actively to the use of products and services within central government and critical infrastructure, and by local and regional authorities. With regard to procurement and contracting procedures, the government is working within the framework of the National Cybersecurity Agenda on additional cybersecurity criteria for procuring IT resources for the government. These criteria will also factor in considerations of economic security in order to boost resilience with regard to state actors.

D. Protecting national security in cases of takeovers and investment
Within the EU the government is working to further strengthen the cooperative mechanism on foreign investment. A framework has been agreed whereby individual member states can assess the risks posed by foreign investment to national security or public order. Additionally the EU foreign investment screening regulation obliges the member states and the European Commission to share information. The regulation requires the establishment of a cooperative mechanism, for which certain processes (e.g. for information-sharing) must be set up, in the Netherlands as elsewhere. The framework does not impose any obligations concerning an investment test, though it does establish guidelines for member states that would like to implement such a test.

Within this European framework the government is working to develop such a test. This is meant to be an 'instrument of last resort' for national security risks, which would allow for the possibility of a customised approach. This would be based on existing sector-based legislation. In this way, national policy preferences on the substance and scope of a broader protection mechanism are also accommodated within a European context. In fleshing out this instrument we will look at 'umbrella legislation' with which existing and future sector-based legislation would be well-aligned. The guiding principle is that a ban resulting from a negative outcome in an investment test will be imposed only if there are no effective alternative protection measures available.

<u>Initiatives related to this issue</u>
In addition to this set of measures to ensure that risks to national security remain manageable, there are also a number of other initiatives in this area, with a particular focus on critical technology and knowledge. The undesirable transfer of knowledge and technology can occur, for example, in cases of bankruptcy and the takeover of startups, and within the research community and academia. The government is examining whether measures can be expanded in this way to include other high-risk countries and to academic courses which involve the acquisition of highly specific technical knowledge.[11]

Thanks to our analysis of financial and economic cyberespionage, we have a clearer picture of this threat. We have also looked into what instruments, complementary to the measures taken under the aegis of the International Cyber Strategy and the National Cybersecurity Agenda, would be useful to mitigate this threat. Additional instruments, such as measures to raise awareness of this threat, will be included in the various policy areas, and in the approach to countering state threats. We also intend to use forms of international cooperation and various diplomatic measures (such as attribution), including those associated with the EU Cyber Diplomacy Toolbox, as well as existing WTO procedures, when appropriate.

[11] See also the letter to parliament on stricter supervision of students and researchers from high-risk countries, 2018-2019, 30 821, no. 70.