National Coordinator for Security and Counterterrorism
Ministry of Justice and Security

> Return address Postbus 16950 2500 BZ The Hague

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Turfmarkt 147
2511 DP The Hague
Postbus 16950
2500 BZ The Hague
www.nctv.nl

Our reference
2573867

Appendix
1

Please quote date of letter and our ref. when replying. Do not raise more than one subject per letter.

Date 18 April 2019
Concerning Countering state threats

An open society with an open economy is the foundation of our form of social organisation and the source of our prosperity. Our open society is characterised by freedom, democracy, the rule of law and an international orientation. Thanks to this openness the Netherlands and its people benefit from the opportunities generated by developments like digitalisation and globalisation. An open economy and free trade have long been key elements of the Netherlands' earning capacity. They generate the necessary financing, economies of scale, sharing of talent and knowledge, and essential incentives to stay competitive. This is one of our great strengths, and it has made the Netherlands a global player in terms of knowledge, innovation, trade and investment, despite its relatively small size. The interdependent nature of the international economy can also foster peaceful cooperation and boost our prosperity. It can also make it easier for the Netherlands to raise certain political issues abroad. In short, our open society and open economy are important and must be protected.

A changing world

At the same time though, the world is changing, and this has implications for our open society and open economy. The global digital transformation is proceeding at a rapid pace, and the realms of geopolitics, security and the economy have become ever more intertwined. New technologies are emerging all the time, and they are becoming more important, or even indispensable, to the way our society functions. In addition, we are witnessing a re-emergence of power politics between rival states, which is causing a shift in the geopolitical arena. Globalisation has brought about increased economic interaction, the internationalisation of labour markets and production processes, and liberalisation of policy on foreign business operations and investment. This creates more opportunities for (covertly or openly) acquiring Dutch technology and companies. New players have appeared on the world stage, and traditional alliances are disappearing or their composition is changing. Against this backdrop, states are becoming more and more assertive about defending their interests, leading to changes in existing relations. In doing so, they are increasingly adopting rules, norms and values that are different from those to which the Netherlands and the international community (in the West) have become so accustomed. As mentioned in the annual reports of the General Intelligence and Security Service (AIVD) and the Defence Intelligence and Security Service (MIVD), states are seeking to gain insight into and influence decision-making processes, facilitate the digital sabotage of critical infrastructure, steal trade secrets, or intimidate and influence their own citizens or former citizens living abroad. More and more countries are focusing on political and/or economic

espionage, and cyber espionage is becoming increasingly complex. In order to assert their power and pursue their political agendas, they make use of cyberattacks, clandestine influencing practices and economic pressure. This is happening on a global scale, so it is not just the Netherlands that is affected but its allies as well.[1] In this changing world it is the task of the Dutch government protect our open society and open economy by reinforcing this openness wherever possible and remaining vigilant to state threats so it can provide protection where necessary.

It is an unfortunate paradox that the freedoms that guarantee this openness also give malicious state actors the possibilities to engage in activities that undermine our national security and thus our freedoms. The openness of our society and economy requires that we seek a careful balance between seizing new opportunities, on the one hand, and protecting national interests and national security, on the other. National security risks must be contained as effectively as possible, with due regard for the trade-off between protecting security interests and the impact this could have on our open society and open economy. In the process we must not lose sight of the pace of the developments in the world around us, including in the digital domain.

Comprehensive approach

The threats to national security posed by these states have ramifications for various policy areas. Such threats impact on democratic processes, digitalisation, economic security, international peace and security, the armed forces and social stability. These issues fall under the portfolios of various ministers and state secretaries. When it comes to monitoring state threats and formulating countermeasures, 'connecting the dots' is essential. These different perspectives are brought together in order to continuously assess where our national security interests might be jeopardised by state actors, and to reflect on what countermeasures should be taken.

Protecting our economy and security requires a customised, proportional approach that takes account of the various interests at play. Broadly speaking, the government sees two ways of better arming ourselves against the risks in this area. First, we must strengthen the Dutch and European economy by bolstering the single market, enhancing competition law and pursuing a modern policy on innovation and industry. An innovative economy is also a less vulnerable economy. Moreover, the government's trade policy aims to maintain a level playing field, strengthen mutual market access and enhance protection of intellectual property rights. This helps prevent one-sided strategic dependence. The letter to parliament on European competitiveness will explain how the government plans to pursue these aims in a European context. Secondly, the government is mindful of developments that could impair the integrity and exclusivity of knowledge and information or interrupt the continuity of services and processes that are vital to the Dutch economy. The appendix to this letter contains the results of the analysis of vulnerabilities in critical sectors. Threats posed by state actors are only one type of possible risk. The government's approach to these economic security risks is therefore broader.[2] The appendix also sets out additional relevant measures, such as stricter legislation and better enforcement of existing legislation, taking into account issues of national security in procurement and contract award procedures, and the design of an assessment tool to spot potential national security risks associated with investment and

[1] Annual reports by the AIVD and MIVD, National Cybersecurity Assessment, Integrated International Security Strategy, Defence White Paper, National Security Profile 2016, Horizonscan NV 2018, Strategic Monitor 2018-2019.
[2] As discussed in the policy document 'Between Naivety and Paranoia' and successive progress reports on economic security.

takeovers, to be used as a last resort. National security is first and foremost a national competence, but closer European cooperation in this area is recommended. The government takes care to ensure that the instruments used to guarantee national security do not cause undue harm to our business and investment climate. Given the open nature of the Dutch and European economy, it is particularly important to make sure that economic security measures are not used for protectionist ends.

Non-state actors can also pose a risk to economic security, but this subject goes beyond the scope of this letter. The purpose of this letter is to inform parliament, on behalf of the government, about the risks associated with state threats, the government's policy on countering such threats, and the key aspects of our approach in the period ahead. The subject of state threats is also addressed in the National Security Strategy, which outlines the government-wide approach to this issue. The Strategy will be released before summer of 2019.

Threats and risks

To promote their own interests and achieve their geopolitical goals, state actors are increasingly using a broad range of instruments that could potentially undermine our democracy and rule of law, and the stability and openness of our society. While often deliberate, systematic and covert, their activities generally do not rise to the level of 'armed conflict' as defined by international law. The tools used by state actors and the activities they engage in can span the whole range of instruments available to a government and may or may not be employed as part of a deliberate strategy of hybrid conflict.[3] Although this does not rise to the level of armed conflict, there is nevertheless a military dimension. Military assets can also be deployed outside the context of armed conflict in order to achieve a strategic goal. Below is an overview of several manifestations of the current (hybrid) threat situation facing the Netherlands, the European Union and NATO.

Digital tools

The biggest threat in the cyber domain is posed by state actors. States use digital technology for the purpose of manipulation (e.g. data manipulation) and sabotage (e.g. disrupting critical processes), disinformation (e.g. disseminating false information on social media and elsewhere during elections) and digital espionage (e.g. gathering sensitive or confidential information).[4] The number of states developing cyberattack capabilities is on the rise, as is the complexity of such attacks. Digital tools must be able to function smoothly for the sake of vital commercial and governmental processes, the earning capacity of businesses and the daily lives of the general public. In the past few years various incidents have made clear that cyberattacks can have a major impact on society and undermine national security.

Economic tools

The blurred boundaries between the public and private sectors in state-led economies raise questions about economic security.[5] Investment in or takeovers of critical infrastructure or companies in the high-tech sector can lead to an undesirable level of dependence, posing risks to the Dutch economy and the

[3] 'Understanding hybrid threats: EPRS at a Glance', June 2015; Munich Security Report 2015, 'Collapsing Order, Reluctant Guardians?' (MSC, 2015); 'Irregular Adversaries and Hybrid Threats: an Assessment-2011' (US Joint Irregular Warfare Center, 2011); F. Hoffman, 'Conflict in the 21st Century: the Rise of Hybrid Wars' (Potomac Institute for Policy Studies, December 2007), 'Χίμαιρα: Een duiding van het fenomeen "hybride dreiging"', National Coordinator for Security and Counterterrorism, April 2019 (reprint of a report from July 2017), www.nctv.nl.
[4] 2018 Cybersecurity Assessment for the Netherlands, annual reports by AIVD and MIVD.
[5] Policy document, 'Investing in Global Prospects', House of Representatives, 2018-2019, 34 952, no. 41.

democratic legal order. This could compromise the continuity of our critical processes or lead to confidential or sensitive information being compromised. A similar risk can arise from the procurement of critical services and products. Some states are also actively engaging in economic espionage.

Foreign interference

State-backed efforts to undermine other states are generally a gradual process that can lead, in time, to serious upheaval and the disruption of an open society and democratic legal order. More specifically, foreign interference can erode the integrity of decision-making at political level and within the civil service, the independent judiciary, free and fair elections and fundamental freedoms like freedom of the press, academic freedom and freedom of expression. In addition, it can also lead to tensions within and between ethnic and religious groups in the Netherlands and erode social cohesion.[6] Undesirable interference by state actors can involve various methods and target various groups, such as diaspora communities, students, the media and politicians. It can also involve clandestine financing. The dissemination of disinformation is another well-established technique.[7]

Dependence on new technologies and critical infrastructure

A number of developments intersect with several of the risks and threats described above. New digital technologies, like blockchain, robotisation and artificial intelligence, are transforming the economy and society at a rapid pace. Digitalisation is the driving force behind innovation and industry,[8] but it can also entail national security risks, such as espionage, sabotage and strategic dependence. This could lead to unwanted dependence with regard to the availability of these technology standards. The above is more or less true of our critical infrastructure as well. The Netherlands is dependent on its critical processes, which are closely interconnected. An outage or disruption could trigger a major chain reaction. This means that critical infrastructure (both physical and digital) has become a bigger target.

Examples in the Netherlands

An overview of specific countries and the methods they use can be found in the annual reports of the AIVD and MIVD, and elsewhere. This risk assessment is supported by the following examples:

- In April 2018, the MIVD, working with the AIVD, disrupted an espionage operation by the GRU, the Russian military intelligence service, against the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague.[9]
- Last January, partly at the initiative of the Netherlands, the European Union imposed sanctions on Iran due to serious concerns about its probable involvement in hostile actions on European soil.[10]
- In 2016 the government took action in response to reports that the religious affairs attaché to the Turkish embassy in the Netherlands, who is also the chair of the Islamitische Stichting Nederland (the Dutch branch of Diyanet), was passing information to Ankara about Dutch organisations and individuals who were suspected of having ties to the Gülen movement. After consultations with the Ministry of Foreign Affairs, the Turkish authorities decided to recall the attaché.[11]

[6] 2016 National Security Profile (Analistennetwerk Nationale Veiligheid, 2016); letter to parliament on foreign interference (NCTV, 16 March 2018).
[7] House of Representatives, 2018-2019, 30 821, no. 51.
[8] 'Investing in Global Prospects', House of Representatives, 2018-2019, 34 952, no. 41, p21.
[9] House of Representatives, 2018-2019, 33 694, no. 22.
[10] House of Representatives, 2018-2019, 35 000-V, no. 56 (Sanctions against Iran on the grounds of undesirable interference).
[11] House of Representatives, 2015-2016, 32 824, no. 194.

- The Dutch government has also received signals from members of the public who are concerned about relatives in Xinjiang province who are being put under pressure by the Chinese authorities to divulge personal information.[12]

Tackling state threats

The following principles are central to our policy on countering state threats:

- The Dutch government is responsible for national security and favours a **a whole of society approach**. To this end, government organisations, security services, the armed forces, the business community and civil society organisations are actively involved in protecting national security interests. In this regard the government is defending public interests, encouraging parties to shoulder their own responsibilities and serving as a good example.
- A **flexible, adaptive and integrated approach** that responds to relevant developments makes it easier to swiftly detect and mitigate risks. Such an approach recognises that internal and external security are inextricably linked. International cooperation is a key element of this approach.
- The approach is **country agnostic**. We aim for a generic approach which can be applied to a threat posed by any state actor whose actions could potentially trigger social disruption, whether directly or indirectly via our allies. Working on the basis of a custom made approach and proportionality, these generic measures are then applied in specific cases.
- The approach does not alter the existing division of responsibility; rather, it uses existing powers and information in a more **harmonised and coordinated** way. As much as possible, we will endeavour to use existing initiatives, instruments, partnerships and information exchange mechanisms, related to issues like cybersecurity, foreign interference and economic security.

The approach to countering state threats consists of a number of generic measures, listed in the table below. Given the threat, the interests at stake and the incidents that have recently unfolded, the emphasis in the coming months will be on the following issues: (1) countering foreign interference aimed at diaspora communities, (2) protecting democratic processes and institutions and (3) economic security. Major steps in these areas have already been taken, and new elements have been identified that require an integrated approach. The appendix contains a description of the approach to these issues, including the results of ex-ante economic security analyses.

Tackling state threats	
A. The 'interests-threat-resilience' system	With the help of our **interests-threat-resilience-system**, the government will determine what security interests should be protected, what the state-based threat is to national security and how to boost resilience. This is an ongoing process which involves the members of the EU and NATO and – within the Netherlands – multiple ministries, local authorities and private organisations. This requires coordination and close contact. • On matters of national security, the Minister of Justice and Security, in consultation with partners at other ministries, focuses on coordination between the various stakeholders, responsibilities, initiatives, projects and information flows.

[12] House of Representatives, 2018-2019, 32 735, no. 209.

	• A recent development on this front is the creation of an Economic Security Task Force to address vulnerabilities and take measures to oversee the creation of a national 5G network.
B. Enhanced information position	The government is also working to **enhance its information position and improve information-sharing practices** between like-minded parties, at both national and international level, so as to identify and interpret potential threats in time. To that end, information-sharing must be made easier and more logical, enabling the creation of a common standard. • Where necessary, interministerial 'trusted communities' will be set up or strengthened. • Working agreements on specific topics will ensure that, if necessary, information can be shared swiftly and acted upon. • We also work closely with our international partners to tackle threats and share best practices. • Embassies play a key role in monitoring the situation abroad and flagging relevant developments, thereby maintaining situational awareness. • Within the EU the Netherlands takes part in the Rapid Alert System, where information can be shared directly in the event of disinformation campaigns. • Civil-military cooperation in the Netherlands is being enhanced.
C. Raising awareness and conducting exercises	**Raising awareness** is a key element of efforts to boost resilience in the face of the threat posed by state actors. • Major efforts are being made to raise awareness of this issue among procurement staff, civil servants, municipalities, the critical infrastructure sectors, CEOs and the public, by means of public events, information campaigns and communications material. A recent example is the awareness-raising campaign on disinformation. • At national and international level, the relevant parties are **practising** identifying and responding to state threats, in part by developing scenarios and using them to **conduct exercises**. The Netherlands will continue to participate in exercises within NATO (CMX) and the EU (PACE).
D. Comprehe n- Sive knowledge developm ent	Knowledge is being built up jointly by means of a **comprehensive research agenda and knowledge development** in the area of resilience to state threats.
E. Defence and deterrence measures	The Netherlands is also committed to further developing measures in the realm of defence and deterrence. • Diplomacy: the government has various diplomatic instruments at its disposal to deal with state threats. • To defend its national security the Netherlands is working **to further develop an effective diplomatic response framework**, wherever possible in collaboration with its international partners. For example, in response to attacks by state actors the Dutch government may now choose to publicly attribute responsibility.

	• Dealing with foreign interference remains a topical issue that involves a growing number of countries. • The government is working to counter political influencing by equipping and protecting political office-holders, exploring the possibility of instituting a mandatory registration policy for lobbyists, and flagging signs of influencing and disinformation to ensure that elections run smoothly and safely. • In the Defence White Paper and the National Plan, the Ministry of Defence is seeking to boost our capabilities in areas like intelligence, cybersecurity and countering hybrid threats. The new Defence White Paper, which will be released next year, will address the further development of these efforts in aid of national and international security.
F. The economy and security	The **instruments used to safeguard our economic security against national security risks** must be in order. This requires a custom made, proportional approach that takes account of the various interests at play. • In terms of economic security the authorities are working to develop an 'investment test' to identify national security risks in corporate takeovers and investment, and to develop and roll out policy and guidelines for procurement and contract award procedures by the state and within the critical infrastructure sector. The authorities are also working to expand sanction orders in connection with the leaking of sensitive technology via academic channels. • In assessing national security risks, they make use of consistent and technologically up-to-date criteria.
G. Digital approach	With the help of the National Cybersecurity Agenda (NCSA), which was sent to the House in April 2018, the International Cyberstrategy and the Integrated International Security Strategy, the government is committed **to keeping the Netherlands digitally secure**. The approach will also take account of the influence exerted by state actors. • For example, the government will invest in boosting the resilience of digital processes and in making infrastructure more robust, and we will enhance our ability to respond forcefully to the increase in cyberthreats and major cyber incidents that threaten national security. • In a separate letter the House will be updated before the summer on the annual progress on the NCSA, in conjunction with the 2019 National Cybersecurity Assessment.
H. International cooperation	In line with the Integrated International Security Strategy, the Netherlands is committed to: • **Working closely with its partners in the EU and NATO, and promoting cooperation *between* these bodies**, in relation to situational awareness, resilience and response. The EU's strategy in this area centres on the 22 actions formulated in the Joint Framework on countering hybrid threats (2016). Within NATO, the key framework is the strategy on countering hybrid warfare (2015). • Maintaining an accurate information position, in close cooperation with international partners so that

	information can be shared – both in the EU and NATO, and in ad hoc formations with like-minded partners. • Promoting the international legal order and an effective multilateral system in relation to state threats. To counter the increasing threat, the Netherlands will, wherever possible, seek to mount a joint response and join with other parties to attribute responsibility for incidents. • Maintaining credible deterrence with our allies (including those in NATO) against state threats. In July 2018 it was decided to create counter hybrid support teams (CHST), NATO units that can advise Allies and offer assistance on hybrid threats. • Using the European Centre of Excellence for Countering Hybrid Threats as a network organisation and platform for developing expertise. The Netherlands joined the Centre in 2018. • Improving cooperation between the various EU institutions in order to address these kinds of issues (e.g. disinformation, elections, cybersecurity, crisis management, critical infrastructure and foreign takeovers) in a coherent way. • With a new European Commission taking office in 2019, there will be a new momentum to push for a more consistent approach to internal security, including state threats.[13]

Conclusion
With this broad and integrated approach, the government continues to build up this country's resilience to state threats. Using such an approach allows us to make connections between incidents that, when observed independently, seem unrelated to national security. These incidents can then be analysed in terms of a possible link to an underlying hybrid or undermining strategy by malicious states or parties acting (perhaps unwittingly) on their behalf.

In recent months the various ministries, in close collaboration with parties from the public and private sectors and the academic community, have been working hard to take this next, government-wide step. By its nature the state threat is prone to change and calls for an adaptive approach. For that reason, under the coordination of the Minister of Justice and Security the government will examine whether parties are adequately equipped to confront this threat. This requires the ongoing monitoring of the threat and opponents' intentions, an up-to-date list of the vital interests at stake and, where necessary, boosting the resilience of those people, processes and information that ensure that our society can remain open, safe and prosperous.

n the months ahead we will seek to translate the ambitions articulated in this approach into specific measures, in close collaboration with the relevant ministries and other partners.

[13] House of Representatives, 2018-2019, State of the European Union 2019, 35 078, no. 1.