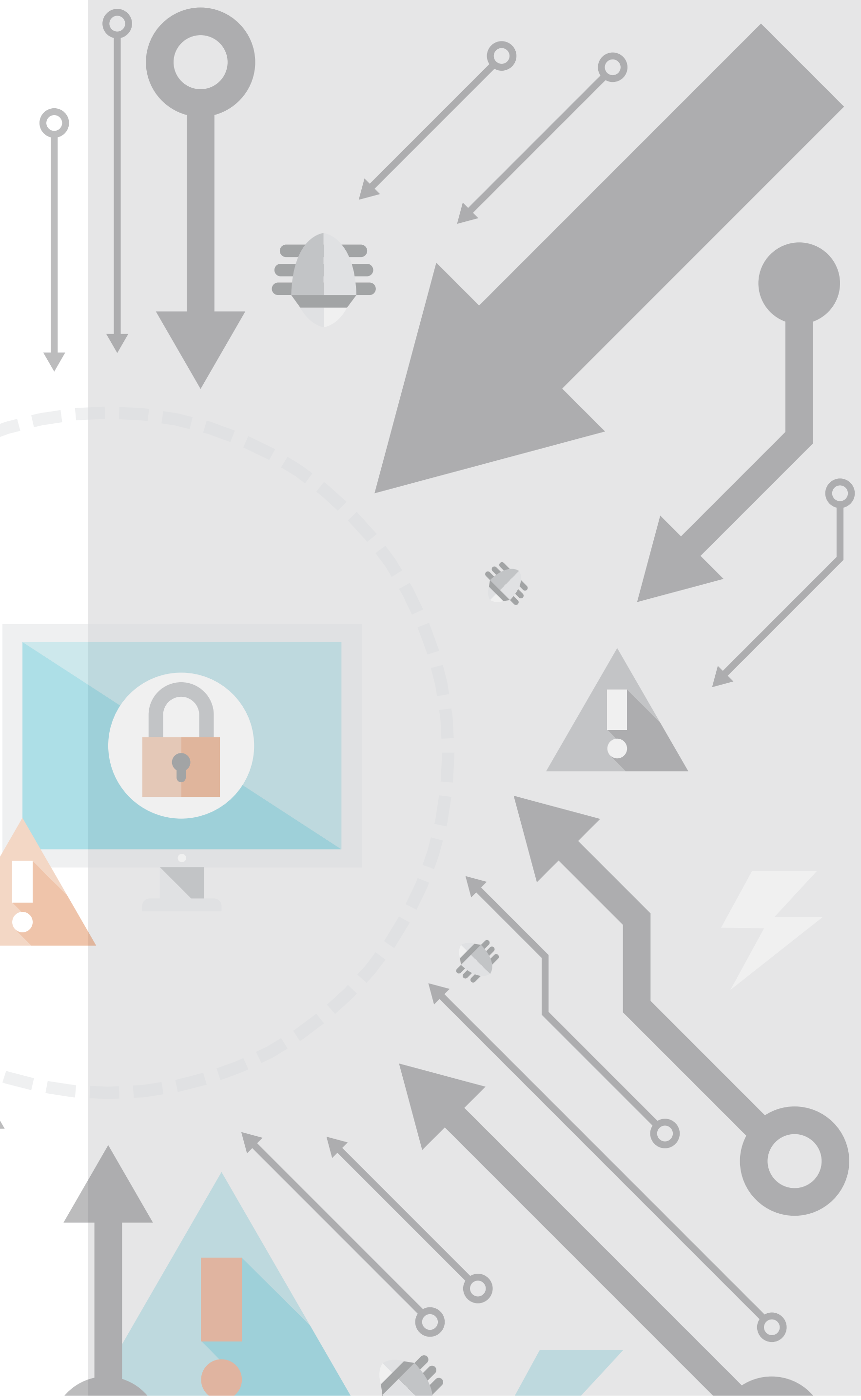
CSR Cyber Security Council

GUIDANCE ON THE USE OF THE ‘ASSESSMENT FRAMEWORK FOR DIGITAL AUTONOMY AND CYBERSECURITY’



CONTENTS

INTRODUCTION

Digital autonomy consists of the capabilities and capacities to take and implement decisions in the digital domain regarding the future of the economy, society and democracy. In its CSR advisory report 'Dutch Digital Autonomy and Cybersecurity'[1], the Cyber Security Council (the Council) has advised that digital autonomy must be placed at the highest political and administrative level, based on an integral vision of cyber resilience. Innovation must be targeted and cyber resilience must be tackled by the government and the business community from a sovereignty perspective. The starting point should be: strong at home, strong in Europe, strong in the rest of the world. This advisory report is based on the study entitled 'Strategic Autonomy and Cybersecurity in the Netherlands'[2] commissioned by the Council from researchers Freddy Dezeure and Paul Timmers. The report provides clear insights into the complex issues, illustrates them with appealing current examples and describes an assessment framework. Commissioned by the Council, researchers Dezeure and Timmers have translated this into this Guidance for the use of the *'Assessment framework for digital autonomy and cybersecurity'*.

Target group and purpose of this guidance

The Guidance has been written primarily for policy makers in government, but private organisations can also use it. Both the government and the business community must make conscious choices when it comes to dependence on ICT products and services. The Guidance supports taking appropriate measures to guarantee digital autonomy in cybersecurity. Going through the assessment framework is preferably a structured and interdisciplinary activity in which (interdepartmental) collaboration and knowledge sharing play a central role.

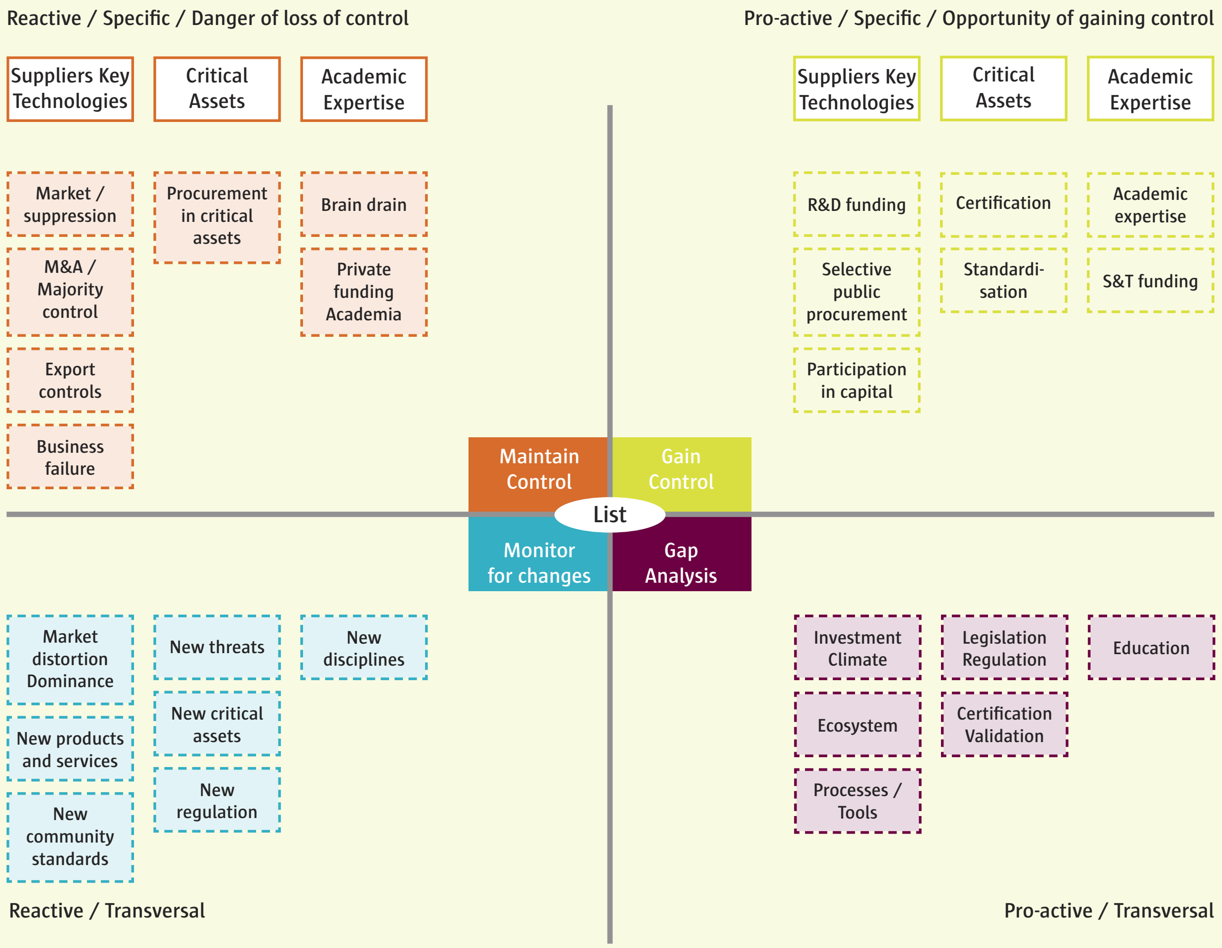
1 CSR Advice 'Dutch Digital Autonomy and Cybersecurity' - CSR Advice 2021, no. 3, May 2021
2 Report 'Strategic Autonomy and Cybersecurity in the Netherlands', Paul Timmers and Freddy Dezeure, January 2021

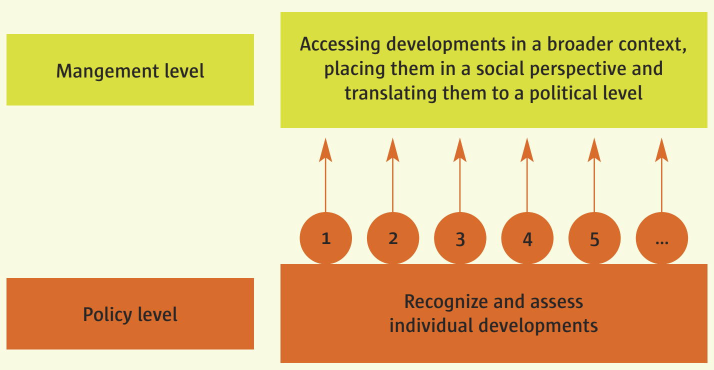
Guide and preparation

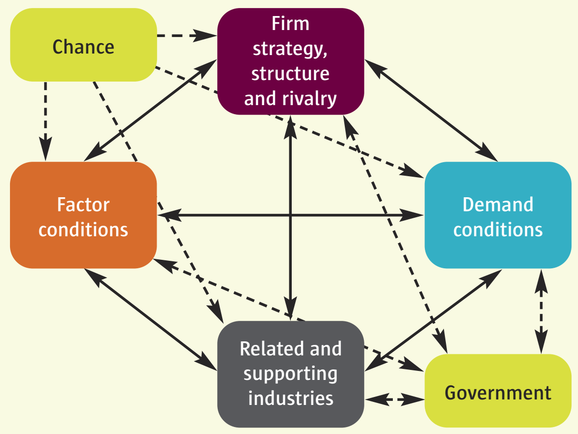
The assessment framework is a graphical method that stimulates and supports the identification and assessment of important developments. Using the Trigger Diagram and Porter models (see Figure 1), it enables the user to order complex issues on digital autonomy in a clear manner and to define and test concrete measures.

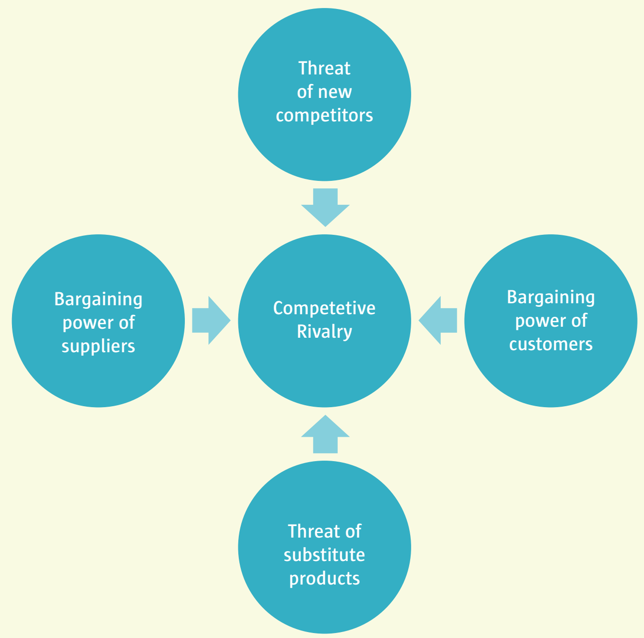
- Chapter 1 describes the logic of the central element of the assessment framework, the Trigger Diagram, and illustrates its use. It contains a concrete description of how to use the Trigger Diagram to identify and assess specific developments. The various quadrants are explained and some examples of their application are given.
- Chapter 2 describes the *management process* for following up this policy development and how to carry it through and secure it in a strategic and continuous way.
- Chapter 3 provides a step-by-step description for the *policy developer* to analyse individual developments. The policy officer can use this to systematically and comprehensively carry out the analysis of problems and appropriate measures.
- Chapter 4, together with its annexes, provides support for the preparation and implementation of the analysis. A practical step-by-step plan and an illustrative questionnaire for carrying out the analysis and identifying measures are included in the appendix.
- A central element when it comes to the capability and resources of digital autonomy is having sufficient control over key technologies and related assets to ensure cybersecurity.
- For an optimal result, it is advisable to carry out the analysis with the help of an interdisciplinary work group that includes (external) specialists with knowledge of, for example, the technical and purchasing domain. If desired, this work group can be facilitated by an expert who has experience in applying the method.

Figure 1: Trigger diagram and Porter models







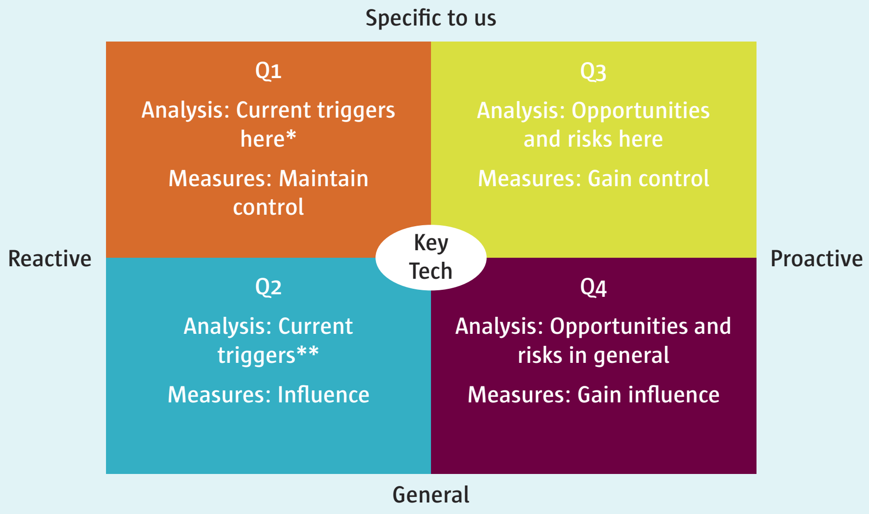


1. PROCESS FOR POLICY MAKERS: USE OF THE TRIGGER DIAGRAM

Where to start?

The central component in the assessment framework is the Trigger Diagram (see Figure 2), an innovative *mind map* to identify risks, opportunities and measures. The Trigger Diagram contains four quadrants, divided by two axes: reactive/proactive and specific/general. This allows the risks (reactive) and opportunities (proactive) to be shown per organisation/company (specific) or for the sector/market (general). This diagram is used both for the problem analysis and for displaying the proposed measures that follow from the analysis.

Figure 2: **Trigger diagram**



* In our enterprise, our government
** In the broader context or elsewhere

What knowledge is needed to make the analysis?

- It is important that there is knowledge about cyber security and about the specific case.
- In addition, an initial overview is needed of the resources (suppliers, customers, knowledge, government) that may play a role. This is the only way to keep an eye on the completeness and logical coherence of the analysis. Market dynamics models, for example from Porter, can be a good tool. Appendix 3[3] of this guide contains an explanation of Porter's model for national competitive strength (Diamond model). This model is intended to analyse national competitiveness, innovation and market dynamics at the country level. Specifically, it deals with suppliers, buyers, factor-conditions (knowledge, capital, etc) and the government which in its role imposes rules and determines policy. It can also be useful to better understand the forces acting on an individual firm with Porter's Five Forces model[4].

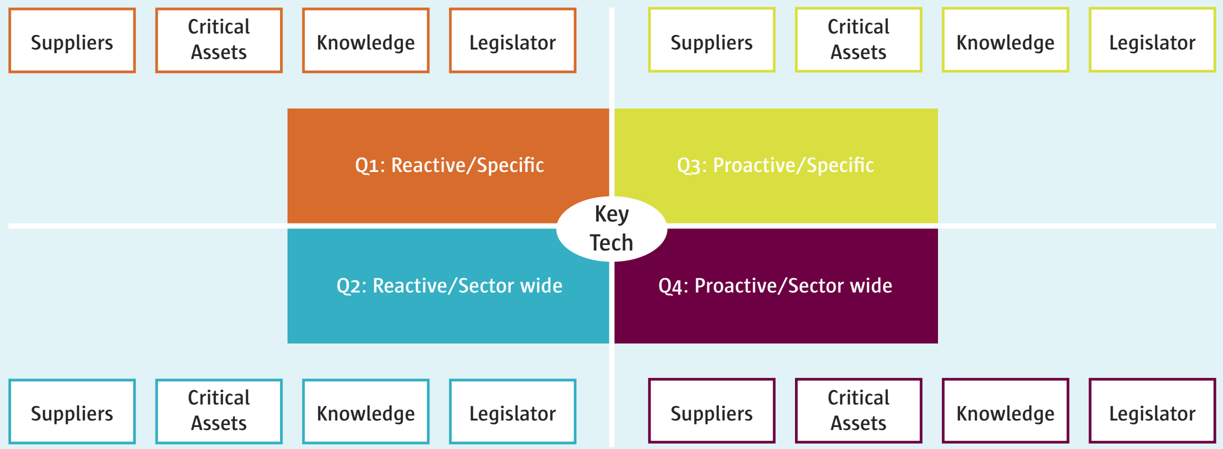
Both the Diamond model and the Five Forces model help to:

1. Verify that all relevant elements are included in the analysis and measures. If this verification leads to new elements then these can still be included as well.
2. Understand the impact of measures. A specific measure can influence other factors at company level (market distortion) and at national level (application of legal requirements, budget, international relations, etc.).

What do we analyse in each quadrant?

Each quadrant contains a number of concrete domains to analyse the opportunities and risks. It also shows possible measures that could have an impact on these domains. These domains are shown in Figure 3 and more specifically in Figure 4.

Figure 3: **Domains in the trigger diagram**



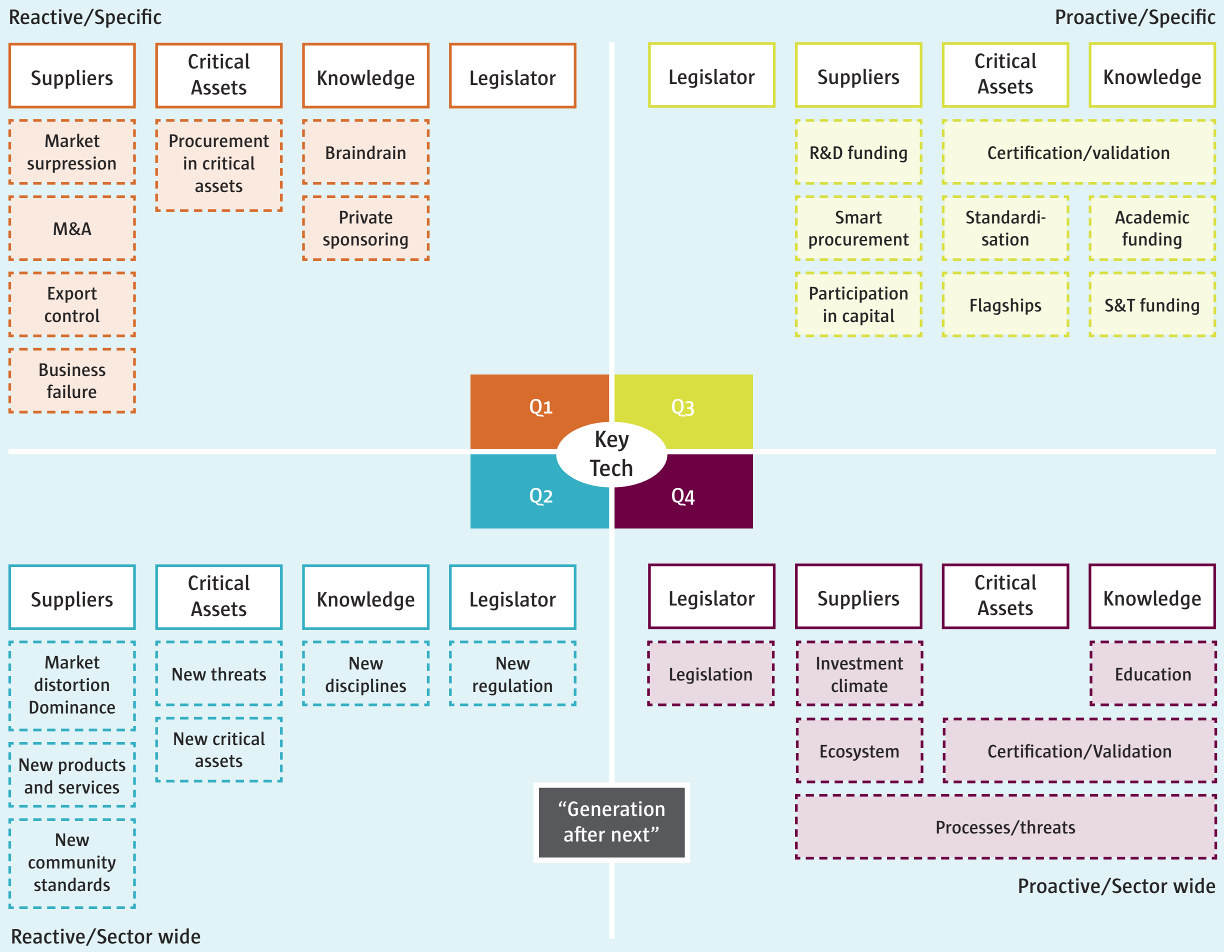
3 Appendix 3: Porter models, Diamond model explanation. However, the user is free to take another model for market dynamics if this allows for verification of the completeness and dynamics of triggers and measures.
4 Appendix 3: Porter models, explanation of the Five Forces model. However, the user is free to use a different model for market dynamics if this allows the completeness and dynamics of triggers and measures to be verified.

What questions should we answer?

- In the first quadrant (Q1: 'reactive and specific'), we identify threats to key assets over which we have sufficient control. Think, for example, of an impending takeover of an important (local) supplier.
- In the second quadrant (Q2: 'reactive/sector-wide'), relevant new developments are mapped, for example a new threat, a new product or new scientific insights. To the right of the middle line, opportunities and anticipations of threats are shown.
- The third quadrant (Q3: 'proactive/specific') contains an analysis of one's own future opportunities and risks and what measures should be taken to gain and maintain control over them. An example is how to gain more control by supporting a start-up in a key technology.
- Finally, in the fourth quadrant (Q4: 'proactive/sector-wide') an analysis is made of the opportunities from the comparison with other countries, for example processes for smart public procurement, investment climate and government processes or means to secure strategic autonomy. Future risks, such as in geopolitics or technology, are also identified here. See also Figures 5 and 6 for a graphical representation of this explanation.

To carry out the analysis and identify measures, a practical step-by-step plan[5] and an illustrative questionnaire have been[6] drawn up in this guide.

Figure 4: **Trigger diagram with domains and specific questions**



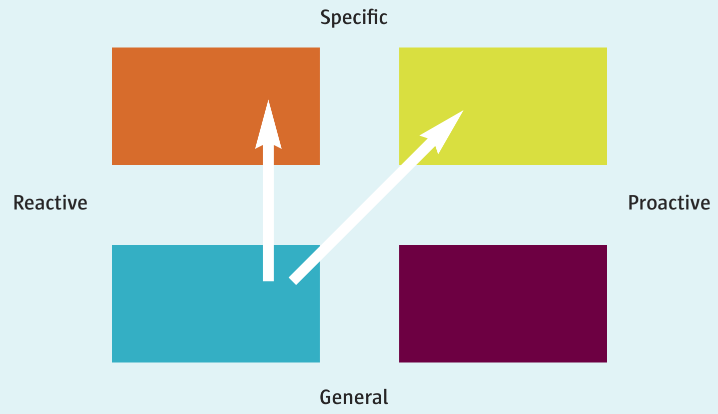
5 Appendix 1: Roadmap for identification of triggers and measures
6 Appendix 2: Illustrative questionnaire to support identification of triggers and measures

Some examples of the use of the trigger diagram

The Trigger Diagram can be approached from different angles. Concrete cases are explained in depth in the research report by Paul Timmers and Freddy Dezeure[7] commissioned by the council. We give a few examples here.

1. Trigger of new and important scientific developments
A key technological/scientific development is identified (Q2). From there, key companies (Q1) are identified that can turn this development into products that improve cyber security and whether we have sufficient control over them. In addition, it may be investigated whether there are new start-ups in the pipeline that can valorise these developments and over which control is desirable (Q3). If necessary, additional measures, such as purchasing conditions, are considered on the basis of market dynamics (Q3). In the report, the case 'R&D' in homomorphic encryption and differential privacy can be found on page 25, the resulting start-ups and the different approaches in other countries on page 32, the role of standardisation and open source initiatives in the control on page 36 and the procurement policy (public and private) on page 38. This specific example is also explained on page 61 of the report.

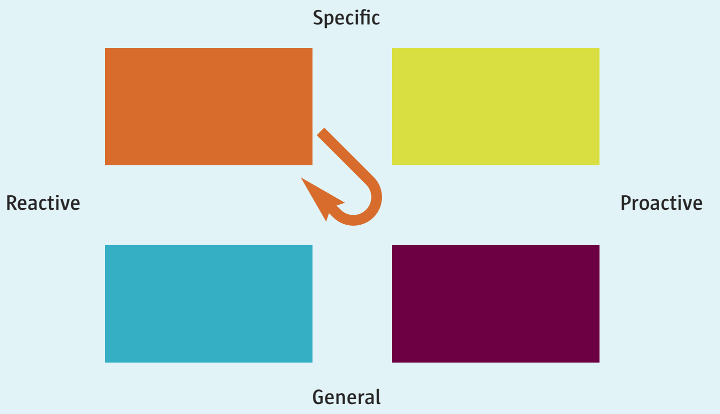
Figure 5: **New scientific development highlights the importance of key companies**



2. Impending takeover of a key company
An impending takeover of a key company that we have control over is identified (Q1). Based on this, appropriate measures can be taken to maintain control. The force analysis provides insight to consider e.g. strategic collaborations and participations. More information on corporate takeovers (M&A) and possible government interventions can be found on page 39 of the report.

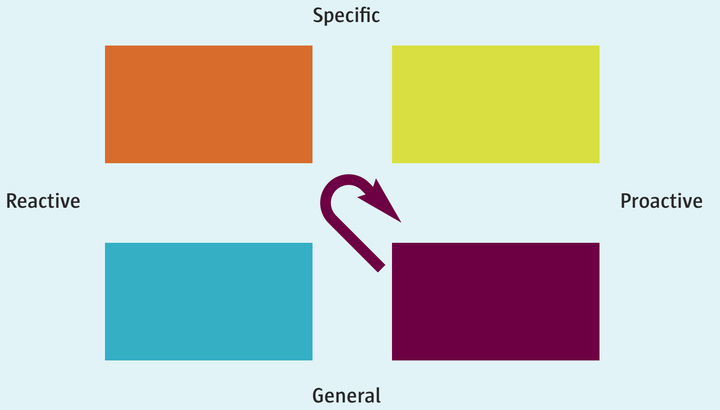
7 Report 'Strategic Autonomy and Cybersecurity in the Netherlands', Paul Timmers and Freddy Dezeure, January 2021

Figure 6: Avoiding the threat of a takeover of a key company



3. Look at approaches from other countries and adopt good practices
Proactively, we look at the comparison of our own policy approach with the approach of other leading countries with high Internet hygiene (Q4). What can we learn from this approach and what measures should we take to improve our own approach? See also Figure 7. It is important to understand the role of government in these countries for the bigger 'picture' of market dynamics. The research report by Timmers and Dezeure provides more information on this on pages 40, 54 and 55.

Figure 7: Approach to studying countries with a 'purer' Internet



4. Other examples in the research report
- Geopolitical pressure as a trigger:
  5G security, with measures such as the EU 5G Security Toolbox and possible government role as a booster (page 58).
- Legislative change as a trigger:
  Revision of the EU NIS Directive and possible supporting measures (page 60).

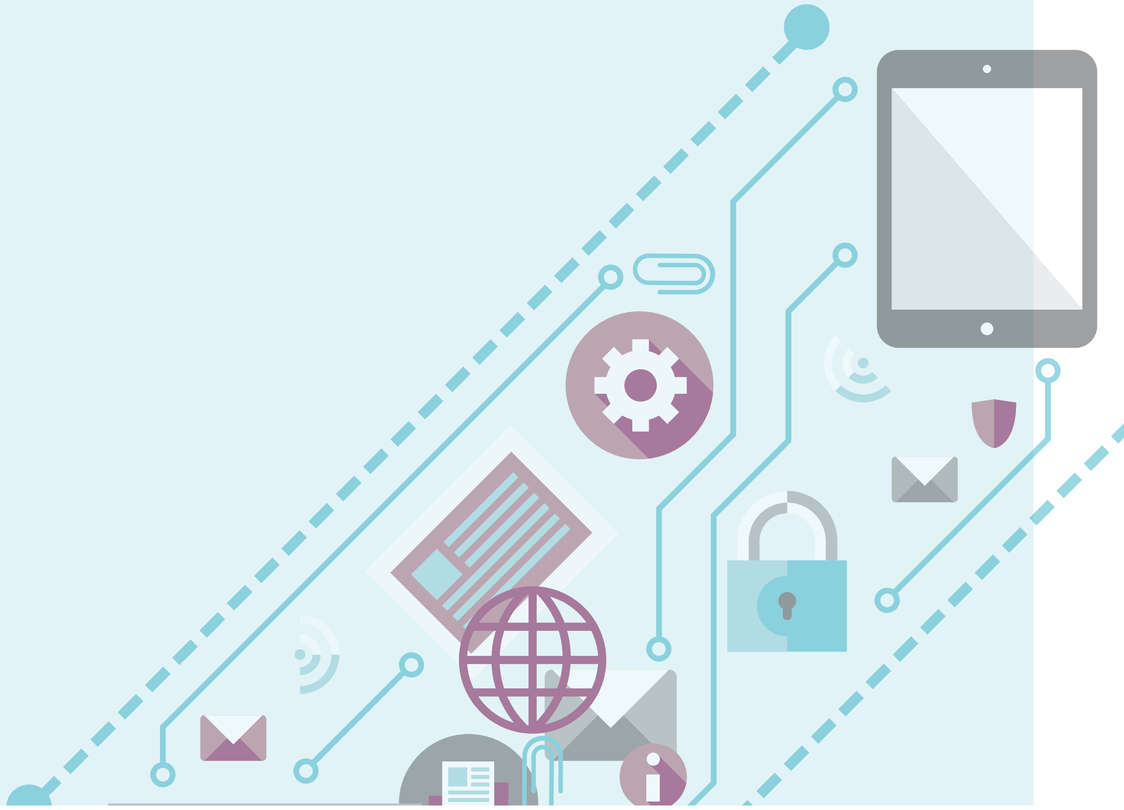
Completeness and coherence

Finally, it is important to verify the completeness and consistency of the analysis and the measures to be taken. Again, it is therefore desirable to refer to the overview of market actors and their relationships. Under time pressure it is easy to forget an important factor (For example: How much does it cost? Is the 'solution' a sticking plaster on the problem or is a long-term policy measure anchored in the solution, such as private-public cooperation or legislation, desirable?).

In this, it is important to monitor the coherence, both in the analysis and in the measures to be taken in relation to concrete technology and structural issues around the organisation/process. See two comments below for an explanation of this.

Note 1:
The analysis probably yields a number of digital key technologies over which the Netherlands has insufficient control. There may be underlying key problems that make strategic autonomy vulnerable even more fundamentally, for example because there is insufficient capacity for strategic planning in government or because there is insufficient knowledge to identify emerging technologies and to take a risk share in them. The risk then is that problems will keep recurring, resulting in a creeping erosion of sovereignty.

Note 2:
The analysis must ultimately lead to concrete policy measures that strengthen strategic (digital) autonomy in cybersecurity. Cybersecurity is about concrete technologies and products and their manufacturing industry. If the analysis leads only to process-based measures (even if they are concrete) without identifying concrete key technologies and companies, there is a real risk that there will be no answer to the current problems of strategic autonomy in cybersecurity.



2. PROCESS AT MANAGEMENT LEVEL

The process at management level presupposes that the assessment framework for various developments is run through from a whole-of-government approach. The 'management level' is where the results of the analysis and the policy proposals are put on the table for decision-making, proactive steering and/or advice to the political level. The management can periodically assess the various analyses and place them in a broad perspective.

The process at management level aims to achieve this through six different steps. These are shown in Figure 8. The objective of this process is:

- Obtaining a good overview of the analyses in the field of digital autonomy;
- To be able to consider these in a broader context and
- Then translate the priorities to the political level.

Figure 8: Steps to be taken within the process at management level

Below is an explanation of each step in this process.

1. Quantity of analysis
The first step is to assess the quantity and selection of developments that have been analysed. The following questions can be helpful in this process: For how many developments has the testing framework for digital autonomy been completed in relation to the quantity of potentially important developments, such as increasing cyber attacks, market developments, European and international policy proposals? Which developments are missing from the analysis that perhaps should have been included and for what reason were they omitted? How often does management receive alerts on important developments? How does this compare to previous reports?

2. Quality of analysis
In step two of the process, the quality of the developments assessed is determined in terms of breadth, depth and coherence of the developments. The following questions can be helpful in this process: What is the degree of insight into the dynamics in the market and between market and government? Is there insight into possible deeper causes for the developments, such as indirect state intervention in foreign suppliers, cooperation regarding cyber defence or the level of knowledge? With regard to the objectives: has the desired control for digital autonomy and cyber security been formulated?[8]

3. Quantity of measures
This third step then looks at the quantity of measures and how they might be classified. Is it possible to prioritise core and supporting measures? A total overview of costs and benefits is also mapped out.

4. Quality of measures
The fourth step of this process is to look at the quality of the measures. The following questions can help: What is the quality of the proposed measures? Has research been carried out beforehand into the possible impact of the measures? Has the relationship between the measures been reasoned out? Is there insight into side effects and have *unintended consequences* been considered, such as a creeping increase in (digital) dependence (e.g. through a lack of coordination in the purchasing process)?

5. Social, economic and democratic impact of measures
The fifth step is to look at how the package of proposed measures can be placed in a social, economic and democratic perspective. The following questions can help: Have ex-post impact indicators been formulated in terms of strategic autonomy (control, capacities, resources)? Are they directly related to the objectives?

6. Political impact of measures
In this last and sixth step of the process, the management will prioritise the measures, including the political dimension. The following questions can help: Is there an analysis of political feasibility of the measures that should lead to more control? Are the political alternatives clearly formulated? What needs to be reported to the Chamber?

8 For example: control or control of a technology, knowledge, standards, activity, investment, EU funds, EU legislation/policy or other developments of interest to the Netherlands.

3. PROCESS FOR GOING THROUGH INDIVIDUAL DEVELOPMENTS AS A POLICY MAKER

The process for going through individual developments at policy level, i.e. as a policy developer, consists of six steps. The result of the analysis will normally be presented to management (Chapter 2). The steps for the policy officer are shown in Figure 9. During this process, a problem analysis is drawn up, objectives are formulated and measures are defined. The order of these steps can be changed depending on the *use case*.

The aim of this process is to help the policy developer to:

- Carry out the analysis in full.
- Formulate and keep in mind the objectives for strategic autonomy.
- Formulate concrete measures for stronger strategic autonomy in cybersecurity.

Figure 9: **Steps to be taken within the process of going through individual developments at policy level**

1. Identifying triggers
The triggers that are plotted in the Trigger Diagram form the starting point and the first step of this process (see also chapter 1 of this guide). Examples are a new type of threat, rising geopolitical tension, pressure to revise EU legislation, a critical business takeover, a new scientific development, but also existing policy can be viewed through the eyes of this model. Also a future scenario can serve as a starting point to start an analysis from.

2. Analysis of dynamics
In the second step of the process, a description is made of the market, regulatory and technology dynamics associated with the triggered triggers, for example using the Porter models[9]. The aim is to gain insight into the context of the triggers, for example the relationships between suppliers and users (related to *supply chain security*), or legal obligations for cyber resilience of critical infrastructures.

3. Case description
The case description is the third step of the process. All elements (triggers and dynamics) from the analysis are described. The purpose of this is to gain insight into how an individual development, i.e. a trigger, can be more than an isolated event or incident in order to be able to respond meaningfully (i.e. not, for example, 'mopping up the situation').

4. Apply focus
The fourth step of the process focuses on those factors that influence cybersecurity and digital autonomy. The intention here is to stay within the mandate of the application of the assessment framework, where the focus is on the intersection of strategic autonomy with cybersecurity. It is quite possible that broader links will be detected, for example, that are not related to cybersecurity. However, this is not part of the intended application of the assessment framework here.

5. Formulating objectives
In the fifth step, the objectives are formulated. The desired result is defined in terms of strategic autonomy. Here, the arguments must become clear as to why this really concerns strategic autonomy, namely, that it concerns the ability and means to take and implement decisions about the longer-term future of the economy, society and democracy (see also the research report by Timmers and Dezeure).

6. Interventions (measures)
Finally, in the last step of the process, based on the formulated objectives, a coherent set of proposed measures is defined together with their expected effectiveness. Here it is important to make clear why the measures will be effective in response to developments and coherent with market dynamics. It is also important to indicate - because this concerns the national interest - which strategic approach is proposed (namely, strategic cooperation with like-minded partners, approach as a global shared interest, best-effort risk management or a combination of these).

9 See also Appendix 3: Porter models

4. SUPPORT

There are two ways to use the assessment framework:

1. The questionnaire is manually run through in a self-selected order.
2. The questionnaire is completed with the help of an online tool[10].

For the application of the first method, this guide includes a practical step-by-step plan for the identification of triggers and measures.[11] This is illustrated by an example in which triggers are identified in Q1 and Q2 and measures in Q1, Q3 and Q4. The second method gives more flexibility than the linear sequence of the questionnaire, which fits better with reality. Moreover, a graphic representation can enrich analysis and insight. Furthermore, all information, including answers to questions, can be recorded and shared with a team using digital support.

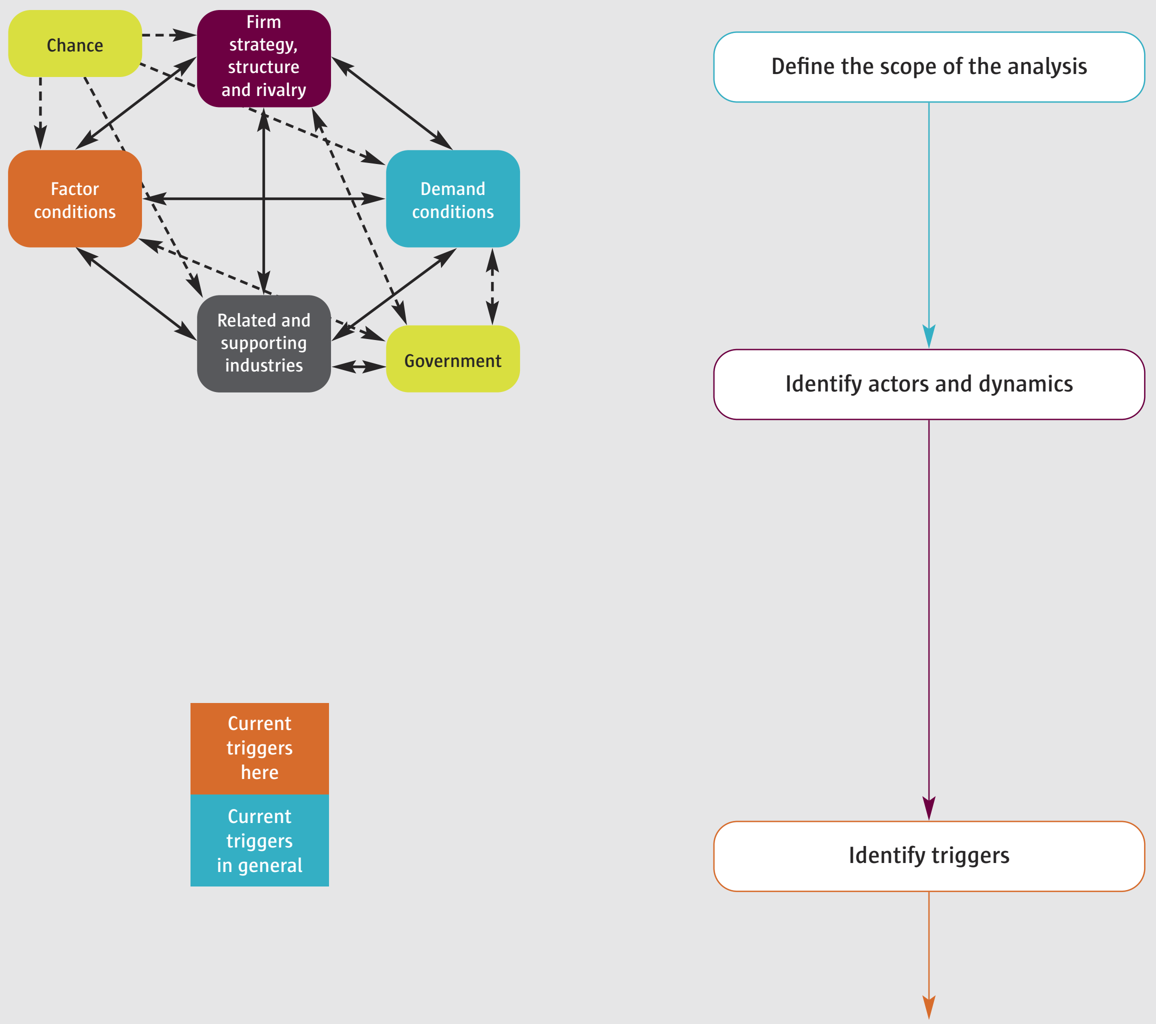
Want to know more?
To find out more about strategic autonomy and cybersecurity, it is advisable to read the research report 'Strategic Autonomy and Cybersecurity in the Netherlands'[12] in its entirety. This contains various examples that may provide inspiration and, above all, the testing framework can be tried out and applied here.

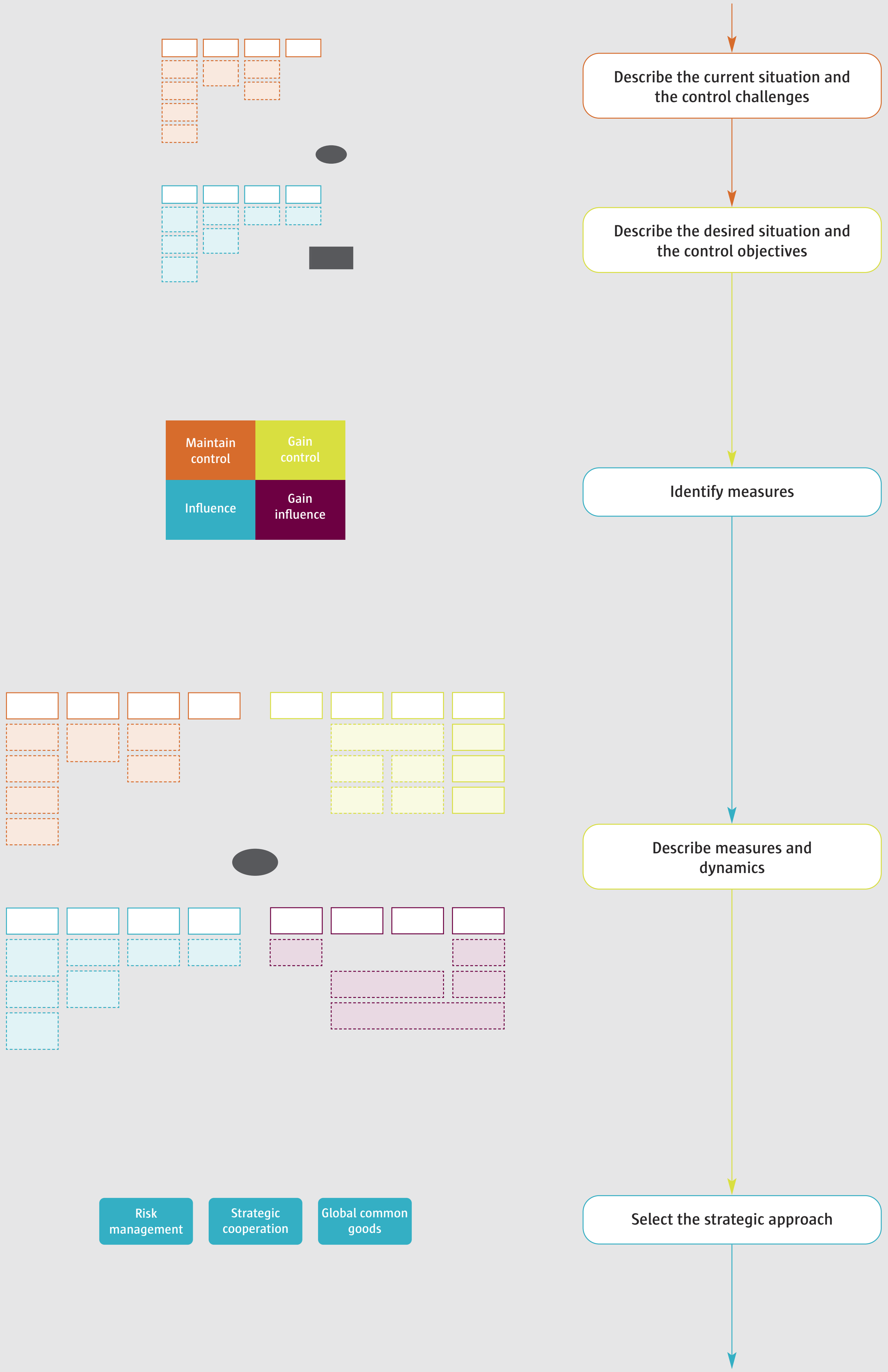
10 For example, with a digital whiteboard.
11 Annex 1: Roadmap for the identification of triggers and measures.
12 Report 'Strategic Autonomy and Cybersecurity in the Netherlands', Paul Timmers and Freddy Dezeure, January 2021

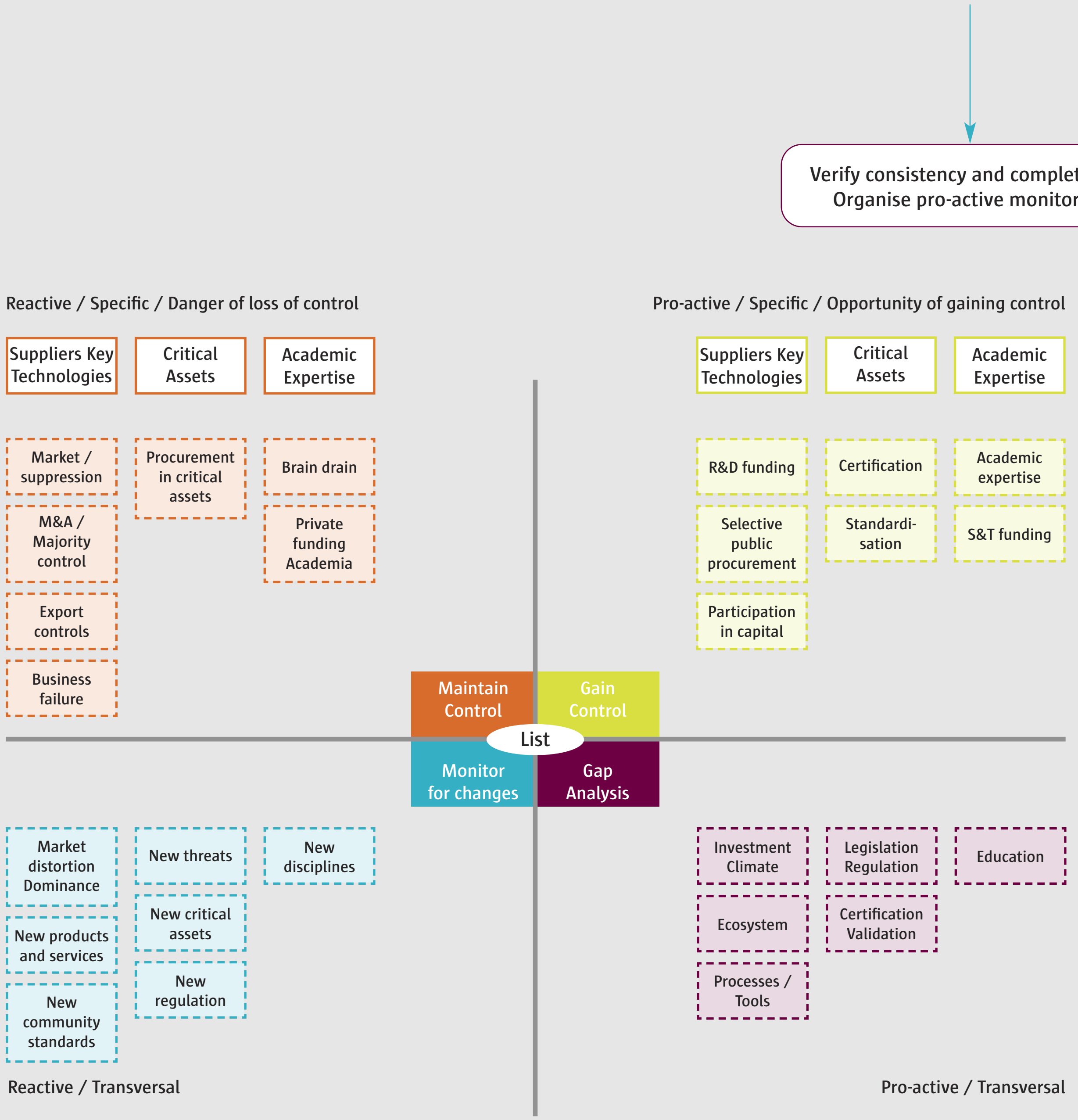
ANNEXES

ANNEX 1:
ROADMAP FOR THE IDENTIFICATION OF TRIGGERS AND MEASURES

Figure 10: Step-by-step plan to be used with illustrative questionnaire as support (for manual use)

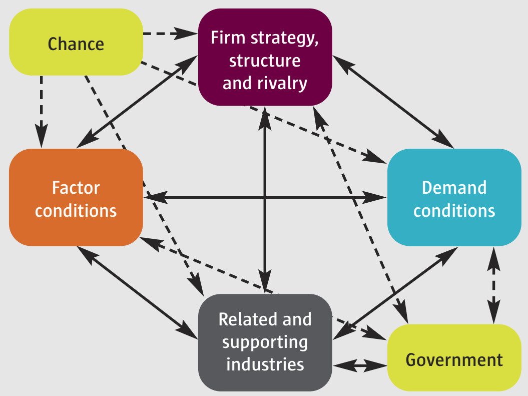






Verify consistency and completeness
Organise pro-active monitoring
Reactive / Specific / Danger of loss of control
Suppliers Key Technologies
Critical Assets
Academic Expertise
Market / suppression
Procurement in critical assets
Brain drain
M&A / Majority control
Private funding Academia
Export controls
Business failure
Pro-active / Specific / Opportunity of gaining control
Suppliers Key Technologies
Critical Assets
Academic Expertise
R&D funding
Certification
Academic expertise
Selective public procurement
Standardi-sation
S&T funding
Participation in capital
Maintain Control
Gain Control
List
Monitor for changes
Gap Analysis
Market distortion Dominance
New threats
New disciplines
New products and services
New critical assets
New community standards
New regulation
Reactive / Transversal
Investment Climate
Legislation Regulation
Education
Ecosystem
Certification Validation
Processes / Tools
Pro-active / Transversal

Threat of new competitors
Bargaining power of suppliers
Competetive Rivalry
Bargaining power of customers
Threat of substitute products



Chance
Firm strategy, structure and rivalry
Factor conditions
Demand conditions
Related and supporting industries
Government

ANNEX 2: ILLUSTRATIVE QUESTIONNAIRE TO SUPPORT IDENTIFICATION OF TRIGGERS AND MEASURES

This questionnaire can be expanded with new questions, under the categories indicated.

Identify local players/resources and dynamics (Porter: diamond model)

Factors

Key technologies
What relevant key technologies for cyber security are available and to what extent are they 'under control'? New technologies may also emerge as a result of supply, threats, regulations, assets and scientific developments. These may be relevant at different stages of the supply chain.

Knowledge in academia, research institutes, industry
Which players are most relevant in this area? Think, for example, of local academics and private, scientific and technical players. To what extent are they controlled?

Venture capital
What does the local market for venture capital (private, public) look like and who controls the main relevant players in it?

Suppliers

Who are the main local suppliers of key technologies? What is their respective market share? What legislation do they apply? Who controls these suppliers?

Buyers

Who are the main buyers in the market (type, country)? What is the share of private and public buyers? Do the respective governments influence private sector decisions in critical infrastructure in their countries? To what extent do public buyers distort the market and allow certain suppliers to dump their prices?

Who are the main local government buyers? To what extent is procurement coordinated (central procurement, common technical standards, certification, validation)?

Connected and supporting industries

Alternative Products
Are there alternative products available that meet the same need? Are there required key products in the supply chain? Which local suppliers do they have? What is their respective market share? How well are they doing in terms of growth, financial situation, capital? What is the level of control we have over them?

Open source ecosystem
Are there any important open source products in this area?

Government as regulator

Laws/regulations
Which rules apply in this sector (worldwide) and how do they influence the KET market? What ability does the Netherlands or the EU have to act? What is the approach of other countries to strategic autonomy? How do other countries oversee the supply chain of key technologies in critical assets? Is there a possible conflict of competence? What level of protection of intellectual property rights is there and to what extent is it enforceable? How important is the social and political awareness and risk appetite of the government for cybersecurity risks? Is there national or European legislation available to take emergency or recovery measures?

International Relations
Are there any geopolitical tensions/sensitivities that need to be considered? What is the level of government support for international standardisation or technological cooperation?

Innovation support
Are support/supervision instruments and mechanisms available to promote and encourage innovation in public support for R&D? Is this sufficient and does it produce a demonstrable result? What is the government's understanding of the innovation issues and the importance of an entrepreneur-friendly ecosystem?

Understanding strategic autonomy
What is the level of awareness and understanding of the strategic autonomy of key stakeholders and decision makers? How mature is the skill and training of decision-makers and implementers?

Critical standards and controls
Are there relevant European and international critical standards and controls in this area?

Identify Triggers - Q1 and Q2 (Trigger Diagram)

Q1: Current triggers with us

Market suppression
Is there an existential threat to an important company (which we control) from market forces pushing it out of business?

Change of control - Mergers and Acquisitions (M&A)
Is there an existing key supplier that is at risk of a change of control by new shareholders (fundraising, mergers and acquisitions). Can this have consequence(s) for strategic (digital) autonomy?

Business failure
Is there a threat to a key enterprise (under control) from bankruptcy (lack of financing, lack of domestic market, etc.)? Is there a critical supplier of key technology, services or infrastructure at risk of disappearing?

Export control risk
Is there any critical technology that might be exported to countries or companies where this is not strategically desirable?

New public tenders
Are there any major infrastructure procurement projects in the government that might affect the cyber security of critical assets?

New procurement by the private sector
Are there any major infrastructure procurement projects in the private sector that might affect the cyber security of critical assets? Is an external purchase of key components in a critical infrastructure being considered?

Lack of academic funding
Are important academic assets, which are crucial for today's technology, such as validating trust or developing new technologies, compromised by the lack of funding?

Braindrain
Is there a risk of losing the most important talent in academia to provide independent advice on the proper functioning of a specific key technology? Is there evidence that leading talents in relevant fields are leaving the country because of better opportunities elsewhere?

Academic sponsorship
Is there a risk for important knowledge assets due to foreign (private) funding? Consider, for example, the possible loss of control over the skills needed to provide independent advice on the proper functioning of key technologies or the possible loss of control over scientific expertise that can serve as a basis for *generation after next*.

Q2: Current triggers in general (sector, market, world)

Market dominance
Is the market sufficiently efficient? Is the EU internal market mature in this area? Are there market developments that could give rise to unchecked dominance? Is there any market distortion? Are there a limited number of suppliers who have built up a quasi-monopoly through their market share or through market-distorting approaches?

New products
Are there any new product or service categories with cyber security implications?

New standards
Are there any new standards in this area (official or sectoral)?

New threats
Are there new (potential) types of cyber threats for which there is insufficient protection, or are existing threats becoming more frequent and greater?

New critical resources
Are there resources that are at increased risk (e.g. critical infrastructure, economy, democracy, freedom of expression, essential values)? What are the relevant threats and what is the potential impact on these resources?

New regulation
Is there any EU legislation in preparation that includes a cyber security component? Is there any foreign legislation in preparation that may create new threats or affect the supply of key technologies?

New disciplines
Are there new or emerging scientific disciplines that can have a cyber security application in terms of threats or mitigations?

Geopolitical pressure
Are there new geopolitical pressures affecting suppliers, users or scientific developments in the field of cyber security?

Generation after next
What relevant replacement technology is emerging with a five-year horizon? What new scientific and technical insights is this new technology based on? Which players currently have the leadership in knowledge and innovation in this field?

Identify measures- Q1, Q2, Q3, Q4 (Trigger diagram)

Q1: Keep control with us

Improving the domestic market
Creating or improving domestic market conditions for KETs in niche markets. Options for government intervention are smart procurement, improving the existing (digital) infrastructure, supporting substitution of foreign KETs.

Imposing conditions related to change of control
Options to consider are golden shares for the government, conditions in investors' agreements (*term sheets*), facilitation of regional investors' participation in capital. EU legislation should also be activated to open up access to platforms, unbundling (DMA, CER regulation).

Provide survival measures
Supporting a major supplier at risk of bankruptcy with legal and financial protection measures.

Blocking output
Refusing the export of key technologies to countries that could jeopardise strategic autonomy. Establishing restrictions on Foreign Direct Investment (FDI).

Conditions for public procurement by public authorities
Establish selection criteria, operating conditions or certifications.

Conditions for new tenders by private undertakings
Impose operating conditions or certifications.

Selective financing
Providing funding for major academic assets (trust validation).

Retaining talents
The measures that can be considered for retaining talents are academic support, career planning and funding for research & development.

Blocking in control - sponsorship
Deny private sponsorship of academic departments or knowledge institutes by legal or other means.

Q2: Increase influence

Regulations and policies
Influencing the development and application of EU regulations, such as certification for ICT security, cyber-risk management and market access, in the phases of definition, negotiation or implementation (e.g. through reference to standards) of EU policies.

Proactively putting emerging themes on the agenda by sharing analyses and national strategies with other Member States (together with a 'coalition of the willing').

Interests in companies
In consultation with other EU Member States, bring up threats against their own companies and defend them in competition cases or in restrictions on foreign direct investment.

Funding
Content direction and prioritisation through the programme committees of EU programmes for research & development, application and implementation of cyber solutions, skills and other investments, such as the Resilience & Recovery Fund, the Digital Europe programme, Connecting Europe Facility, Horizon Europe and the European Defense Fund).

Standards and norms
Supporting participation of local companies and knowledge institutes in international standardisation, multilateral standardisation (such as for defence with NATO or in the financial sector) or bilateral pre-standardisation (such as with the United States).

Supporting participation of ministries and stakeholders in international cyber security norms, confidence and capacity building measures (such as in UN GGE and UN OEWG).

Supporting the participation of researchers and industry in open source initiatives.

Q3: Gain and build control, seize opportunities with us

R&D funding
Financing the development of new key technologies by controlled enterprises. Supporting research & development of key technologies by start-up companies.

Smart tendering
Privileged purchase of 'controlled' companies (public procurement exceptions, smart purchases, launching customer). Providing assistance to start-ups (e.g. by taking Proof of Concept (PoC) against payment, providing exceptions on existence and financial criteria).

Participation in capital
Government participation in enterprises producing a key technology (golden share, government share, conditions in agreements).

Export support
Providing public support for relevant licences or insuring credit risk.
Certification of operating conditions.

Developing and financing certification schemes that enable operators to operate critical infrastructure or to procure reliable solutions.

Standards
Implementation of the standardisation and interoperability of key technologies.

Flagships
Establishing large-scale infrastructure projects that support critical services. Alignment with European flagships.

"Generation after next" - research & development
Use innovation funding and research & development funding for the generation after next technologies in this area.

Securing funding
Securing funding for academic expertise that can validate confidence in (external) market solutions. Independent validation of core claims by vendors so that buyers can rely on these claims.

Q4: Gaining and building influence, seizing opportunities in general

Investment climate
Create a legal framework that promotes risk investment and entrepreneurship. Compare the environment for these investments of the home country with countries that are successful in innovation (e.g. the United States, the United Kingdom, China and Israel), looking at legal, fiscal and financial conditions (e.g. stock options, recruitment/redundancy)?

Ecosystem
Facilitate an ecosystem that helps and encourages a start-up, for example by providing an overview with an inventory of funds, network of entrepreneurs and business angels. Compare the ecosystem (entrepreneurial networks, transparency of the venture capital market, activities of business angels, mentoring/accelerators) between your own country and countries that are very successful in innovation. Consider, for example, differences in legal, fiscal and financial conditions that can be transposed.

Processes and tools
Consider examples of government processes and instruments that stimulate innovation and industrial application of new technologies. Good practice examples are available, such as In-Q-Tel, Darpa/IARPA, Defence Strategy, Selective Purchase Policy (DIU in the US), Key Technologies List.

Laws/regulations
Adapting legislation to promote strategic autonomy. Consider, for example, public procurement exemptions, competition policy, foreign investment restrictions, unbundling, data management, trusted infrastructure, etc. Consider examples in other countries that are inspiring to go beyond EU legislation in the area of Mergers and Acquisitions (M&A) and possibly mobilise cyber diplomacy.

Standards
Promote active participation in the international standardisation and interoperability of key technologies.

Certification/accreditation
Implementing an infrastructure and tools to promote certification and accreditation, ensuring built-in security and trust. Promoting wider adoption of reliable and trustworthy technology and providing transparency on the balance between price and security.

Processes and tools
Defining and implementing processes and tools that support digital autonomy in the field of critical service providers. Learning from examples of publicly funded/organised processes and tools in other countries that encourage innovation and industrial application of new technologies that enhance security. Assessing opportunities to use intelligence insights to improve the protection of private companies and society as a whole. Another example is scenario planning and how other countries do this.

Education, training, counselling
Good practices in other countries to bring entrepreneurial mindsets and skills closer to technical and scientific faculties. Learn from successful recipes for training and incubation. Support exchange mechanisms to immerse entrepreneurs for a short period in thriving ecosystems. Also promote networking and exchange between successful entrepreneurs (exits, angels) and newcomers.

Science and technology processes and tools
Promote nodes of excellence in selected KETs, using existing examples as inspiration and comparison with other EU hotspots. Consider to what extent we can stimulate innovation and growth by investing in science, research & development in KETs while maintaining control. How to improve the impact by applying successful practices from other countries.

Strategic autonomy approach
Develop a national approach to strategic autonomy and cyber security with integrated, proactive processes and tools for policy development and monitoring.

Definition of the desired situation

"AS IS" situation
Provide a summary of the current situation, including relevant areas such as suppliers/customers, factor conditions (academic knowledge and critical resources) and the nature of government intervention. The analysis should include a description of factors over which insufficient control is exercised to determine the future in terms of strategic (digital) autonomy.

"TO BE" situation
Provide a brief description of the desired situation, including relevant areas, such as suppliers/customers, academic knowledge, critical resources and the nature of government intervention. Also pay attention to the targeted expansion of control. How and to what extent do the proposed measures improve strategic (digital) autonomy? Are they consistent and adequate? Have the possible harmful and negative effects been assessed and mitigated?

Implementation options

Risk management
Which risk assessment model should be followed (national or European)? What is the risk appetite and to what extent can we mitigate the risk? What is the residual risk and how is it mitigated?

Strategic partnership
Which 'like-minded' government partners are there and for which objectives? Which private partners (PPP) are there and for which objectives? Strategic interdependence or adaptation of trade/FDI policies? Is there a complementary mutual dependency with non-Like-minded parties? If so, is this dependency stable or can it be misused ('weaponised')?

Common global interest
Is there a global platform available that can be used for support? If so, for what purpose and in what way? Which non-governmental partners should be supported? Which actions should be chosen for Dutch (cyber)diplomacy to promote the common interest at global level?

Verification of completeness and coherence (Porter models)

When the measures concern a single company, use a model that provides insight into the company's relationships with suppliers, customers, (emerging) alternative products/services and competitors. Possible questions are: how stable and strong is that company's competitive position? What factors determine this position, such as government support? Do the measures affect the competitive position? Are the measures compatible with EU legislation or WTO rules, or just a concrete implementation of national or EU legislation?

In many cases, the analysis and measures relate to a sector as a whole. In this case, a model can be used that shows the factors and market dynamics for the sector concerned. Possible questions that may be helpful here are: Are all relevant factors and actors and their interactions included? What is the extent and sustainability of funding? Is there any leverage of EU funds? Can the government promote scale with export promotion? Is there a synergy between customer and sector interests, for example through flagship projects? Are there non-profit initiatives that government should support, such as open source developments or cybersecurity analysis? Is the support of a sector or selective cooperation with a number of companies permissible in relation to competition rules (EU, WTO) or justifiable with exception clauses, such as Art 346 TFEU (national security)?

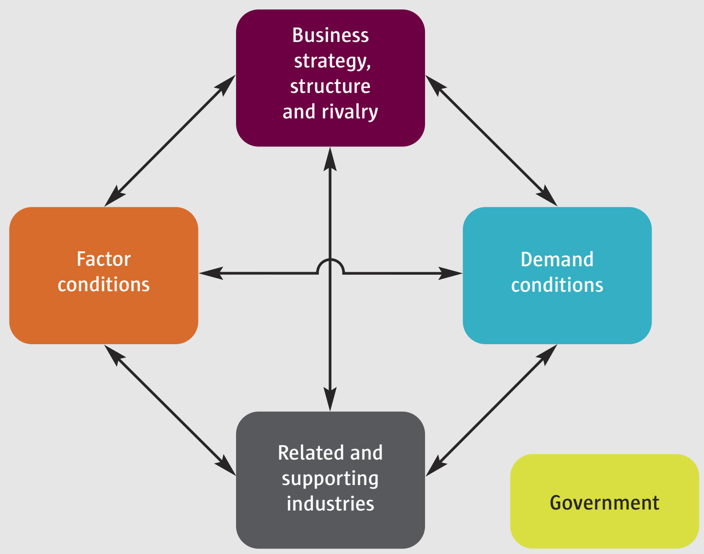
ANNEX 3: PORTER MODELS

Michael Porter developed two widely used models in the 1980s and 1990s, namely the Diamond model and the Five Forces model. With the help of these models, it is possible to map and classify existing situations and shifts on a national or company level. They allow the dynamics to be described in an explicit narrative.

Diamond model

The first model[13] is designed to analyse national competitiveness, innovation and market dynamics at the country level. This is also called the Diamond model.

Figure 11: **Diamond model**



A brief description of the elements, based on the given reference:

- *Factor conditions*: The country's position in terms of production factors necessary to compete, such as skilled labour, knowledge, infrastructure, capital or ecosystem more specifically in the relevant sector.
- *Demand conditions*: The nature of the demand in the home market for the products or services in the relevant sector.
- *Related and supporting industries*: The presence or absence in the country of subcontracting and other related industries, especially those that are internationally present and competitive.
- *Business strategy, structure and rivalry*: The conditions that determine how businesses are formed, organised and managed, as well as the nature of domestic rivalry.
- *Government*: This refers to the role of the government in the sense of public policy, whereby the government both imposes conditions on market players and stimulates the market (government as challenger and as catalyst). Government can only be successful if it works in tandem with favourable other conditions in the model.

13 https://hbr.org/1990/03/the-competitive-advantage-of-nations

Five Forces model

The second model, also called the Five Forces model (see Figure 12), is for developing a business strategy[14].

Figure 12: **Five Forces model**

A brief description of the main elements in this model:

- *Threat of new competitors*: new competitors bring additional production capacity to the market, putting pressure on existing players.
- *Bargaining power of suppliers:* dominant suppliers can keep more value for themselves by raising prices, reducing the quality of their products or transferring costs to their customers.
- *Bargaining power of customers*: dominant buyers can keep more value for themselves by pushing prices down, demanding more quality or more service and playing off suppliers against each other.
- *Threat of substitute products*: alternative solutions can replace the product or service by performing the same function in a different way.
- *Rivalry with existing competitors*: can take many forms, such as discounts, advertising, new products and improving services.

14 https://www.isc.hbs.edu/strategy/business-strategy/Pages/the-five-forces.aspx

CSR Cyber Security Council