Technology Assessment Framework

Authors

Timon Osinga, Lisa Soldaat, Wieger Voskens, Sacha de Wolf

November 2024

TNO innovation for life

Identifying and interpreting future (technological) developments is necessary in order to be able to anticipate the increasing complexity, uncertainty and degree of change in the world around us. On the one hand, this anticipation can provide opportunities and seize them, and on the other hand, organizations can be better prepared for new threats. This anticipation function is particularly important for organisations in the Defence and National Security Domain, both to seize opportunities and to anticipate possible future threats.

Technology Watch and Assessments

A technology watch is aimed at identifying technological developments and possible innovations (applications of technologies) that may have an impact on an organisation, a field or a domain (Peters & Thönissen, 2019). Technology surveys are almost always linked to a technology assessment, because merely an overview of trends and developments provides little interpretation and guidance (see Figure 1).

A technology assessment involves evaluating opportunities and threats of technological trends and developments and possible innovations for an organisation, a field or a domain (Peters & Thönissen, 2019). The field has its origins in the public sector, where it serves as a method to improve (strategic) decision-making processes. In this context, the aim of a technology assessment is to inform policymakers by assessing the short- and long-term impact of new technological applications within various domains (such as societal or economic)
(Tran & Daim, 2008).

TNO Technology Assessment Framework

This document serves as a framework for conducting TNO technology assessments, developed within the TNO Programme RVO Technology Watch 2024. The Technology Assessment Framework is an addendum to the 'Guideline TNO Technology Watch' delivered in 2023. Both documents contribute to improving the quality of TNO technology watch and assessments, by ensuring methodological consistency. Both the Guideline TNO Technology Watch and this Technology Assessment Framework serve as a tool: every technology watch and assessment always requires (partial) customization.

This Technology Assessment Framework can be used as a starting document for discussions with (potential) clients, or as inspiration for designing new project proposals. It provides an overview and elaboration of aspects for scoping, assessment criteria and various possible perspectives, which can support the assessment phase of a technology watch.

The framework distinguishes between three different levels, within which choices must be made. These choices will shape the final technology assessment.

Figure 1: Phases in a technology Watch, incl. assessment

Overview

The TNO Technology Assessment Framework distinguishes three different (subsequent) levels, within which choices must be made. These choices will ultimately shape the technology assessment.

Each level and the corresponding options will be explained in more detail in subsequent pages.

Level 1 Scoping

The choices that need to be made at this first level determine the scope and question that will be used for the technology assessment in question. The factors to be considered are as follows:

- **Level of abstraction:** is it strategic, operational or tactical level?
- **Scope technology:** is a (key) technology, a sub-technology or an application of a technology being considered?
- **TRL:** which TRL phase does the scope focus on? TRL 1-3 (Watch phase), TRL 4-6 (development phase), TRL 7-8 (demonstration phase) or TRL 9 (implementation phase)?
- **Term:** what is the timeframe? Is the development and/or impact in the short, medium or long term considered?

Level 2 Assessment criteria

The second level describes the assessment criteria that determine whether the chosen technology poses a threat and/or opportunity to the client. The (general) assessment criteria used for this are as follows:

- **Impact:** what is the impact when a technology is deployed?
- **Feasibility/probability:** to what extent is it feasible and/or likely that technologies will be used?
- **Threat:** based on the impact and feasibility/probability, what is the threat or opportunity of the technology?

Level 3 Angles

The third level describes the angles from which the technology assessment will be carried out. A choice can be made in various perspectives: from a perspective on the macro-environment (using the DESTEP model), from a national security perspective and from an organizational perspective (such as specifically the defence organization):

- **Macro-environment (DESTEP):** a model that can be used to map factors that have an impact on the macro-environment. Like; demographic, economic, socio-cultural, technological, ecological, and/or political-legal aspects.
- **National security:** factors on which technology can have an impact, which may have a disruptive effect on society.
- **Organisational perspective (such as specifically the defence organisation):** factors on which technology can have an impact within specific organisations (such as the defence organisation and its actions).

Level 1: Scoping

As mentioned, the choices made at this first level determine the scope and question for the technology assessment in question. To this end, the level of abstraction, scope of the technology, TRL and time frame are examined.

1.1 Level of abstraction

What is the level of abstraction of the technology assessment that the issue focuses on?

In general, for example for national security organizations, the **strategic level** is considered (long term, such as organizational policy); **tactical level** (medium term); or **operational level** (short term, such as day-to-day business operations).

Within the defence organisation, these levels of abstraction have a different definition, namely:

- **Strategic:** both the political-strategic level (coordination, development and use of power) and the military-strategic level (coordination, development and use of military power)
- **Operational:** the level that provides the link between the military-strategic objectives and the tactical deployment of units in which the campaign is designed, planned, executed and completed in the Joint Operations Area.
- **Tactical:** tactics are the manner in which formations and units are deployed in order to carry out military activities in a certain context and sequence to achieve (military) effects in relation to the objectives of the operational level of military action.

1.2 Scope technology

What level of detail of the technology itself is being looked at? An assessment becomes easier the more tangible it is.

- **(Key) technology:** the (general) (key) technology itself at the highest level of abstraction, for example 'quantum technology'.
- **Sub-technology:** a subcategory of a technology, for example 'quantum computing', 'quantum computation' and 'quantum sensing'.
- **Application of a technology:** for example, 'quantum imaging', 'quantum enabled radar', and 'quantum computing for big data analysis'.

1.3 TRL

Which Technology Readiness Level (TRL) of technologies is in scope?

- **Exploratory phase (TRL 1-3):** fundamental research into the basic principles of an innovation; formulation of technological concept and its practical applications; research into the applicability of concept on an experimental basis; testing and validation of hypotheses.
- **Development phase (TRL 4-6):** testing of Proof-of-Concept (PoC), research into the operation of the technological concept in a relevant development; extensive testing and demonstration of prototype in relevant test environment; insight into the operation of the concept.
- **Demonstration phase (TRL 7-8):** testing and demonstrating the concept in an operational user environment; testing of technological operation; certification; definition of the financial frameworks for production and launch.
- **Implementation phase (TRL 9):** innovation is technically and commercially ready; ready for production and ready for launch in the desired market environment.

1.4 Term

What are the deadlines for the technology assessment?

- **Short:** a short timeframe, for example within the next 5 years.
- **Medium:** a medium timeframe, for example between 5 and 10 years.
- **Long:** a long timeframe, for example from 10 years and beyond.

Level 2: Assessment criteria

Based on the choices made within level 1 (scoping), the assessment criteria to be used for the technology assessment will then have to be determined. The impact of a technology is often determined, together with the (expected) feasibility/probability of realizing the innovation. Based on this, it is possible to determine whether the technology poses a threat or an opportunity for the client.

The criteria that may fall under this are broken down here between *primary criteria* (recommended) and *possible additional criteria* (possible to include, depending on the issue).

2.1 Impact

Impact is about the (expected) contribution of the technology to the objectives of the person who sets the needs. What is the impact, in generic terms, when an application of a technology is deployed?

Primary criteria:

- **Operational added value:** the degree of impact of the technology application on the operation. How high is the potential added value on a strategic, operational and/or tactical level? Does the use of a technology make something more effective, efficient, faster, more flexible? What is the impact on the *joint functions*, to what extent does the technology application contribute to achieving specific mission goals, how does it affect the organizational dimension, or does it potentially threaten one of the national security interests?

Possible additional criteria:

- **Duration of impact:** effects that last only a very short time (hours) are likely to have a lower impact than effects that last a long time (months)
- **Convergence of impact:** some technologies can have a greater effect when combined or linked to other technologies (also known as the 'convergence of technologies'). This criterion refers to the potential cumulative effect of the combination of technologies. Think of AI, which can have a powerful impact when for example, combined with quantum technology (and vice versa).
- **Psychosocial impact:** the impact on society, even if the technology is not actually used, but only acts as a deterrent, can be significant (e.g. unrest and mistrust).
- **Geographical impact:** the impact of a technology used by an actor can range from only local impact to regional, national or even global impact. Think of specific cyberattacks that affect global supply chains.
- **Cross-domain impact:** a technology can have an impact on a specific sub-domain, or can have effects on multiple domains (e.g. GPS disruptions that have an impact on the financial system, navigation system, etc.)

2.2 Feasibility/probability

It is about the (expected) feasibility of realizing the innovation. How likely is it that applications of technologies will be used, both by friendly and enemy actors?

Primary criteria:

- **Absorption capacity:** the capacity of an organisation to absorb knowledge, its use in the development and deployment of innovations, and embedding it in the organisation.
- **Cost:** estimated investment required to deploy the technology. It is attractive to use technologies that are relatively cheap in terms of money (purchase and exploitation) or effort (manpower) and that have a positive cost-effectiveness for an actor.
- **Development time (TRL):** estimated time required to make a technology operationally viable. Time to applicability – from development to deployment. In what period can the innovation be considered practically applicable (provided that there is sufficient foundation and attention)?

- **Knowledge:** the extent to which an organization has access to the right knowledge base for the development and eventual deployment of the technology. An organization can have access to the right knowledge base because it is present within its own organization, or because the organization can use an existing knowledge base at third parties.
- **Linking industry:** the extent to which an organisation is able and willing to cooperate with industry for the development and eventual deployment of the technology.
- **Ethical/legal:** the extent to which the technology fits within the current ethical and legal frameworks of an organization.

Possible additional criteria:

- **International cooperation:** the extent to which an organisation cooperates internationally, or is dependent on it, for the development and eventual deployment of the technology.
- **Resources:** the extent to which an organization is dependent on resources that the organization does not have at its disposal, such as raw materials or facilities (for example, to test the technology).
- **Accessibility:** technologies that are widely available are more likely to be deployed, as they can be easily obtained and used by many state and non-state actors.
- **Sustainability:** technologies that endure for a long time or technologies that are rapidly evolving and under development are both attractive. The latter because they can be quickly adapted and changed to the current situation.
- **Ease of use:** technologies that are easy to use and require minimal training tend to be more attractive to actors, as they can be deployed quickly and used to achieve the desired effects.
- **Non-attribution capability**: technologies that, when used in an application, are impossible or difficult to detect, or impossible or difficult to attribute to a specific actor. Technologies that can be used in the cyber/virtual domain or technologies that support autonomous operations/systems often qualify for this. It also includes technologies with dual-use applications, as they can be used for benign purposes at the same time, complicating distinguishing between legitimate and illegitimate uses of the technology.
- **Remote employment*: t***echnologies that enable an actor to stay out of the 'danger zone' and quickly bridge large distances. Technologies that support autonomous long-distance operations or technologies that can be used in the virtual domain usually offer the possibility of working remotely. A higher degree of autonomy of a technology could require to less manpower and might enable unmanned/independent decision-making and operation.

2.3 Threat and/or opportunity

In addition to assessing the impact and feasibility/probability of the technology, it is possible to estimate whether the technology poses an opportunity and/or a threat to the client.

Whether the technology is seen as an opportunity or a threat depends on the perspective: does one look at one's own efforts, or those of an enemy actor? If the technology is assessed from the perspective of enemy deployment, it is possible to conduct additional research into the possible capabilities of specific relevant enemy actors. This allows a more realistic assessment to be made of how real the threat is or can become.

Level 3: Angles

After determining the scoping (level 1) and the assessment criteria used (level 2), the specific perspectives that are in line with the issue can be determined. These perspectives establish the frameworks in which the technology will be assessed.

These perspectives have been elaborated at three levels, namely that of the macro-environment, that of national security and that of the organisational dimension of specific security organisations. For the benefit of the defence organisation, a specific focus is placed on being able to assess a technology within defence operations.

3.1 Macro Environment (DESTEP)

Several models are possible for mapping the macro environment, including DESTEP, DIMEFIL and PMESII/ASCOPE. Within this framework, DESTEP is specifically highlighted:

- **Demographic:** development of the composition of the population, growth and size, including age, level of education, ethnic composition, etc.
- **Economic:** factors that influence the economic condition of a country, region or the world, such as purchasing power, economic growth, unemployment, government debt, etc.
- **Social/cultural:** factors that influence the social and cultural norms and values of (individuals in) a country or area, such as religion, behavioural norms, social trends, etc.
- **Technological:** factors that determine the development of technologies and science, products and therefore societies such as patents, automation, R&D funds, etc.
- **Ecological:** factors that relate to the physical environment of the earth (land, sea, air and space) and their impact on living organisms including people such as climate change, sustainability, water table, drought, etc.
- **Political/legal:** factors that relate to the political system and legal frameworks in a country, region or the world.

3.2 National security

Impact of the technology on national security interests. If one or more of these interests are seriously affected, there is a possible disruptive effect on society.

- **Territorial security:** the undisturbed functioning of the Netherlands and its EU and NATO allies as independent states in the broad sense, or in territorial security in the narrow sense.
- **Physical safety:** the undisturbed functioning of people in the Netherlands and their environment.
- **Economic security:** the undisturbed functioning of the Netherlands as an effective and efficient economy.
- **Ecological safety:** the undisturbed survival of the natural habitat in and near the Netherlands.
- **Social and political stability:** the undisturbed survival of a social climate in which individuals can function undisturbed and groups of people can live well together within the achievements of the Dutch democratic rule of law and the values shared therein.
- **International legal order:** the functioning of the international system of norms and agreements, aimed at international peace and security.

3.3 Organisational dimension

What organisational dimension does the technology have an effect on?

- **People:** focuses on the people within the organization in question, such as: education and training, availability of qualified people and knowledge management.
- **Operation:** focuses on the primary business processes (national security organizations) and/or operations (defence and operational organizations within the national security domain).
- **Organization and process:** focuses on the organization itself, such as: organizational structures, processes,

objectives (national security) and/or mandate (Defence).

- **Material:** focuses on the necessary resources and material needed to carry out primary business processes and/or operations, such as systems or specific defence equipment.

Joint functions (perspective Defence operation)

Functions of military action are a conceptual tool for commander and staff in integrating, synchronizing and directing capabilities and activities in operations. The strength of the functions of military action lies in their integration: together they provide the military capability of a unit. They must therefore always be considered in their mutual context.

- **Movement and Manoeuvre:** involves directing military capability where it has the greatest effect; this involves both the physical component of an opponent in a positional or geographical sense, and influencing the 'will of the enemy' or the 'perception of the actor' in order to gain the most advantageous position in relation to the opponent or other actor.
- **Fires:** creates a wide range of physical and psychological effects on actors in a direct or indirect way. It gives the commander the opportunity to seize on the physical component of the opponent, to infringe on his judgment and moral component.
- **Command and Control (C2):** command and control refers to the leadership and direction of a military organization to achieve its objectives, consisting of leadership, decision-making and command. Planning, direction, coordination and control guarantee the vertical and horizontal integration of (military) units and allocated resources.
- **Intelligence:** the result of knowledge and understanding of the activities, possibilities and intentions of all relevant actors and factors. Intelligence provides the most complete picture possible of the situation and is a prerequisite for success in any operation.
- **Information activities:** on the one hand, involves the use of information as a means to modify the opinions, views and perceptions of actors and to change their behaviour through strategic communication, information operations, psychological warfare and press information. On the other hand, information is crucial within one's own decision-making processes.
- **Sustainment:** Sustainment includes the support with material, medical, financial and human resources required to build and maintain military capabilities, which is important for maintaining and continuing operations until the mission is completed.
- **Protection:** the primary purpose of protection is to maintain freedom of action, so that a successful execution of the assignment remains possible. It includes all activities related to company safety (both in defence and security). Protection is aimed at preventing undesirable effects on the own force by limiting risks and, if possible, neutralising them.
- **Civil-military cooperation:** supporting a military mission through coordination and cooperation between the military action and civilian actors, at strategic, operational and tactical levels. This includes the national civilian population, local authorities, (inter)national and non-governmental organisations and institutions.

Use case: practical application

To indicate how the TNO Technology Assessment Framework can be applied in practice, the following use case has been drawn up. The choices that will shape the technology assessment are indicated in the boxes, with a brief explanation of these choices below.

Use case: technology assessment CLSK

- The (fictitious) question from the client is as follows: *"What are the most relevant technologies for the air domain in the next 15 years?"*
- The client is interested in both opportunities for their own organization and threats (e.g. 'how feasible is it for an enemy actor to use this technology')
- NATO's Emerging Disruptive Technologies (EDT) are taken as a starting point

Level 1 Scoping

Abstraction level:
- Strategic
- **Operational**
- **Tactical**

Since the technology assessment focuses specifically on the air domain of the Ministry of Defence, the operational and tactical level are examined.

Scope technology:
- **(Key) technology**
- Sub-technology
- Application of a technology

Because NATO's EDTs are taken as a starting point, the focus is on (key) technologies. The technology assessment becomes easier the more concrete it is, so it may be possible to break these down into specific technology applications prior to the assessment.

TRL
- Watch phase (TRL 1-3)
- **Development phase (TRL 4-6)**
- **Demonstration phase (TRL 7-8)**
- Implementation phase (TRL 9)

Because the time horizon is set at the present to the next 15 years, TRL 4-8 are probably the most relevant.

Term
- **Short (e.g. present – 5 years)**
- **Medium (e.g. between 5-10 years)**
- Long (e.g. from 10 years old)

In this case, the time horizon has already been determined by the client up to 15 years.

Level 2 Assessment criteria

Impact
- Primary criteria:
  - **Operational added value**
- Possible additional criteria:
  - Duration of impact
  - **Convergence of impact**
  - Psychosocial impact
  - Geographical impact
  - Cross-domain impact

'Operational added value' is a primary criterion when it comes to issues for the Ministry of Defence. In addition, the criteria 'convergence of impact' are probably interesting, as it concerns EDT technologies (high level of abstraction).

Use case: practical application

Feasibility/probability

- Primary criteria:
  - **Absorption capacity**
  - **Cost**
  - **Development Time (TRL)**
  - **Knowledge**
  - **Coupling industry**
  - **Ethical/Legal**
- Possible additional criteria:
  - International cooperation
  - Resources
  - Accesibility
  - **Sustainability**
  - Ease of use
  - Possibility of *non-attribution*
  - *Remote employment*

In order to estimate the feasibility/probability of being able to deploy technologies, both by one's own organization and by enemy organizations, the primary criteria mentioned are necessary.

Specifically for the air domain, it can also be interesting to pay attention to 'sustainability' (CLSK usually has to deal with long life cycles of platforms and weapon systems)

Threat and/or opportunity

Within this specific issue, the client is interested in both the threat of a technology (feasibility/probability of technology deployment by enemy actors and the expected impact) and the opportunities of a technology (possible feasibility/probability of deployment by own organization and the expected impact).

Level 3 Angles

Macro Environment (DESTEP)

- Demographic
- Economic
- Social/cultural
- Technological
- Ecological
- Political/Legal

National security

- Territorial safety
- Physical safety
- Economic security
- Ecological safety
- Social and political stability
- International Order of Law

Organisational dimension

- **Person**
- **Operation**
  - **Manoeuvre**
  - **Fires**
  - **Command and Control (C2)**
  - **Intelligence**
  - **Information activities**
  - **Sustainment**
  - **Protection**
  - **Civil-military cooperation**
- **Organization and process**
- **Material**

The perspective of the organisational dimension is the most self-explanatory, as the issue focuses on the operational/tactical level of the Ministry of Defence.

Contact

Timon Osinga

Timon.Osinga@TNO.nl
+ 31 (0)6 25 30 27 39

Lisa Soldier

Lisa.Soldaat@TNO.nl
+31 (0)6 15 30 38 03