Disruption in society – TA to the rescue?

EPTA Report 2022

EPTA

European Parliamentary Technology Assessment

Imprint

European Parliamentary Technology Assessment (EPTA)

eptanetwork.org

Berlin, 2022

Online available at www.tab-beim-bundestag.de/epta-report-2022

Disruption in society – TA to the rescue?

EPTA Report 2022

EPTA
European Parliamentary Technology Assessment

TAB
BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Contents

Preface

Distinguished reader,

this report is the result of a joint effort of members of the *European Parliamentary Technology Assessment* (EPTA) network. The members of the EPTA network advise parliaments in Europe and beyond on the possible social, economic and environmental impact of new sciences and technologies. Currently EPTA has 25 members (13 full and 12 associate). The EPTA network aims to strengthen the role of technology assessment in parliamentary decision-making and to establish links between different TA bodies worldwide.

Using three exemplary topics, we highlight the main theme of this report »Disruption in society – TA to the rescue?«:

(1) critical infrastructures (such as electricity, water supply, Internet) whose failure must be prevented at almost all costs;
(2) autonomous systems that make decisions with potentially far-reaching consequences;
(3) natural areas under severe pressure to »tip over« due to climate change and other human activities.

This report consists of 18 individual contributions of EPTA members giving their unique perspectives on specific aspects of the topics based on their recent experience. In the introductory synthesis, the individual contributions have been analysed and summarised to present overarching themes and to illustrate the various roles EPTA members have taken to support their parliaments in addressing disruptions. The report was produced at the initiative of TAB, which held the EPTA presidency in 2022. The contributions were synthesized by the editorial team: Michel Bermond (OPECST, FR), Reinhard Grünwald (TAB, DE), Walter Peissl (ITA, AT) and Tore Tennøe (NBT, NO).

1 Is disruption the new normal?

»Beware of innovation in politics«, George Washington is said to have uttered on his deathbed. To innovate used to be associated with excessive novelty, without a proper purpose or end.[1] Since then, the status of innovation has changed fundamentally. Revolutionary technologies such as electricity, assembly lines, refrigerators, and cars has been regarded as key to economic and societal progress, and an important subject for policymakers.

The breakthrough of digital technologies, from the PC and the internet to the smartphone and artificial intelligence, has carried the celebration of innovation to new heights. So-called »disruptive innovation« is turning markets and social practises upside-down in media, travel and elsewhere, with AirBnb and Uber as much quoted examples. To its proponents in Silicon Valley, this radical technological change is an inevitable and ultimately progressive consequence of digitalisation. Disruption is trumpeted as the norm.

In parallel, a string of crises has brought to the fore a less benevolent form of disruption, namely major disturbances in society at large. Following the great recession of 2007-2009, not only financial systems, but also trade and international relations were disrupted, and arguably also domestic political discourse in many countries. The COVID-19 pandemic started as a health crisis, but the weight of the disease and the countermeasures soon lead to an economic crisis, and furthermore, a social disruption with strict lockdowns and school closures.

The Russian war of aggression in Ukraine is also a major disturbance to the international order and energy infrastructure in Europe and the rest of the world. With the looming climate and nature crises in mind, it is fair to say that societal disruption seems to be the new normal.

In all the crises mentioned above, technology plays a significant role, either as a root cause, a catalyst, a modifier or a solution. Technology Assessment (TA) explores how current technological developments affect the world we live in and aim to contribute to the formation of public and political opinion. In this report, we analyse and assess three different types of disruption, with different implications for policymaking and society.

Critical infrastructure – interdependent and vulnerable

The first type is the disruption of the very technological systems that we have become dependent on. *Critical infrastructures* – water and energy supply, food, transport, health and communication – are essential to economic, social well-being, national security or even the functioning of society as a whole.

In other words, failures of critical infrastructures must be prevented at almost any cost. The first big challenge is to map out and understand the risks and vulnerabilities at play. One major factor analysed here is the rapid digitalisation of everything; cities are getting smarter, administrative processes are going online, water distribution networks increasingly rely on automation and a

[1] Lepore, Jill: »The disruption machine«. The New Yorker, 23 July, 2014. https://www.newyorker.com/magazine/2014/06/23/the-disruption-machine

digital infrastructure, and billions of (embedded) devices are being connected to the internet of things (IoT). Cyberattacks on infrastructure can be made from anywhere in the world, and only needs to succeed once, while the defender needs a 100 percent success rate.

This challenge is exacerbated by interdependencies and cascading effects: Damage in one sector (such as electricity) might have a profound impact in a different sector (such as distribution of medicines to patients) and can thus lead to transboundary crises.

How to increase resilience for critical infrastructure is, naturally, the other big challenge. Effective measures might have considerable trade-offs with welfare for citizens, climate policy, or human rights.

Autonomous systems – when humans lose control

Our second type of disruption is about *autonomous systems*. Here the loss of human control or oversight is not a bug, but a defining feature of the technology. Autonomous systems are meant to plan and execute actions with minimal human involvement. The advent of new, powerful models for artificial intelligence such as GPT-3 – which can write prose indistinguishable from a human author[2] – shows that autonomous systems have the potential to disrupt professions and markets, and perhaps lead to forms of inscrutable discrimination.

An even more existential challenge is the introduction of autonomous weapons systems that can perform both target selection, the decision to attack and authorisation of engagement. This might lead to entirely new and unpredictable dynamics in future conflicts. How to maintain a meaningful human involvement in vital decisions, regulate this technology in a situation of fierce competition and secrecy, and be able to analyse the different scenarios, are thus key questions for policymakers.

The disruption of nature

The third, and final, theme in this report is *the disruption of nature*. Environmental historians use the term »the great acceleration« to describe the radical transformation of our relationship with our natural habitat since 1945.[3] Our environment is transformed by our own activities, and human-made climate change is reinforcing this on an even larger scale.

The challenge here is something of a paradox: How can we use science and technology to mitigate a problem that was created by our use of technology in the first place? The case of near-natural forest conversion shows that policy here needs to address many conflicting goals (conservation, species protection, climate mitigation and adaptation, sustainable use of raw materials etc) simultaneously and strategically. Or perhaps we should relinquish control and leave the forest to the self-regulation of the trees and its ecosystem partners?

[2] perhaps this piece was produced by GPT-3?!

[3] Tooze, Adam: Shutdown. How COVID shook the world's economy, p 291-292. Allen Lane, 2021.

In this report EPTA members present 18 case studies on these three facets of disruption. This provides an excellent overview of the diversity and richness of approaches in the EPTA community to support Parliaments across Europe and beyond to deal with disruptive change.

2 Critical infrastructures – how to avoid disruptions?

Running tap water, full shelves in supermarkets, medical care, cashless payments – these and other essential services have become a given in modern societies. Memories of supply crises date back to the last century and we trust that services that work today will continue to do so tomorrow. However, events such as the international financial crisis, the COVID-19 pandemic and the war in Ukraine have made visible that this feeling may be misleading. These and other threats (e.g. natural disasters, technical failure or human error, cyberattacks) can cause sudden disruptions, damage or failure of critical infrastructures (CI). Given our dependency on CI, major infrastructure failure would cause significant harm to people and result in severe societal disruptions.

In a study of the German TAB in 2011[4] it was demonstrated drastically, that after only a few days, the supply of the population with (vital) goods and services can no longer be secured in an affected area.

- After the onset of the power blackout, some telecommunications and data services fail immediately. Battery powered mobile networks may function for a few days. However, due to the increased volume of calls, these are mostly overloaded.
- Public-law broadcasting corporations are better prepared and are able to continue transmissions. However, citizens are unable to receive broadcasts via their televisions. Radio represents one of the most important information channels.
- Electrically driven transport modes, especially rail transport, either fail immediately or after a few hours.
- Road traffic becomes chaotic, as traffic lights fail and junctions, tunnels and barrier systems are blocked. There are numerous accidents and emergency services encounter major difficulties in carrying out their duties. Since most petrol stations are out of action, most vehicles remain at a standstill and local public transport can only be maintained at a rudimentary level.
- The striking effects are not restricted to the transport sector – if logistics fail, cascading effects will emerge and induce a breakdown in food supply for consumers, nursing facilities, hospitals and the like. In our networked society just-in-time-production and delivery-on-demand prevail. In concrete terms, this means that hospitals, for example, only have supplies of necessary medicines and other important aids for a few days on hand, and if replenishment fails, medical treatments are severely impeded or even impossible. Emergency generators usually only have a fuel supply for a few days. Getting supplies under the circumstances described is a major challenge.

[4] https://publikationen.bibliothek.kit.edu/140085927/120049880

According to the European Critical Infrastructure Directive[5] »critical infrastructure« means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions«. CI include the sectors of water and energy supply, food, transport, health and communication. Broader definitions can vary from country to country and include, in addition to the above, the sectors of waste disposal, finance and insurance, media and culture, and governmental administration.

All these sectors are more or less interconnected and increasingly dependent on each other. This dependency has been reinforced by digitalisation, which helps on the one hand to manage complex systems more smoothly and efficiently, but on the other hand raises the dependency on communication networks and electricity. At the same time, energy systems are under stress due to the need to drive the energy transition away from fossil fuels to renewables. This has introduced another level of complexity into the systems. Interdependencies also increase the likelihood of cascading effects, in which damage in one sector has an impact in completely different areas and can thus lead to cross-section crises.

The examples in this report show that EPTA members have been working on CI for a long time and contribute to raising awareness of the potential societal consequences of CI damage. While some are generally concerned with CI and issues of electricity supply, digitalisation and communication (DE, AT), others focus on digitalisation and energy transition issues (NL). Particular attention is also paid to cybersecurity issues and the vulnerability of IoT systems (NO, EP). Communication in the event of a crisis should be as secure and simple as possible, which leads to the question to what extent modernisation and standardisation can help (PT). The electrification of the transport sector (SE), which in turn has repercussions for other systems, is analysed as contribution to achieving the 2030 climate goals. Finally, the EPTA-member from Wallonia was directly involved in the ex-post analysis of the flooding in 2021 in order to draw conclusions for future emergency planning.

The complexity of CI implies a relatively high number of involved stakeholders. Due to the cross-sectoral structure of CI, in most countries there is a shared responsibility between public institutions (federal ministries, regional authorities, task forces, etc.) and private companies providing CI services. A widespread problem is that pressure to save money in public budgets and the prioritisation of the efficiency paradigm in private companies are causing systems to »dry up«. Often savings are made on maintenance and renewal work or the provision of backup systems that are used only at rare occasions. When it comes to physical parts of the CI, such as dams, this could have direct catastrophic consequences. For the software parts of CI this is perhaps even more problematic, as it may compromise the security of the systems and provides easier targets for cyber attackers.

Institutional responsibility on CI issues is usually based on national or regional regulation. This in turn builds in part on the ECI Directive 2008/114/EC 1, which is also supplemented at the European

[5] 2008/114/EG https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

level by the European Programme for Critical Infrastructure Protection (EPCIP).[6] As the COVID-19 pandemic has shown, global interconnectedness can very quickly lead to disturbances and even disruptions in key areas of society, suggesting that regaining European sovereignty in industrial and technological matters should be a top priority.

Societal and political importance

Citizens become aware of the paramount importance of the CI especially when a failure or worse, a disaster happens. The floods in Wallonia and Germany in July 2021 were such a catastrophe. Various attacks on the IT infrastructure of regions, municipalities, universities and other public institutions that disable public services for days, weeks or even months are further examples. At the same time, tales about looming large-scale blackouts in the power supply are booming and are also being fuelled in the media. This reduces the perceived level of security among the population and creates a sense of unease.

The COVID-19 pandemic has revealed that modern societies turn out to be less stable and more vulnerable to sudden shocks than many had assumed. Recent attacks on underwater gas pipelines in the Baltic Sea made very clear to almost everyone how vulnerable modern societies are. Therefore protection of CI is a high priority in many European countries. In most of them cybersecurity was predominant since the early 2020ies.[7] Some measures, which were meant to raise security, turned out to be problematic from a human rights perspective and fuelled discussions on data protection, privacy, freedom of speech etc. in several countries.

3 Autonomous systems – human in the crosshairs of the machine

Autonomous systems are software-based or robotic systems that can plan and execute actions without or with minimal human involvement. Autonomous systems are being introduced at an accelerating pace in many different areas, where they often redefine the rules of the game, heavily impacting economic and social wellbeing in many countries around the world. This is foreseeable, for example, in transportation (autonomous cars, ships, trains and aircraft) and, in the future, possibly in care for the elderly and the sick (care robotics). But pure software systems are also in use, for example in the form of algorithmic decision-making systems in finance (determining creditworthiness of customers), human resources (applicant screening and selection) or, for example, in the penal system (determining the probability of recidivism).

Actions of autonomous systems can have significant consequences. Accidents of self-driving cars with fatalities have been reported and stirred public debates about the impacts of autonomous cars on society. Another current example is the Dutch child benefit scandal, in which the tax agency wrongly accused 26,000 parents of fraud, based solely on the assessment of an algorithmic system. This highlights a central topic in the political debate: how to prevent algorithmic systems from

[6] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

[7] See the European NIS Directive (2016/1148) https://eur-lex.europa.eu/eli/dir/2016/1148/oj and the respective national implementations.

discriminating against specific groups in society (gender, sexual orientation, age, ethnic origin, religious beliefs or other).

Autonomous weapon systems (AWS) are of particular concern, because literally decisions of life and death are involved. Sending autonomous systems onto the battlefield and exploiting their advantages, for example their speed of evaluating sensor data, without having to endanger the lives of one's own soldiers, sounds attractive from a military point of view at first glance.

Automation and autonomy are already used today for a wide range of functions in weapon systems (including searching and identifying potential targets using sensor data, tracking targets, prioritizing and determining when to attack them). The expansion of autonomous functions of weapon systems is therefore on the agenda in all technologically advanced countries. However, until now, target selection, the decision to attack and finally the authorisation of the weapon engagement are carried out by a human commander or operator.

An AWS would be able to perform all of these steps, including target selection and engagement, on its own with no (or minimal) human involvement. Proponents of this development argue that AWS may have humanitarian benefits, since military operations could be carried out more precisely, thus better protecting civilians and civilian infrastructure. Critics, on the other hand, express concerns as to whether it would be ethically justifiable, politically responsible and permissible under (international) law to delegate decisions on the life and death of humans to machines. The development and possible use of AWS would also entail security policy risks as well as the danger of armament spirals and uncontrolled proliferation of potentially risky technologies.

The increasing use of automated and future autonomous weapons systems might represent a paradigm shift that will revolutionise warfare in the 21st century. International preventive arms control efforts to contain the obvious risks of AWS are currently making little headway. Among other things, some states point out that not enough reliable knowledge is yet available to weigh up the opportunities and risks of AWS. The original task of technology assessment is to analyse possible impacts of the development and deployment of AWS and thus provide the orientation knowledge urgently needed for this difficult assessment. This is a major challenge, as technological development is very dynamic.

Situation in different countries

In many countries, (semi)autonomous systems are developed and used on a pilot scale in a wide variety of sectors, such as finance, healthcare, agriculture, mobility, energy, social security and the military domain.

Currently a number of countries use weapon systems with some degree of autonomy, for example short-range air defence systems that can operate in a purely automatic mode to intercept incoming projectiles (e. g. rockets, artillery and mortar shells). Even if this can be classified as an autonomous weapon system, there is still quite a long way to go until weapon systems enter the scene that can move freely in a cluttered, dynamic and hostile environment and carry out complex missions on their own.

A step in this direction are weapon systems like the British Dual Mode Brimstone guided missile, which can search a specific area to identify, track, and strike vehicles using sensor data. Uncrewed air, sea, and land-based vehicles designed for weapons delivery can operate with a high level of autonomy. Most developments have been in the aerial domain. Currently the UK operates the MQ-9 Reaper, several others are under development, some of them designed to operate in a swarm. Uncrewed offensive weapons are not used to make firing decisions without human authorisation, although this technical capability exists.

There is a massive investment into development of increasingly autonomous systems in some countries, e. g. in the Netherlands for (armed) sensor systems. The UK strives for AI-capable systems for military applications across the land, air, sea, and cyber domains. Systems are in use or development for military applications including intelligence, surveillance and reconnaissance, data analysis, and weapons systems.

As a reaction to Russia's war of aggression Germany decided that 100 billion Euro will be provided, in order to modernise the armed forces and to close existing capability gaps immediately. A considerable part of this fund will be invested in the armament of Heron TP uncrewed drones, and in the development of the European Future Combat Air System. FCAS is a »System of systems« which consists of a new combat aircraft, envisaged to work together with unmanned components, so-called remote carriers (manned-unmanned teaming) and an Air Combat Cloud, which ensures real-time information for all involved subsystems.

Stakeholders

There are various stakeholders contributing to the research and discourse around automation in military technology and its future implications. These include think tanks, academic stakeholders (universities, research funding bodies), NGOs, the ICRC.

The UK Government expresses its ambition in a comprehensive Defence AI Strategy, that the Ministry of Defence (MoD) published in June 2022, which sets out how it plans to adopt and exploit AI. To this end the UK Government recently established a Defence AI Centre (DAIC) to coordinate the UK's development of AI-enabled technologies for defence.

In contrast to the UK, the German Armed Forces keep a low profile in the public debates on the issue of AWS. The only publicly available official document that deals at length with AI in the Bundeswehr is from 2019 and focusses only on the land domain. One of the reasons for this seems to be that there is currently no consolidated government position on AWS presumably because of differing views by the Ministry of Defence and the Foreign Office.

A very special approach is visible in the Netherlands: Research and innovation in the domain of AI is pushed forward in a collaborative way by the government together with private and civil society actors in form of public private partnerships like the »Dutch AI Coalition« (NL AIC). Ethical, legal and social aspects (ELSA) are included at a very early stage. Through field and innovation labs the government aims to »stimulate viable AI solutions for societal challenges«, including a Defence ELSA Lab.

Legislation in place and in consideration

A number of existing laws regulate the use of autonomous systems like algorithmic decision systems, such as the General Data Protection Regulation, administrative law, procedural law and sectoral laws. Apart from the national level, the EU is a key player in terms of stimulating responsible innovation in the digital domain. A range of existing policies, frameworks, regulations and principles are relevant to the technologies and challenges related to autonomous systems. In the last two years some groundbreaking documents were issued: Declaration on European Digital Rights and Principles (proposed January 2022), Path to the Digital Decade (proposed September 2021), AI Act (proposed April 2021), 2030 Digital Compass: the European way for the Digital Decade (proposed March 2021), Lisbon Declaration – Digital Democracy with a Purpose (adopted 2021)

Very relevant for AWS is the upcoming AI Act, that specifies requirements regarding transparency, explainability and accountability of high-risk AI systems. However, debate remains if these requirements are sufficient.

The European Parliament (EP) took a weighty stand when it adopted the resolution on AWS, that called for the adoption of an EU common position on lethal autonomous weapon systems that ensures meaningful human control over the critical functions of weapon systems. It was stressed that the EU's role in global disarmament and non-proliferation efforts needs to be expanded, that the EU needs to speak in relevant forums with one voice and that best practices should be shared on the matter of lethal autonomous weapon systems, to garner input from experts, academics and civil society. The EP calls for an EU legal framework on AI with definitions and ethical principles, including its military use.

Societal and political debate

The societal and policy debate on autonomous systems in general started in many countries around 2013 – 2015. In the beginning, for example in the Netherlands, it focused mainly on the fear of mass unemployment due to the rise of robotics. After that, the debate broadened up to more ethical, societal and legal issues relating to AI. Gradually, safeguarding human rights and public values became a more prominent part of Dutch digitisation policy. The latest discussion points are non-discrimination, explainability and accountability.

In terms of AWS, the national debates are very much shaped by national self-perception with regard to military affairs and its significance for foreign policy. For example in Germany there has been a lot of controversy in Parliament and in public fora about the question whether Germany should procure armed UCAVs (Unmanned Combat Aerial Vehicles). After years of fierce debate, the Bundestag decided in 2018 to procure optionally armable Heron TP drones by way of leasing them from the Israeli manufacturer. Only this year it was finally decided that the option to arm the Heron TP will actually be used. A similar debate took place in the Netherlands: In April 2022, the Dutch Parliament has agreed that the Dutch army is allowed (in specific circumstances) to arm unmanned drones. Up until then, unmanned vehicle areas were only allowed to gather intelligence.

In the UK there is much less hesitation in this respect, as long as, like the Defence AI Strategy of the UK Government states, weapons which identify, select and attack targets have »context-appropriate human involvement«. However the question remains, what exactly is meant by that.

The key question of what kind of human involvement or control is required in order that AWS can be operated conforming with international humanitarian law and with ethical principles is debated internationally under the roof of the CCW (Convention on Certain Conventional Weapons) in Geneva. But the current situation is not very favourable for an international agreement on any kind of arms control issue. This is a serious problem in the context of the CCW, since decisions can only be taken by consensus. The currently most likely outcome of the ongoing talks is therefore a complete failure. This means that other forums than the CCW must be sought for actors willing to strive for some kind of regulation of AWS.

4 Nature under pressure – human as a disruptive force

Rapidly advancing climate change, the rising world population and the overexploitation of natural resources are putting nature and its ecosystems under massive pressure. The age in which we live is therefore also referred to as the Anthropocene – an age in which humans are shaping the earth on a geological scale, often with disruptive force.

Global forests, being particularly sensitive, diverse ecosystems, are especially affected by this development. They are not only resources of global significance, and thus an economic factor, but also fulfill central functions for the preservation of biodiversity and climate protection (CO_2 storage). Forests provide habitat for 80 % of amphibian species, 75 % of bird species and 68 % of mammal species, and tropical forests contain about 60 % of all vascular plant species on the planet.

Forests are crucial for mitigating climate change. They contain more than half the global carbon stock in soils and vegetation. Despite a continued reduction in area, forests still absorb more carbon than they emit mainly due to reforestation and improved forest management.

In addition, forests have a range of other positive impacts on local and global climate, by affecting albedo and regulating atmospheric humidity. This helps, for example, to keep certain areas habitable in the hot summer months. Not to forget the social uses like recreation and hunting.

Due to its enormous importance, Catalonian, German and Greek EPTA bodies devoted their contribution to this topic.

At first glance, Catalan forests seem to thrive: since 1990, the forested area has increased by approximately 30%. But actually the outlook is grim. The forest sector contributes only a marginal percent to GDP, Catalan forests' ability to provide ecosystem services is declining, intensive resource extraction in some regions, while abandoning others, is compromising biodiversity levels. Furthermore, like other Mediterranean regions, Catalonia is subject to intense and frequent wildfires.

In Germany, forests today face threats, which are the consequence of a series of actions taken starting more than 200 years ago. Largely deforested landscapes were quite typical of Germany around 1800. From around the middle of the 19th century, large areas were afforested with fast-growing spruce and pine stands, mainly for economic reasons. Today, forest ecosystems are once again facing a major challenge: the extreme drought years since 2018, together with storms and bark beetle infestations could lead to a complete destabilization if the current forest ecosystems do not become more resilient.

Different to these two broader views, the contribution of Greece is focused on wildfire management. The damages and effects of fire on ecosystems is diverse and there are references to alterations in the composition of species, in the roots of trees and soil, and in the properties of water infiltration after fire. In addition, under current climate change, it is expected that extreme rainfall events may accelerate soil erosion in burnt areas.

Other topics are equally typical of the »Nature under pressure« theme. Surrounded by the ocean, Japan has had a serious problem with marine litter, which primarily consists of plastic waste, since around 2000; therefore, the NDL contribution is all about plastic waste management. TA-Swiss decided not to focus on a specific environment but on the consequences of a global phenomenon; therefore, it submitted two contributions on some specific aspects of greenhouse gas (GHG) emissions.

The solutions: straightforward or complex?

Solutions sometimes look rather straightforward – at least in their broad principles. Greece identified unmanned aerial vehicles (drones) as a promising way for burned land to be reforested and anti-erosion measures to be implemented. Drones are able to »sow« large numbers of tree seeds on a daily basis, covering, in a short time, very large areas, as well as areas which are particularly difficult to access. Switzerland hopes that the so-called »Negative Emissions Technologies« (NET) can help to offset the residual GHG emissions, as they are designed to remove CO_2 from the atmosphere and store it through biological and technical processes or use it as feedstock. In the agricultural sector, vegetal substitutes to milk and meat can be found, reducing environmental pressures of animal agriculture.

Sometimes however, straightforward solutions do not exist. Considering the complexity of forests as an eco-socio-system, this is not surprising. The key challenge is to rethink forest management principles in order to design a true multifunctional process, where climate change mitigation, biodiversity conservation and the development of a circular bioeconomy are taken into account.

Concepts are being developed, e.g. in Catalonia attempt are made to internalise forest externalities in the economy and to complement traditional forestry revenues with payment of ecoservices. In Germany the paradigm of »permanent forestry« evolved, which avoids clear-cutting, instead only single targeted trees are felled and classical forest protection measures are kept to a minimum. But to put these concepts into praxis is easy to say but hard to implement.

Orientation of public policies

Dealing with these extremely important environmental issues, governments usually use the full range of available tools. On a strategic level, framework policies are put in place. For instance in 2021, the Catalan Government approved the *Catalan Bioeconomy Strategy 2030 (EBC 2030)*. Its main goal is to promote the sustainable development of the Catalan economy by promoting the production of local renewable biological resources. Another example is the Japanese *Resource Circulation Strategy for Plastics* (RCSP) to promote plastic resource circulation, published in May 2019.

These strategies are then enacted by legislation like the Japanese *Plastic Resource Circulation Act* (PRCA), which aims at encouraging voluntary efforts by all stakeholders involved in whole lifecycle of plastics, from designing products to disposing plastic waste. In 2023, Switzerland will organize a referendum in order to decide whether CO2 storage should be entirely national or could be possible abroad; directives for implementing NET could be included in the overall *CO2 Act* revision, due by 2025.

With the strategic framework and supporting legislation in place, direct action can follow suit focusing on specific issues. That is the case in Greece with the project »Study of the Adjacent Environment and Characteristics of the Selected Areas for Drone Seeding«. Another Example is the Catalan EBC 2030 which is accompanied by an Action Plan to be executed 2021-2023, structured around seven strategic objectives.

Societal and political debate

Decisions to be made on how to meet the challenges of »Nature under pressure« affect the interests of numerous stakeholders. Governments, municipalities, businesses, consumers, environmental groups, etc. have very different views in some cases. It is therefore not surprising that a lively, sometimes even heated, debate would emerge in society.

In Germany, the debate unfolds on the very principles of commercial forest use and active forest management, especially the question of the extent to which reforestation of damaged areas with non-native climate-resilient tree species should be permitted. Nature conservation associations and ecologists are calling for a fundamental paradigm shift, arguing that the forest, as a natural ecosystem, can only develop its self-regulatory powers if it is largely left on its own. It is demanded to withdraw up to 30% of the forest area from any use. Forestry companies and forestry associations oppose this and point out – supported by parts of the scientific community – that natural processes cannot keep up with the speed of climate change and that human intervention is therefore urgently needed.

Tensions arise about the (proven or alleged) consequences of the considered policies as well. Carbon sequestration in trees and surface soils involves reversing deforestation, reforestation, increasing soil carbon levels and enhancing wetlands; this opens up great debates in Switzerland about the implementation of these practices for agriculture and land use. Here a clear interlink exists to the topic of plant-based alternatives to meat and milk. If traditional pastoral practices in alpine regions were hindered, the landscape would change drastically, and the ecological benefits of lifestock production would disappear (for example, it contributes to biodiversity if it is sustainable and extensive).

5 Parliamentary Technology Assessment to the rescue?

In these current times of multiple crises and looming disruptions, what can Parliamentary Technology Assessment (PTA) do to help guiding our societies into calmer waters? The main task of PTA is to provide the political decision-making process with a current and reliable scientific basis. Technology assessment is valuable by demonstrating possible implications of technologies and thereby initiating public debate. PTA develops options for action and analyses their impacts to support Members of Parliament to make informed decisions.

The contributions of the EPTA member institutions featured in this report show that there is a range of functions that they have performed for their parliaments:

The »technology radar«

In many countries, PTA serves as a »technology radar« for parliaments, eg. by monitoring international developments of various socio-technical innovations (NO, AT). An approach used frequently in many variants is foresight. STOA (European Parliament), for example, has adopted foresight practices for studies of science and technology-related policy issues that are complicated and/or have a controversial nature. This applies particularly to areas where clear-cut policy options are difficult to formulate, or the controversial nature of the issue can hinder the acceptance of policies. An ambitious concept of a »crisis radar« is currently being developed by TAB (DE), aimed at strengthening the resilience of society, politics and the economy by means of crisis early detection. Early studies on power outages (NL and DE) contributed to a heightened awareness of the increasing vulnerability of modern societies.

The »what-if« generator

Even tough PTA is a forward-looking activity it is hardly ever about predicting what the future will look like. Typically, PTA approaches possible future developments by generating »what-if« scenarios. Good examples can be found in projects that mapped possible consequences of an assumed large-scale failure of the core digital and/or electrical infrastructure (NO, DE). Scenario methods are particularly well suited to investigate dynamics in systems and how they play out. An essential question for PTA is to what extent scenarios like this are sufficiently integrated on a national political level.

The »wide-angle-lens«

TA, as an intermediary between different stakeholders, can also influence the processes of emergency planning and response. Those directly involved in the processes are often so preoccupied with their own systems and dynamics that communication with others falls short. However, it has been shown, especially through the creation of »big picture« plans and related training, that this intersectoral and interdisciplinary interaction with stakeholders, significantly increases collaboration in the event of an emergency and thus contributes to improved resilience.

The long tradition of some EPTA members in the field of digitalization, information technology and security research (NL, AT) induced very early public debates on problematic developments with respect to fundamental rights and democratic deficits, but also opened up the perspective to a broader platform of public values, such as human dignity, equity and equality, autonomy, balances of power and sustainability (NL).

The »sense dog«

PTA has very successfully adopted the role of a »sense dog«, putting issues on the agenda before they become virulent. For example early 2017, the Rathenau Instituut (NL) concluded in a report entitled »Urgent upgrade« that the government, industry and society were not yet adequately prepared to deal with the arising ethical, legal and societal issues digital technologies raise. All actors needed to take action to steer the digital society in the desired direction. This report turned out to be a pivotal publication, as it initiated political and public debate on digitalisation on a large scale in the Netherlands.

A »helping hand« for Parliamentary scrutiny

Some activities of POST (UK) can be described more like a »Sherpa«, very directly supporting parliamentary activity including scrutiny of the Government's defence AI strategy and other committee inquiry work.

A »step stone« for a safe tread

A very similar role is performed e. g. by TAB (DE), which delivers solid and reliable assessments as background information and reliable footing on issues of parliamentary concern (»step stone«).

The »open street map« for policy options

Finally, one of the most important roles of PTA is to develop and assess a variety of policy options that improve the capacity of society to deal with disruption. E. g. by making supply chains more resilient and the industrial and social environment capable to adapt, tackling all possible challenges of the new situation. The main task remains to provide Parliaments with a balanced and easily understandable summary of the potential outcomes of alternative policy options. Thereby contributing to increasing resilience by supporting the preparedness of policy makers to face disruption.

The point of departure for this report is the notion that societal disruptions are becoming more frequent, pervasive, and related to technology. This does not mean, however, that they are inevitable. The disruption we have described are all ultimately human made, and can be mitigated, shaped, or even averted by our own actions and political decisions.

In this report EPTA members present 18 case studies on these three facets of disruption. This provides an excellent overview of the diversity and richness of approaches in the EPTA community to support Parliaments across Europe and beyond to deal with disruptive change.

The final authority to judge the usefulness of PTA is – of course – the Members of Parliament and Parliaments as a whole. Given the enormous demand for PTA studies by all EPTA Parliaments in recent years, combined with the steadily increasing number of EPTA members around the world, the authors of this report are not afraid of the verdict.«

EPTA Member Contributions

Critical infrastructures – how to avoid disruptions?

Austria – Institute of Technology Assessment of the Austrian Academy of Sciences (OeAW ITA)

Disruptive Risks for Critical Infrastructures in Austria

Jaro Krieger-Lamina

What is it about?

Our modern society heavily relies on the functioning of its infrastructures. Outages are rare and generally resolved quite fast without causing further issues in other sectors. A large-scale failure, affecting a high number of citizens and/or lasting for a long time period can be seen as a disruptive risk to our society because, beyond threats to lives and the health of people, economic loss etc., it could cause a traumatic experience on individual and societal level that has the potential to permanently change the way we live.

Additionally, the ongoing developments, like the necessary transition of the energy system, the increasing complexity and mutual dependencies between critical infrastructures involve disruptive risks for their providers, on an organisational and systemic level.

Therefore, a high emphasis is put on the operational security of these infrastructures, that are relevant for our day-to-day life. The introduction to the call for submissions to this report even stated «*… whose failure must be prevented at all costs*«.

Beside the fact that the term »at all costs« is worth a discussion for its own (one might think of what we are willing to sacrifice in terms of freedom and civil rights to potentially raise the security of critical infrastructures from terrorist attacks), one of the big questions to which we most probably won't be able to find a definitive answer is, whether this is possible at all. Not only because we see the rising complexity in the systems our societies rely upon on a daily basis, but particularly because we most probably cannot expect from any (technical) system, even with redundancies, to work without failure for an undefined amount of time. What we can strive for is a certain percentage/amount of security which has to be produced (normally by human labour and the use of different resources) and resilient organisations and societies; administrations which are prepared and to a certain extent able to deal with uncertainty in highly dynamic crisis management situations. If we see, for example, that the use of a certain technology poses a disruptive risk to our society, with such measures we might be able to shift disruptive risks to a level where they might become risks that can be handled. And then it is possible to decide whether the costs for managing the risk and the potential damage are acceptable, or it is necessary to follow a different path.

That no-one is able to reliably predict a blackout lies within the nature of such an event. If it could be foreseen it would be possible to counteract with stabilizing measures in the power grid. The fact that it is a blackout (and not just a situation of limited power supplies) tells us, it was not possible to see that coming and react accordingly.

And this might be true for other, similar types of critical situations. The increasing complexity and co-dependencies across all different sectors of critical infrastructures has led to the type of a so-called cross-linked crises. The developments during other critical situations, like for example floods, which might also have supra-regional effects, can often be predicted more accurately because they follow certain linear patterns. Whereas this type of cross-linked crisis typically is due to its complexity a highly dynamic situation, in which actions and counter-measures in every subsystem could easily influence all the other affected areas; and often there won't be any not affected areas. In addition, these events are often categorized as so called »high impact low probability (HILP)« events, or as Renn would name it: they are in the »Damocles« class of risks.[8] In other words, they can deal potentially devastating damage but they have a probability of occurrence so low that probably no-one working today had to manage a situation like this before.

This calls for decisions under uncertainty, rapidly changing situational awareness, a high variety of needs when it comes to resources and manpower, and an interdisciplinary crisis management team with a lot of different competencies and experiences. The latter might even be more helpful than a very detailed emergency plan, because of these unforeseeable natures of such events, and because emergency plans might work perfectly when just one critical infrastructure provider has to deal with a catastrophe, but plans on organisational level will probably fail if all providers are affected by a certain situation.

What is the state of play?

Despite the maybe dystopian problem description the actual state of preparedness for situations like this seems to be quite good in Austria. For example, the topic of a blackout in the transmission network on national or even European level has been dealt with quite extensively on all organisational levels: in academia, in the administration, in organizations, in the industry and in the area of civil protection. Of course, the high pace of developments in this sector, in particular necessary to meet the ambitious goals of the transition to a sustainable energy system, demands for constant improvements. But if it is possible to deal with a situation like this, there is also a lot of preparedness for other crises. Also, the experiences of the ongoing pandemic taught the providers of critical infrastructures a lot, e.g. about diversifying personnel resources.

Especially the national regulation to reach the energy system transition goals for 2030 and beyond in 2021 revived the discussions on the security of electric power supplies. But the worries about systemic shortcomings have been overtaken by the uncertainties caused by the war in the Ukraine, the accompanying severe fossil fuel price increases and the more than obvious consequences of climate change this summer.

[8] Renn, Ortwin (2008): Risk Governance: Coping with Uncertainty in a Complex World; Earthscan/Routledge, London.

Who are the key stakeholders?

When it comes to critical infrastructures, the central player is the Federal Ministry of Interior in Austria. It is acting as a platform for critical infrastructure operators and other stakeholders in its role as leading organisation in the Austrian federal crisis and catastrophe protection management (Staatliches Krisen- und Katastrophenschutzmanagement – SKKM). In case of an emergency or crisis above regional level it would act as the coordinating organisation and information hub for all involved parties. It organises the work on special topics the SKKM is focussing on, connects different stakeholders, organises drills and disaster control exercises on national level, establishes radiocommunication between emergency services and critical infrastructures and hosts sectoral meetings.

The critical infrastructure operators are to a high percentage small to medium sized private companies, although in some of them public authorities are majority shareholders. Which companies are providers of critical infrastructures is defined by the Austrian Federal Chancellery, which is working together with the Ministry of Interior in the context of the Austrian Programme for Critical Infrastructures Protection.

The Austrian Armed Forces are allowed to support territorial entities upon request in case of a crisis. The area of civil protection is within the competency of the nine countries (Bundesländer) in Austria. In accordance with the federal programme for critical infrastructures protection there also exist nine country programmes for the protection of critical infrastructures.

Why is this important?

Like for any other European country working critical infrastructures are essential. The ongoing transformations and changes challenge the felt level of security in the population. An often heard argument, for example, is that renewable energy production will increase the risk of blackouts, insinuating that everything was working fine up until now (and neglecting other views like a new form of production might also need different infrastructure for transport, storage or distribution). Like with other societal transformations, there might be an increasing feeling of insecurity with the upcoming changes in the energy system, in the mobility sector, etc. Nevertheless, there is also a steadily increasing acceptance of renewable energy sources. In addition, the first two decades in this century were framed by the fear of terrorist attacks, migration and financial insecurities. Although the impact on the Austrian population was quite limited, like in other countries these topics often have been discussed and reported about in the context of security. This so called securitization also leads to an increased feeling of insecurity since there seems to be a challenge for security (instead of a financial challenge to the welfare system or a challenge to distributive justice). The pandemic since 2020, the polarisation within the population around vaccinations and counter-measures regarding the spreading of the virus, and finally the war in the Ukraine, with the caused economic difficulties for disadvantaged sections of the population, further advanced this feeling of insecurity and the idea that our society and democracy might be much more vulnerable to systemic shocks than one would have anticipated.

Therefore, the outage of critical infrastructures might not only lead to factual service interruptions, which would be a huge problem for itself, but also fuel this feeling of insecurity even further, which could lead to people losing trust in the political system, which seemingly cannot protect them. This would help political extremists destabilise the fundaments of the modern liberal democratic state.

Societal and political relevance and debate

Ongoing debate

There is along Cambridge Analytica[9] and others an ongoing debate on the influence of new technologies on society and democracy but regarding critical infrastructures the public debate focuses mostly on cybersecurity.

The last TA conference in Vienna (2021) under the title »Digital. Direct. Democratic.«[10] was dealing with the impact of technologies and the TA research on technologies upon democracy.

Legislation in place

In 2014 the Austrian government decided on a new master plan for the protection of critical infrastructures. This decision was based on the original programme for critical infrastructure protection from the year 2008. The new plan documented the ongoing work and already accomplished tasks and was rolled forward by the Austrian Federal Chancellery and the Ministry of Interior. Amongst others (like the Austrian Cyber Security Strategy[11], the Austrian Security Strategy[12] etc.) the Austrian Programme for the Protection of Critical Infrastructures (APCIP 2014)[13] is part of the Austrian security policy. The most important aim of this programme is the ongoing support for the critical infrastructures' operators, especially concerning business continuity planning, security management and risk management. This supportive task is done primarily by the Directorate for State Protection and Intelligence Services (Direktion Staatsschutz und Nachrichtendienst – DSN, formerly known as Federal Office for the Protection of the Constitution and for Fighting Terrorism/Bundesamt für Verfassungsschutz und Terrorismusbekämpfung – BVT).

The term critical infrastructures can be found in the criminal code (Strafgesetzbuch) and the so called Sicherheitspolizeigesetz (SPG §22 Abs. 1 Z. 6), although these two codes use different definitions. The NIS-Directive was implemented in national law by the so called Netz- und Informationssystemsicherheitsgesetz (NISG), which defines the providers of relevant services (Betreiber wesentlicher Dienste), which are not congruent to the list of critical infrastructure providers. The

[9] More about the Facebook-Cambridge Analytica data scandal: https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal.

[10] https://www.oeaw.ac.at/en/ita/veranstaltungen/vergangene-veranstaltungen/konferenzen/nta9-ta21-konferenz.

[11] Austrian Cyber Security Strategy: https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf.

[12] Austrian Security Strategy: https://www.bundesheer.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf.

[13] Österreichisches Programm zum Schutz kritischer Infrastrukturen: https://www.bundeskanzleramt.gv.at/dam/jcr:bb6a1a41-eb1d-4552-96da-9b460bbc5c0b/%C3%96sterreichisches%20Programm%20zum%20Schutz%20kritischer%20Infrastrukturen%20(APCIP).pdf.

latter one is defined in a decree by the Austrian Federal Chancellery upon suggestion by the Ministry of Interior. The list consists of 377 (number from 2019[14]) companies across all sectors and is not public. The companies on the list are informed by an official notification of the Federal Chancellery.

Current political or legislative proposals

The most relevant seems to be the »Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities«.[15] It aims at harmonizing the work done in the different member states, amongst others regarding definitions of what critical infrastructures are, and by straightening out shortcomings in the preparedness of and support for critical infrastructures' providers.

The most recent one is the decree on cell broadcasts to inform the population of any critical situations. Besides the alarms by sirens in the future all mobile network providers have to establish the interface for the authorised authorities (one in each country (Landeswarnzentralen) and the Ministry of Interior) to send cell broadcasts. This will be the late national implementation of the respective EU directive on the European Electronic Communication Code (EECC).[16]

Science/evidence-based inputs guiding political decision-making

The Institute of Technology Assessment and the Austrian Institute of Technology are supporting the members of the Austrian Parliament by providing monitoring reports on new and emerging technologies and potential needs for regulation.[17]

For years there is a research funding programme for security research in Austria, called KIRAS, which aims at bringing together academia, industries and administrative or law enforcement entities. A lot of research dealing with the protection of critical infrastructures is financed by this programme. It is complementing the FORTE programme which funds defence technology research.

Recently, the fear of a blackout has been increasingly discussed in the media (print and electronic). From the point of view of civil society, the main focus is on information and precautionary measures helping the population in the event of a blackout. Prominent among these is the Civil Protection Association (Zivilschutzverband).

[14] Peschhorn, Wolfgang (Minister of the Interior) (2019): Response to a parliamentary enquiry, reference number (GZ): BMI-LR2220/0331-II/2019, https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_03396/imfname_757716.pdf.

[15] European Commission (2020): Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0829&from=EN

[16] The European Parliament and the Council of the European Union (2018): Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN

[17] https://www.oeaw.ac.at/en/ita/projects/monitoring-for-the-austrian-parliament

Role of TA in the debates

Since the Institute of Technology Assessment (ITA) at the Austrian Academy of Sciences has a long research tradition regarding the impact of digitalisation processes on society, the protection of critical infrastructures from emerging risks stemming from digitalisation was an obvious topic, as well as the balance between the implementation of surveillance-orientated security technologies in the protection of critical infrastructures versus fundamental rights and civil liberties.

Another research focus at ITA deals with all aspects of the ongoing transition of the energy system.

Both, the reliability of information and communication infrastructures, as well as the security of electric power supplies are crucial for the functioning of all critical infrastructures. These dependencies are the reason why communication and electricity are not only critical infrastructures themselves but are also of cross-sectional importance.

Therefore, concluded research projects dealt, amongst others, with the acceptability of smart meters[18], the Austrian cybersecurity landscape[19], the security of electric power supplies[20], the dependencies on power and communication infrastructures[21], the acceptance and acceptability of surveillance-orientated security technologies[22], and a still ongoing project is dealing with the consequences of a large-scale, long lasting internet outage in Austria.[23]

Has TA made an impact on the ongoing debates?

Definitely. What we see is the increasing attention our work gets during the last years. Politicians, stakeholders, lay people are looking for answers, for decision support or even unprejudiced solutions. ITAs work for the Austrian parliament during the last years was successful and, hopefully, might be prolonged for the next years. At the same time delivering impartial information and objective research results to ongoing societal discussions was often appreciated, which can also be seen at the increasing media coverage of our work.

[18] Peissl, Walter., Čas, Johann., Sterbik-Lamina, Jaro., Suschek-Berger, Jürgen (2012): Smart New World? Key Factors for an Effective and Acceptable Deployment of Smart Meters – Projekt-Endbericht. Wien.

[19] Latzenhofer, Martin, Schauer, Stefan, Sommerer, Niklas, Zieser, Maximilian (2021): Cybersecurity: Systematisierung, Forschungsstand und Innovationspotenziale, https://www.parlament.gv.at/ZUSD/PDF/Cybersecurity_Endbericht_final_211217_BF.pdf.

[20] Allhutter, Doris, Bettin, Stefan, Brunner, Helfried, Kleinferchner, Julia, Krieger-Lamina, Jaro, Ornetzeder, Michael, Strauß, Stefan (2022): Sichere Stromversorgung und Blackout-Vorsorge in Österreich – Entwicklungen, Risiken und mögliche Schutzmaßnahmen, https://www.parlament.gv.at/ZUSD/PDF/Blackout_Versorgungssicherheit_Endbericht_200122_BF.pdf.

[21] Strauß, Stefan, Krieger-Lamina, Jaro (2017): Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven. Projekt-Endbericht. Wien. doi:/10.1553/ITA-pb-2017-01.

[22] The EU-funded SurPriSe project (2012-2015) produced a lot of reports for different aspects of the project, which can all be found here: http://surprise-project.eu/dissemination/research-results/.

[23] Yet, there is no final report available for the ISIDOR project. Publication is envisaged for November 2022. The link to the final report will then be found on the project's website: https://www.oeaw.ac.at/en/ita/projects/isidor-whats-cracking-without-the-internet.

TA helps to bridge gaps between different interests and different actors in society. If we brought people together in the course of a TA project, putting stakeholders around the iconic round table, it was often for the first time they were talking and listening to each other. Not because of ignorance, but because it might not be so easy to see the big picture, with all involved parties, during the day-to-day work.

TA can assist in seeing the unintended consequences of technology use, the things no-one wanted to look at in the first place. It is able to increase inclusiveness and, following its mission, is often seen as non-partisan, inter- and transdisciplinary source of advice to politics and society.

Lessons learned from TA

When looking at critical situations for operators of critical infrastructures it becomes clear that it is necessary to step back and look at the bigger picture. A problem in the logistics sector is a problem for almost all other areas of day-to-day life. A problem with electric power supply or the communication infrastructure will immediately become a problem of everyone else. The complexity and interdependencies are growing fast. While at a first glance a logistics problem often only means a delay in delivering goods, this can also become critical, for example in the health sector where often no big amounts of medication are on stock, because they are delivered three times a day or more often during normal operations. Like the health sector all other sectors are relying on logistics. But even more urgent is the supply with electricity and communication channels.

Increasing efficiency in the systems during the last decades also eliminated buffers and redundancies that would be helpful in a crisis; the convergence of communication infrastructures and the use of shared resources (like cloud services or outsourced IT services) are examples for that.

So one way to improve the capacity to act in a crisis could be to reinstall these buffers, even if it might not be economically worthwile and will just pay off during a critical situation – just like an insurance.

Another option could be to accept limits to efficiency, to connecting/networking different systems, to digitalisation etc., ultimately to the use of (certain) technology, if it endangers security.

And, with all the technology in use, if the acting people know each other personally, this is an enormous plus in managing a crisis.

It is necessary to prepare for dire situations. Increasing resilience, raising awareness for what might come up in the future, simulating and training all kind of critical situations regularly, keeping essential goods on stock, increasing autonomy (on different levels as appropriate: regional, national or EU wide), reducing dependencies etc. will help to manage a crisis. But at the same time, we have to find out what we are preparing for. Three weeks without electricity in a European country would be a catastrophe. But since this was learned during the last years all the relevant actors (critical infrastructure operators, administrations, companies, organisations etc.) prepared for a blackout. Nowadays the restoration time might be more in the range of days, which still is a problem, but a manageable situation. Of course, this again might increase if for example the potential consequences of climate change and the severe weather conditions caused by this process are not taken seriously.

It is necessary to reflect one's own situation, as an individual and as society, to see risks and upcoming issues. In a faster changing, more dynamic environment this needs to be done more often than in the past, maybe even constantly in some areas. But it is necessary to keep a clear head and see where it is necessary to invest and put available resources.

European Parliament – Panel for the Future of Science and Technology (STOA)

What is it about?

Current geopolitical challenge

Being closest both geopolitically and economically to Ukraine, Europe's economy is currently considerably vulnerable. The OECD recently published a simulation[24] of the likely effects of war and commodity price changes, showing drops in growth almost twice as large in the Eurozone as in the US. While the consequences of Russia's actions and disruptions to the European supply chains are still not fully felt, the EU needs to start preparing for these crises; as food, energy, satellite communications and the semiconductors supply chain are currently at risk.

Main challenges and requirements along the technological value chain

Security and connectivity technologies will continue to influence almost every aspect of our societies due to the steadily advancing digitalisation and the continuing uptake of IoT devices. The main challenge is to develop these technologies according to European values and regulations, ensuring that they meet European standards and safety requirements. The ongoing development of these technologies must be permanently guaranteed to keep up with the ongoing cybersecurity race with attackers and hackers. Detected vulnerabilities are closed immediately, mitigating cyber threats and guaranteeing security of critical infrastructures.

A crucial challenge is the lack of large and influential IT companies in the field of security and connectivity technologies in Europe. Europe is reduced to the role of a user and depends on hardware and software from few non-European players. This dependence on a few players could also end up in a vendor lock-in. Development of open interfaces, open standards, open-source software, European standardisation and certification can help overcome these risks. The open standardisation and certification approach enables a modular and vendor-independent integration and replacement of software and hardware components. European players need support in their research activities and in developing new business models to create open eco-systems and a diverse portfolio of available products and equipment alternatives for critical infrastructures.

Societal and political relevance and debate

Political debates on the European definition of technological sovereignty

The political discussion on technological sovereignty is longstanding and stems from concerns about losing global economic clout and geopolitical influence due to an overreliance on foreign providers in certain key technologies.[25]

[24] https://www.oecd.org/economy/Interim-economic-outlook-report-march-2022.pdf

[25] Bauer M. and Erixon F. (2020) Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls. In: ECIPE occasional paper.

Over the past year, attention has increasingly been paid to technological sovereignty, which is now included in many national agendas. In February 2020, the European Commission unveiled its ideas and actions regarding how Europe can retain its technological and digital sovereignty and become a global leader in its Communication on Shaping Europe's digital future.[26] It further defines that technological sovereignty starts with ensuring the integrity and resilience of our data infrastructure, networks, and communications. For this, Europe needs the right conditions to develop and deploy its own capacities and reduce its dependency on other parts of the globe for Key Enabling Technologies (KET). As President of the European Commission, Ursula von der Leyen has set the objective of achieving technological sovereignty in some critical technology areas by 2024.[27] Specifically, she describes sovereignty as »the capability that Europe must have to make its own choices, based on its own values, respecting its own rules«.

This concept of technological sovereignty should, however, not be understood as defined against anyone else, but instead, as based on the needs of Europeans and the European social model. This is illustrated by the Commission in the digital area with the aim of a European society powered by digital solutions that are strongly rooted in our common values and that enrich the lives of all citizens: people must have the opportunity to develop personally, to choose freely and safely, to engage in society. Data should be available to all and will support society to gain the most from innovation and competition. This digital Europe should reflect the best of Europe – openness, fairness, diversity, democracy, and confidence.[28]

In early 2020, the lack of resilience showcased by the Covid-19 pandemic reinvigorated debates on technological and industrial sovereignty in Europe. The pandemic paralysed many value chains, which had been trimmed over past years to be as efficient as possible through just-in-time and lean production methods. Specifically, European Commissioner for the Internal Market, Thierry Breton recognised how the pandemic has revealed the lack of access to protective equipment, while the overreliance on a few third countries highlighted the strategic importance of some previously neglected value chains.[29]

EU policies in place

Some work has already been done[30] regarding the impact on food security and the response of the EU to Russia's war on Ukraine in this area. The Ukraine war and its impact on energy supply is being broadly analysed[31] and there is already work being done by the EC on moving away from Russian energy supplies. The REPowerEU package[32] that was adopted on 8 March 2022 aims to accelerate the ongoing clean energy transition, by boosting renewables and energy efficiency. This package builds on several pieces of legislation in co-decision process, including the Energy Performance of

[26] European Commission (2020) Communication: Shaping Europe's digital future.

[27] Ursula von der Leyen (18 February 2020): Tech sovereignty key for EU's future goals. In: The Irish Examiner.

[28] European Commission (2020) Communication: Shaping Europe's digital future.

[29] European Commission (September 2020) News. Europe: The Keys to Sovereignty.

[30] https://epthinktank.eu/2022/04/11/russias-war-on-ukraine-impact-on-food-security-and-eu-response/

[31] https://epthinktank.eu/2022/04/06/the-ukraine-war-and-energy-supply-what-think-tanks-are-thinking/

[32] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3131

Buildings Directive[33] (EPBD). Buildings account for 34% of the gas consumption in the EU, so it is an important sector for tackle if we want to improve EU energy security, and in particular the EU dependency on Russian gas.

Technological sovereignty and R&D&I are currently high on the political agenda, which has resulted in the adoption of several unprecedented policies that will support the development of KETs. In particular, this concerns policy options that support their commercialisation and early adoption of innovation. For example, higher technology readiness levels (TRLs) and commercialisation of a variety of digital technologies (AI, cybersecurity and connectivity) are targeted by the digital Europe programme. Deployment of a range of KETs that enable green and digital economy will be promoted through the European Green Deal and Recovery and Resilience Facility[34], as well as the national recovery plans, which seem to prioritise research, innovation and education.[35]

The current European AI Act proposal[36] classifies the AI systems intended to be used as safety components in the management and operation of critical infrastructure (road traffic and the supply of water, gas, heating and electricity) as high-risk, since their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities.

Role of TA in the debates

Technology assessment (TA) is called upon to provide strategic information to feed into the political debate. The scope of the TA approach can be divided into three main categories:

Firstly to present and analyse the state of play in the different areas mentioned above regarding infrastructures and the supply chain, especially where they are most critical and where they that can be expected to be most affected by disruption due to the present geopolitical situation. The use of the STEEPED approach[37] is recommended to help ensure that this technology-related issue is investigated over the most extensive (»360 degree«) range of perspectives.

Secondly, to review the current potential contemplating strengths and weaknesses in the face of disruption, including the main risks, opportunities, conditions and requirements. To cover and take into account the position of the different actors, a description of possible stakeholders is required (»stakeholders' analysis«). This is a list of relevant actors, including scientists, policy-makers, industry, end users, NGOs, as well as any other special interest and pressure groups. This should specially

[33] https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficient-buildings/energy-performance-buildings-directive_en

[34] For instance, the Member States are encouraged to enhance their research and other efforts in ICT (5G connectivity, cybersecurity), AI, microelectronics, semi-conductors and to strengthen key value chains and access to critical raw materials. See European Commission, Guidelines to Member States Recovery and Resilience Plans – Part 1, 2021.

[35] Based on reviewing the published national recovery and resilience plans of France, Germany, Italy and Spain.

[36] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

[37] STOA Guidelines for foresight-based policy analysis https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690031/EPRS_STU(2021)690031_EN.pdf

include those affected by the present disruption as well as actors that may become key in facing the new challenges posed.

Lastly, based on specific study findings, TA can offer and assess policy options for creating an ecosystem in the EU that will be able to face disruption making the supply chain more resilient and the industrial and social environment capable to adapt, tackling all possible challenges of the new situation and the expected evolution of global markets. TA reports list possible courses for policy action, and assess them for their possible impacts, including their impact on society, a wide range of possible intended and unintended impacts (and – if applicable – even possible perverse effects on other policies). For assessing the listed policy options in this way, they have to be explained, and their potential relative disadvantages and benefits are to be described. Such an options assessment provide MEPs with a balanced and easily understandable summary of the potential outcomes of alternative policy options regarding ways to ensure the preparedness of the EU to face disruption, especially in the areas mentioned.

STOA contributions to this topic

STOA has a study on Artificial intelligence in the agri-food sector: applications, risks and impacts and a study on Preparedness plan for Europe: Addressing food, energy and technological security in the pipeline.

STOA has recently published a study on Key enabling technologies for Europe's technological sovereignty[38] and a study on Splinternets: Addressing the renewed debate on internet fragmentation.[39]

Has TA made an impact on the ongoing debates?

In view of the current international context, the overall objective of TA is to provide evidence for policy-making on the subject introduced above and whose relevance to the work of the European Parliament. TA in the European Parliament aims at supporting the ongoing discussions in relation to the suggested preparedness plan would provide legislators in the related European Parliament's committees with data and insights that they can use when discussing files such as the European Chips Act, the Energy Efficiency Directive, the Renewable Energy Directive III, the Energy Taxation Directive, the upcoming Cyber Resilience Act, the EU AI Act and the future industrial strategies; or even others such as European Green Deal, CAP and Farm to Fork Strategy.

TA reviews the current disruption and security challenges from the perspective of how science and technology can be affected by these events while also becoming a fundamental asset to provide resilience. TA identifies weaknesses, assess risks, and recommend coordinated solutions and alternatives to expected supply chain disruptions in critical areas such as the four that are the subject of an ongoing STOA study: food security, energy security, semiconductors and satellite communications. TA provides some policy options that could feed into the work of the EP in the possible development of a preparedness plan.

[38] https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697184/EPRS_STU(2021)697184_EN.pdf

[39] https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729530/EPRS_STU(2022)729530_EN.pdf

What are the lessons learned from TA?

The situation derived from the Russian attack on Ukraine shows the huge impact that disruptions on supply chains can have in the economy of the EU, particularly in its agri-food sector.[40] Being applications so close to its original purpose, digital technologies have a huge potential to help optimize the management of production and distribution of strategic goods such as microchips, water and energy generation and transport (from hidrocarbures to renewables, hidrogen and grid management), as well as fertilizers, pesticides and food products such as meat and also grain.

As an overarching policy action that could improve European performance in KETs, the original KETs strategy of 2012 needs to be updated and overhauled.[41] This would increase awareness of the importance and the challenges of new technologies, reinforce Member States' joint commitments, and provide a stronger focus and support for national actions (e.g. national actions planned under the EU Recovery and Resilience Facility). The new KETs strategy should be nuanced: it could assign different levels of priority to different KETs, based on how the EU scores in global comparison and where the KET-specific weaknesses lie (see the analysis of the EU's global leadership in Section 3.2). The KETs strategy could then envisage more targeted actions for »stronger' KETs and »weaker« KETs.

The new KETs-based strategy could integrate R&D&I policy with elements of industrial policy and include a common European agenda or action plan under EU leadership. One of the objectives could be the nurturing of European champions, including by supporting cross-border cooperation and projects and granting State aid or competition law exemptions (e.g. by extending the use of IP-CEI). Such coordination of resources would help in competing with large countries such as China or the USA. However, these efforts should lead to the creation and strengthening of value chains across Member States, and not national champions, by encouraging all Member States to participate and by monitoring whether funding is in line with the conditions set in State aid rules, as well as whether it also benefits SMEs.

Further to this work on KETs, STOA keeps working in other areas also related to critical infrastructures and technologies in order to minimize the effect of disruption. The EU cannot afford to miss the opportunities offered by new technologies but it can still lead responsible development while maintaining ethical values and standards. By setting these standards, the EU can pave the way to ethical technology worldwide, while also ensuring that the EU remains competitive.

[40] https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)729367

[41] European Commission, A European strategy for Key Enabling Technologies – A bridge to growth and jobs, COM(2012) 341 of 26.06.2012. There are several EU-level strategies that mention KETs and provide specific actions that would support KETs, like the New Industrial Strategy for Europe and An SME Strategy for a sustainable and digital Europe. These strategies can provide some building blocks and supporting structures for KETs strategy.

Policy options for a KETs-based strategy[42]

Policy options	Actor and enablers	Feasibility
1. A common European agenda updating the strategy for KETs culminating in an action plan under the EU's leadership.	European Commission with Member States, and relevant industry stakeholders	This action could build on the previous KET strategy and start as a discussion forum generating commitments and slowly building an action plan.
2. Support development of European champions by supporting cross-border cooperation through State aid and competition law exemptions.	European Commission with Member States	Existing tools such as IPCEI facilitate this action, other similar tools could be developed. Market power, competition issues, and different Member States' needs should be considered closely.
3. Promote bottom-up processes for smart regional specialisation and monitor as well as facilitate the inclusion of SMEs in the strategy through one-stop shops and intermediary organisations.	European Commission with representatives of regions and SMEs	Existing platforms such as the Smart Specialisation Platform and the European Cluster Collaboration Platform could be used to involve regions and SMEs in developing the joint strategy and monitor their inclusion.
4. Target development of KETs through earmarking funds for KET investments.	European Commission with Member States	Could be implemented under newly adopted, improved financial instruments, such as Horizon Europe.
5. Strengthen KETs observatory focus on measuring the impact of policies and regulations and sharing best practices for forward-thinking policy-making, and monitoring the follow-up on KET strategy.	European Commission with AIT observatory and KET specific observatories	The existing observatory could be easily expanded to cover policy indicators. It would be difficult to come up with measurable indicators.
6. A continuous policy dialogue to update KET strategy and investigate new areas based on new findings.	European Commission with Member States, relevant industry and academic stakeholders	Setting up a forum that includes EU and Member State representatives could be relatively easy. However, ensuring follow-up actions and that commitments are made is more difficult.
7. Investigate the economic impact of science espionage at European level through a study.	European Commission, research and industry stakeholders.	Science espionage is a topic that has recently gained more attention and could be investigated further.

Although there is already work being done on the subject, there is a real need to conduct further research when all these areas are combined to explore the policy and procedural translation of this work into practical, applicable requirements. TA is called upon to analyze the interaction between the four specific topics that have been highlighted here, as there are strong interdependencies, for example between energy and food security as well as between semiconductors (and raw materials used in general) and the energy transition.

[42] by Tiana Ramahandry, Vincent Bonneau, Emarildo Bani and Nikita Vlasov from IDATE Digiworld, Michael Flickenschild and Olga Batura from ECORYS, and Nikolay Tcholtchev, Philipp Lämmel and Michell Boerger from Fraunhofer FOKUS in STOA study on Key enabling technologies for Europe's technological sovereignty https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697184/EPRS_STU(2021)697184_EN.pdf

Germany – Office of Technology Assessment at the German Bundestag (TAB)

What is it about?

Critical infrastructures are those infrastructures whose functioning is vital or essential to economic, social well-being, national security or the functioning of the State. Given our dependency on services provided by critical infrastructures, a major infrastructure failure can result in severe societal disruptions and threaten the good functioning of society. For example, an analysis of TAB revealed the dramatic consequences of a prolonged and widespread power blackout (see box »What happens during a blackout?«). The protection of critical infrastructures is considered as a central task for public and private actors. Currently, critical infrastructures cover 10 sectors – energy, food, finance and insurance industry, health, information technology and telecommunication, media and culture, municipal waste, government and public administration, transport and traffic, as well as water.[43] All organizations in these sectors, regardless of their size, are considered to be critical infrastructures (BSI 2020, p. 52).

What is the state of play?

In Germany, critical sectors are being digitalized at a rapid pace. On the one hand, cities are getting »smarter« and many administrative processes are now available online. On the other hand, industrial systems, which are the backbone of many critical services, are being connected via IT-systems to communicate information in real time. For instance, water distribution networks increasingly rely on automation technologies and a digital infrastructure to treat and distribute drinking water. Digital solutions are also seen as essential to better prepare for and react to severe weather events such as droughts or heavy rainfall. In addition to digitalization, the dependency of critical sectors from one another increases. This is particularly the case for the transport sector which is experiencing a massive boom towards electrical vehicles.

Who are the key stakeholders?

Critical infrastructures in Germany are predominantly privately organized, hence the protection of critical infrastructures is acknowledged as a joint task of the state, society, business and industry. One major challenge is the high fragmentation of some critical sectors. In the water sector for instance, there exists approximately 5.500 drinking water suppliers, the majority of them are small or medium enterprises. Not all of them can provide the necessary IT security expert knowledge in-house, but have to recourse to external service providers. On the part of the state, two national authorities share responsibility for the protection of critical infrastructures in Germany: the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) is in

[43] https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html (12.7.2022)

charge of matters related to information security and the Federal Office of Civil Protection and Disaster Assistance (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK) is the authority concerned for the physical protection of critical infrastructures.

Why is this important?

The protection of Critical Infrastructure and Resilience Society are becoming high priority topics for politics. As everywhere around the world, the COVID-19 pandemic has revealed that modern societies turn out to be less stable and more vulnerable to sudden shocks than many had assumed. Further crises of this magnitude cannot be ruled out in the future. Financial crashes, global migration movements, climate change and the scarcity of resources are developments and events that – with regard to their synergistic interaction within the framework of societal development paths – can lead to escalations of a hitherto unknown kind.

Cyberattacks on critical infrastructures have noticeably increased over the last years. In July 2021, for example, hackers encrypted the IT infrastructure of the administrative district Anhalt-Bitterfeld thereby paralyzing administrative processes like social and maintenance payments or vehicle registration. This led to the declaration of a cyber disaster for the first time in Germany. Besides pandemics and wars, Germany has to be prepared to face natural catastrophes. In July 2021, a flood hit western parts of Germany as well as parts of Belgium, France, the Netherlands, Luxembourg hard, caused enormous damage to buildings and infrastructures and left over 180 dead people alone in Germany.

The war in Ukraine has revived worries among the German population about serious supply bottlenecks with energy or food that were long believed to belong to the past. Following Russia's voluntary reduction of gas exports to Germany and bearing in mind Germany's dependency on this energy source, the government considers the gas supply situation as tense and a worsening of the situation cannot be ruled out. In addition, the BSI qualifies the situation in the cyberspace as tense to critical.

In light of this event, decision-makers started to rethink the abilities of infrastructures and society in Germany to respond, absorb, adapt or recover to severe disruptive events.

Societal and political relevance and debate

Ongoing debate

The protection of critical infrastructures and resilience of society have risen to be high priority issues not only for German policy-makers but also for stakeholders in government, national or subnational administrative bodies, science, business and industry. In this context, experts stress that competences need to be further developed and an all-of-society approach implemented in Germany.[44] Others emphasize that it is becoming more and more important not only to collect information about IT-security incidents, but also to train key actors on a regular basis to deal with system failures that may threaten the supply of critical services. To do so, strengthening the networks of operators of critical infrastructures in order for the community to learn from incidents and »near misses« is brought forward as one key element of a strategy. [45] In some critical sectors, only a minority of companies regularly check the IT-security status of their systems, include security concerns in the design of their products or have an emergency management plan.[46] Beyond prevention, measures to improve preparedness are also discussed intensively. Building up reserves requires to coordinate national and European efforts, ensure synergies between critical infrastructures (e.g. transport, energy and food sectors)[47] and take unnecessary expenditures or detrimental side-effects such as generating risks for the economy or disturb supply in other countries into account.[48]

Legislation in place

Although the specific definition of critical infrastructures differs from one country to another, most OECD countries have established an inventory of assets and put in place regulations, programmes or incentive mechanisms to strengthen the resilience of critical infrastructure to shock events (OECD 2020, p. 46).

In Germany, the first political steps towards protecting critical infrastructures on federal government level date back to the 1990s. In 1997, an inter-ministerial working group was established to assess the risks and threats to infrastructures that may result from vulnerabilities in information and communication systems. In light of the working group's results, the BSI established a new division dedicated to the protection of critical infrastructures. Yet, the terrorist attacks of September 11, 2001 in the USA raised attention towards a whole new kind of risk: terrorism. As a consequence, a broader risk approach (all-hazards approach) was established.

[44] Tiesler, R. (2022): Schriftliche Stellungnahme des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe im Rahmen der öffentlichen Anhörung des Ausschusses für Inneres und Heimat »Ein Jahr nach der Flutkatastrophe – Ausblick auf die Zukunft des Bevölkerungsschutzes am 4. Juli 2022. Bonn. https://www.bundestag.de/resource/blob/902128/1cc94666b940f3c96d53f4b71d05d79b/20-4-80-I-data.pdf

[45] Fuhr, D. (2022): Kommentar: Chaos und Resilienz bei Kritischen Infrastrukturen. Nur wer den Krisenfall probt, lernt mit ihm umzugehen. Und wer die kleinen Katastrophen nicht akzeptiert, kann die großen erst recht nicht bewältigen. In: Heise Online. 02.07.2022. https://www.heise.de/meinung/Kommentar-Chaos-und-Resilienz-bei-Kritischen-Infrastrukturen-7158825.html

[46] Kabel, C. (2022): Nach Cyberattacke in Darmstadt: Fachleute fordern Umdenken bei Unternehmen. In: Frankfurter Rundschau. 21.06.2022. https://www.fr.de/rhein-main/darmstadt/nach-cyberattacke-in-darmstadt-fachleute-fordern-umdenken-bei-unternehmen-91623110.html https://www.fr.de/rhein-main/darmstadt/nach-cyberattacke-in-darmstadt-fachleute-fordern-umdenken-bei-unternehmen-91623110.html

[47] Bundesrechnungshof, Abschließende Mitteilung an das Bundesministerium für Ernährung und Landwirtschaft über die Prüfung zur Ernährungsnotfallvorsorge des Bundes [wie Fn. 68], S. 30.

[48] Rudolff, B. (2022): Wirtschaftliche Resilienz: Kompass oder Catchword? Welche Fallstricke und Folgeeffekte die EU im Krisenmanagement beachten muss. SWP-Studie 2022/S 01, 07.02.2022, 37 pages. https://www.swp-berlin.org/10.18449/2022S01/

In 2009, the German National Strategy for Critical Infrastructures Protection (CIP strategy) was adopted. It summarizes the Federal Administration's aims and objectives and its political-strategic approach to actively address matters of critical infrastructure protection (Federal Ministry of the Interior 2009). The strategy gives voluntary commitments by the private sector priority over statutory regulations. To enable and foster voluntary cooperation, various public private partnerships were founded such as the Alliance for Cybersecurity or UP KRITIS. UP KRITIS gathers over 700 actors across operators of critical infrastructures, their associations and the government agencies. In working groups, the actors develop security standards, identify best-practices and draw recommendations for the prevention of crises. In addition, the actors involved organize emergency exercises. The organizations that participate in UP KRITIS also share information about the current threat landscape with one another (BSI 2020, p. 55).

However, the voluntary approach turned out to be insufficient to achieve an appropriate level of information security across all critical sectors. In order to improve this situation, the IT Security Act was adopted by the German Federal Government in 2015. This Act obliges operators of critical infrastructures that provide critical services to a population of more than 500.000 persons[49] to meet state-of-the-art IT security standards and to report IT security incidents to the BSI. One year later, the EU directive 2016/1148 set out the foundation for a common level of security of network and information systems across the European Union (NIS-Directive) to be implemented by the EU member states in their national legislation until 2018.

Current political or legislative proposals

At the moment, a new EU directive to strengthen the resilience of critical infrastructures is being prepared and discussed. Once enacted, member states will have to introduce a national strategy to enhance the resilience of critical infrastructures and carry out a risk assessment at least every four years. Operators of critical infrastructures will need to identify the relevant risks that may significantly disrupt the provision of essential services, take appropriate measures to ensure their resilience and notify disruptive incidents to the competent authorities (Council of the EU 2022).

On July 12th, the German Federal Ministry of the Interior presented its new cybersecurity agenda.[50] According to the agenda, small and medium enterprises in critical sectors will receive more support in the future. In addition, the information flow between the federal state and the regions will be strengthened and sector-specific Cyber Emergency Response Teams will be established by operators of critical infrastructures. A focus will also be on the security of IT supply chains and on awareness and cyber-resilience projects.

[49] Specifics about how to calculate this are set by law

[50] https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/07/cybersicherheitsagenda.html (15.7.2022)

Role of TA in the debates

TAB contributions to this topic?

Vulnerabilities of society or critical infrastructures, the consequences of infrastructure failures or strategies for crisis prevention and management are issues that keep TAB busy since its first days. For example, over ten years ago TAB intensively studied the vulnerability of modern society by rigorously analyzing the consequences of a large-scale and longer-term blackout in electricity supply (see box »What happens during a blackout?«).

Box – What happens during a blackout?

In 2011, TAB finalized a report on the consequences of a prolonged and widespread power blackout. By means of comprehensive consequence analyses, the report drastically demonstrated that after only a few days, the supply of the population with (vital) goods and services can no longer be guaranteed in the affected area. Several sectors were examined more closely.

- Information technology and telecommunications: After the onset of the power blackout, some telecommunications and data services fail immediately. Battery powered mobile networks may function for a few days. However, due to the increased volume of calls, these are mostly overloaded. Public-law broadcasting corporations are better prepared and are able to continue transmissions. However, citizens are unable to receive broadcasts via their televisions. Radio represents one of the most important information channels.
- Transport and traffic: Electrically driven transport modes, especially rail transport, either fail immediately or after a few hours. Road traffic becomes chaotic, as junctions, tunnels and barrier systems are blocked. There are numerous accidents and emergency services encounter major difficulties in carrying out their duties. Since most petrol stations are out of action, most vehicles become stranded and local public transport can only be maintained at a rudimentary level.
- Water supply: Electrically operated pumps are especially critical for guaranteeing water supply. After just a very short time without electricity, water infrastructure systems can no longer be operated. It becomes impossible to maintain normal personal hygiene and the ability to prepare food and drinks is limited. Another consequence is a growing risk of fires, as people attempt to cook or heat and light their homes without electricity. However, the loss of water supply also impairs fire-fighting capabilities.
- Food supply: In animal husbandry, as soon as the supply of fuel for emergency power generators is exhausted, the animals start to suffer because it is impossible to supply them manually with food, water and fresh air. Pigs and poultry kept in groups of several thousand animals often don’t even survive the first hours. The food processing sector comes to an immediate standstill and stocks of frozen or chilled foodstuffs spoil. Shelves in retail warehouses empty within a few days.
- Health care system: After just 24 hours, there is a marked decline in the health sector’s ability to function. Hospitals or dialysis centers can maintain only limited operations with the aid of

emergency power generators. However, most doctors' surgeries and pharmacies can't continue operating without electricity. Bottlenecks in the supply of insulin, blood products and dialysis fluids have dramatic consequences.

- Financial services: Individual sub-sectors of the financial services sector appear relatively resilient. However, the communication paths between the market actors prove less robust. In the affected area, it is no longer possible to process financial services. Many banks close after a few days. As cash dispensers have also stopped working, the supply of cash to the population threatens to collapse. People become afraid they will no longer be able to buy food and obtain other daily requisites.

Currently, TAB explores the chances and challenges that digitalisation raise for critical infrastructures using water and waste management as examples. For instance, automation technology is already being used in water management. It can take over simple monitoring, control and regulation functions based on sensor data. However, a consistent collection, networking and algorithm-based evaluation of the existing large datasets in analogy to Industry 4.0 solutions is hardly taking place at present. In the waste management sector, some municipalities are experimenting with »intelligent« waste containers that transmit the respective fill level to the scheduling system. The aim is to optimize emptying schedule, calculate efficient routes for waste collection vehicles, and improve operational work structures and new forms of inter-municipal cooperation. At the same time, digitalisation and networking increase the complexity of infrastructures and thus also the risks of technical and human errors. Smart infrastructures also offer new entry points for cybercrime. In addition, this generally increases their dependence on functioning power and IT infrastructures. Consequently, this may result in power failures or IT disruptions having far more serious extent than they used to.

In 2021, TAB launched the TA-project »Crisis radar – strengthening the resilience of society, politics and the economy by means of crisis prediction«. For both the prevention and management of profound crises, it is crucial to identify first signs at an early stage. The earlier a crisis development can be detected, the sooner preventive and reactive measures can be initiated. In addition to the early detection of threats, knowledge about particular vulnerabilities is a fundamental prerequisite for developing strategies to increase the resilience of society, politics and the economy. Against this background, the TA project examines how a system to continuously detect and anticipate crises would have to be designed and institutionally anchored – also at the international level – to enable an early crisis and risk management. There are two central questions resulting from this: What are the deficits in the early detection of systemic threats? Which instruments, institutions and consultation mechanisms in the political sphere would need to be improved or still need to be created in order to ensure a swift, comprehensive and sustainable response to crisis events? The projects runs until 2023.

In addition, TAB explores the criticality and vulnerability of critical sectors. For instance, TAB has started a project on the Cybersecurity of food supply chains. The focus lays on the evaluation of the dependency of food companies to ICT and digital solutions and the risks associated with their failure.

Lessons learned from TA

The authors of the project exploring the effects of a prolonged and widespread power outage in Germany demonstrated that after only a few days, the supply of the population with (vital) goods and services can no longer be guaranteed in the affected area. That would amount to a national catastrophe. To foster resilient societies, that are able to cope with such far reaching incidents, scientific knowledge about the consequences and possible counter measures is necessary. It needs to be targeted and prioritized for the different stakeholders involved, namely politics, public authorities, companies and civil society. TA aims to implement that and to prepare societies with scientific knowledge to be able to increase the resilience of critical systems.

Impact of TA

The main conclusion of the blackout report shook up politicians, competent government authorities like the Federal Ministry of the Interior which provided an extensive statement on the outcomes of the report. The government acknowledged the necessity to improve the regulatory framework for the management of risks and crisis related to power supply and to improve partnerships between private and public actors in the field. [51] After the publication of the report, issues surrounding a possible blackout were thematized over and over again in plenary sessions of the Parliament. In particular, the report was instrumental in discussing the organization of civil protection in Germany[52] as well as issues of energy security and energy dependency, in particular from Russia.[53] In addition, the government started projects and activities in the field of power failure prevention and emergency power supply and has funded several research projects in the field. The BKK developed guidelines for operators of critical infrastructures as well as for citizens and authorities about how to prepare for and deal with a power failure. BKK also has worked closely with stakeholders to develop emergency plans. Furthermore, in 2020/2021 the government supported measures regarding emergency power supply of drinking water.[54] The TAB-report is still used as a blueprint by parliamentary groups who seek to set measures to improve civil security on the agenda of the government.[55]

Over 10 years after its publication, media still regularly refers to the study and its conclusions, thereby making the report one of the most successful TAB reports ever issued. As the dependency of

[51] Bundesregierung (2011): Stellungnahme der Bundesregierung zum Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) Technikfolgenabschätzung (TA). TA-Projekt: Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung vom 27. April 2011, BT-Drs. 17/5672

[52] Deutscher Bundestag (2012): Stenographischer Bericht der 162. Sitzung. 17. Wahlperiode in Berlin am 1. März 2012. Plenarprotokoll 17/162

[53] Deutscher Bundestag (2011): Stenographischer Bericht der 114. Sitzung. 17. Wahlperiode in Berlin am 9. Juni 2011. Plenarprotokoll 17/114 https://dserver.bundestag.de/btp/17/17114.pdf

[54] Deutscher Bundestag (2021): Schriftliche Fragen mit den in der Woche vom 15. November 2021 eingegangenen Antworten der Bundesregierung. Drucksache 20/104. https://dserver.bundestag.de/btd/20/001/2000104.pdf p. 18

[55] AFD (2021): Blackout und Brownout verhindern – Energieversorgung sicherstellen. Antrag der der Abgeordneten Karsten Hilse… und der Fraktion AFD. Deutscher Bundestag, Drucksache Nr. 20/34, Berlin https://dserver.bundestag.de/btd/20/000/2000034.pdf

our society from electricity is growing and cyberattacks multiply, the report is still being cited by the media to emphasize the concrete consequences of a major system failure.[56]

Preliminary results from the project »Crisis radar« were presented and discussed on June 22nd at the Parliament.[57] The discussion raised interest among politicians and some results were taken up in the press. In particular, it was emphasized that there is a need for a better use of digital tools to improve early warning systems, which requires collecting data in real time.[58] The media also stressed some results from an empirical representative study about the perception of the corona-crisis by the population and its aftermath.[59]

References

Federal Ministry of the interior (2009): National Strategy for Critical Infrastructure Protection (CIP Strategy) https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.html

BSI (2020): The State of IT Security in Germany in 2020. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2020.pdf?__blob=publicationFile&v=2

Council of the EU (2022): EU resilience: Council presidency and European Parliament reach political agreement to strengthen the resilience of critical entities, https://www.consilium.europa.eu/en/press/press-releases/2022/06/28/eu-resilience-council-presidency-and-european-parliament-reach-political-agreement-to-strengthen-the-resilience-of-critical-entities/

[56] Eberl, J. (2022): Möglicher Stromausfall. Bei einem Blackout droht der Kollaps. In: tagesschau, 07.03.2022. https://www.tagesschau.de/wirtschaft/technologie/blackout-deutschland-101.html

[57] Deutscher Bundestag (2022): Experten betonen Notwendigkeit von Pandemie-Frühwarnsystemen. https://www.bundestag.de/dokumente/textarchiv/2022/kw25-pa-bildung-fachgespraech-896474 (15.07.2022)

[58] Ronzheimer, M. (2022): Lehre aus der Corona-Pandemie:Gewappnet für Krisen? In: taz, 23.06.2022. https://taz.de/Lehre-aus-der-Corona-Pandemie/!5859874/

[59] Oertel, B.; Kahlisch, C.; Sonk, M.; Evers-Wölk, M. (2022): Wie schätzen Bürger/innen die Coronapandemie und ihre Folgen ein? Ergebnisse einer Repräsentativbefragung. TAB-Sensor Nr. 5. https://publikationen.bibliothek.kit.edu/1000147830

Netherlands – Rathenau Instituut

Governing the Dutch twin energy and digital transition: dealing with disruptions

Romy Dekker, Rinie van Est

What is it about?

Limiting global warming is necessary to keep large parts of Europe livable. This disruptive development forces the EU into an energy transition and to reduce its net greenhouse gas emissions by at least 55% by 2030, compared to 1990 levels. Reinforced by geopolitical shifts caused by Russia's military aggression against Ukraine, the importance of a more resilient, clean energy system is widely acknowledged, but by no means self-evident (JRC 2022). To facilitate the transition, energy systems need to be adjusted to integrate distributed generation of energy from renewable sources and deal with the expected increase in electricity demand. However, this should not come at the expense of the reliability of the energy supply; disruptions could have severe societal consequences.

Digital technologies are seen by European and national policymakers as a means to prevent such disruptions and facilitate the energy transition. They can match supply and demand at a more decentralized level, within the available grid capacity, forecast energy production and consumption and empower citizens to become active consumers. Digitization also enables the introduction of new companies and services. Innovative new parties such as »aggregators« and »smart energy communities« are popping up. Against these opportunities, there are also concerns about the potentially disruptive consequences of a digitized energy system, such as in the fields of cybersecurity and digital sovereignty. The proper governance of this so-called twin transition demands a better understanding of how digital technologies can contribute to a just energy transition.

What is the state of play?

Because of the energy transition, the Netherlands faces a shortage of grid capacity in several regions, which both delays the energy transition and jeopardizes the reliability of the energy supply (Rathenau Instituut 2022a). Making the energy supply low-carbon thus has consequences for the reliability and the affordability of the Dutch energy system. System operators, therefore, make huge investments in the electricity grid to solve this issue. In addition, the energy sector is actively exploring the potential of digital technologies and data to improve the energy system's flexibility. System operators even advocate only connecting smart assets to the electricity grid, like smart charging stations, smart heat pumps and smart solar panels (Netbeheer Nederland 2022). The Ministry of Economic Affairs and Climate (In Dutch: EZK) views data as a »necessary and promising raw material« for the energy system (EZK 2021).

In 2019, the Netherlands Authority for Consumers and Markets warned that the current system for exchanging data is not suitable for facilitating the energy transition (ACM 2019). Moreover, the Ministry of EZK finds the availability, accessibility and quality of data insufficient (EZK 2021).

While steps are being taken to upgrade the current governance, the Rathenau Instituut (2022) concluded that those steps are not yet sufficient to ensure that the use of digital technologies and data contributes to a just energy transition.

Who are the key stakeholders?

The Ministry of Economic Affairs and Climate is responsible for developing energy policies. There are three relevant authorities for supervising the twin energy and digital transition:

The Netherlands Authority for Consumers and Markets regulates the energy sector with an eye to affordability, reliability, and sustainability;

The Radiocommunications Agency Netherlands is concerned with the integrity of (vital) networks and services, the incorrect and/or unsafe use of equipment that can cause disruptions to these (vital) networks and the measurement results from digital meters and the (digital) measurement chain (Deloitte 2021);

The Dutch Data Protection Authority supervises the processing of personal data to ensure compliance with laws that regulate the use of personal data.

Until recently, the Dutch energy sector had a clear playing field. There were a limited number of actors, each with their role within the energy system. Broadly speaking, the main stakeholders can be divided into system operators and market players. The system operators have a legal task and are responsible for the proper functioning, maintenance and possible expansion of the transmission and distribution networks, the transport of energy and facilitating the functioning of the (free) energy market. Netbeheer Nederland represents them in societal and political debates. The market players fulfil at least one of the following (licensable) roles: consumer, producer, supplier, program responsible party or party responsible for metering. The parties fulfilling these roles must also comply with certain legal obligations, for example when using data. Energie Nederland represents the majority of these parties.

However, the playing field is beginning to change (Rathenau Instituut 2022a). There is a greater diversity of actors and activities emerging. Smart energy communities, for example, use digital technologies and data to carry out energy activities for the benefit of their members (e.g. joint consumption, production, supply or storage) and may be active in the energy market (directly, or indirectly through an aggregator). An example of a new activity is that of aggregation. Parties that provide a digital aggregation service, act as intermediaries, or digital platforms, between other parties, such as prosumers (consumers who also produce energy) and network operators. In addition, the suppliers of (digital) technology and services are also playing an increasingly important role in the energy transition.

Players who perform such new roles and activities are generally not so well represented in political and public debates. However, this is also changing: EnergieSamen (the overarching organization for energy communities) and Techniek Nederland (the overarching organization for the installation sector), for example, are increasingly acknowledged as important stakeholders and involved in debates on the new Energy Law and the new sector agreement system for data sharing (MFFBAS).

Why is this important?

According to the Dutch government, »digitalisation is essential for the development of flexible energy networks, for the efficient use of the energy system, and to limit the costs of [the energy] transition« (Nederland Digitaal 2021, p.11). The large-scale roll-out of smart meters, which started in the Netherlands in 2012, improved the availability of more detailed metering and consumption data. To use that data, the exchange of data needs to be better organized from a legal and organizational point of view. However, according to the ministry of EZK, this »not only places higher demands on data availability (frequency and quality) but also on the mitigation of cyber-related risks« (EZK 2021, p.7). Moreover, enabling the (responsible) use of digital technology and data is urgent given the target of 55% emission reduction that the Netherlands wants to achieve by 2030 and the problems that are already arising in the fields of network capacity and security of supply (Rathenau Instituut 2022a).

Societal and political relevance and debate

Ongoing debate

Since the early 2000s, governments all over Europe made efforts to introduce smart meters. In 2008, the Minister of Economic Affairs proposed an amendment to the Electricity Act of 1998 to enable the rollout of smart meters in the Netherlands. This proposal sparked a heated debate about privacy, security and transparency issues (Rathenau Instituut 2022a). By joining the public and political debate, interest groups, supervisors and representatives contributed to the negotiation of the criteria for the introduction of the meter – a process previously dominated by policymakers and energy sector incumbents.

During the last decade, the use of digital technologies and data has become an increasing priority on the agendas of European and national policymakers and energy sector parties. This has to do with the expectation that their use can help facilitate the energy transition. This development is also in line with national policies and strategies in the field of digitization and data sharing (e.g. EZK 2019a; EZK 2019b; Nederland Digitaal 2021). More recently, the political and public debate on the use of data and digitization for the energy transition has centred around the previously mentioned new Energy Law and a new sectoral agreement system to share data. This debate focuses primarily on the removal of barriers to the use of smart meter data, concerning consumer privacy and system security.

Legislation in place

European and national sector-specific, as well as more general legislation and regulations regulate the use of digital technologies and data in the energy sector (Rathenau Instituut 2022a). The rules and agreements that determine who has what responsibility for the use of digital technologies and data in the energy sector are spread over various laws, regulations and codes. The Electricity Act 1998 is the most important law that lays down the tasks and responsibilities of energy market players. Because the energy sector was much less digitized at the time, the link with data is not always made clear in that law. At present, numerous »codes« therefore supplement the law, in which the overarching rules are further elaborated. These codes relate to the activities of network operators, suppliers and metering companies. There are codes for determining prices (tariff codes), connections, measurements and transmission capacity (technical codes) and the exchange of data (Information Code Electricity and Gas). In addition, there are also European-defined codes with direct effect.

Current political or legislative proposals

At the European level, the European Commission is working on an action plan for the digitization of the energy sector, to achieve a »safe, efficient and sustainable energy infrastructure« (EC 2021). The action plan is part of a broader European data strategy, in which the Commission identifies the energy domain as one of nine »data spaces« within and between which data should be exchanged more effectively. The Dutch government also wants to encourage the sharing and use of energy data. It does this through a broader digitization policy (EZK 2019a; EZK 2019b; Nederland Digitaal 2021) and policy and legislation specifically aimed at the energy domain (EZK 2021). Policy and legislative actions, such as the new Energy Law, are primarily intended to remove existing barriers to the use of data. For example, the Dutch government sees challenges in the areas of data availability and accessibility and data quality. The use of data in the energy domain also requires a review of data exchange processes and a reassessment of consumer rights, such as privacy and control over data, partly in line with other recent European legislation, such as the General Data Protection Regulation (GDPR).

Science/evidence-based inputs guiding political decision-making

Over the past five years, various research institutes have stimulated the political and public debate on the opportunities and risks of digitization for the energy transition. In 2017, the Netherlands Environmental Assessment Agency concluded that if the digitization of the electricity system remains ungoverned, it could put public values such as accessibility, transparency and security of supply under pressure (PBL 2017). In 2018, the Council for the Environment and Infrastructure raised the question of whether the government can sufficiently guarantee the reliability of our power supply, now that the digitization of the electricity system is entering a new phase (Rli 2018). They concluded that there was attention to risks related to cybersecurity, but that there was an insufficient insight into other vulnerabilities, particularly those related to the parts of the energy system not in public ownership. In 2019, the Rathenau Instituut highlighted the importance of retaining democratic control over the digitization of the energy system, safeguarding public values such as privacy, security and autonomy and equal power relations (Rathenau Instituut 2019).

More recently, the Rathenau Instituut (2021) concluded that at present, there is increasing attention to public values in the energy transition, such as in the new Energy Law. However, more work is needed to ensure that the use of digital technologies and data contributes to a just energy transition (Rathenau Instituut 2022). For example, extra policies and agreements are needed to enable smart energy management systems and smart assets can communicate with each other. Moreover, the government and sector parties do not yet have all relevant data in their sight: current legislation and regulations mainly focus on smart meter data, while agreements such as on data quality or security, are also needed for the use of data from, for example, heat pumps, charging stations or inverters for solar panels.

Role of TA in the debates

Rathenau Instituuts' contributions to this topic?

As early as 1994, the Rathenau Instituut published a report on the effects of power outages in the Netherlands and ways to increase the country's resilience (Rathenau Instituut 1994). In 2011, the Rathenau Instituut investigated with the help of several experts how the Netherlands can keep its energy supply economically and socially acceptable, considering that every energy technology leads to societal issues and concerns (Ganzevles & Van Est 2011). The book concluded that in the coming decades, the Netherlands would have to deal with an increasingly controversial energy supply in terms of affordability and the living environment. We can now conclude that this has turned out to be an accurate prediction. In 2016, the Ministry of Economic Affairs announced that it would organize an energy dialogue because of the opposition to all kinds of energy technologies. The Rathenau Instituut formulated eleven lessons that the government could use for this dialogue (Rathenau Instituut 2016).

In the meantime, the Rathenau Instituut conducted extensive research on the impact of digital technologies on society (see also the chapter on Autonomous Systems in the Netherlands). The report »Urgent upgrade: Protect public values in our digitized society« marks the starting point for the political and social debate on the ethical, legal and social aspects of digitization in the Netherlands (Rathenau Instituut 2017). In 2019, the Rathenau Instituut started to explore the societal impact of the twin green and digital transition from two perspectives. We investigated how the use of digital technologies and data can contribute to a just energy transition (Van Est & Dekker 2019; Rathenau Instituut 2019; Rathenau Instituut 2020; Rathenau Instituut 2022a) and investigated the societal value of data centres and decision-making about their location (Masson et al. 2020; Rathenau Instituut 2022b).

Has TA made an impact on the ongoing debates?

The work of the Rathenau Instituut has played an important role in stimulating the general public and political debate about the impact of digitization on society. This has led to the discussion about digitization not only looking at privacy and cyber security but at a broader platform of public values, such as human dignity, equity and equality, autonomy, balances of power and sustainability. More recently, this has also been the case for our work on the twin transition. We contributed to the early identification of the opportunities and risks of digitization and identified governance challenges. Moreover, we observed that public values, such as control over data and privacy and security, have taken a more central role in political debates and legislation and regulations, such as the new Energy Law. The public debate has also been stimulated through the Club van Wageningen, a network of influential pioneers from energy companies, network operators, scientists, prosumers, ministries and start-ups, that want to maintain the values of fair, inclusive and democratic governance in the energy system of the future. The Rathenau Instituut plays an active role in the Club van Wageningen and the debate on value-driven digitization in the energy sector.

Lessons learned from TA

The Rathenau Instituut has broadened the public and political debate on the role of digitization in the energy transition by starting from the question of how digital technology and data can contribute to a »just« of »fair« transition. It became clear that better availability and access to energy data alone is not enough to ensure that the use of data contributes to a just transition. The governance of data and digital technologies should also address challenges characteristic of digitization projects (e.g. rapid technology obsolescence, interoperability of systems and assets or cyber resilience challenges). And ensure a good societal embedding of digital energy practices (which, for example, also requires knowledge and resources from citizens, communities or companies that want to contribute to the transition). When setting up governance, the guiding question must be how the use of digital technologies and data can contribute to policy goals (such as an affordable, reliable, safe, spatially adaptable and clean energy system) and how broadly shared public values can be safeguarded in this process (including privacy, equity, fairness, transparency or equal balances of power). After all, digital technologies and data are a means – and not an end in themselves.

References

ACM (2019). Visie datagovernance energie. Den Haag: Autoriteit Consument & Markt.

Deloitte (2021). Verkenning rollen Agentschap Telecom in de energietransitie. Amsterdam: Deloitte Financial Advisory B.V.

EC (2021). Digitalisering van de energiesector – EU-actieplan. Website European Commission. https://ec.europa.eu/info/law/better-regulation/have-yoursay/initiatives/13141-Digitalisering-van-de-energiesector-EU-actieplan_nl

Est, van R. & Dekker, R. (2019). Alles draait om adequate datagovernance: hoe de energietransitie digitaliseringskwesties urgent maakt. Den Haag: Ministerie van Economische Zaken en Klimaat.

EZK (2019a). Nederland Digitaal: De Nederlandse visie op datadeling tussen bedrijven. Den Haag: Ministerie van Economische Zaken en Klimaat.

EZK (2019b). Nederlandse Digitaliseringsstrategie 2.0. Den Haag: Ministerie van Economische Zaken en Klimaat.

EZK (2021). Memorie van toelichting wetsvoorstel Energiewet – deel I (algemeen) (versie 17 november 2021). Den Haag: Ministerie van Economische Zaken en Klimaat.

Ganzevles, J. & R. van Est (red.) (2011). Energie in 2030 – Maatschappelijke keuzes van nu. Den Haag: Rathenau Instituut.

JRC (2022). Towards a green and digital future. Key requirements for successful twin transitions in the Europe Union. Brussels: Joint Research Centre. (Auteurs: Muench, S., Stoermer, E., Jensen, K., Asikainen, T., Salvi, M. & Scapolo, F)

Masson, E., R. Dekker en R. van Est (2020). Waardevol digitaliseren voor de energietransitie. Website Raad voor de Leefomgeving en Infrastructuur. https://www.rli.nl/sites/default/files/essay_1_waardevol_digitaliseren_voor_de_energietransitie_-_rathenau_instituut_-_def_0.pdf

Netbeheer Nederland (2022). Quickscan coalitieakkoord energiesysteem. Den Haag: Netbeheer Nederland.

Rathenau Instituut (1994). Stroomloos. Kwetsbaarheid van de samenleving; gevolgen van verstoringen van de elektriciteitsvoorziening. Den Haag: Rathenau Instituut. (Auteurs: Steekskamp, I. & A. van Wijk)

Rathenau Instituut (2016). Elf lessen voor een goede Energiedialoog. Den Haag: Rathenau Instituut. (Auteurs: Est, R. van & A. van Waes m.m.v. A. de Vries)

Rathenau Instituut (2017). Urgent upgrade. Protect public values in our digitized society. Den Haag: Rathenau Instituut. (Auteurs: Kool, L., J. Timmer en R. van Est)

Rathenau Instituut (2019) Beheer energiedata vanuit algemeen nut. Zet digitalisering in voor schone, betrouwbare, veilige en betaalbare energie voor iedereen. Den Haag: Rathenau Instituut.

Rathenau Instituut (2020). Hoe duurzame energie en digitalisering samenhangen.

Website Rathenau Instituut. https://www.rathenau.nl/nl/digitale-samenleving/hoeduurzame-energie-en-digitalisering-samenhangen

Rathenau Instituut (2021). Reactie op wetsvoorstel »Energiewet«. Den Haag: Rathenau Instituut

Rathenau Instituut (2022a). Stroom van data – Energiedata benutten voor een maatschappelijk verantwoorde energietransitie. Den Haag: Rathenau Instituut. (Auteurs: Dekker, R., E. Masson, R. de Jong en R. van Est)

Rathenau Instituut (2022b). Datacentra in publiek perspectief: Naar een nationaal beleidskader voor de digitale infrastructuur. Den Haag: Rathenau Instituut.

PBL (2017). Mobiliteit en elektriciteit in het digitale tijdperk: Publieke waarden onder spanning. Den Haag: Planbureau voor de Leefomgeving (auteurs: Hollander, G. de, M. Vonk, D. Snellen, H. Huitzing).

Rli (2018). Stroomvoorziening onder digitale spanning. Den Haag: Raad voor de Leefomgeving en Infrastructuur.

Norway – Norwegian Board of Technology (Teknologirådet)

Critical Infrastructure, Cybersecurity, and the Internet of Things

Critical infrastructure and societal services are increasingly reliant on the internet. Cybersecurity is now protecting not only information but also our physical safety.

Cyber tools have given attackers »the perfect weapon«:[60] They are cheap, effective, and hard to detect. Attacks can be made from anywhere in the world. The attacker only needs to succeed once, while the defender needs a 100 percent success rate. It is versatile and can be used for espionage, sabotage, and economic gain. While attacks have so far had limited impact on critical infrastructure in Norway, the growth in digitalization and hacking attacks gives evidence to the threat.

The Internet of Things (IoT) encompasses a multitude of internet-connected objects equipped with computers, sensors, and actuators. The term IoT first came into use for describing consumer electronics, particularly in the context of smart homes. Increasingly, IoT also includes critical infrastructure, industry, and essential societal services.

By interconnecting objects and services, IoT has been characterized as a world-sized robot that senses, thinks, and acts. This changes society in ways we can't predict in detail, both for good and bad.[61] 5G is currently being rolled out in several countries, allowing more units to be connected per square kilometer. The number of IoT units worldwide is expected to grow from 12 billion in 2020 to 31 billion in 2025.[62] This interconnectedness means that a digital attack can disrupt not just information, but also physical infrastructure, societal functions, and people's lives.

While physical technologies early on had to adopt a safety-by-design for any implementation, digital technologies have maintained a launch-fast-and-patch-later approach. The constant app updates we see on our phones are a testament to this. This allows for fast development and rapid evolution of the technologies. As physical technologies increasingly become digital, the two safety paradigms are merging.

State of play: A growing gap between threats and capabilities

Norway is highly digitalized, and the energy, financial, and health sector is becoming increasingly integrated with digital services and functions. The digitalization of critical infrastructure offers benefits in speed and functionality but also exposes society to the threat of crippling attacks on a major scale.

[60] Sanger, D. E.(2018) The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age

[61] Schneier, B., The Internet of Things Will Be the World's Biggest Robot, https://www.schneier.com/blog/archives/2016/02/the_internet_of_1.html

[62] State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time

Norway is ranked in the top five of the European Commission's Digital Economy and Society Index.[63] The mobile broadband take-up is 99%, and 92% of internet users use government e-services. Norway is highly reliant on electricity, which is used for most heating and increasingly also for charging electric vehicles. The electrical infrastructure has more points of attack and disruption can impact the critical societal functions of heating, cooking, and transportation.

The global trend of increasing cyber-attacks is also present in Norway.[64] The Norwegian National Cyber Security Centre registered a threefold increase in serious incidents from 2019 to 2020.[65] In their report »Risk 2022«, the Norwegian National Security Agency (NSM) warns that the gap between threats and security capabilities is growing wider.[66]

In recent years, Norway has seen several large-scale cyber-attacks and disruptions that show the emerging vulnerabilities:

Societal functions: The municipality of Østre Toten was a victim of a ransomware attack in January 2021. Data concerning healthcare, welfare, and child services was made unavailable. It took over a month before working conditions were restored and citizens could use healthcare, welfare, and child services as normal.

Physical impact: The hotel chain Nordic Choice was attacked in December 2021. Booking and key card systems were disrupted in 200 hotels across Scandinavia, preventing guests from accessing their rooms.

Food supply: Nortura, Norway's largest meat supplier, was attacked in December 2021. All IT systems were shut down, stopping meat production for 13 days.

Financial services: Payment card terminals in most stores throughout the country stopped functioning for several hours during some of the busiest shopping hours the day before Norway's national day, the 17th of May 2022.

Key stakeholders: An additional layer of responsibility

The Ministry of Justice and Public Security is responsible for coordinating digital security in the civilian sector. In addition, individual companies and area-specific regulating bodies are responsible for maintaining services critical to society. These stakeholders represent a traditional view of security being assured through safety-by-design.

IoT and smart homes increasingly challenge this view by bringing vulnerabilities to people's homes. For instance, Norway has experienced significant growth in the sale of electric vehicles in recent

[63] European Commission (2022), Digital Economy and Society Index (DESI) 2022 https://digital-strategy.ec.europa.eu/en/policies/desi-norway

[64] Samfunnssikkerhet i en usikker verden. Meld. St. 5 (2020-2021) https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf

[65] The Norwegian National Security Authority, Nasjonalt digitalt risikobilde 2021 https://nsm.no/getfile.php/137495-1635323653/NSM/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf

[66] The Norwegian National Security Authority, Risiko 2022 https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

years. This means that a large part of the fuel supply – a critical function – is placed in private homes and dependent on the electricity grid. Internet-connected chargers are often used to optimize charging when electricity prices are low. Furthermore, health and care services delivered to smart homes can also have vulnerabilities.

An additional layer of security has been created to counter the digital vulnerabilities in critical infrastructure. Many sectors delivering critical functions are connected to one of several national computer emergency response teams (CERT). These include HelseCERT for health services or KraftCERT for power services. The lack of a national CERT for the water supply has been highlighted as far back as 2015.[67] Currently, the municipalities handle cybersecurity for water supply on their own, and there is a lack of national coordination.

Societal and political debates

Digital vulnerability

The 2015 Norwegian Official Report »Digital vulnerability – secure society«[68] raised the alarm on possible consequences of Norway's high degree of digitalization. While it has increased efficiency and modernization benefits, the risk and vulnerability have also grown. Long and complex value chains make it difficult to detect and prevent cyberattacks. In addition, most telecommunication depends on a single core network for virtually all digital value chains. As a result of this report, The Norwegian Communications Authority (NKOM) has started pilot projects to construct an alternative core network.[69] The core network still has significant vulnerabilities, however, and digital value chains have only grown longer and more complex.

In 2017 NKOM pointed out that nearly all of Norway's international internet traffic was routed through a small number of fiber cables in Sweden. The lack of redundancy in critical telecommunications infrastructure was highlighted as a concern. [70] Since then, construction of several new undersea cables has commenced, providing additional international internet connections for Norway.

[67] NOU 2015:13 Digital sårbarhet – sikkert samfunn https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

[68] NOU 2015:13 Committee of Digital Vulnerabilities in Society – English Summary https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/9.pdf

[69] The Norwegian Communications Authority (NKOM): Quarterly report 1/2021 https://www.nkom.no/rapporter-og-dokumenter/tertialrapport-1-2021

[70] NKOM: Robuste og sikre nasjonale transportnett – målbilder og sårbarhetsreduserende tiltak (2017) https://www.regjeringen.no/contentassets/e5a6166743d949e8a703f9feae23dc0f/robin_rapport.pdf

Security vs. privacy

The interests of public safety can lead to proposals to introduce new and intrusive surveillance methods that conflict with privacy. An expert report was released in 2016: »Digital Border Defense,« which recommended giving the Norwegian Intelligence Service access to data traffic passing Norway's border through fiber optical cables. The background was »the rise of cross-border threats and the increased occurrence of cyber threats targeted at state bodies and private operators.«[71]

The proposed Digital Border Defense launched a heated debate concerning the trade-off between security and privacy. The Norwegian Data Protection Authority argued that the Digital Border Defense, as proposed, would lead to mass surveillance of Norwegian citizens. The authority also questioned whether the proposed border defense would be targeted enough to help prevent crime. A new Intelligence Service Act was passed in Norway in 2020, which included a somewhat limited version of the border defense named »facilitated data collection.« The limits and restrictions for the data collection are still being debated, and there is significant opposition against the overall measure.

Who can be trusted to provide critical infrastructure?

5G is currently being rolled out in Norway and will become a critical infrastructure for areas such as health, industry, and emergency communication. Security obligations for 5G infrastructure providers became an issue of much debate in Norway.[72] The industry-leading Chinese firm Huawei was expected to win the contracts in Norway, but its ties to the Chinese government created controversy. As part of a new security act, a minimum of 50 percent of 5G base stations should be delivered from countries with which Norway has security cooperation.[73] The Swedish company Ericsson won the contracts for building most of the 5G infrastructure in Norway.

Role of Technology Assessment

Horizon scanning

Technology Assessment (TA) can provide early analyses of opportunities, risks, and political options for new technologies. An essential role for The Norwegian Board of Technology (NBT) is its function as a »technology radar« for the Parliament, placing new and important technologies on the agenda at an early stage. This is done through writing policy briefs, regular meetings with the Parliaments' *Techno Group,* and contributing knowledge to government reports. In recent years, NBT has

[71] Norwegian Ministeries: List of measures – National Cyber Security Strategy for Norway (2019) https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/list-of-measures--national-cyber-security-strategy-for-norway.pdf

[72] The Norwegian Board of Technology (2019): 5G – what does it mean for Norway? https://teknologiradet.no/wp-content/uploads/sites/105/2019/05/5G_english.pdf

[73] Friis, Karsten (2021): Huawei, 5G and Security: Technological Limitations and Political Responses https://www.nupi.no/en/publications/cristin-pub/huawei-5g-and-security-technological-limitations-and-political-responses

contributed to describing technology trends for several green papers on digital security. This includes IoT, wearable devices, autonomous transport, the blockchain, 3D printing, and drones. NBT placed 5G on the agenda early on and has recently provided information about the risks and opportunities of Digital Central Bank Currencies, which may be important for the future of financial systems.

Scenarios

Scenario methods can help create future-oriented policies. The Norwegian Directorate for Civil Protection (DSB) has published reports on crisis scenarios for several years. Their most recent scenario report from 2019[74] explores possible consequences of two types of devastating cyber-attack:

A digital attack on the core network infrastructure would hinder access to TV, radio, the internet, emergency networks, transport, and payments. Such an attack was estimated to have severe consequences for society's stability and lead to loss of lives.

A digital attack on the financial infrastructure was estimated to have severe economic consequences and damage trust in society.

An essential question for Parliamentary Technology Assessment is to what extent foresight and scenarios are sufficiently integrated on a national political level. In this and many previous reports, DSB described a flu-like pandemic as the most likely high-impact incident Norway could face. Still, Norway had not yet developed a governance framework for a pandemic that was sufficiently holistic when COVID-19 hit.[75]

While the DSB scenarios explore consequences and preparedness for emergencies, scenario methods can also be used to map out options for shaping the technology and explore value-based questions. The Norwegian Board of Technology is a partner of the RELINK research project[76], which examines vulnerabilities in smart homes. The premise for the project is that households constitute a weak link in the overall digital security of society. NBTs main role in this project is to develop scenarios that will examine policy options for the security of smart home technology.

Involving citizens and stakeholders

From the start of the RELINK project, citizens have been involved in describing their use of technology and their perception of risks. Scenario-building will use citizens' experiences as a point of departure. Furthermore, the scenarios will be discussed with stakeholders, which will help formulate policy advice. The end goal of the project is to provide citizens and households with tools to enable better digital risk evaluation.

[74] The Norwegian Directorate for Civil Protection (2019): Analyses of Crisis Scenarios https://www.dsb.no/rapporter-og-evalueringer/analyses-of-crisis-scenarios-2019/

[75] EPTA Report 2021: Norway's contribution (p. 87) https://eptanetwork.org/images/documents/EPTAreport_2021_lessons_from_the_COVID19_pandemic.pdf

[76] RELINK project website: https://uni.oslomet.no/relink/

Technical analyses for evaluating risks

Analyzing and finding security flaws in digital equipment can be time-consuming and technically challenging.[77] As part of the RELINK project, NBT has partnered with cybersecurity experts to open the black box of smart home devices by analyzing one hundred apps used to manage IoT devices sold on the Norwegian market. This will provide a better basis for scenario development and give a better understanding of the vulnerabilities and risks connected to smart homes.

For the future of Technology Assessment, other combinations of methods could be useful to explore. For instance, digital twins are increasingly being used to test and simulate cybersecurity in critical infrastructure.[78] Combining scenarios from TA with such simulations could be helpful to strengthen the impact of policy advice.

[77] Karsten Friis and Olav Lysne, 2022: 5G-sikkerhet: Norge mellom Stormaktene. p. 153

[78] Kumar, Sarad, Venugopalan, Wong, Leu (2022): An electric power digital twin for cyber security testing, research, and education https://www.sciencedirect.com/science/article/abs/pii/S0045790622003196

Portugal – Observatory of Technology Assessment (OAT)

Mission Critical Communication: a technology assessment approach for Smart City scenarios

Débora Vanessa Campos Freire[79]

Abstract

This article presents an overview of the challenges faced by Public Protection & Disaster Relief (PPDR) agencies to modernize narrowband Mission Critical Communication (MCC) networks of Land Mobile Radio (LMR), migrating to, or integrating them with Long Term Evolution (LTE) 4G and 5G networks, and aggregating intelligent services. This study is being further developed at the Observatory of Technology Assessment in Portugal.

Keywords: Mission Critical Communication; Smart City; Public Protection & Disaster Relief (PPDR); 5G; Long Term Evolution (LTE); Emergency First Responders (EFR).

Introduction

The agencies that act in emergency situations, such as police forces, firefighters, rescue squads and emergency medical services, are called Emergency First Responders (EFR). EFRs are the first actors in crisis situations, working in the area called Public Protection & Disaster Relief (PPDR). Radio-communication networks are one of the main support tools for PPDR agencies. Therefore, they are called Mission Critical Communications (MCC), and there are specific international protocols for these technologies. According to the GSM Association[80], Critical Communication (CC) are used in situations »where human life and other values for society are at risk and where timely and reliable communications between EFRs is essential to avoid or at least mitigate damage«. Although, CC are also applicable to many other sectors of society and industries, the term Mission Critical Communication (MCC) is used to refer to the communication made by EFRs working at PPDR agencies, using also terms as Mission Critical voice and Mission Critical services (Lair & Mayer, 2017; Yy et al., 2018).

MCC is a technology globally used by public agencies that develops works in PPDR areas, most part of the PPDR agencies still uses the LMR generation system, a digital system based on trunked radio technology[81], conceived for priority use of voice, with very limited capabilities for data applications, providing bandwidth of 12.5 kHz on average, which allows sending text messages only. Currently

[79] NOVA School of Science and Technology, New University of Lisbon – dv.freire@campus.fct.unl.pt

[80] Is an industry organization that represents the interests of mobile network operators worldwide with more than750 mobile operators and 400 companies as GSMA members (GSMA, 2018)

[81] Is a technology that involves two-way radio, allowing the sharing of a few radio frequency bands between a large number of users.

there are three MCC LMR standards, namely APCO-25[82]4, TETRA[83]5 and TETRAPOL[84]6. The LMR system used nowadays do not have enough bandwidth to enable the use of intelligent resources, and they are not sufficiently standardized to allow the technology integration, which means, if PPDR agencies are using different LMR standards they are not able to communicate with each other. However, given the technological evolution present today, it is necessary to modernize these systems, enabling an efficient performance of PPDR agencies based on data analysis and systems integration in a Smart City environment.

Broadband Mission Critical Communication

With the intention of developing the MCC for broadband, allowing system integration and data traffic, the TETRA and Critical Communications Association (TCCA), an association representing all standards of MCC, indicated LTE (4G) as the broadband technology for MCC (Doumi et al., 2013; Freire, 2019). LTE uses standardization defined by 3GPP.[85] Through broadband communication, the technological capabilities are expected to be transformed, such as, PPDR agencies accessing data in real time, and modifying the way the police act and investigates; firefighters receiving real-time information from fire sites, through drones providing images over a dedicated 5G network; medical emergency services receiving help from hospital doctors through the use of augmented reality; remotely controlled machines for the most diverse purposes. Security, control, network availability, costs, management, and regulatory affairs are big concerns (Freire & Cândido, 2020).

Also, the evolution of 4G, the 5G network, is ready to improve Public Safety networks, as highlighted by C. Cui, Zhou, and Chen (2022, p. 427) »Legacy public safety networks require modernization to improve the safety, situational awareness and operational effectiveness for first responders and the application of 5G technology can solve this problem well«. In addition, the standardization of 5G for MCC will bring the possibility to offer new services and operation modes, such as, Non-Terrestrial Network (NTN), allowing satellites to be used as base stations (named in 4G as eNodeB, and 5G as gNodeB). Nowadays, in isolate areas as Amazonia, the PPDR agencies are facing several communications problems using LMR networks, and satellite phones have a high cost. This type of solution can improve communications in places where is difficult to install and operate radiocommunication system for critical mission.

In addition to the advantages of using broadband networks, networks standardized by 3GPP have solutions developed together with various actors, such as, industries, companies, and research centers, enabling more interfaces to be open. That opening can bring benefits due to the diversity of equipment manufactures, and solution providers. Also, with MCC operating in 4G and 5G networks, bringing to the MCC ecosystem actors that previously developed solutions only for commer-

[82] Apco 25 has standards defined by Telecommunications Industry Association (TIA) (2002)

[83] TETRA has standards defined by European Telecommunications Standards Institute (ETSI) (2020).

[84] TETRAPOL has standards defined by TETRAPOL forum (2022).

[85] Is a collaborative project between seven telecommunications organizations, producing technical specificationsfor mobile networks from 3G (3GPP, 2018).

cial mobile networks. Although, the 3GGP sets the technological standard but does not set a standard for the digital transition of the PPDR agencies. Through the literature review and through interviews and data analysis in Freire (2019), was possible to conclude that vendors and experts understanding that some models are viable, namely:

- *Dedicated solution*: broadband networks for the PPDR agencies.
- *Hybrid solution*: most network resources are under control of agencies, sharing RAN resources with Mobile Network Operators (MNO)s; agencies build some RAN if necessary.
- *Secure Mobile Virtual Network Operator (S-MVNO)*: control and security of the user base and apps, RAN of MNOs, possibility of coverage from multiple MNOs.
- *Through MNOs*: agencies use operator networks; coverage may not be tied to one MNO if legislation allows national roaming for PPDR; priority and preemption for EFRs over regular users depends on country regulatory issues; technically, LTE user prioritization can occur through priority levels, preemption capability and preemption vulnerability, Allocation and Retention Priority (ARP).

Some Use Cases of Mission Critical Communication through Broadband Networks

FirstNet, in USA, and the Emergency Services Mobile Communications Program (ESMCP), in UK, adopted a mix of LMR and LTE networks as a solution. LMR offers narrowband voice capacity for MCC, with restricted data rates but with wide area coverage, in addition to LMR direct mode. FirstNet and ESMCP provide MCC broadband (Emergency Services Mobile Communications Programme (ESMCP), 2022; FirstNet Authority, 2022).

The European Union (EU) is working on a pan-European broadband mobile system for PPDR, which is in its third and final phase. BroadWay Pre-Commercial Procurement started on October 8th 2021, initiated by the signature of awarded contracts to the two first ranked consortia of the Phase 3 call-off competition, following their successful completion of the Phase 2 (Prototype Phase) (BroadWay, 2022; Public Safety Communication Europe PSCE, 2020).

MVNO solutions are being used in Mexico, with a gradual migration of the LMR TETRAPOL from TDM to IP. Airbus provides broadband for Public Safety through the »Red Compartida«, which has 90 MHz bandwidth, in 700 MHz. ALTAN is a Mobile Virtual Network Enabler (MVNE) and provides broadband for Airbus, which performs the interoperability between TETRAPOL IP and ALTAN network as MVNO (Freire, 2019).

Dubai (Hill, 2019/March 28) and South Korea (Baek Byung-yeul, 2020/Feb. 05) are some examples of national LTE network for PPDR. Sendai developed a private LTE network, with drones for alert and rescue assistance in case of tsunamis (Nokia, 2020). Australia are using the Telstra LANES Emergency, mission critical communications with prioritized access, preferential data treatment and self-dimensioning bandwidth on commercial LTE network (Telstra, 2022).

Information Technology integrated with Broadband Mission Critical Communication

In PPDR area, there are several motivations to the use of technology of information as Internet of Things (IoT) devices and Big Data, intending to help the society, as reducing crimes rates and in responsiveness emergency situations. Although, to make a decision about which information technology the PPDRs agencies should use, is necessary a better understanding about the types of data that should be collect, the sensors to be used, the computation techniques and the data mining tools options to assist in data mining process, intending to find knowledge in databases and information visualization through classification and real-time analysis. And then, make a decision about which of that information should be shared at the communication technology system, and in which way.

Combining those source information with the traditional government monitoring system, providing basis for the design of early warning information management system. An information platform allowing transmitting warning messages to authorities, even dealing with incidents before they occur to prevent emergencies from occurring, driven by different goals to realize the overall safety of the city and citizens (Atat et al., 2018; D. Cui, 2015; Wu & Yu, 2020). The so-called »smart city public safety emergency management«[86] (Wang & Li, 2021, p. 169) should make full use of Internet, Internet of Things (IoT), Cloud Computing, and system integration in a smart city scenario, allowing emergency management system to play a positive role in urban safety governance.

For disaster events applications the use of Big Data can improve the accuracy and scientificity of the emergency decision-making made by the commanders, where some sensors can be triggered to do actions, as initiate water spray fire fighting measures when the smoke concentration exceeds a threshold, and the dispatcher center can better allocate the emergency resources according to on site data reading from sensing techniques as context-aware physical sensors and social sensing. In the Figure 1 is shown a summary about the cyber-physical systems panorama found in the literature review for PPDR purposes. Nowadays, with the social computing, the citizen can contribute to the emergency system as a source data, being an actor of the system as showed below. The multiplicity of scenarios and use cases justifies that a Technological Assessment are carried out, considering different aspects involving the technology application, as showed in the Figure 2.

[86] It can be inferred from the literature review that Smart City Public Safety Emergency management refers to systems used in Smart City for both applications, emergencies such as disasters, and for Public Security, also referred just by Smart City.

Figure 1 – Cyber-physical systems panorama for PPDR purposes

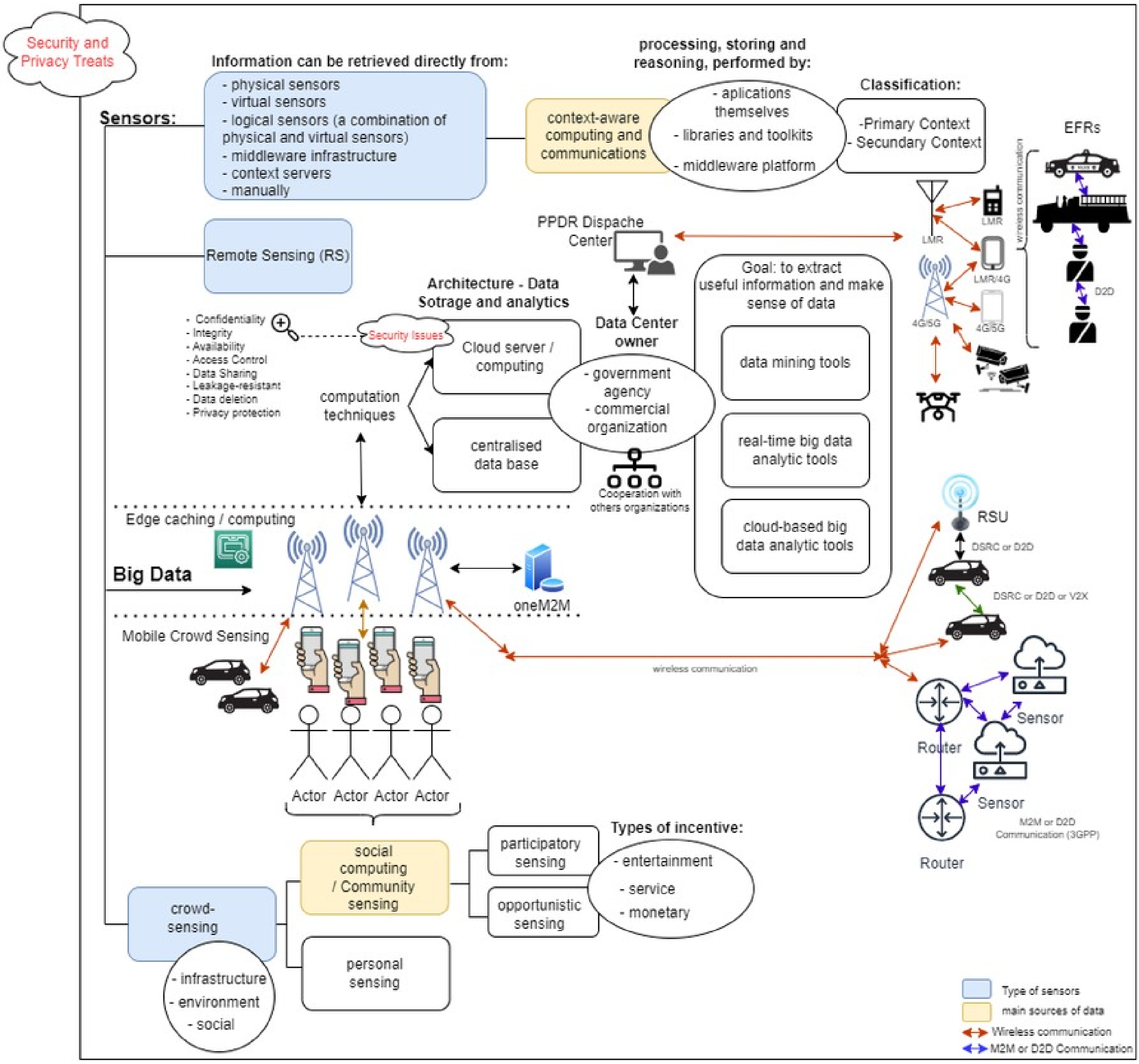
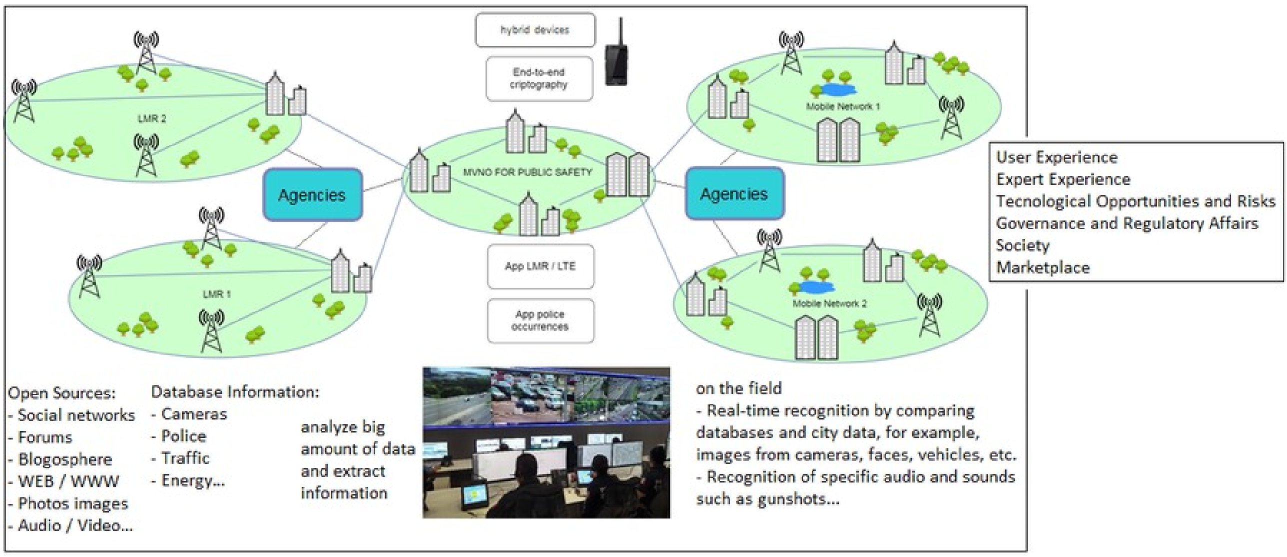


Figure 2 – Possible scenarios



User Experience
Expert Experience
Tecnological Opportunities and Risks
Governance and Regulatory Affairs
Society
Marketplace

Open Sources:
- Social networks
- Forums
- Blogosphere
- WEB / WWW
- Photos images
- Audio / Video...

Database Information:
- Cameras
- Police
- Traffic
- Energy...

analyze big amount of data and extract information

on the field
- Real-time recognition by comparing databases and city data, for example, images from cameras, faces, vehicles, etc.
- Recognition of specific audio and sounds such as gunshots...

Summary and insights

As the Information and Communication Technology (ICT) sector is experiencing a significant growth in development and solutions, it is expected several technological solutions intending to improve the PPDR services, nevertheless, it should be better analyzed how the agencies should make the digital transition for each applied case, and how about the society consequences. Portugal, as many countries, still doesn't have a Smart City Public Safety Emergency management, as still doesn't have a particular solution implemented for broadband MCC, in that sense, the constructions of scenarios, role of the Technology Assessment, can help the PPDR agencies in the technological decision-making process of the Digital Transformation of MCC, considering Smart City options, without increasing the risks of massive disruptions in society.

The technological integration also lead to debates related to data protection and privacy. Individuals are increasingly exposed, with the invasion of privacy becoming difficult to regulate due to the combination of corporate giants owning the data, the global breadth of cyberspace, and the relationship with the States policies. The use of broadband networks with systems integration by PPDR agencies in Smart City Scenario, allows the possibility of accessing various information from different agencies, such as, electricity, water, gas, police, traffic agencies, and different sources as crowdsourcing and IoT devices, also combined with artificial intelligence. That use can bring negative consequences for society in terms of privacy and government control over citizens if there is no proper regulation, as the use of crowd-sourced information combined with artificial intelligence in the algorithmic bias to construct predictive policing models as discussed in Lum and Isaac (2016).

In addition to the technological analysis, democratic states and the society should reflect on what surveillance and privacy would be and the limit of access to information in the cities. Intending to maximize the positive effects and minimize the negative effects, the Technology Assessment can help governments and civil society, to find possible paths for the evolution of the cities, meeting an ethical, legal, and appropriate social pact, strengthening democracy, institutions, and citizens through transparency and scientificity to the decision-making process of a technological decision that affects the society.

References

3GPP. (2018). 3GPP Global Initiative LTE. online. Retrieved from http://www.3gpp.org/ technologies/keywords-acronyms/98-lte

Atat, R., Liu, L., Wu, J., Li, G., Ye, C., & Yi, Y. (2018, Nov.). Big Data Meet Cyber-Physical Systems: A Panoramic Survey. IEEE Access: Special Section on Internet-Of-Things (Iot) Big Data Trust Management, 6, 73603 – 73636. Retrieved from DOI:10.1109/ ACCESS.2018.2878681

Baek Byung-yeul. (2020/Feb. 05). KT begins public safety network project. on-line (The Korea Times). Retrieved from https://www.koreatimes.co.kr/www/tech/2018/ 12/133_260835.html

BroadWay. (2022). BroadWay is Procuring Innovation activity to enable a pan-European broadband mobile system for PPDR, validated by sustainable test and evaluation capabilities. on-line. Retrieved from https://www.broadway-info.eu/

Cui, C., Zhou, G., & Chen, C. (2022). Research on Intelligent Mobile Police Application Based on 5G Technology. In 2022 ieee international conference on electrical engineering, big data and algorithms (eebda) (pp. 426 – 429). Retrieved from https://doi.org/ 10.1109/EEBDA53927.2022.9744766

Cui, D. (2015). Risk Early Warning Index System in the Field of Public Safety in Big Data Era. In 2015 sixth international conference on intelligent systems design and engineering applications (isdea) (pp. 704 – 707). Guiyang, China. Retrieved from doi:10.1109/ISDEA.2015.180

Doumi, T. L., Dolan, M. F., Tatesh, S., Casati, A., Tsirtsis, G., Anchan, K., & Flore, D. (2013). LTE for public safety networks. IEEE Communications Magazine, 51(2), 106 – 112. Retrieved from http://dx.doi.org/10.1109/MCOM.2013.6461193

Emergency Services Mobile Communications Programme (ESMCP). (2022). Emergency Services Network. online. Retrieved from https://www.gov.uk/government/ publications/the-emergency-services-mobile-communications-programme/ emergency-services-network

European Telecommunications Standards Institute (ETSI). (2020). ETSI EN 300 392-5 V2.7.1 (2020-04). Retrieved from https://www.etsi.org/de-liver/etsi_en/300300_300399/30039205/02.07.01_60/en_30039205v020701p.pdf

FirstNet Authority. (2022). About the First Responder Network Authority. on-line. Retrieved from https://firstnet.gov/

Freire, D. V. C. (2019). Proposta de Metodologia de Avaliação Tecnológica para Comunicações Críticas (Mestrado em Ciência da Informação, Universidade Federal de Santa Catarina (UFSC)). Retrieved from https://repositorio.ufsc.br/handle/ 123456789/206430

Freire, D. V. C., & Cândido, A. C. (2020, Jul/Dez). O Aspecto Informacional no Levantamento de Cenários para Comunicações Críticas em Segurança Pública no Brasil. Revista Conhecimento em Ação, 5(2), 76 – 97. Retrieved from https://doi.org/10.47681/ rca.v5i2.34167

GSMA. (2018). Network 2020: Mission Critical Communications (Tech. Rep.). Retrieved from https://www.gsma.com/futurenetworks/wp-content/uploads/ 2017/02/767-Mission-critical-communications-low-res.pdf

Hill, K. (2019/March 28). Where is public safety LTE being explored around the world? on-line (RCR Wireless News). Retrieved from https://www.rcrwireless.com/20190328/network-infrastructure/where-is-public-safety-lte-being-explored-around-the-world

Lair, Y., & Mayer, G. (2017). Mission Critical Services in 3GPP. on-line. Retrieved from https://www.3gpp.org/news-events/3gpp-news/1875-mc_services

Lum, K., & Isaac, W. (2016, October). To predict and serve? Significance, 13(5), 14 – 19. Retrieved from https://doi.org/10.1111/j.1740-9713.2016.00960.x

Nokia. (2020). Sendai City deploys connected drones for disaster alert and rescue. on-line. Retrieved from https://www.youtube.com/watch?v=_VbET8XiN_I

Public Safety Communication Europe PSCE. (2020). H2020 BroadWay PCP Project. on-line. Retrieved from https://www.youtube.com/watch?v=IwbTs4Gq_yA

Telecommunications Industry Association (TIA). (2002). Compendium of Emergency Communications and Communications Network Security-related Work Activities within the Telecommunications Industry Association (TIA). on-line. Retrieved from https://web.archive.org/web/20111216004655/http://tiaonline.org/ standards/technology/ciphs/documents/EMTEL_sec.pdf

Telstra. (2022). Telstra LANES Emergency service. on-line. Retrieved from https://www.telstra.com.au/business-enterprise/industries/public-safety/lanes-emergency

TETRAPOL forum. (2022). TETRAPOL forum. online. Retrieved from https:// www.tetrapol.com/

Wang, S., & Li, M. (2021). Research on public safety emergency management of »Smart city«. In 2021 2nd international conference on computer science and management technology (iccsmt) (pp. 169 – 172). Shanghai, China: IEEE. Retrieved from doi: 10.1109/ICCSMT54525.2021.00041

Wu, Q., & Yu, X. (2020). Research on Public Safety Management under the Application of Big Data and Internet of Things. In 2020 international conference on big data economy and information management (bdeim) (pp. 9 – 12). Zhengzhou, China: IEEE. Retrieved from doi:10.1109/BDEIM52318.2020.00010

Yy, W., Xu, H., Nguyen, J., Blasch, E., Hematian, A., & Gao, W. (2018, Dec.). Survey of Public Safety Communications: User-Side and Network-Side Solutions and Future Directions. Special Section on Emerging Technologies for Device to Device Communications, 6(18), 70397 – 70425. Retrieved from https://ieeexplore.ieee.org/document/8523665

Sweden – Evaluation and Research Secretariat (ERS) of the Swedish Riksdag

What is it about?

Transportation is a critical infrastructure that distributes goods, facilitates trade, social interaction, and correlates to economic growth. At the same time, transportation has negative environmental consequences, in particular greenhouse gases. Domestic transport in Sweden emit a third of the nation's total CO2 emissions. Electrification of the transport sector has become a top priority for the Government to reach national climate targets and with the intention to become one of the world's first fossil-free welfare states.

What is the state of play?

In the last few years, the Government has put in place a large number of instruments to further the electrification of the transport sector. For example, an electric bus premium was introduced in 2016, electric vehicle premium in 2018, requirements for charging infrastructure adjacent to buildings in 2020, tax reduction for the installation of green technology and investment aid for the development of public fast charging stations in 2021.

The proportion of chargeable vehicles has increased faster than has been predicted. Electric cars constituted 43 percent of new car sales in 2021. The deployment of electric buses and light lorries is slower, and constituted 7 and 27 percent respectively of the newly registered vehicles.[87] Reliable data covering charging infrastructure is lacking but deployment seems to have kept pace with the increase in chargeable vehicles.[88] The first electric road allowing electric vehicles to access electricity for propulsion and battery charging while driving is to be completed by the end of 2025.[89]

Who are the key stakeholders?

A complex and cross sectoral system has many stakeholders. When it comes to the Government the Ministry of Infrastructure, the Ministry of the Environment, the Ministry of Finance, the Ministry of Defence and the Ministry of Enterprise and Innovation are involved in the electrification of the transport sector. Key government agencies include the Swedish Transport Administration, The Swedish Transport Agency, The Swedish Maritime Administration, The Swedish Energy Agency, the state-owned energy enterprise responsible for electrical grid infrastructure and transmission systems (*Svenska Kraftnät)*, The Swedish Environmental Protection Agency, The Swedish National Board of Housing, Building and Planning, and The National Land Survey.

[87] Trafikanalys (2022). Eldrivna vägfordon – ägande, regional analys och möjlig utveckling till 2030. Rapport 2022:12, s. 17-18.

[88] SOU 2021:48, I en värld som ställer om – Sverige utan fossila drivmedel 2040, p.402.

[89] https://www.regeringen.se/regeringens-politik/transportsektorn-elektrifieras/el-3/

Other stakeholders include standardisation bodies in both the energy and transport sectors, electric power markets, industry associations, fuel suppliers, owners and operators of transport infrastructure, vehicle buyers and owners, and consumers of transport services (passengers and logistics providers).[90] Actors linking the energy and transport sectors, such as capital market representatives who manage the flow of capital to infrastructure and capacity development projects also deserve a mention. An evolving integrated transport and energy sector also produces new types of stakeholders, such as prosumers.[91]

Why is this important?

According to the *Committee of Transport and Communications*, the transition to a sustainable transport system is one of the greatest challenges facing transport policy. Designing a sustainable transport system is of great importance for long-term sustainable development.[92] The electrification of the transport sector is important in order to reach climate targets, but also for economic development and the creation of new job opportunities.

Societal and political relevance and debate

Ongoing debate

According to the *Committee of Transport and Communications*, the transport sector has comparatively good prerequisites to reduce emissions through electrification, but also through increased transport efficiency, more efficient vehicles and vessels and a shift from fossil fuels to sustainable renewable fuels. In a long-term perspective, planning of housing and infrastructure also contribute to reduce emissions. Strong action is needed in all these areas to achieve the climate goals, according to the Committee, not least in electrification and sustainable renewable fuels.[93]

Electrification of the transport sector has become a prominent climate mitigation measure. Other measures, such as policies to promote a transport-efficient society have been weak in comparison, according to *The Swedish Climate Policy Council* (an independent scientific council with the task to assess if the overall policy of the Government is compatible with the climate goals).[94] The *Swedish 2030-secretariat* – an industry advocacy group – proposes a broader range of solutions to achieve a significant reduction in greenhouse gas emissions. Such different solutions will increase the need for analysis from a systemic perspective and an increased need for collaboration with societal stakeholders. Further, they note that despite the existence of many concrete instruments and initiatives that drive development forward, Sweden lacks a comprehensive transport policy action plan, and that there is an urgent need to identify and quantify the results of decisions taken, and to identify complementary measures to achieve the goals based on a systemic approach. They claim there are

[90] Daniels, David et al. (2022). Samspelet mellan energisystemet och transportsystemet. VTI rapport 1128.

[91] Palm, Jenny et al. (2018), Sufficiency, change, and flexibility: Critically examining the energy consumption profiles of solar PV prosumers in Sweden, Energy Research & Social Science, Vol. 39.

[92] Bet. 2020/21:TU16, Framtidens infrastruktur.

[93] Bet. 2020/21:TU16, Framtidens infrastruktur, p. 44.

[94] Klimatpolitiska rådet (2021). Klimatpolitiska rådets årsrapport. Stockholm: Klimatpolitiska rådet.

gaps in knowledge about how the transformation of the transport sector links to the transformation of the energy system as a whole, and how large the potential for measures to achieve a more transport-efficient society really is. Finally, they claim that the availability of energy and raw material resources are overestimated.[95]

Researchers have also pointed to the negative effects on the environment and geopolitical risks involved in an increased use of batteries.[96] Other researchers claim that the process of electrification is too slow.[97] The energy advocacy organisation *Energiföretagen*, calls for a prompt updating of laws and regulations based on a systemic approach to the energy system«[98]

The phasing out of fossil fuels and increased electrification brings major efficiency and climate gains, but also new challenges, according to *The Confederation of Swedish Enterprise*. They argue that the use of fossil fuels has provided an opportunity to store energy cost-effectively over longer periods of time and has led to a diversification of useful energy sources in the transport sector and industry. This in turn has contributed to a more robust energy supply. But now that electrification is coming on strong, it may mean increased vulnerability, as it entails that alternative energy sources become fewer. They claim that the number of interruptions due to likely increases in power cuts and power shortages risks leading to high costs for society. As electrification of transportation progresses, they claim that these costs will increase.[99]

Legislation in place

The European Commission has adopted a series of legislative proposals setting out how it intends to achieve climate neutrality in the EU by 2050, including the intermediate target of an at least 55 percent net reduction in greenhouse gas emissions by 2030. The Swedish Parliament has decided on a stricter target to reduce greenhouse gas emissions from domestic transport (not including domestic aviation), by at least 70 per cent by 2030 compared to 2010, and to meet the target of zero emissions by 2045.[100]

Current political or legislative proposals

In February 2022, the Government decided on *a national strategy* for electrification with the purpose of climate change mitigation.[101] In June 2022 an advisory council with top CEOs and Director Generals was introduced support the implementation of the strategy.

The Government has furthermore set up an *electrification commission* to accelerate electrification of the transport sector. The Commission's work covers all forms of electrification for passenger and

[95] https://www.2030sekretariatet.se/2030-pusslet/

[96] Hesselgren Mia et al. (2022). Elektrifiering av transporter är inte problemfritt. Dagens Nyheter, August 26, 2020.

[97] See for example Nilsson, Mats: Elektrifieringsstrategin ännu ett dokument i raden, March 18, 2022.

[98] Energiföretagen, March 30, 2021: Elektrifieringen kräver snabba lagändringar.

[99] Svenskt näringsliv (2022). Risk- och sårbarhetsanalys av utökad elektrifiering av svenska samhället.

[100] Prop. 2016/17:146, Ett klimatpolitiskt ramverk för Sverige, bet. 2016/17:MJU24, Ett klimatpolitiskt ramverk för Sverige, rskr. 2016/17:320.

[101] Regeringskansliet (2022). Nationell strategi för elektrifiering – en trygg, konkurrenskraftig och hållbar elförsörjning för en historisk klimatomställning.

freight transport in all modes of transport. In order to achieve the climate and transport policy objectives, road transport should be mainly electrified in the longer term.[102] The mandate states that the Commission's work should consider the objectives decided by Parliament within the policy sectors of transport, industry, energy and climate. The Commission shall also consider the impact of electrification on overall defence, on the emergency preparedness of society and on the robustness and vulnerability of the infrastructure and transport system.[103]

A Government commission of inquiry tasked with proposing a regulatory framework for the construction, operation and maintenance of electric roads published its report in August 2021. The inquiry came up with a number of proposals on, for example, the establishment of fees for using electric roads, conditions for access and technical requirements for electric vehicles.[104] The proposals have been circulated for comment to stakeholders and the comments are presently being processed by the Government.

Science/evidence-based inputs guiding political decision-making

The Government has requested a large number of investigations with the purpose of gaining knowledge about transport electrification. *The Swedish National Road and Transport Research Institute (VTI)*, for example, is an independent research institute that has recently published studies by order of the Government. The topics of these studies include 1) the digitalisation and innovation to accelerate electrification[105], 2) the interaction between energy and transport systems[106], 3) costs, finance and business models[107], 4) the state of knowledge of the key stakeholders in the transport sector[108] 5) economic efficiency of measures to accelerate electrification.[109]

The Government has also commissioned work to The Swedish Environmental Protection Agency to investigate environmental consequences of electrification. The government agency Transport Analysis also provides decision-makers in the field of transport policy with policy advice through reviews, follows up and evaluations of proposed and implemented measures. Two large commissions of inquiry that involve the role of electrification of the transport sector have been set up by the Government recently, and published in June 2021 and May 2022 respectively.[110]

[102] Prop. 2020/21:151, Framtidens infrastruktur hållbara investeringar i hela Sverige, p. 33.

[103] Infrastrukturdepartementet I2020/02592, Elektrifieringskommissionens uppdrag.

[104] SOU 2021:73, Regler för statliga elvägar.

[105] Nordin, Lina and Andersson, Jeanette (2022). Digitaliseringens möjligheter att effektivisera och påskynda elektrifieringen av transporter – inklusive rättsliga förutsättningar. VTI rapport 1109.

[106] Daniels, David et al. (2022). Samspelet mellan energisystemet och transportsystemet. VTI rapport 1128.

[107] Björk, Lisa et al. (2022). Kostnader, finansiering och affärsmodeller. VTI rapport 1110.

[108] Stelling, Petra and Brunner, Sabrina (2022). Regeringsuppdrag om elektrifieringen av transporter: kunskapsläget hos transportsektorns nyckelaktörer. VTI rapport 1131.

[109] Pydokke, Roger (2022). Samhällsekonomiskt effektiva åtgärder och styrmedel för att påskynda elektrifieringen av vägtransporter. VTI rapport 1129.

[110] SOU 2021:48, I en värld som ställer om – Sverige utan fossila drivmedel 2040, and SOU 2022:21, Rätt för klimatet.

Role of TA in the debates

ERS contributions to the topic

ERS is currently conducting a pre-study on the topic of the electrification of the whole transport sector (i.e. all means of transportation) which involves mapping out the large number of initiatives, investigations and commissions that have been initiated. It also involves mapping out known barriers for an increased electrification. Departing from the pre-study, parliamentarians will decide on focus for a main study in October/November.

EPTA Member Contributions

Autonomous systems – humans in the crosshairs of the machine

European Parliament – Panel for the Future of Science and Technology (STOA)

What is it about?

As artificial intelligence (AI) systems become more autonomous, a doctrinal paradigm shift may be needed. Given the foreseeable pervasiveness of AI, questions arise about how this new technology should be defined and classified in legal and ethical terms.[111] An analysis of the key legal initiatives in this field in Europe is required for reaching the understanding needed to engage in clear-headed reflection about AI's legal and socio-ethical challenges, as well as a meaningful debate about how the current EU acquis may need to be adjusted to the new technological realities. As AI systems are used in more common and consequential contexts and will soon be applied in safety critical applications, such as clinical decision support and autonomous systems, there is increasing attention on whether, how and to what extent they should be regulated.

Artificial intelligence is empowering what has arguably become one of the most important trends in the automotive industry: autonomous vehicles.[112] Manufacturers are already equipping their entry-level vehicles with emergency braking, collision warning and blind spot monitoring, and offering other advanced driver assistance systems (ADAS) as options, such as autopilot, auto lane change, autopark and summon. Even when these ADAS still require a human in the loop, they are clearly pushing towards level 5 vehicle automation.[113]

The report on *Artificial intelligence in a digital age*[114] released by the European Parliament's Special Committee on Artificial Intelligence in a Digital Age (AIDA) analyses the future impact of AI in the digital age, balancing its benefits towards certain risks on the EU economy, in particular on health, infrastructure, sustainability, transport, agriculture, energy, defence, industry, democracy, e-government, employment, skills and education. It pays special attention to the production and use of lethal autonomous weapons systems to stress that AI-enabled systems can under no circumstances be allowed to replace human decision-making involving the legal principles of distinction, proportionality and precaution. Looking towards 2040, the global innovation and technology landscape is expected to evolve significantly, driving change in the nature of warfare as well as in the capabilities, concepts and doctrines employed by actors on the battlefield. As such, there is a need to understand this technological change and explore its potential influence and impact on the future battlefield, in order to formulate policies and investment decisions that are as future-proof as possible.

Key stakeholders at EU level

- European Parliament's Legal Affairs Committee (JURI); Industry, Research and Energy (ITRE); Civil Liberties and Justice and Home Affairs Committee (LIBE); Internal Market and Consumer

[111] https://www.europarl.europa.eu/stoa/en/document/EPRS_BRI(2019)634427

[112] https://www.europarl.europa.eu/stoa/en/document/EPRS_ATA(2020)656317

[113] https://www.sae.org/standards/content/j3016_201806/

[114] https://www.europarl.europa.eu/cmsdata/246872/A9-0088_2022_EN.pdf

Protection Committee (IMCO); Special temporary Committee on Artificial Intelligence in a Digital Age committee (AIDA); Foreign Affairs Committee (AFET); Subcommittee on Security and Defence (SEDE).
- European Commission; European External Action Service (EEAS)

Societal and political relevance and debate

Existing AI- and robotic-based autonomous systems already present big challenges for safety, unpredictability, regulatory frameworks and the distribution of power.[115] But in the close future they may be integrated and merged with other emerging technologies. Vehicles may be equipped with in-car facial recognition, voice recognition or bio-tracking technologies to allow for a smoother human-machine interaction or even compliance with safe driving standards (e.g. to alert/nudge/stop the driver when their psycho-physical conditions are not good enough for driving.[116] Cars may even be equipped with brain-machine interfaces to allow more direct control from drivers and/or the possibility of people with disabilities to drive. This is not such a far-fetched scenario considering that people with paralysis can already have some control on wheelchairs[117], and one of the biggest players in self-driving technology, Tesla's Elon Musk, has already been investing in brain-machine interaction.[118] This will create a convergence of the above-mentioned ethical issues with self-driving cars with those traditionally associated with self-tracking[119] and brain-machine interface technologies: an impact on people's intimate life[120] and risks for serious violations of personal autonomy and human rights.[121]

In the last decade, the global and European security environment saw a number of strategic, political, economic and technological trends consolidating and leading to greater instability and conflict.[122] In particular, following almost two decades of relative stability in its neighbourhood, the EU was confronted with significant security challenges. Countries in its eastern neighbourhood faced a

[115] https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2022)729543

[116] Hawkins, Andrew J. 2019. »Volvo Will Use In-Car Cameras to Combat Drunk and Distracted Driving.« The Verge. March 20, 2019. https://www.theverge.com/2019/3/20/18274235/volvo-driver-monitoring-camera-drunk-distracted-driving.

[117] Galán, F., M. Nuttin, E. Lew, P. W. Ferrez, G. Vanacker, J. Philips, and J. Del R. Millán. 2008. »A Brain-Actuated Wheelchair: Asynchronous and Non-Invasive Brain-Computer Interfaces for Continuous Control of Robots.« Clinical Neurophysiology: Official Journal of the International Federation of Clinical Neurophysiology 119 (9): 2159–69. https://doi.org/10.1016/j.clinph.2008.06.001.

[118] Neate, Rupert. 2022. »Elon Musk's Brain Chip Firm Neuralink Lines up Clinical Trials in Humans.« The Guardian, January 20, 2022, sec. Technology. https://www.theguardian.com/technology/2022/jan/20/elon-musk-brain-chip-firm-neuralink-lines-up-clinical-trials-in-humans.

[119] Lanzing, Marjolein. 2016. »The Transparent Self.« Ethics and Information Technology 18 (1): 9–16. https://doi.org/10.1007/s10676-016-9396-y

[120] Mecacci, Giulio, and Pim Haselager. 2019. »Identifying Criteria for the Evaluation of the Implications of Brain Reading for Mental Privacy.« Science and Engineering Ethics 25 (2): 443–61. https://doi.org/10.1007/s11948-017-0003-3

[121] Ienca, Marcello, and Roberto Andorno. 2017. »Towards New Human Rights in the Age of Neuroscience and Neurotechnology.« Life Sciences, Society and Policy 13 (1): 5. https://doi.org/10.1186/s40504-017-0050-1

[122] See European Commission (2017a).

range of security threats and vulnerabilities in the military, economic, political and energy spheres. Further, the failure of a number of states across the south-eastern Mediterranean region, the Sahel and sub-Saharan Africa generated a series of conflicts, crises and ungoverned spaces in which instability could breed and have further impacts on the European stage.[123] Today, the Russian war of aggression against Ukraine dominates the EU security agenda.

EU legislation in place and political or legislative proposals

The EU is already doing quite a lot to stimulate (responsible) innovation in the digital domain. A range of existing policies, frameworks, regulations and principles are relevant to the technologies and challenges related to autonomous systems. These include, but are not limited to: Declaration on European Digital Rights and Principles (proposed January 2022), Path to the Digital Decade (proposed September 2021), AI Act (proposed April 2021), 2030 Digital Compass: the European way for the Digital Decade (proposed March 2021), Lisbon Declaration – Digital Democracy with a Purpose (adopted 2021), Tallinn Declaration on eGovernment (2017), Rome Declaration on Responsible Research and Innovation in Europe (2014).

In a Resolution[124] on *Autonomous weapon systems*, the European Parliament (EP) called for the adoption of an EU common position on lethal autonomous weapon systems that ensures meaningful human control over the critical functions of weapon systems. The EP considered that human involvement and oversight are central to the lethal decision-making process, and stressed the fundamental importance of preventing the production of any lethal autonomous weapon system lacking human control in critical functions such as target selection and engagement. It also noted that such systems could malfunction on account of badly written code or a cyber-attack perpetrated by an enemy state or a non-state actor. It underlined the fact that none of the weapons or weapon systems currently operated by EU forces are lethal autonomous weapon systems. Members called for the expansion of the EU's role in global disarmament and non-proliferation efforts, and stressed the need for the EU to speak in relevant forums with one voice and share best practices on the matter of lethal autonomous weapon systems, to garner input from experts, academics and civil society.

The EP resolution[125] on Artificial intelligence: Questions of interpretation and application of international law in so far as the Union is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice calls for an EU legal framework on AI with definitions and ethical principles, including its military use. It also calls on the EU and its member states to ensure AI and related technologies are human-centred (i.e. intended for the service of humanity and the common good). MEPs stress that human dignity and human rights must be respected in all EU defence-related activities. AI-enabled systems must allow humans to exert meaningful control, so they can assume responsibility and accountability for their use. The use of lethal autonomous weapon systems (LAWS) raises fundamental ethical and legal questions on human control. MEPs reiterate their call for an EU strategy to prohibit them as well as a ban on so-called »killer robots«.

[123] See European Commission (2017a).

[124] https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.html

[125] https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1647869&l=en&t=E

The decision to select a target and take lethal action using an autonomous weapon system must always be made by a human exercising meaningful control and judgement, in line with the principles of proportionality and necessity.

Increased recognition of the strategic, political, economic and technological trends has led, in recent years, to a sustained call for a stronger EU in the areas of security and defence at the highest political levels. Commitments to a greater role for the EU in the areas of common security and defence translated into a number of concrete policies that have a direct impact on European defence.

An EU Global Strategy puts the EU on a path towards strategic autonomy and the development of full spectrum defence capabilities. Following a strategic review of changes in the global environment conducted by the European Commission Vice-President High Representative (HR/VP) in consultations with EU Member states, the EU launched its »Global Strategy for European Foreign and Security Policy« (EU GSS) in 2016. The EU GSS recognises that ongoing crises and conflicts in the EU's neighbourhood pose a threat to the Union. As such, the EU GSS sets out an ambitious vision of policies, instruments, and capabilities towards achieving strategic autonomy.[126]

The current draft AI Act[127] shall not apply to AI systems developed or used exclusively for military purposes because their use falls under the exclusive remit of the Common Foreign and Security Policy.

Science/evidence-based inputs guiding political decision-making

The EU policy and regulatory context on emerging technologies in security and defence is shaped by a comprehensive agenda on innovation and harnessing the benefits of digital and advanced technologies, while proactively guarding against possible risks. The European Commission spearheaded this agenda through the 2011 adoption the »Innovation Union« a flagship initiative of the Europe 2020 strategy.[128] The EU's agenda on innovation and emerging technologies has seen advancement via the April 2019 »digital package«.[129] This package detailed the Commission's recommendations for the EU approach towards harnessing the benefits of advanced technologies.

The European Parliament, in its Resolution[130] on *Artificial intelligence in a digital age* stresses that the EU's AI strategy must not overlook the military and security considerations and concerns that arise from the global deployment of AI technologies. Members emphasised the challenge of reaching a consensus within the global community on minimum standards for the responsible use of AI and expressed concern about military research and development on autonomous lethal weapons systems. The Parliament concludes that the Member States should continue to train their

[126] See EEAS (2016).

[127] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en

[128] See European Commission (2011).

[129] See European Commission (2020a).

[130] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_EN.html

Overview of key recent EU policy and regulation on advanced technologies in security and defence[131]

Date	Author	Title
February 2013	European Commission	Cybersecurity Strategy for the European Union: An Open, Safe and Secure Cyberspace
July 2013	European Commission	Communication: Towards a more competitive and efficient defence and security sector
August 2013	European Parliament and the Council	Directive on Attacks against Information Systems
June 2014	European Commission	Report: A New Deal for European Defence
April 2016	European Commission	Joint Framework on Countering Hybrid Threats
June 2016	HRVP	A Global Strategy for the European Union's Foreign and Security Policy
July 2016	European Parliament and the Council	EU Network and Information Security (NIS) Directive
November 2016	European Commission	European Defence Action Plan
November 2016	HRVP	EU Implementation Plan on Security and Defence
June 2017	European Commission	Communication Launching the European Defence Fund
April 2018	European Commission	EU AI Strategy (AI for Europe)
June 2018	European Commission	Joint Communication – Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats
December 2018	European Commission	Coordinated Plan on AI
December 2018	European Commission	Action Plan against Disinformation
April 2019	AI HLEG	Ethics Guidelines for Trustworthy AI
April 2019	European Commission	EU Cybersecurity Act
May 2019	Finland, Estonia, France, Germany, the Netherlands	Digitalization and AI in Defence – Food for Thought Paper
June 2019	European Parliament and the Council	The Open Data Directive
June 2019	AI HLEG	Policy and Investment Recommendations for Trustworthy AI
February 2020	European Commission	White Paper on AI – A European approach to excellence and trust
February 2020	European Commission	European Data Strategy

military staff to ensure that they have the necessary digital skills to use AI in control, operational and communication systems; welcomes the European Defence Fund's approach to lethal autonomous weapons systems and its Article 10(6); highlights the importance of the European Defence

[131] https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)690038

Fund in supporting cross-border cooperation between EU countries in military AI research, developing state-of-the-art defence technologies and constructing the necessary infrastructure, namely data centres with strong cyber capabilities.

Role of TA in the debates

The new socio-political situation is pushing the EU institutions and Member States to pursue a broad range of capability development initiatives in a coherent and coordinated manner, ensure the development of an agile regulatory and organisational environment, and guide investments in the technologies most relevant to the European context. That requires an assessment of the risks, challenges and opportunities relating to the new and emerging technologies. Specially, and in the actual socio-political context, those that are most expected to shape the future battlefield up to 2040; as well as the implications stemming from consideration of individual technologies, and a cross-cutting analysis of their interactions with broader political, social, economic and environmental trends. In this context, a European Parliament's STOA on *Innovative technologies shaping the 2040 battlefield*[132] identifies three broad policy options for EU and Member States:

- Pursuing a broad range of capability development initiatives;
- Ensuring the development of an environment characterised by the necessary regulatory and organisational agility and absorption capacity;
- Facilitate EU investments and research, development, technology and innovation (RDT&I) activities in relevant new and emerging technologies by strengthening collaboration with industry.

In relation to the future battlefield dynamics, AI, machine learning and Big Data have near groundbreaking impact on the speed and complexity of decision-making on the battlefield. This reflects the contributions of technologies in this cluster to rapidly process large quantities of data, creating efficiency opportunities for the armed forces as well as challenges in relation to reduced decision-making and reaction timeframes.

Ethics and human rights protections represent a crucial factor in the context of future development and uptake of autonomous systems. Existing research documents various ethical considerations relating to autonomous weapons systems raised by International Humanitarian Law (IHL) and the Law of Armed Conflict (LOAC). These considerations include potential challenges pertaining to:

- The principles of distinction (i.e. distinguishing between combatants and civilians in the battlefield);
- Proportionality (i.e. balance of the loss of life and damage in relation to the expected military advantage)
- Military necessity (i.e. inflicting damage on an enemy only in pursuit of military objectives);
- Unnecessary suffering (i.e. prohibiting systems or weapons causing excessive injury or unnecessary suffering).

[132] Study written by Jacopo Bellasio, Linda Slapakova, Luke Huxtable, James Black, Theodora Ogden and Livia Dawaele of RAND Europe, at the request of the Panel for the Future of Science and Technology (STOA) 02-08-2022 https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)690038

Has TA made an impact on the ongoing debates?

Autonomous machines underpinned by AI are expected to become a general-purpose technology, embedded in many aspects of our daily lives. These machines will possess the capability to respond to changes in the local environment without human intervention, thereby creating numerous new network interactions.[133] In order to prepare future-proof policies on today's complex policy matters, the European Parliament needs to rely on technology assessment (TA) to gain the required insights and understanding of topics such as this, where technology plays a fundamental role. Since 2015, the Panel for the Future of Science and Technology (STOA) has adopted foresight practices for studies of science and technology-related policy issues that are complicated and/or have a controversial nature. This applies particularly to areas where clear-cut policy options are difficult to formulate or the controversial nature of the issue can hinder the acceptance of policies. This »scientific foresight« approach broadens the traditional TA practices by adding an emphasis on possible societal impacts of the policy options considered at the European Parliament.[134]

In the particular case of AI and autonomous machines, a number of STOA's briefing sessions and studies have informed and shaped the debates in the EP AIDA Special Committee from the very start, and have fed into the parliamentary hearings on AI, and into the AIDA report on on Artificial intelligence in a digital age, especially regarding the security & defence aspects of autonomous systems.[135]

Lessons learned from TA

AI systems have raised serious concerns about bias and discrimination, for example with regard to race or gender. For AI-driven autonomous devices, more specifically, two important concerns are:

- Meaningful human control and liability: Robotic systems that can – to a larger or smaller degree – take autonomous decisions and have the ability to physically harm people, have raised discussions about (a) how ethical factors can and should be taken into account into those decisions and about (b) safeguarding the ability of humans to maintain meaningful human control and take responsibility for the actions of the system. The most prominent examples of such systems are autonomous vehicles and weapon systems.[136,137]
- Employment and the future of work: New possibilities to intelligently automate more and more tasks and types of work have raised a lot of discussion. One main concern is the possibility of mass unemployment, an issue of justice and fair distribution. Another topic of discussion is the changing nature of work and its implications for our capabilities to realize a good, meaningful life.

[133] https://www.impgroup.org/uploads/papers/11115.pdf

[134] https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)690031

[135] https://www.europarl.europa.eu/cmsdata/246872/A9-0088_2022_EN.pdf

[136] Gordon, John-Stewart, and Sven Nyholm. 2021. »Ethics of Artificial Intelligence.« In Internet Encyclopedia of Philosophy. https://iep.utm.edu/ethic-ai/

[137] Müller, Vincent C. 2021. »Ethics of Artificial Intelligence and Robotics.« In Stanford Encyclopedia of Philosophy, summer 2021. https://plato.stanford.edu/archives/sum2021/entries/ethics-ai/

Advances in robotics and autonomous systems may present various EU-specific opportunities in the field of defence. The development of a common platform for autonomous systems, mirroring similar concepts developed by international partners (e.g. Australia), could present a significant opportunity for EU MS capabilities increasing interoperability and facilitating plug-and-play use of systems from different MS in the context of joint missions and operations under CSDP.[138] Further to advances in efforts to exploit opportunities provided by autonomous systems in the military context, there may also be significant opportunity for the EU to provide greater leadership in international multilateral efforts to strengthen safeguards against the proliferation and use of autonomous systems without meaningful human control, discussed further below.[139] Autonomous systems in defence applications raise a serious ethical challenge for decision making on the use of force, as the consequences of the use of autonomous systems are generally less predictable, with the links between intention and consequences appearing more diluted or removed.[140]

These factors underpin emerging international consensus on the necessity to establish and ensure meaningful human control.[141] Relevant technological specifications for autonomous systems with meaningful human control include predictability of behaviour of an autonomous system by an operator, maintaining operator ability to intervene and alter the behaviour of a system, and the speed at which commands provided by an operator are processed and actions.[142] The ability of operators to understand how autonomous systems interpret data and formulate corresponding actions is also key; though this is a potentially significant challenge particularly for highly complex systems.[143]

[138] RAND Europe workshop (October 2020)

[139] RAND Europe interview (INT06, October 2020).

[140] See Boulanin et al. (2020).

[141] RAND Europe interview (INT06, 27 October 2020).

[142] See Ekelhof and Persi Paoli (2020).

[143] See Torossian (2020).

Germany – Office of Technology Assessment at the German Bundestag (TAB)

What is it about?

Enormous technological progress in the field of artificial intelligence (AI) is enabling a plethora of new applications that are about to penetrate and fundamentally transform all areas of the economy and life. This development does not stop at the military sector: research and development projects worldwide aim at increasing the degree of autonomy of military systems as well as the military use of AI.

Some features render autonomous weapon systems attractive for military decision makers: they can perform »dull, dirty and dangerous« missions allowing own soldiers to be kept out of harms way, they can process and analyse very fast huge amounts of data from diverse sources and they have a big advantage in terms of reaction speed compared to humans. To »fight at machine speed« in order to be ahead of the opponents' actions is one main vision for wars of the future fought by autonomous systems.

Why this is important?

In the past decades German defence policy has been characterized by a certain restraint in terms of weapons, armaments and the use of military force, mainly for reasons of historical responsibility for the atrocities committed by Nazi-Germany during World War II. However because of Russias war of aggression against Ukraine Chancellor Scholz in his landmark speech on February 27, 2022 has announced a »turning point« (Zeitenwende) in this respect. As a consequence, it was decided that a »special fund« in the amount of 100 billion Euro will be provided, in order to modernise the armed forces and to close existing capability gaps immediately (Deutscher Bundestag 2022a). A considerable part of this fund will be invested in the armament of Heron TP drones, and in the development of the European Future Combat Air System (FCAS, see below).[144] Some voices fear that these decisions could exacerbate existing conflicts and fuel a spiraling arms race of AWS.

What is the state of play?

There are examples of weapon systems that qualify as »autonomous« in the sense that they can select and attack targets without or with only minimal human involvement, and which are already being used by the German armed forces and, indeed, by many technologically advanced states around the globe. There are for instance short-range air defence systems that can operate in a purely automatic mode to intercept incoming projectiles (e.g. rockets, artillery and mortar shells). Even if this can be classified as an autonomous weapon system, there is still quite a long way to go until autonomous systems can move freely in a cluttered, dynamic and hostile environment and carry out complex missions on their own.

[144] https://www.bmvg.de/de/aktuelles/ministerin-wir-sorgen-fuer-voll-einsatzbereite-bundeswehr-5438596

A major step in this direction is expected from two main European defense development projects currently under way. In FCAS (Future Combat Air System) a new combat aircraft is envisaged to work together with unmanned components, so-called remote carriers (manned-unmanned teaming), an Air Combat Cloud ensures real-time information for all involved subsystems. It is planned that FCAS successively replaces existing platforms from 2040 onward.[145] Similarly for the ground domain, there is the MGCS (Main Ground Combat System) which may include a main battle tank interlinked with unmanned, including autonomous ground and aerial vehicles.[146] Both FCAS and MGCS follow a »system of systems« approach, where different functions are implemented in subsystems that can be distributed globally (including in space orbits) and which are networked together.

Who are the key stakeholders?

The discourse in Germany on AWS in expert circles and public forums is actively being driven forward by think tanks (like the German Institute for International and Security Affairs, SWP[147], the International Panel on the Regulation of Autonomous Weapons, iPRAW[148], or the Institute for Peace Research and Security Policy, ISFH)[149]), research institutions (e.g. the Fraunhofer Segment for Defense and Security, VVS[150]), and NGOs (e.g. the International Committee for Robot Arms Control, ICRAC[151]). The International Committee of the Red Cross (ICRC) plays a special role, since it is the only NGO which has an official status in the context of the United Nations and (international) humanitarian law. Defence industry regularly pursues a two-pronged communication strategy: On the one hand it promotes the autonomous capabilities of its latest products, e.g. at trade fairs and exhibitions. On the other hand, when ethical and legal questions are asked, it emphasises that its weapon systems always feature enough human control so that they comply with all international rules and regulations.

The Bundeswehr keeps a low profile in the public debates on the issue of AWS. Unlike other countries like the UK that have a current »Defence Artificial Intelligence Strategy« (Ministry of Defence 2022), the only publicly available official document that deals at length with AI in the Bundeswehr is from 2019 and focusses only on land forces (Army Concepts and Capabilities Development Centre 2019). One of the reasons for this may be, that there is currently no consolidated government position on AWS presumably because of differing views by the Ministry of Defence and the Foreign Office (Hoffberger-Pippan, Vohs, Köhler 2022).

[145] See here: https://www.vvs.fraunhofer.de/en/topics/FCAS.html

[146] https://en.wikipedia.org/wiki/Main_Ground_Combat_System

[147] https://www.swp-berlin.org/en/

[148] https://www.ipraw.org/

[149] https://ifsh.de/en

[150] https://www.vvs.fraunhofer.de/en.html

[151] https://www.icrac.net/

As far as online and traditional media are concerned, AWS are a difficult topic: One very rarely sees differentiated media coverage of the topic because the »killer robot« and »Terminator« narratives are so strong and difficult to overcome.

Societal and political relevance and debate

Ongoing debate

There has been a lot of controversy in Parliament and in public fora about the question whether Germany should procure armed UCAVs (Unmanned Combat Aerial Vehicles). The debate picked up momentum in 2013, when the Government announced the intention to purchase such weapon systems.

Main argument of the »pro« side was that Germany owes its troops on the ground (e.g. in international peacebuilding missions like the one in Afghanistan the Bundeswehr participated 2001-2021) a maximum of protection and UCAVs would provide this capability (Deutscher Bundestag 2019).

The »con« arguments were based very much on the notion that armed drones, even if they are remote-controlled, are a first step towards autonomous weapons which raise fundamental international law, human rights and ethical questions (Deutscher Bundestag 2013b).

In 2018 the Bundestag decided to procure optionally armable Heron TP drones by way of leasing them from the israeli manufacturer. (https://www.bmvg.de/de/themen/entscheidung-heron-tp-wird-beschafft-25610). Only this year it was finally decided that the option to arm the Heron TP will actually be used. The financial means for this are provided by the »special fund« (see above) (Deutscher Bundestag 2022b).

Legislation in place

Since 2013 when the then coalition parties declared that »Germany will advocate the inclusion of UCAVs in international disarmament and arms control regimes and work for a ban under international law on fully automated weapons systems that deprive humans of the decision to use weapons« (CDU, CSU, SPD 2013, S. 124, English translation by TAB) all following governments issued similar statements. However, the exact meaning of these statements remain somewhat unclear, because some of the terms used are ill-defined, first and foremost the term »autonomy« (or »fully automated« for that matter). The German AI strategy issued in 2018 and updated in 2020 is not helpful in this respect either, because the topic AWS is only lightly touched upon (Bundesregierung 2018, S.32, 2020 S. 24).

Current political or legislative proposals

Germany continues to play a very active role in the talks on regulating AWS, which have been held since 2014 under the roof of the UN Convention on Certain Conventional Weapons (CCW). An initiative launched jointly with France in 2021 to precisely define and differentiate between fully and partially autonomous systems seemed promising to advance the negotiation process. But the current situation is not very favourable for an international agreement on any kind of arms control issue.

This is a serious problem in the context of the CCW, since decisions can only be taken by consensus. The currently most likely outcome of the ongoing talks is therefore a complete failure. This means that other forums than the CCW must be sought for actors willing to strive for some kind of regulation of AWS (Hoffberger-Pippan, Vohs, Köhler 2022).

Role of TA in the debates

The development and possible use of AWS raises so many questions which the international community has only begun to address: Is it ethically justifiable and politically responsible to develop weapon systems that can possibly apply lethal force without sufficient human control? Is their deployment compatible with the principles of international humanitarian law? Does their proliferation trigger new arms races? And what are the consequences for international security as well as regional and strategic stability?

Even developers of high-tech weapon systems using AI have begun to recognize the need to take notice of these questions and to seek answers, if only to promote public acceptance. A prominent example is the establishment of an Ethics Panel to critically monitor the FCAS development in an attempt to a »responsible use of new technologies« (like AI).[152]

TA and related activities, like systems analysis, responsible research and innovation (RRI), foresight, policy analysis, security studies and many more, are key to provide the factual and analytical basis to approach these questions.

TABs' contribution to this topic

Preventive arms control of new technologies is an area of research that TAB has taken up regularly (TAB 1996, 2003, 2010). In 2020 a comprehensive report on AWS has been published, that covered a wide range of aspects: By means of an inventory of already existing and developing systems, it is illustrated which functions modern weapons systems are able to perform autonomously today and in the foreseeable future. Based on these military capabilities, possible deployment scenarios for AWS are discussed followed by an analysis of the resulting security policy implications. In this context, the focus is on questions of whether the possible use of AWS would lead to more or less warlike violence, what effects on regional stability and strategic balance could be expected and whether new arms races might be triggered. Whether, and if so to what extent, the use of lethal force by autonomously operating machines is morally acceptable is the core question of the ethical debate on AWS. This debate is described in detail in the report. Closely related to ethical questions is the issue of whether and under what circumstances AWS could be used in compliance with the norms of international humanitarian law.

The findings were presented in the Bundestag at a sitting of the standing Subcommittee on Disarmament, Arms Control and Non-Proliferation and also on occasion of a workshop with MPs and experts on Nov. 6, 2020.[153]

[152] http://www.fcas-forum.eu/en/articles/responsible-use-of-artificial-intelligence-in-fcas

[153] https://www.youtube.com/watch?v=ADDtY0_RhcI

Has TA made an impact on the ongoing debates?

A direct impact of TAB-Reports on debates and decisions of the Bundestag is notoriously difficult to pinpoint, but it seems that the TAB-Reports on AWS did have a noticeable influence on the debates. One indication for this was a motion towards a ban of AWS issued by DIE LINKE in which the TAB-Report is quoted in great detail, which is very unusual (Deutscher Bundestag 2021). There also is a continued interest and broad coverage of the report in traditional and online media.[154,155,156,157]

Lessons learned from TA

The increasing use of automated or future autonomous weapon systems could represent a paradigm shift that would revolutionize warfare in the 21st century. AWS raise numerous questions, both in terms of their compliance with the principles of international humanitarian law and the impact that their proliferation and deployment could have, especially in relation to potential armaments dynamics, international security, regional and -technical stability.

There is currently a window of opportunity to use an internationally coordinated, targeted approach to contain the potential threats that AWS could pose. This window is gradually closing with progressive technological development and the continuous integration of autonomous functions in weapon systems of all kinds. However, the international security policy environment is currently not conducive to a trusting international dialogue and serious disarmament efforts. This underscores the urgency to take action to stimulate international dialogue, increase transparency and confidence and limit identified risks of AWS. Political and diplomatic initiatives in this regard require persevering efforts and a broad discourse involving science and civil society.

References

Army Concepts and Capabilities Development Centre (2019): »Artificial Intelligence (AI) in Land Forces« Position Paper https://www.bundeswehr.de/resource/blob/156026/79046a24322feb96b2d8cce168315249/download-positionspapier-englische-version-data.pdf

Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (2020): Autonome Waffensysteme https://publikationen.bibliothek.kit.edu/1000127160/94886769

Bundesregierung (2018): Strategie Künstliche Intelligenz der Bundesregierung

https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie.pdf&cid=728

[154] https://www.spiegel.de/wissenschaft/technik/wettlauf-der-kampfroboter-a-3e1db4c9-8b1d-425c-b5f7-3996e44a7f83

[155] https://www.killer-roboter-stoppen.de/2020/11/oeffentliches-fachgespraech-im-deutschen-bundestag-menschliche-kontrolle-ueber-gewaltanwendung-muss-erhalten-bleiben/

[156] https://web.de/magazine/panorama/angst-flash-schaffen-autonome-waffen-kriegsgefahr-35374420

[157] https://taz.de/Drohnen-mit-todbringender-Fracht/!5786782/

Bundesregierung (2020): Strategie Künstliche Intelligenz der Bundesregierung – Fortschreibung 2020 https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/201201_Fortschreibung_KI-Strategie.pdf&cid=947

CDU, CSU, SPD (2012): »Deutschlands Zukunft gestalten – Koalitionsvertrag zwischen CDU, CSU und SPD« https://archiv.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf (06.07.2022)

Deutscher Bundestag (2013a): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Herbert Behrens, Annette Groth, et al. und der Fraktion DIE LINKE. – Drucksache 17/11978 – »Integration von schweren Drohnen in den allgemeinen zivilen Luftraum« Drucksache 17/12136 21.01.2013

Deutscher Bundestag (2013b): Antrag der Abgeordneten Agnes Brugger, Volker Beck (Köln), Marieluise Beck (Bremen) et al. und der Fraktion BÜNDNIS 90/DIE GRÜNEN: »Keine bewaffneten Drohnen für die Bundeswehr – Internationale Rüstungskontrolle von bewaffneten unbemannten Systemen voranbringen« Drucksache 17/13235 24.04.2013

Deutscher Bundestag (2013c): Antwort der Bundesregierung auf die Große Anfrage der Abgeordneten Dr. Rolf Mützenich, Dr. Hans-Peter Bartels, Rainer Arnold, et al. und der Fraktion der SPD – Drucksache 17/11102 – »Haltung der Bundesregierung zum Erwerb und Einsatz von Kampfdrohnen« Drucksache 17/13655 29.05.2013

Deutscher Bundestag (2019): Beschlussempfehlung und Bericht des Verteidigungsausschusses (12. Ausschuss) zu dem Antrag der Abgeordneten Dr. Marcus Faber, Alexander Graf Lambsdorff, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/15675 – »Schutz der Soldatinnen und Soldaten der Bundeswehr durch die Beschaffung von bewaffneten Drohnen stärken« Drucksache 19/16149 18.12.2019

Deutscher Bundestag (2021): Antrag der Abgeordneten Matthias Höhn, Heike Hänsel, Dr. Alexander S. Neu, et al. und der Fraktion DIE LINKE. »Für ein Verbot autonomer Waffensysteme« Drucksache 19/26299 28.01.2021

Deutscher Bundestag (2022a): Gesetzentwurf der Bundesregierung »Entwurf eines Gesetzes zur Änderung des Grundgesetzes (Artikel 87a)« Drucksache 20/1410 13.04.2022

Deutscher Bundestag (2022b): Beschlussempfehlung und Bericht des Haushaltsausschusses (8. Ausschuss) zu dem Gesetzentwurf der Bundesregierung –Drucksache 20/1409 – »Entwurf eines Gesetzes zur Errichtung eines »Sondervermögens Bundeswehr« (Bundeswehrsondervermögensgesetz – BwSVermG)« Drucksache 20/2090 01.06.2022

Hoffberger-Pippan, E.; Vohs, V.; Köhler, P. (2022): »Autonomous Weapons Systems: UN Expert Talks Facing Failure. Time to consider Alternative Formats«, SWP Comment No. 43, July 2022 https://www.swp-berlin.org/en/publication/autonomous-weapons-systems-un-expert-talks-facing-failuretime-to-consider-alternative-formats (14.07.2022)

Ministry of Defence (2022): »Defence Artificial Intelligence Strategy«. June 2022 https://qna.files.parliament.uk/ws-attachments/1470486/original/20220610-Defence_AI_Strategy_Final.pdf (14.07.2022)

TAB (1996): Kontrollkriterien für die Bewertung und Entscheidung bezüglich neuer Technologien im Rüstungsbereich. https://www.tab-beim-bundestag.de/english/projects_kontrollkriterienfur-die-bewertung-und-entscheidung-bezueglich-neuer-technologien-im-ruestungsbereich.php

TAB (2003): Militärische Nutzung des Weltraums und Möglichkeiten der Rüstungskontrolle im Weltraum https://www.tab-beim-bundestag.de/english/projects_militaerische-nutzung-des-weltraums-und-moeglichkeiten-der-ruestungskontrolle-im-weltraum.php

TAB (2010): Status quo and perspectives of the military use of unmanned platforms https://www.tab-beim-bundestag.de/english/team_stand-und-perspektiven-der-militarischen-nutzung-unbemannter-systeme.php

TAB (2020): Autonomous weapon systems. https://www.tab-beim-bundestag.de/english/team_autonomous-weapon-systems.php

Netherlands – Rathenau Instituut

What is it about?

Autonomous systems are software-based or robotic systems that can plan and execute actions largely independently. They do so by 1) collecting data, for example via sensors, 2) analyzing that data, via machine learning, and 3) by acting upon that data, for example via actuators that turn a machine on or off. Autonomous systems usually comprise a cluster of technologies, including robotics, data analytics, or cloud technologies. Autonomous systems are developed for, or used in, a wide variety of domains, such as finance, human resources, agriculture, social security, transport or military purposes (autonomous weapons).

Not all systems developed are – nor aspire to be – fully autonomous. In fact, many innovation and policy questions specifically relate to the desired degree of autonomy: what decisions do we leave to machines? Where is human oversight necessary? After the child benefit scandal[158], in which the Dutch tax agency wrongly accused 26,000 parents of fraud, a central topic in the political debate is about how to prevent algorithmic systems from discriminating against specific groups in society. In the Netherlands, AI systems, or algorithmic systems, is more commonly used to debate such questions than »autonomous systems«.

What is the state of play?

In the Netherlands, (semi)autonomous systems are developed and piloted in a wide variety of sectors, such as finance, healthcare, agriculture, mobility, energy, social security and the military domain. AI is considered a key enabling technology by the government, or called a »system technology« after a report by the Dutch Scientific Council on AI (WRR, 2021).

Through field and innovation labs the government aims to »stimulate viable AI solutions for societal challenges« (Ministry of Economic Affairs and Climate change, 2019). In many domains the government has set up dedicated research and innovation programmes in collaboration with private actors and civil society. The AI Ned programme[159] is one of the largest programmes in which 18 »ELSA Labs« (researching Societal, Ethical and Legal issues) are currently funded, including a Defence ELSA Lab.[160] The AI Ned programme further consists of six research and development themes. One theme, »embedded systems« is specifically focused towards fully autonomous systems. Other themes, such as »hybrid AI« have as point of departure that humans and machines will need to work together in a meaningful way.

[158] Between 2013 and 2019, the Dutch government wrongly accused an estimated 26,000 parents of making fraudulent child benefit claims, based on algorithms using demographic variables, such as migrant background. Families were ruined, financially and emotionally. The government is still working to compensate the parents for the wrong doing of the government and other institutions.

[159] https://nlaic.com/en/ained-programme/

[160] https://nlaic.com/en/use-case/elsa-lab-defence/

Regarding military systems, the Dutch Ministry of Defence wants to invest in several autonomous systems, such as autonomous (armed) sensor systems, and unmanned and autonomous weapon systems (Ministry of Defence, 2022a, Ministry of Defence 2022b).

Who are the key stakeholders?

Concerning the general development and uptake of AI, the ministry of Economic Affairs and Climate Change and Ministry of Home Affairs play a central role. The public private partnership Dutch AI Coalition (NL AIC) executes the AI Ned programme. It consists of a network of state and private actors, including municipalities, companies, universities and other research institutes.[161] In specific domains, different stakeholders play a role. For example, in the field of AI and healthcare, hospitals, patient organisations participate in innovation labs and in the societal and political debate. In the field autonomous weapons, the ministry of defence, universities and research universities including HCSS and Clingendael, TNO, Marin, and ngo's like Pax and Human Rights Watch, as well as advisory councils from the governments such as the Council for International Affairs and the Advisory Committee on Public International Law, are involved in drafting policies and innovation labs.

Why is this important?

The Dutch governments expects AI to be a »game changer«, a technology that will influence economic growth, prosperity and wellbeing in the Netherlands and the world (Ministry of Economic Affairs, 2019). It also considers AI to be of enormous help to deal with grand societal challenges, such as climate change, food safety, healthcare and an aging population. The Dutch governments considers the Netherlands to lack behind in investing and deploying AI, and therefore aims to speed up development and use of AI (Ministry of Economic Affairs 2019).

In the first AI strategy of the Netherlands, the domains of safety and security, healthcare, food safety and agriculture, energy transition and sustainability are mentioned as key domains for the Netherlands (Ministry of Economic Affair s2019). These domains largely correspond with traditional important sectors of the Dutch economy. In the AI Ned programme four focus areas are specified: 1) Energy and Sustainability, 2) Healthcare, 3) Mobility, Transport and Logistics and 4) Technical Industry (NLAIC, 2021).

Societal and political relevance and debate

Ongoing debate

In the last five years the attention in the Dutch societal and political debate for the impact of autonomous systems increased. In 2013 – 2015, the Dutch societal and policy debate focused mainly on the fear of mass unemployment due to the rise of robotics (Rathenau Instituut 2015). After that, the

[161] NLAIC was set up by the Confederation of the Netherlands Industry and Employers for Dutch SMEs, the Ministry of Economic Affairs and Climate Policy, research organisation TNO, Seedlink, Philips, Ahold Delhaize, IBM and the Dutch Digital Delta Top Team.

debate broadened up to more ethical, societal and legal issues relating to AI. Gradually, safeguarding human rights and public values became a more prominent part of Dutch digitization policy (Ministry of Economic Affairs 2018). The work of the High Level Expert Group on AI from the European Commission also formed an important basis for Dutch policy. As indicated above, the childcare benefit scandal demonstrated in a painful way how risks of AI systems can manifest in reality. In the most recent digitization strategy, protecting public values and human rights play a dominant role, especially non-discrimination, explainability and accountability (Ministry of Home Affairs, 2022).

In the last ten years, there is also societal and political debate about the use of autonomous weapons. Parliament has organized several expert hearings on the topics[162], and the Rathenau Instituut, as well as the Advisory Council for International Affairs and the Advisory Committee on Public International Law advised the government at an early stage about the ethical and legal issues (Rathenau Instituut 2012, AIV/CAVV 2015). Whilst the European Parliament[163] and 28 UN-countries[164] made pleas in 2018 to prohibit the use of autonomous weapons, the Dutch government was, until recently, not in favour of a ban on the development of autonomous weapon systems (Ministry of Foreign Affairs, 2016).

This position has changed after a renewed advice from the AIV and CAVV (2021). The councils conclude that for fully autonomous systems, no meaningful human control is considered possible, therefore these systems should be prohibited. For partially autonomous weapon systems, the councils deem meaningful human control and oversight is possible, but more specific international regulation is required to do so. The government adopted this advice, and now supports an international ban on *fully autonomous* weapon systems, and aims to regulate partially autonomous weapons (Ministry of Foreign Affairs 2021). A changing geopolitical landscape and the increasing use of such systems by countries such as US, China, Russia, Israel, Turkey and South-Korea are playing a role in this decision.

Legislation in place

Autonomous systems do not exist in a legal vacuum. They are regulated by existing laws, such as the General Data Protection Regulation, administrative law, procedural law and sectoral laws. The GDPR for example protects citizens from automated decision making (article 22)[165], and administrative law demands that the governments explains to a citizen how a decision was made.

Since 2017, the Dutch government has commissioned research to see if updates to the legal framework are necessary[166], but limited actual changes have been made so far. The government did develop »soft law«, i.e. guidelines for responsible system design (such as impact assessments and non-discrimination guidelines) and invested in stronger oversight (Rathenau Instituut 2021). Ever since

[162] The Rathenau Institute also contributed to such parliamentary hearings, see (Rathenau Instituut, 2019).

[163] https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.html

[164] https://www.stopkillerrobots.org/wp-content/uploads/2018/11/KRC_CountryViews22Nov2018.pdf

[165] The article in the GDPR is criticized for being too limited in scope, as mostly decisions are not fully automated.

[166] See for example Vetzo et al 2018; Kulk and van Deursen (2020); van der Sloot and van Scendel (2020)

the childcare benefit scandal, the House of Representatives is keeping a closer watch on governmental algorithmic systems.[167]

Since April 2022, the Dutch parliament has agreed that the Dutch army is allowed (in specific circumstances) to arm unmanned drones. Up until then, unmanned vehicle areas were only allowed to gather intelligence.[168] The decision was criticized by experts and NGOs, who urge the government to first regulate the use of such systems before deploying them.[169]

Current political or legislative proposals

The upcoming AI Act from the European Commission specifies requirements regarding transparency, explainability and accountability to high risk AI systems.[170] However, debate remains if these requirements are sufficient. The government further aims to strengthen oversight, and has announced to establish an »Algorithmic Authority« to monitor transparency and non-discrimination of algorithmic systems.[171] A preliminary public algorithmic registry should be operational by the end of 2022 (Ministry of Home Affairs, 2022).

Science/evidence-based inputs guiding political decision-making

Early 2017, the Rathenau Instituut concluded in »Urgent upgrade« that the government, industry and society were not yet adequately prepared to deal with the arising ethical, legal and societal issues digital technologies raise (Rathenau Instituut 2017a).[172] All actors needed to take action to steer the digital society in the desired direction. The report formed the start of an intensified debate about the digital society. In the past five years, a wide array of advisory councils, universities and research institutes, NGOs, companies, municipalities, representatives of specific groups in society think about the impact of AI, are involved in responsible innovation projects, or write policy briefs to inform and advice policy makers and politicians. In 2021, the House of Representatives established a committee dedicated to Digital Affairs, including AI. However, the most recent report from the Netherlands Scientific Council for Government Policy calls for further societal involvement to ensure successful and responsible AI innovations (WRR 2021).

[167] For example, motions are tabled to make a human rights impact assessment for government systems mandatory, and to create an algorithmic 'registry', to inform citizens about which algorithms are in use https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2022Z06024&did=2022D12329

[168] Motion tabled by Lid Valstar, https://zoek.officielebekendmakingen.nl/kst-35925-X-69

[169] https://www.volkskrant.nl/nieuws-achtergrond/kamermeerderheid-voor-bewapende-drones-overhaast-en-kort-door-de-bocht-zeggen-experts~bd47496c/

[170] The AI Act does not include the military domain, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

[171] https://www.kabinetsformatie2021.nl/documenten/publicaties/2021/12/15/coalitieakkoord-omzien-naar-elkaar-vooruitkijken-naar-de-toekomst. The aim is to have this supervisory body operational in 2023

[172] The report was written after a motion tabled by the Dutch senate, questioning the ethical issues of the digital society https://zoek.officielebekendmakingen.nl/kst-CVIII-S.html.

Role of TA in the debates

Rathenau Instituuts' contribution to this topic

The Rathenau Instituut has published since 2012 about autonomous systems. In »Robots everywhere: automation from love to war« (2012, updated in 2016) we gave an overview of ethical, legal and societal issues of robotics in five domains: at home, healthcare, traffic, law enforcement and in the military. Important policy recommendations were to develop a political vision regarding the development and use of robots, prohibit autonomous weapons, make use of autonomous car systems, and to start thinking about how to use robots in healthcare. At the time, limited to no policy was in place regarding robotic and autonomous systems. In subsequent publications, we focused more in depth on these domains or specific technologies.[173]

In 2015, the House of Representatives requested our research about the potential impact of robotics on employment. The publication »Working on the robot society: Visions and insights from science concerning the relationship between technology and employment« showed the relation between technology, employment, productivity and prosperity over 200 years. It concluded that the Netherlands should be better prepared to make use of the opportunities of these technologies, whilst also pointing out that certain groups will be highly vulnerable for further robotization and automation.

In 2017, we published »Urgent upgrade« and »Human rights in the robot age«. This latter report was commissioned by Parliamentary Assembly of the Council of Europe and investigated to what extent our current human rights are addressing upcoming issues of robotics, AI, virtual and augmented reality. We recommended two new human rights: the right not to be measured, analysed or coached, and the right to meaningful human contact.

Next to reports, we prepared short, specific briefs to parliament, addressing specific questions for political debates or policy hearings, for example about autonomous weapons (Rathenau Instituut 2019), responsible development and use of AI (Rathenau Instituut, 2020).

Has TA made an impact on the ongoing debates?

The reports of the Rathenau Instituut were published early in political and societal debates. As such they were successful in putting ethical, legal and society issues regarding autonomous systems on the policy agenda. Several reports were directly requested by parliament. With »Working on the robot society« we managed to create a common ground in the political debate, making all political parties aware of the opportunities, but also pointing the vulnerability of specific groups. In hindsight, Urgent Upgrade turned out to be a pivotal publication, as it initiated political and public debate on digitalisation on a large scale in the Netherlands. With subsequent outreach and publications, we contributed to building the governance system regarding ethical, societal and legal issues regarding AI, for example by informing the National Digitalisation Strategy, helping with the establishment of a standing Committee on Digital Affairs, informing and educating the Upper and Lower

[173] See for example publications about e-coaches (Rathenau Instituut 2014a), or Intimate technology (Rathenau Instituut 2014b) about the fading boundary between humans and machines.

Houses of representatives. The various ministries frequently use our reports and expertise to prepare policy.

Lessons learned from TA

The Rathenau Instituut was able to show not only the issues at stake, but also indicated that at that time, the governance ecosystem was not sufficiently equipped to deal with the upcoming issues. An important next step was to invest in this ecosystem, meaning for example that NGOs extended their activities, making supervisory bodies aware that they needed to prepare and build new expertise and capacities in order to execute their task, and showing to politicians that they needed to get more grip on political debates. Getting all actors mobilized improved the societal debate about relevant issues and political decision making.

References

AIV/CAVV (2015) Autonome wapensystemen. De noodzaak van betekenisvolle menselijke controle. https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2015/10/02/autonome-wapensystemen

AIV/CAVV (2021) Autonome wapensystemen. Het belang van reguleren en investeren. https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2021/12/03/autonome-wapensystemen

Kulk and van Deursen (2020) Juridische aspecten van algoritmen die besluiten nemen. Een verkennend onderzoek. Universiteit Utrecht. https://repository.wodc.nl/bitstream/handle/20.500.12832/2417/2947_volledige_tekst_tcm28-452340.pdf?sequence=2&isAllowed=y

Ministry of Defence (2022a) Defensienota. Den Haag https://www.defensie.nl/onderwerpen/defensienota-2022/downloads/beleidsnota-s/2022/06/01/defensienota-2022

Ministry of Defence (2022b) Strategische kennis en innovatieagenda 2021-2025, https://www.defensie.nl/downloads/publicaties/2020/11/25/strategische-kennis--en-innovatieagenda-2021-2025

Ministry of Economic Affairs (2018) Nationale Digitaliseringsstrategie. Den Haag. https://www.rijksoverheid.nl/documenten/rapporten/2018/06/01/nederlandse-digitaliseringsstrategie

Ministry of Economic Affairs (2019) Strategisch Actieplan voor Artificiële Intelligentie. Den Haag. https://open.overheid.nl/repository/ronl-e14cdcee-690c-4995-9870-fa4141319d6f/1/pdf/Rapport%20SAPAI.pdf

Ministry of Foreign Affairs (2016) Kabinetsreactie op AIV/ CAVV-advies »Autonome wapensystemen: de noodzaak van betekenisvolle controle«. Kabinetsreactie op Autonome wapensystemen | Kabinetsreactie | Adviesraad Internationale Vraagstukken

Ministry of Home Affairs (2022) Hoofdlijnenbrief digitalisering, https://www.rijksoverheid.nl/documenten/kamerstukken/2022/03/08/kamerbrief-hoofdlijnen-beleid-voor-digitalisering

NLAIC (2021) Artificiële Intelligentie. Nederland aan de slag met AI voor welvaart en welzijn. https://ained.nl/wp-content/uploads/2022/02/Publicatie_AiNed_Investeringsprogramma.pdf

Rathenau Instituut (2012) Overal robots. Automatisering van de liefde tot aan de dood. Royakkers, L., F. Daemen, R. van Est. Den Haag: Rathenau Instituut. https://www.rathenau.nl/nl/digitale-samenleving/overal-robots

Rathenau Instituut (2014a) Sincere support. The rise of the e-coach. Kool, L., J. Timmer en R. van Est. Den Haag: Rathenau Instituut. https://www.rathenau.nl/en/digitale-samenleving/sincere-support

Rathenau Instituut (2014b) Intimate technology. The battle for our body and behavior. Est, R. van, with assistance of V. Rerimassie, I . van Keulen & G. Dorren. Den Haag: Rathenau Instituut. https://www.rathenau.nl/en/digitale-samenleving/intimate-technology

Rathenau Instituut (2015) Working on the robot society: Visions and insights from science concerning the relationship between technology and employment. R. van Est and L. Kool (eds). Den Haag: Rathenau Instituut. https://www.rathenau.nl/sites/default/files/2018-05/RATH_Working_on_the_Robot_Society_01.pdf

Rathenau Instituut (2017a) Urgent upgrade. Protect public values in our digitized society. Kool, L., J. Timmer en R. van Est. Den Haag: Rathenau Instituut. https://www.rathenau.nl/en/digitale-samenleving/urgent-upgrade

Rathenau Instituut (2017b) Human rights in the robot age. Challenges arising from the use of robotics, artificial intelligence and virtual and augmented reality. R. van Est en J. Gerritsen, with the assistance of L. Kool. Den Haag: Rathenau Instituut. https://www.rathenau.nl/en/digitale-samenleving/human-rights-robot-age

Rathenau Instituut (2019) Uitdagingen voor regulering van drones en killer robots. Inbreng rondetafelgesprek Tweede Kamer. https://www.rathenau.nl/nl/digitale-samenleving/uitdagingen-voor-regulering-van-drones-en-killer-robots

Rathenau Instituut (2020) Zeven acties voor verantwoord innoveren met AI. Bericht aan het Parlement. Inbreng debat over AI en sleuteltechnologieën. https://www.rathenau.nl/nl/berichten-aan-het-parlement/zeven-acties-voor-verantwoord-innoveren-met-ai

Rathenau Instituut (2021) Grip op algoritmische besluitvorming bij de overheid. De rol van de Eerste Kamer. J. Hamer, R. de Jong en L. Kool. Den Haag: Rathenau Instituut. https://www.rathenau.nl/nl/digitale-zeggenschap/grip-op-algoritmische-besluitvorming-bij-de-overheid-de-rol-van-de-eerste

Royakkers, L. and R. van Est (2016) Just ordinary robots: automation from love to war. Routledge

van der Sloot and S. van Schendel (2020) De modernisering van het Nederlands procesrecht in het licht van big data: procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een datagedreven samenleving. Universiteit van Tilburg. https://research.tilburguniversity.edu/en/publications/de-modernisering-van-het-nederlands-procesrecht-in-het-licht-van-

Vetzo, M., J. Gerrards and R. Nehmelmann (2018) Algoritmes en grondrechten. Universiteit Utrecht. Den Haag: Boom Juridisch. https://www.uu.nl/sites/default/files/rebo-montaigne-algoritmes_en_grondrechten.pdf

WRR (2021) Opgave AI. De nieuwe systeemtechnologie. Den Haag. https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie

United Kingdom – Parliamentary Office of Science and Technology (POST)

Automation in military operations

Lorna Christie

What is it about?

Many military systems feature automation, including robotic systems that carry out physical tasks, and entirely software-based systems used for tasks such as data analysis.[1,2] Automation can increase the efficiency and effectiveness of existing military tasks,[3–5] and can relieve personnel of »dull, dirty, and dangerous« activities.[6,7] Advances in robotics, and digital technologies such as artificial intelligence (AI), are now enabling more sophisticated systems to be developed. These are capable of carrying out a wider range of tasks autonomously, and can determine their own course of action by making decisions about how they operate.[8] AI-enabled systems are likely to be increasingly important tools for supporting military decision making.

While autonomous systems have the potential to improve the speed and quality of military decision making, there are concerns about the use of the technology, particularly in applications that involve significant decisions about individuals. For example, the potential use of such systems in identifying, tracking, and engaging targets for attack. The ethical and legal concerns around autonomous weapons systems are the subject of extensive debate in the UK and internationally.[9]

Box 1: Glossary

Terminology in this area is inconsistent, with key terms often used interchangeably.

- *Automated system*: An automated system is one that has been instructed to automatically perform a set of specific tasks or series of tasks within human-set parameters.[38] This typically includes basic or repetitive tasks.
- *Autonomous system*: The Defence Science and Technology Laboratory (Dstl, an executive agency of the UK's Ministry of Defence) defines an autonomous system as one that can exhibit autonomy. There is no agreed definition of autonomy,[8,39] but Dstl defines it as »the characteristic of a system using artificial intelligence (AI) to determine its own course of action by making its own decisions«.[40] An autonomous system can respond to situations that were not pre-programmed.[40]
- *Artificial intelligence (AI)*: There is no universally agreed definition of AI, but it usually refers to a broad set of computational techniques that can perform tasks normally requiring human intelligence (POSTnote 637).[3,49] AI is an enabling technology for higher levels of autonomy.
- *Uncrewed vehicles*: The move towards greater levels of autonomy has allowed »uncrewed« vehicles to be developed that do not have a pilot or driver on board.[41–44] Some are operated *via* remote control, and others include varying levels of autonomy.[45,46] The most established type

of uncrewed military systems are uncrewed aerial vehicles, or »drones«, which have versatile uses.[30,47,48]

- *Machine learning (ML)*: is a branch of AI that has underpinned the most recent advances in technologies with autonomous capabilities (POSTnote 633).

Many experts view autonomous capability on a spectrum relating to the level of human supervision a system has, although there is debate about where certain systems should be placed. The UK Ministry of Defence has outlined 5 broad levels of autonomy in its »autonomy spectrum framework« ranging from »human operated« to »highly autonomous«.[3] There is also varying and inconsistent terminology used in this area, with disagreement about whether some systems should be described as »automated« or »autonomous«.[10-12] Box 1 outlines the key definitions used in this report.

Why is this important?

The UK Government has recognised the military advantages of autonomous systems and artificial intelligence (AI) and the integral role they are likely to play in the future of defence. In its 2021 »Integrated Review« and 2020 »Integrated Operating Concept«, it stated its commitment to embrace new and emerging technologies, including autonomous systems and AI.[13] As part of its Integrated Review, the UK Government said that future military capability will be »*less defined by numbers of people or platforms and more about information-centricity, automation and a culture of innovation and experimentation.*« The Government has committed to invest £6.6 bn (€7.6 bn) in defence research and development over the next four years. Recent investment programmes include project NELSON, which aims to integrate data science into naval operations; and the Future Combat Air System, which will deliver a mix of crewed, uncrewed and autonomous systems for the Royal Air Force.[6,14-16] In June 2022, the Ministry of Defence (MoD) published its Defence AI Strategy, which sets out how it plans to adopt and exploit AI.

What is the state of play?

The UK is investing in, developing and deploying autonomous and AI-capable systems for military applications across the land, air, sea, and cyber domains. Systems are in use or development for military applications including intelligence, surveillance and reconnaissance, data analysis, and weapons systems.

Intelligence, surveillance, and reconnaissance

Automation is increasingly being applied to intelligence, surveillance, and reconnaissance (ISR), often using uncrewed vehicles (Box 1).[17,18] Uncrewed land, air, and sea vehicles fitted with sensors can obtain data such as audio, video footage, thermal images, and radar signals, and feed it back to human operators.[26] Some systems can navigate autonomously,[19] or autonomously identify and track targets for potential attack.[20,21] The UK has several ISR drones in service, with others being trialled. These range from very small »mini« drones that are similar in weight to a smartphone, up to large fixed-wing systems that can fly thousands of miles.[22-24] One system being trialled in the UK is a mini helicopter called the »Ghost« drone, which can fly autonomously and identify and track targets using algorithms for image analysis.[25,26]

Data analysis

AI can be used in the analysis of very large datasets and can discern patterns that might not be observed by a human analyst. This is likely to be applied increasingly in the field to inform tactical decisions, for example by providing information about the surroundings, identifying targets, or predicting enemy actions. The British army deployed AI for situational awareness during Exercise Spring Storm in Estonia in 2021,[27] and Dstl has a project using machine learning to support satellite image analysis.[3] There is also interest in using AI to analyse language in audio or text: During the current crisis in Ukraine, one US company demonstrated the use of machine learning to analyse audio from Russian radio communications.[28,29]

Weapons systems

Weapons systems featuring automation have been developed for defensive and offensive applications. These include systems ranging from those which respond automatically to external inputs to more sophisticated AI-based systems:

- *Defensive systems*: Automatic air defence systems can identify and respond to incoming airborne threats with faster reaction times than a human operator. Such systems have been in use for over 20 years;[30] one report estimated that they are in use by 89 countries.[55] Systems currently in use can launch munitions from the sea or land and are used in response to incoming missiles or aircraft. The UK operates the Phalanx CIWS air defence system.
- *Guided missiles*: Offensive missiles are in use that can alter their path in-flight to reach a target without human input.[31-35] The British Dual Mode Brimstone (DMB) missile,[36] first used in combat in Afghanistan in 2009,[37] can be pre-programmed to search a specific area to identify, track, and strike vehicles using sensor data.[38]
- *Uncrewed vehicles for weapons delivery*: Uncrewed air, sea,[39,40] and land-based[41,42] vehicles designed for weapons delivery can operate with a high level of autonomy. Such systems can autonomously search for, identify, and track targets. Most developments have been in the aerial domain. The only armed drone capable of autonomous flight the UK operates is the MQ-9 Reaper,[43] but several others are under development.[22,44] The MoD is also developing »swarming« drones. Uncrewed offensive weapons are not used to make firing decisions without human authorisation, although this technical capability exists. Reported exceptions are rare and contested (Box 2).[45–50]

Who are the key stakeholders?

There are various stakeholders contributing to the research and discourse in the UK around automation in military technology and its future implications. These include think tanks such as the Royal United Services Institute (RUSI) and Chatham House. NGOs that have been central in the ethical debate around autonomous weapons systems include Article 36, Drone Wars UK, Human

Rights Watch and the International Committee for Robot Arms Control (ICRAC). Stop Killer Robots, an international coalition of more than 180 NGOs, has also been a key voice in these debates, and has called for new international law on autonomous weapons systems (discussed later).

A number of academic stakeholders are involved in research projects looking at different aspects of automation in military technology. The UK's research funding body, UK Research and Innovation (UKRI) has a multidisciplinary research programme on »*Trustworthy Autonomous Systems*«, which funds research into how autonomous systems can be built in a way that society can trust.[51] As part of this, UK researchers are carrying out various defence-related projects, such as investigating trust in autonomous systems among the armed forces.[52]

As mentioned earlier, the UK Government is a key stakeholder in this area and has been driving forward its ambition to develop and deploy autonomous and AI-capable systems for the military. The Government recently established a Defence AI Centre (DAIC) to coordinate the UK»s development of AI-enabled technologies for defence.[53] This includes facilitating collaborations with academia, with research hubs established at the Universities of Newcastle and Exeter, and the Alan Turing Institute.[54–56] The MoD also collaborates closely with industry partners in the UK and internationally to test and develop AI and autonomous technology. Notable UK-based companies that are developing automated and AI-based technology for defence applications include BAE Systems, Rolls Royce and QinetiQ.[57–59]

Societal and political relevance and debate

Ongoing debate

Much of the debate in this area focuses on legal and ethical issues around weapons systems with autonomous capability. However, certain unarmed systems (for example, software-based decision support tools) may play a key role in identifying targets, and hence may raise many of the same ethical issues as those that also deploy a weapon.[10,60,61] International debate centres around »lethal autonomous weapons systems« (LAWS), however, this term has no universally agreed definition, and is used to refer to a wide range of weapons with different autonomous capabilities.[10,62] Reports of the use of LAWS are highly contested (Box 2).[45–50]

Box 2 – Kargu-2 case study

A 2021 report published by a panel of UN experts described the deployment of the Turkish Kargu-2 drone in Libya in 2020 as the use of a LAWS, reporting that the systems had been »programmed to attack targets without requiring data connectivity between the operator and the munition«.[186] Subsequent media reporting suggested this may have been the first time soldiers had been killed by autonomous weapons systems acting without human oversight. However, others have disputed this, highlighting that the report does not explicitly say human beings were killed, and pointing to uncertainty around the modes in which the systems were used.[187,188]

Many stakeholders believe that some form of human control of weapons and targeting systems must be maintained to be legally and ethically acceptable.[63–65] Certain organisations, such as the Stop

Killer Robots campaign, have called for a prohibition on autonomous weapons systems that cannot be operated with »meaningful human control«, and all autonomous weapons systems that target humans. They also suggest regulations to ensure sufficient human control is maintained in practice.[61,66–69] In its 2022 Defence AI Strategy, the UK Government stated that weapons which identify, select and attack targets must have »context-appropriate human involvement«. In response, some NGOs calling for regulation have said that more clarity is needed on how »context-appropriate human involvement« should be assessed or understood.[70]

Legislation in place

There is currently no legislation specific to the use of automation or AI for military applications. The use of automation and AI is governed by existing International Humanitarian Law,[71,72] but how this law relates to new technologies is debated.[73–75] In 2022, the MoD published ethical principles for the use of AI in defence in partnership with the Centre for Data Ethics and Innovation (CDEI, a Government body established to provide advice on enabling the trustworthy use of data and AI).[76] There are many examples of principles and guidelines on more general use of AI at the UK and international level.[77–80] However, some stakeholders have noted that public bodies may be uncertain about which principles to follow. The 2021 CDEI AI Barometer study found it is difficult for industry to adapt general regulations to specific contexts.[81]

Currently political or legislative proposals

The UN Convention on Certain Conventional Weapons (CCW) has discussed possible legislation of LAWS since 2014. It published guiding principles in 2019,[82] but these are non-binding, and no further agreement has been reached. While most nations represented at the CCW support new regulation of LAWS, others, including the UK, US, and Russia have argued that existing International Humanitarian Law is adequate.[63,83,84] A group of around 3800 individuals (including AI researchers) and 270 organisations have signed a pledge calling for regulations and laws against lethal autonomous weapons.[85]

Role of TA in the debates

POST contribution to this topic

POST produced a briefing on Automation in Military Operations in 2015 (POSTnote 511) and is currently preparing an updated briefing on this topic, due for publication in September 2022. This update is expected to support parliamentary activity including scrutiny of the Government's defence AI strategy and other committee inquiry work. POST has also looked at the applications of automation and AI in other areas beyond defence, including AI in healthcare (POSTnote 637), AI in policing and security, and automation and the workforce (POSTnote 534). Some of POST's analyses have focussed on cross-sector issues raised by AI, such as the explainability of machine learning (POSTnote 633).

Has TA made an impact on the ongoing debates?

It is challenging to measure the impact of POST publications, as it is difficult to track how reports are used and work may be used without being referenced. However, POST's 2015 briefing on Automation in Military Operations has been cited in academic and NGO literature,[86–88] indicating its contribution to the wider debate around automation and AI in military operations. Following the publication of POST's 2015 briefing, the House of Commons Defence Committee launched an inquiry on »robotics and artificial intelligence«, with accountability and liability of autonomous military systems raised as key issues. POST's more recent report on Interpretable Machine Learning has been cited in academic literature and was extensively quoted in an article by a UK law firm.[89]

In addition, policy analyses, public deliberation exercises and wargaming studies produced by various other organisations play an important role in developing a full understanding of the opportunities and risks around AI and automation and the future implications of this technology. Some recent key defence-specific policy reports and analyses have been produced by RUSI and the UKRI Trustworthy Autonomous Systems hub.[90,91] Beyond defence, the UK's Ada Lovelace Institute has played a key role in convening experts and supporting debate around how data and AI affect people and society more broadly, with evidence feeding into Government consultations and select committee inquiries.

Lessons learned from TA

Automation and AI are likely to be increasingly integrated into military systems for various applications, which will have key implications for militaries globally. One of the main implications is likely to be changes to the roles and skills required of military personnel. For example, there is likely to be an increase in demand for developers and operators of autonomous systems with relevant technical knowledge. In many areas, autonomous systems are expected to play a support function to humans, or work with them in »human-machine teams«. More research is needed on the most effective ways for humans and machines to collaborate as AI systems become increasingly sophisticated.[91,92]

Automation and AI may also change the nature of future conflict. For example, some experts have raised concerns that increasing use of autonomy in weapons systems risks escalating conflict by removing humans from the battlefield and reducing hesitancy to use force.[93,94] A recent wargame report by RAND (which played out a conflict scenario involving the US, China, Japan, South Korea, and North Korea) found that widespread AI and autonomous systems could lead to inadvertent escalation and crisis instability, partly due to the increased speed of AI-supported decision making.[95] Escalation may also be caused by unintended behaviour of automated systems.[96]

The CCW will continue to act as a forum for discussion around autonomous weapons systems, and the UK has been an active participant in these meetings. However, as noted previously, while some states have called for legislation of LAWS, the UK has argued that existing international humanitarian law is sufficient to regulate their use. Given the lack of consensus at the CCW, several commentators have suggested that some countries may seek to agree international law on these systems outside of the CCW, although whether this will happen, and what form it may take, is currently unclear. [74,97]

References

1. Emma, H. (2020). Managing the military's big data challenge. Military Embedded Systems.
2. Rossiter, A. (2020). The impact of robotics and autonomous systems (RAS) across the conflict spectrum. Small Wars Insur., Vol 31, 691–700. Routledge.
3. Defence Artificial Intelligence Strategy. GOV.UK.
4. (2018). Joint Concept Note 1/18 Human-Machine Teaming. Ministry of Defence Development, Concepts and Doctrine Centre.
5. (2016). AI fighter pilot wins in combat simulation. BBC News.
6. Great Britain et al. (2021). Defence in a competitive age.
7. (2021). Robotics and autonomous systems: defence science and technology capability. Defence Science and Technology Laboratory.
8. What is Automation? International Society of Automation.
9. Morgan, F. E. et al. (2020). Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. RAND Corporation.
10. Taddeo, M. et al. (2021). A Comparative Analysis of the Definitions of Autonomous Weapons.
11. Bode, I. et al. (2022). Autonomous Weapons Systems and International Norms. McGill-Queen's University Press.
12. Huang, H.-M. et al. (2005). A Framework For Autonomy Levels For Unmanned Systems. in Proceedings of the AUVSI's Unmanned Systems North America.
13. Mills, C. (2021). Integrated Review 2021: emerging defence technologies. House of Commons Library, UK Parliament.
14. (2018). Royal Navy: NELSON Data Platform Product Development – Digital Marketplace. Programme NELSON, Information Warfare, Royal Navy, Ministry of Defence.
15. (2019). NELSON Data Platform Beta – Live Development – Digital Marketplace. Royal Navy, Ministry of Defence.
16. (2019). Cutting-edge technology on show in Royal Navy exercise | Royal Navy. Royal Navy.
17. Reis, J. et al. (2021). High-Tech Defense Industries: Developing Autonomous Intelligent Systems. Appl. Sci., Vol 11, 4920. Multidisciplinary Digital Publishing Institute.
18. Frank Wolfe (2020). Autonomous ISR Assets Likely A Big Defense Growth Area. Aviation Today.
19. Simpson, S. (2022). Autonomous Navigation & Positioning for Drones, UAV, UGV, USV & AUV. Unmanned Systems Technology.
20. Reddie, A. et al. (2019). Unmanned Underwater Vehicle (UUV) Systems for Submarine Detection. On the Radar.
21. Kumar, M. et al. (2021). Recent developments on target tracking problems: A review. Ocean Eng., Vol 236, 109558.
22. (2022). An overview of Britain's drones and drone development projects. Drone Wars UK.
23. MOD signs £65-million contract for Protector aircraft. GOV.UK.
24. Mark Watson (2021). The future has landed – SkyGuardian arrives in the UK. NATS Blog.
25. (2021). Drone swarms support Commando Forces trials in a first for the UK's armed forces. Royal Navy.

26. Shanahan, J. G. et al. (2020). Introduction to Computer Vision and Real Time Deep Learning-based Object Detection. in Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 3523–3524. Association for Computing Machinery.
27. (2021). Artificial Intelligence used on British Army operation for the first time. The British Army.
28. Gourley, S. (2022). A New Era of Warfare: How AI Unlocks Intelligence from Russian Radio Chatter in Minutes. PrimerAI.
29. Knight, W. (2022). As Russia Plots Its Next Move, an AI Listens to the Chatter. Wired.
30. Gray, M. et al. (2021). Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment. 34. NATO Cooperative Cyber Defence Centre of Excellence.
31. (2019). From Sea Wolf to Sea Ceptor – the Royal Navy's defensive shield. Navy Lookout.
32. Exocet AM39 | Maritime Superiority, Exocet Solution. MBDA.
33. Jonathan Beale (2018). Syria air strikes: RAF used »fire and forget« missiles to minimise risk. BBC News.
34. Storm Shadow/SCALP | Air Dominance. MBDA.
35. (2018). Lockheed awarded almost $632 million for Hellfire missiles for the Netherlands and Japan. The Defense Post.
36. Brimstone | Air Dominance. MBDA.
37. (2011). Dual Mode Brimstone. MBDA.
38. (2021). Brimstone. Missile Threat.
39. Crumley, B. (2021). China develops a fully autonomous underwater attack drone. DroneDJ.
40. Osborn, K. (2021). Navy Pursues Large Undersea Attack Drones. The National Interest. The Center for the National Interest.
41. (2022). Land Industrial Strategy. Ministry of Defence.
42. Simpson, S. (2022). Autonomous Ground Vehicles (AGV) & Robotics. Unmanned Systems Technology.
43. MQ-9A »Reaper«. General Atomics Aeronautical Systems Inc.
44. RAF Protector: What Is The Aircraft And What Can It Do? Forces Network.
45. Tingley, B. (2021). Marines Train With Handheld Swarming Drones That Can Also Be Fired From 40mm Grenade Launchers. The Drive.
46. Will Meddings [@WillJMeddings] (2021). Ulrike, just to be clear, although the system is in use, the version we are using is hand launched and does not include any munitions – it is purely used for surveillance and reconnaissance. Twitter.
47. Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council. United Nations Security Council.
48. Beyza Arslan An Evaluation of Lethal Autonomous Weapon Systems Under the Law of Armed Conflict and the Question of Kargu-2. Hukukçular Derneği.
49. Vincent, J. (2021). Have autonomous robots started killing in war? The reality is messier than it appears. The Verge.

50. Zachary Kallenborn (2021). Was a flying killer robot used in Libya? Quite possibly. Bulletin of the Atomic Scientists.
51. (2020). New Trustworthy Autonomous Systems projects launched. UKRI.
52. Public Policy Southampton Trustworthy Autonomous Systems (TAS) Hub. University of Southampton.
53. Defence Artificial Intelligence Centre. GOV.UK.
54. (2022). New Dstl site opened in Newcastle. Business and Partnerships – Newcastle University.
55. (2022). Dstl launches Defence Data Research Centre. Defence Science and Technology Laboratory.
56. (2022). Launching the Defence Centre for AI Research. Defence Science and Technology Laboratory.
57. Rolls-Royce (2021). Rolls-Royce secures UK MOD funding for innovative technology to support naval autonomy.
58. QinetiQ Robotics and Autonomous Systems. QinetiQ.
59. BAE Systems Autonomous Systems. BAE Systems | United Kingdom.
60. (2018). Ethics and autonomous weapon systems: An ethical basis for human control? International Committee of the Red Cross.
61. (2019). Targeting People. Article 36.
62. Klare, M. T. (2020). The Pentagon's Next Project: Automated War. The Nation.
63. (2020). Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control. Human Rights Watch.
64. Our policy position. Stop Killer Robots.
65. Heather M. Roff (2016). Meaningful Human Control, Artificial Intelligence and Autonomous Weapons. Article 36.
66. Problems with autonomous weapons. Stop Killer Robots.
67. (2021). Lethal Autonomous Weapons Exist; They Must Be Banned. IEEE Spectrum.
68. (2021). Advisory Note on Autonomous Weapon Systems that Target Humans. Campaign to Stop Killer Robots.
69. (2021). ICRC position on autonomous weapon systems. International Committee of the Red Cross.
70. Stop Killer Robots (2022). New UK Government position on »autonomous weapons« – recognises that lines need to be drawn, but lacks detail, or signs of real leadership. Article 36.
71. (2014). War & Law. International Committee of the Red Cross.
72. (2022). Autonomous weapons: The ICRC calls on states to take steps towards treaty negotiations. International Committee of the Red Cross.
73. (2017). New Technologies in Warfare and International Humanitarian Law – World. Institute for Defence Studies and Aanlyses and International Committee of the Red Cross.
74. (2021). Killer Robots: Negotiate New Law to Protect Humanity. Human Rights Watch.
75. (2014). New technologies and IHL. International Committee of the Red Cross.
76. Ben Kelly (2022). Enabling the responsible use of AI in defence. Centre for Data Ethics and Innovation.
77. IEEE SA – IEEE 7001-2021. IEEE Standards Association.

78. Jobin, A. et al. (2019). The global landscape of AI ethics guidelines. Nat. Mach. Intell., Vol 1, 389–399. Nature Publishing Group.
79. (2021). The EU Artificial Intelligence Act. The Artificial Intelligence Act.
80. (1807). Establishing a pro-innovation approach to regulating AI. Department for Digital, Culture, Media & Sport, Department for Business, Energy & Industrial Strategy, and Office for Artificial Intelligence.
81. (2021). AI Barometer 2021. Centre for Data Ethics and Innovation.
82. (2019). Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. The United Nations Convention on Certain Conventional Weapons.
83. (2013). The next generation: the UN considers the potential of lethal autonomous robots – All Party Parliamentary Group on Drones and Modern Conflict. All-Party Parliamentary Group on Drones and Modern Conflict.
84. Hoffberger-Pippan, E. et al. (2022). Autonomous Weapons Systems: UN Expert Talks Facing Failure. 7. German Institute for International and Security Affairs.
85. (2018). Autonomous Weapons: Pledge. Future of Life Institute.
86. Kopuletý, M. et al. (2018). Advanced Military Robots Supporting Engineer Reconnaissance in Military Operations. in Modelling and Simulation for Autonomous Systems. (ed. Mazal, J.) 285–302. Springer International Publishing.
87. Nainggolan, J. H. P. (2018). Military Application of Unmanned Underwater Vehicles: In Quest of a New Legal Regime? Culture & International Law. Indones. J. Int. Law, Vol 16, 61–83.
88. Watts, T. et al. (2021). Meaning-less human control: Lessons from air defence systems for lethal autonomous weapons. Drone Wars UK, Centre for War Studies, and University of Southern Denmark.
89. Whittaker, T. (2020). Interpretable machine learning – an overview by the Parliamentary Office of Science and Technology (via Passle). Burges Salmon.
90. Balis, C. et al. (2022). Trust in AI: Rethinking Future Command. RUSI.
91. Krause, J. (2021). Trusted autonomous systems in defence: A policy landscape review. UKRI TAS Hub.
92. Stowers, K. et al. (2021). Improving Teamwork Competencies in Human-Machine Teams: Perspectives From Team Science. Front. Psychol., Vol 12,
93. Blanchard, A. et al. (2022). Autonomous weapon systems and jus ad bellum. AI Soc.,
94. Merel Ekelhof et al. (2020). Swarm Robotics. United Nations Institute for Disarmament Research.
95. Wong, Y. H. et al. (2020). Deterrence in the Age of Thinking Machines. RAND Corporation.
96. (2021). National Security Commission on Artificial Intelligence Final Report. National Security Commission on Artificial Intelligence.
97. United Nations Association – UK (2021). Historic opportunity to regulate killer robots fails but hope emerges for new route. UNA-UK.

EPTA Member Contributions

Nature under pressure – humans as a disruptive force

Catalonia – The Advisory Board of the Parliament of Catalonia for Science and Technology (CAPCIT)

Resilient Landscapes, Climate-Smart Forestry and Circular Bioeconomy. The case of Catalonia.

The role of forests under the present scenario of global change

We are facing unprecedented global environmental changes: climate, water, food, energy security, population, and urban expansion. A paradigm shift is required to adapt to global change through the implementation of a new, feasible and sustainable socio-economic model within the planetary boundaries where forests are expected to play an essential role.

Forests cover 31 percent of the earth's surface and are a vital global ecosystem: they provide important ecosystem services (*hereinafter* ES), benefits that ecosystems bring to society and improve the welfare of populations; they are a key element in mitigating climate change by sequestering carbon to build up biomass and in the process; release oxygen and evapotranspire water; generate 1m^3 of wood, trees store 1 tonne of CO_2 and release more than half a tonne of oxygen.

Furthermore, they are essential to the maintenance of life on our planet: biodiversity, water (forests provide 75% of the total freshwater volume), and soil. Approximately half of the forest area is relatively intact, with over a third being primary forest. While the net loss of forest area has decreased significantly since 1990, deforestation and forest degradation continue to occur at an alarming rate, resulting in significant loss of biodiversity[174] (FAO, 2022).

However, global figures should be interpreted correctly when focusing on specific areas. For instance, in Europe, forest area covers 37% of EU land, capturing 10% of CO2 emissions.

Catalonia is a 32.000 km^2 Mediterranean region holding a population of 7.7 million people. The most important economic sectors are industry, services, and tourism, receiving over 20 million tourists per year. Population is concentrated around the Barcelona hub and along the Mediterranean Sea coast. Even so, Catalonia is a country of forests: 65% of the Catalan territory are forests (2.1 million hectares), and 42% is wooded, forest areas constitute 30% of the Nature 2000 network, while 76% of the forest surface is private (with around 228.000 forest owners). In recent decades, the area and density of forests have increased significantly, mainly because of socioeconomic factors: agriculture, rural abandonment, and low timber prices, which are among the most representative.

Since 1990, the forested area has increased by approximately 30%, while the standing volume has doubled, resulting in a total forest area of 2.1 million hectares (65% of the total surface in the region). This creates a complex scenario for a Mediterranean region where forests provide multiple essential ecosystem services beyond timber or carbon sequestration and the effects of climate change are being felt (drought, risk of extreme forest fires).

[174] FAO and UNEP. 2020. The State of the World's Forests 2020. Forests, biodiversity and people. Rome https://doi.org/10.4060/ca8642en

Promoting the resilience of agroforest landscapes by implementing Climate-Smart Forestry

Socio-ecological resilience understood on a landscape scale, or applied to a landscape, can be defined as the ability of a landscape to sustain desired ecological functions, biodiversity, and social and economic activities over time, despite the multitude of known stressors and future uncertainties. However, to apply the concept of socio-ecological resilience to a particular region or landscape, an in-depth knowledge of the concept is necessary. This includes both historical conditions, current conditions, the change factors that have occurred, as well as potential future trends.

Recognizing the scale at which the concept should be applied is remarkable because the resilience of a landscape (regional scale) will focus on different elements and drivers of change, than when concentrating on smaller scales such as a forest stand, a stretch of river or a single agricultural enterprise (local scale).

In the case of Catalan Forest ecosystems and agroforest landscapes, their resilience derives from genetic diversity, species of fauna and flora, forest, agricultural and scrubland habitats, ecological functions necessary to sustain biodiversity in the long term, ecosystems, and socio-economic activities that ensure food sovereignty, blue water provisioning and other key ecosystems goods and services.

Current and future environmental and socioeconomic stressors include both chronic factors that have long-term effects on ecosystems and one-time events. Threats are loss and fragmentation of habitats, overexploitation of natural resources, increasing demand for bioproducts, fluctuations in the market prices of agricultural and forestry products, extreme climatic episodes (drought, floods), steady climate change (increase in temperature, erratic precipitation regime), invasive exotic species, wildfires, and diseases.

Wildfires are especially critical in South Europe. Only in 2022, over 720.000 ha burned in Southern European countries, representing 95% of the total area affected in Europe.

In Catalonia, 547 fire ignitions were reported and burned 78 fires of more than 1 ha and 2 extreme wildfires of more than 500 ha accounting for more than 6.000 ha burned. In the near future, sever fire regimes are expected in Mediterranean countries due to climate change and land uses. Current fire management policies are reaching their upper limit of application because more human and economic resources allocated to extinguishing fires do not mean a direct increase in extinguishment capacity of the fire brigades.

While weather conditions largely determine fire regimes in southern Europe, fire policies should change and aim for a reduction in the overall severity of landscape-wide fires, rather than a mere reduction in total burnt area. Emphasis should be placed on the control of vegetation (fuel), in other words the management of its spatial planning and the promotion of fire-resistant and/or fire-resilient forest types.

As in many other southern European regions, in Catalonia, the abandonment of pastures and agriculture mostly in remote, mountainous areas since the mid-20th century has led to a steady increase of the forest surface, the standing forest volume has tripled over the last 40 years, and 34% of Catalan forests are estimated to be relatively young (established after 1960). Nevertheless, the forest sector represents only 0.06% of the total gross domestic product and employs ca. 32.000 people. Forest management is rarely a profitable activity because the costs of forestry operations are relatively high, mainly due to accessibility constraints, while timber prices are low.

It is estimated that annually, forests grow ca. 2.9 million m^3 on average but, only 30% of this annual growth is harvested. Indeed, only 10% of the annual wood consumption comes from local forests and most of the Catalan wood transforming industries are based on low-added value forest products. The use of wood for energy (stella, pellet, and firewood) is gaining relevance in the Catalan bioenergy market and the apparent consumption in 2020 was over 0.4 million tonnes.

Catalonian forests provide multiple ecosystem services in the Mediterranean, as well as conditions for global change. However, over the last 25 years, the capacity of forests to capture carbon has decreased by 15-20% in inland and Mediterranean forests (not in Alpine biogeographical region). Forest growth and low management rates have decreased blue water and runoff by 29%, although forest ecosystems have prevented soil erosion. The risk of extreme forest fires has never ceased to increase, and the overall health of forests could be compromised due to stressful conditions, new diseases related to world trade, or adverse weather events.

Biodiversity levels have kept in general, but some decreases are reported in mature forests and bushes ecosystems, because less openings are created. Although Catalan forests are a habitat for a rich biodiversity exemplary of Mediterranean ecosystems, its biodiversity has also experienced negative trends and in the last 20 years, native vertebrate and invertebrate populations have shrunk by an average of 25% and the loss in population numbers is more than 50% for species living in rivers, lakes and marshlands, 30% for farmland and grassland species and 10% in forests and scrubland species.

The underlying cause of biodiversity loss is a socio-economic model that leads to intensive resource extraction in some regions, while abandoning others, indeed, changes in land use are the main direct cause of biodiversity loss, although climate change and the arrival of invasive exotic species are also having an increasing impact[175] (The State of Nature in Catalonia, 2020).

To achieve the Green Deal objectives for 2030 and 2050, advanced decision support tools are being implemented and developed, to diagnose and define improved multi-objective scenarios involving multiple stakeholders in land use and landscape management (Trasobares et al., 2022).[176] The challenge therefore relies on re-thinking and upgrade the principles underlying multifunctional forest management, that by its own ensures the ecological, social, and economic values of the forest ecosystems, guaranteeing the sustainable provision of goods and services, to also consider climate

[175] Brotons, L.; Pou, N.; Herrando, S.; Bota, G.; Villero, D.; Garrabou, J.; Ordóñez, J. L.; Anton, M.; Gual, G.; Recoder, L.; Alcaraz, J.; Pla, M.; Sainz de la Maza, P.; Pont, S. and Pino, J. (2020) The State of Nature in Catalonia 2020. Catalan Ministry of Territory and Sustainability. Government of Catalonia. Barcelona.

[176] Trasobares, A.; Mola-Yudego, B.; Aquilué, N.; González-Olabarria, J.-R.; Garcia-Gonzalo, J.; García-Valdés, R.; De Cáceres, M. (2022). Nationwide climate-sensitive models for stand dynamics and forest scenario simulation, Forest Ecology and Management,505:119909. https://doi.org/10.1016/j.foreco.2021.119909.

change mitigation purposes, biodiversity conservation, and the promotion of circular bioeconomy. Over the last few years, the term Climate-Smart Forestry[177] (CSF) has been thereby introduced and constitutes an essential next step in the pursuit of sustainable forest management objectives and the forest sector's response to the threat of climate change.

The CSF concept considers not only forests and wood supply chains, but also the substitution effects of materials and energy. Thus, CSF builds on three main pillars: (1) *increasing carbon storage both in forests and wood products, while maintain the provisioning of other ecosystem services*; (2) *enhancing the health and resilience of forests by using adaptive forest management*; and (3) *using wood resources to substitute non-renewable, carbon-intensive materials.*

To implement CSF in Mediterranean regions, forest management options and silvicultural prescriptions could include, but are not limited to, adjustments to final thinning and cutting schedules (leading to additional growth and higher quality raw material while reducing fire risk), regrowth with on-site species adapted to warmer and drier environmental conditions, planting site-adapted species from other provenances, or the substitution of tree species to produce wood products with higher live spans. In fact, higher harvest levels combined with effective use of forest products means that substantial increases in the production of long-lived wood products could significantly contribute to climate change mitigation, circular bioeconomy, and the provision of multiple ecosystem services, compared to reducing harvest levels with the exclusive aim of increasing forest carbon stocks. During their service life, long-living wood products act as carbon pools, and after it, they can substitute emission-intensive fossil fuels if converted to biomass for energy, or even functionally substitute other non-renewable products and materials.

Advanced modelling and decision-support tools are being implemented and developed, to first diagnose the current state of the forests and the provision of ecosystem services, but importantly, to co-design and project climate-smart multi-objective forest landscape scenarios involving multiple stakeholders. Scenarios and assessments of ecosystem services arising from these approaches provide the basis for discussing the territorial implementation of forest policies consistent with the principles of the CSF and the Catalan Bioeconomy Strategy 2030 (hereinafter EBC2030) objectives.

In turn, multi-criteria optimization tools allow depicting the trade-offs between different ecosystem services and ease agreements between different stakeholders to solve controversial situations. These evaluations are necessary to reward carbon sequestration and establish a payment system for ecosystem services, complementing traditional forestry revenue flows by internalizing forest externalities in the economy.

Towards the achievement of Green Deal objectives: Circular bioeconomy and payment for ecosystem services

The scientific scenarios derived from this can be used for: the territorial implementation of forest policies and the recently approved EBC2030 and to reward carbon sequestration and other key ES, thus complementing traditional forestry revenue flows (payments for ES).

[177] https://blog.efi.int/adapting-forests-to-the-new-normal/

In 2021, the Catalan Government approved the EBC2030, under the auspices of the Ministry of Climate Action, Food and Rural Agenda, the roadmap for the transition to an economic model based on the optimal use of renewable biological resources that are not currently being used to ultimately, create products with greater added value. Its main goal is to promote the sustainable development of the Catalan economy by promoting the production of local renewable biological resources.

This provides new life for forest, agri-food and marine products and ensures the sustainable delivery of ecosystem services to move towards a circular bioeconomy, taking into account the pressing need for adaptation and mitigation in the face of the climate emergency. EBC2030 will make it possible to improve the competitiveness and sustainability of the first sector, by creating jobs, connecting actors from very distant sectors and boosting the generation of knowledge as an engine of change. To achieve these goals, research and innovation are playing a fundamental role in helping to generate new proposals that allow this transition to be carried out efficiently and sustainably.

The Action Plan for the period 2021-2023 of the EBC2030 is structured around seven strategic objectives that will serve to give a new boost to the bioeconomy in Catalonia. Four of them are tightly linked to the generation of economic activity: (1) *improve the use of Catalonia's biomass through the characterization, quantification, optimization of management and distribution*; (2) *develop a business fabric based on the circular bioeconomy throughout the territory, with special attention to the first sector*; (3) *promote the use and consumption of bioproducts, bioenergy and biomaterials in the market*; and (4) *promote resilient agroforest landscapes and the sustainable provision of multiple ecosystem services in the context of the Catalan circular bioeconomy.*

In conclusion, to address nature under current pressures in a period of growing risks due to climate change and natural disturbances, changes in socio-economic and territorial models and improvement approaches for policy making must be implemented.

Regarding the socio-economic changes: (1) promote multiple ES provision and resilience of agroforest landscapes for Green Deal implementation requires efficient mechanisms and policy approaches; (2) integrate and coordinate the various policy frameworks (Bioeconomy strategy, Forest strategy, Biodiversity strategy, Farm to Fork, LULUCF, CAP, among others); (3) EC proposed new targets[178] which require that the entire EU LULUCF sector would need to remove approximately an additional 100 Mt CO2eq./yr. by 2035 and 170 Mt CO2eq./yr. by 2050.

In relation to the improvement of approaches for policy making, in various EU regions, support on sustainable management is more required than planting trees. In this sense, (1) *multi-objective territorial management planning and CSF provide the basis for combining mitigation and adaptation measures by identifying trade-offs between ES*; (2) *landscape level offers high potential for policy making territorial implementation* (environmental, social, economic, legal factors and main stakeholders involved); (3) *potential of financial-policy making mechanisms incentivizing bioeconomy implementation and resilience, biodiversity enhancement, by complementing forest owners/managers revenues related to market values with PES.*

[178] https://blog.efi.int/adapting-forests-to-the-new-normal/

Germany – Office of Technology Assessment at the German Bundestag (TAB)

What is it about

Germany is one of the most densely forested countries in Europe, with approximately 30% of its land covered by forest. However, the Germans' relationship with the forest goes much deeper than this figure can express. At least since the Romantic period, i.e. from about the end of the 18th century, forests have played a prominent role in German poetry and painting and have been an important part of the national cultural identity ever since. Germany is also the country where modern forestry science was founded: in 1734/35, the first forestry education was established at the University of Jena[179] , 21 years after the Freiberg chief miner Hans Carl von Carlowitz published the work »Sylvicultura oeconomica«. It is considered the first standard work on forestry and the origin of the concept of sustainability.

Von Carlowitz developed the idea of sustainable forestry use when he observed the then completely unregulated deforestation in his native region of Saxony, triggered by an energy crisis and the strong demand for wood. Largely deforested landscapes were quite typical of Germany around 1800. Climatic conditions also played a role, as Central Europe was characterized by a relatively cool climate from the 15th to the 19th century (Little Ice Age), which resulted in an increased demand for firewood. From around the middle of the 19th century, large areas were afforested with fast-growing spruce and pine stands, mainly for economic reasons. The changeable history of the German forest thus reflects in an almost typical way the interplay of (over)use and protection, as is known for many natural areas worldwide today.

Currently, forest ecosystems in Germany are once again facing a major challenge: The extreme drought years since 2018, together with storms and bark beetle infestations, have led to the death of numerous forest stands. In spruce, beech and oak, three of the main tree species, more than 40% of the trees show significant crown thinning and are thus considered severely damaged. Only every fifth tree is still considered healthy.[180] The ongoing climate change as one of the main drivers of this development threatens to lead to a further deterioration of the forest condition in the future and, in the long term, to a complete destabilization of the current forest ecosystems if they do not become more resilient to climate changes. That this can only be achieved by converting coniferous forest monocultures to more natural mixed forests is beyond question, both politically and socially. However, in view of the different utilization interests as well as the exorbitant costs caused by forest conversion, the ways of implementation are more controversial than ever.

[179] https://www.forstwirtschaft-in-deutschland.de/aktuelles/news-detailansicht/news/thueringen-ist-geburtsland-der-modernen-forstwissenschaft/

[180] https://tiwo-wze.shinyapps.io/WZE_app/

Ongoing debate

In Germany, a gradual forest conversion from monotonous, unnatural coniferous forests to diversely structured mixed forests has already been taking place for several decades. In the management of forests, a new paradigm has prevailed since the 1980s, especially in the western German states, which is referred to as »permanent forestry« (Dauerwald). This largely avoids clear-cutting, instead only single targeted trees are felled and classical forest protection measures are kept to a minimum. As a result, the share of hardwood increased from 34% in 1990 to 55% in 2012 (BMEL 2018). Nevertheless, it should be noted that permanent forest management is not yet consistently implemented on a large scale and has become established mainly in those forests that are publicly owned. However, this only affects about half of the forest. The rest belongs to private forest owners who either have a strong economic interest in wood utilization (in the case of larger forest enterprises) or hardly any financial means to actively promote forest conversion. These include, for example, most small forest owners, who have less than 20 ha of forest, but still account for 50% of the private forest. As a result, large areas of Germany are still characterized by particularly endangered monotonous coniferous forests, which are in urgent need of forest conversion in Germany. According to calculations by the Thünen Institute of Forest Ecosystems, this includes 2.2 million ha of spruce forests, plus about 400,000 ha of damaged areas that currently need to be reforested (Bolte et al. 2021). In order to cope with forest conversion by about 2050, almost 100,000 ha of forest would have to be adapted annually (UBA 2019).

In view of this enormous challenge, an intensive and extremely controversial debate has flared up in Germany about the best measures to be taken to adapt forests to climate change (Popkin 2021). At its core is the question of the extent to which commercial forest use and active forest management, especially reforestation of damaged areas with non-native climate-resilient tree species, among others, should be permitted. Nature conservation associations and ecologists in particular are calling for a fundamental paradigm shift in this regard, arguing that the forest, as a natural ecosystem, can only develop its self-regulatory powers if it is largely left on its own. German forestry as a whole is accused of serious mistakes, and is even considered to be a major part of the problem (Knapp et al. 2021). It is demanded to withdraw up to 30% of the forest area from any use. Forestry companies and forestry associations oppose this and point out – supported by parts of the scientific community – that natural processes cannot keep up with the speed of climate change and that human intervention is therefore urgently needed to preserve forests in the long term. Reference is also made to the climate policy significance of the renewable raw material wood, which is to be used increasingly in the future as a building and other material to replace cement, which is more harmful to the climate. Another important, but somewhat separate interest group is the influential hunting associations, which are often still opposed to more intensive hunting of the enormous and growing game populations in many places. However, this would be urgently needed, since the heavy browsing massively hinders the natural regeneration of the forest stands.

The positions seem to be largely irreconcilable, and increasingly the debate is sliding into a political dispute that makes it difficult to engage in a factual discussion (DVFFA 2019). The reasons for this are not only scientific uncertainties overlaid by fundamentally divergent interests and goals, but also the complex regulatory situation in Germany. Due to the federal system, responsibilities are distributed in a complicated manner between the federal government, federal states, and local governments, making it difficult to uniformly manage forest restructuring and balance the various interests. Primary competencies in regulating hunting as well as forest management lie with the federal states, while the federal government is only responsible for the general regulatory framework.

One of the few decisive areas of federal forest policy action relates to financial support for forestry, which has moved to the center of the forestry debate. One of the central controversial issues is which funding concepts can be used to provide forest owners with meaningful support for the reforestation of damaged areas and forest conversion. In response to the immense forest damage, the last federal government still held a national forest summit in 2019, at which the federal and state governments discussed suitable aid with the participation of scientific experts and forestry stakeholders. The result was the largest aid package for the German forestry sector to date, comprising around 1.5 billion euros. This included 500 million euros for the conservation and sustainable management of forests in the form of an area-based one-off payment. The current German government has announced a new funding concept designed to provide targeted support for ecosystem services in the forest, but is also linked to specific conditions. For example, clear-cutting is prohibited, predominantly native tree species must be planted during reforestation, and large forests are to be given space for natural forest development.[181] The program is endowed with 200 million euros per year (a total of 900 million euros until 2026), but the forestry associations consider this to be too low; they also criticize in particular the obligation to set aside forest areas. In view of the estimated financial requirements for forest conversion, which are put at around 1.4 billion euros per year (Bolte et al. 2021), this sum is indeed likely to be only a first small step – so there is no end in sight to the forestry debate in Germany for the foreseeable future.

Role of TA in the debates

At first glance, it may seem somewhat unusual that TA is being asked at all in the context of climate change-induced forest restructuring – where technological aspects may not be in the foreground. But most certainly TA can and should play a stronger role even in these intensive discourses conducted here, which is not yet the case in Germany. For the time being, however, it would be important to have a precise contextual problem orientation: Are the »right« questions actually being asked in the discourses on »forest conversion«, which often go something like this: »Which measures, including innovative ones, can we use to best convert the forests in a climate-sensitive manner«? Or don't such questions rather miss the (actual) problem? After all, the »ongoing exceptional situation« of rapid and massive climate change, together with other social and technological disruptive developments, belongs to the complex of »global change« in which our socio-ecological systems are undergoing very far-reaching, very rapid and irreversible changes. The above questions about saving or shaping forests imply seemingly correct (and ethically valuable) points of orienta-

[181] https://www.bmel.de/SharedDocs/Pressemitteilungen/DE/2022/93-wald-foerderprogramm.html

tion, as if it were doubtlessly and without exception in human power (or science) to preserve or restore something, moreover often with the (rather unreflective) claim to be able to steer and, if necessary, save in a scientifically sound manner.

However, it is highly probable that not only the (vast majority of) human livelihoods and lifestyles, but also the forests we have known up to now are undergoing a fundamental transformation. However, what follows from this does not seem to have been fully understood, neither in forest science, nor in practical forest management, nor in the administrations and (nature conservation) associations. Admittedly, the increasing climate change is perceived as a major cut in the way forests have been managed up to now, and massive countermeasures are demanded; but how exactly new adaptation strategies could work, with which trees and which processes the forests are to be »converted«, is often disputed and unclear. Awareness of the fact that we are dealing with a fundamental (and possibly unsolvable) uncertainty about the future, including a loss of effectiveness of the hitherto established (and functioning) scientific tools, methods and procedures – ultimately even a disruption of our established world views – is only very slowly penetrating the consciousness of forest practitioners, scientists and politicians (Bauhus 2021).

How realistic is or would be the (realization of the) ideal of being able to manage the complex forest ecosystems in a planned manner based on the ethical principle of sustainability in the long term and in a way that preserves the forests? In the acute reality (and practice) it seems to be rather the case that the (silvicultural) sustainability of forests must rather be seen against the background of deep problems of knowledge and decision-making. Silvicultural strategies are ultimately closely tied to permanent regularities given by the environment. All of this has made and will make forests »a conglomerate of the planned and the unforeseen, the expected and the accidental«, much more so than the »inventors« of sustainability strategies might like (Bauhus 2021, p. 35). There is much to suggest that disruptions such as those of climate change run counter to the frequently postulated claim that the climate-resilient and climate-adapted transformation of forests can be effectively managed in a targeted manner. It seems more sensible to consider natural uncontrolled succession processes more strongly in forest conversion strategies (Böhmer 2022; Ibisch 2021). In view of the high degree of environmental complexity and the lack of knowledge for action, the approach to forest ecosystems, which has so far been characterized by planning and action optimism, may have to be adapted and forest science and management may also have to undergo a fundamental transformation.

For TA, this means, as a consequence, to understand and accompany this transformation under the conditions of ignorance and uncertainty in an innovative and conceptual way, and to do so with the help of experimentation, but also by fostering self-regulating mechanisms as well as the initiation and promotion of new learning behavior. The concept of real-world labs (Wagner/Grunwald 2015), which is also being tested in initial approaches in the forest,[182] represents an interesting example of transformation approaches that may succeed in this situation and are also participatory. Real-word labs are implemented in a specific, spatial and temporal configuration and must take into account

[182] https://www.waldlabor.ch/vision

both the socio-cultural and political contexts – e.g. the infrastructures of the region and its landscape (including the associated) forests, but also deal with the specifics of the lifeworld practices up to the economic performance of the region/location.

If, for example, projects for climate-sensitive adaptation and development of forest ecosystems are to succeed in the sense of providing services of general interest for as many social groups as possible, substantial cooperation between the stakeholders involved is a necessary prerequisite for achieving the goals. The private and state forest owners, the forest administrations and enterprises, as well as the foresters and hunters have to work out jointly supported solutions. This will most likely require a comprehensive change in mentalities and ways of thinking, for example in forestry practice, education and consulting. The purely use-oriented perspective on forests would have to be expanded to include aspects of community-based forest management in order to safeguard and develop the diverse functions of forests. Accordingly, the financial aspects (remuneration, support, compensation) – for example, for forest owners and municipalities, which fulfill their responsibility for the future of forests in a special way – would also have to be aligned with this public welfare (BfN 2020).

With its expertise in evaluating new innovations (e.g. satellite-based monitoring), but above all its many years of experience in shaping participatory processes, TA can and should contribute to designing approaches to a climate robust development of forest stands supported by a broad social consensus. On the basis of regionally differentiated analyses, local adaptation problems should be identified and brought together with the knowledge of local forestry experts. In further steps, guidelines for cooperation would have to be agreed upon in order to consolidate capacity building and confidence building, and ultimately to ensure a lasting and shared »system view« and transformative knowledge to guide action (Hahne 2021).

It is clear that near-natural forest conversion is an extremely complex field of action that encompasses many conflicting goals (nature conservation and species protection, climate protection and adaptation, sustainable use of raw materials, etc.), various levels of action and options for measures, and requires a long-term, strategic approach. Some of these aspects are addressed in TAB's ongoing TA project »Near-natural forest conversion in times of climate change« (duration 2021 to 2023).[183] For example, the forestry, technical, economic and socio-cultural aspects of near-natural forest conversion, including regulatory control and participatory involvement options, are being analyzed and political options for action derived for members of the German Bundestag.

References

Bauhus, J. (2021): Optionen für die Anpassung unserer Wälder an den Klimawandel. In: Höltermann, A. (Hg.): Sind unsere Wälder noch zu retten? Eine Tagung zur Zukunft unserer Wälder. BfN-Skripten 600. Bonn-Bad Godesberg, S. 11-24

[183] https://www.tab-beim-bundestag.de/english/projects_near-natural-forest-conversion-in-times-of-climate-change.php

BfN (Bundesamt für Naturschutz) (Hg.) (2020): Wälder im Klimawandel: Steigerung von Anpassungsfähigkeit und Resilienz durch mehr Vielfalt und Heterogenität. Ein Positionspapier des BfN, Bonn-Bad Godesberg

Böhmer, H.J. (2022): Beim nächsten Wald wird alles anders. Das Ökosystem verstehen. Stuttgart

Bolte, A.; Höhl, M.; Hennig, P. et al. (2021). Zukunftsaufgabe Waldanpassung. AFZ-DerWald 4. S. 12-16

BMEL (Bundesministerium für Ernährung und Landwirtschaft) (2018). Der Wald in Deutschland. Ausgewählte Ergebnisse der dritten Bundeswaldinventur

DVFFA (Deutscher Verband Forstlicher Forschungsanstalten) (2019): Anpassung der Wälder an den Klimawandel Positionspapier des Deutschen Verbandes Forstlicher Forschungsanstalten (DVFFA)

Hahne, U. (2021): Interventionen in Prozessen der Stadt- und Regionalentwicklung. Anmerkungen zum Format Reallabore der Nachhaltigkeit aus planungswissenschaftlicher Sicht. https://doi.org/10.14512/rur.54

Ibisch, P.L. (2021): Plädoyer für einen ökosystembasierten Umgang mit der Waldkrise. In: Höltermann, A. (Hg.): Sind unsere Wälder noch zu retten? Eine Tagung zur Zukunft unserer Wälder. BfN-Skripten 600. Bonn-Bad Godesberg, S. 6-10

Knapp, H.; Klaus, S.; Fähser, L. (Hg.) (2021): Der Holzweg. Wald im Widerstreit der Interessen. Gesellschaft für Ökologische Kommunikation mbH, München

Popkin, G. (2021): Forest fight. In: Science (New York, N.Y.) 374(6572), S. 1184-1189

UBA (Umweltbundesamt) (2019). Monitoringbericht 2019 zur Deutschen Anpassungsstrategie an den Klimawandel. https://www.umweltbundesamt.de/sites/default/files/medien/1410/publikationen/das_monitoringbericht_2019_barrierefrei.pdf.

Wagner, F.; Grunwald, A. (2015): Reallabore als Forschungs- und Transformationsinstrument. In: GAIA 24 (1), S. 26-31

Greece – Greek Permanent Committee on Research and Technology (GPCRT)

Forests under pressure

Mediterranean ecosystems provide particular habitat and climate conditions due to seasonality between winter and summer. In these environments and at different scales of intensity and recurrence, fire has been present as a modifying agent of vegetal landscapes.[184] The damages and effects of fire on ecosystems is diverse and there are references to alterations in the composition of species, in the roots of trees and soil, and in the properties of water infiltration after fire. In addition, under current climate change, it is expected that extreme rainfall events may accelerate soil erosion in burnt areas. In this context, post-fire management strategies are crucial to implement as soon as possible after the event as they aim to reduce the magnitude of the impact generated by forest fires.[185]

Greece is characterized by rich biodiversity and forests are a precious ecological nest. More than 6200 endemic flora species[186] and 23130 fauna species[187] live and reproduce here, directly affected by forest degradation. Forests, other than their important ecological value, are also a financial resource, as many activities depend on them.[188] The main forest exploitation activities in Greece[189] are wood and non-wood production, like resin, honey, wild plants, livestock etc., also affected significantly. Additionally, attention is given to the social uses like recreation and hunting.

The Forestry Service is the main agency for the development, protection and management of the country's public forests, the forestry policy and forestry technical supervision and surveillance of non-public forests. It operates under the supervision of the General Secretariat of Forests of the

[184] Plaza A., Castillo M., Naulin P., Seed and seedling interactions in three tree species from Mediterranean forests as a knowledge base for ecological restoration, Journal of Environmental Management 316 (2022) 115241.

[185] Gonzalez-Romero J., Lopez-Vicente M., Gomez-Sanchez E., Pena-Molina E, Galletero P., Plaza-Alvarez P., Fajardo-Cantos A., Moya D., De las Heras J., Lucas-Borja M.E., Post-fire management effects on hillslope-stream sediment connectivity in a Mediterranean forest ecosystem, Journal of Environmental Management 316 (2022) 115212.

[186] Koulelis P., Solomou A., Fassouli V., Sustainability Constraints in Greece. Focusing on Forest Management and Biodiversity, 9th International Conference on Information and Communication Technologies in Agriculture, Thessaloniki 2020, Legakis, A. (2010) Threatened, Protected and Endemic species of Greece, zoological museum, department of biology, University of Athens., Georgiou, K. and Delipetrou, P. (2011) CHLORIS database: Endemic, Threatened and Protected plants of Greece, University of Athens.

[187] Legakis, A. and Maragkou, P. (2009) The Red Book of Endangered Animals of Greece, Hellenic Zoological Society, Athens, p. 528.

[188] Sargentis G.-F, Ioannidis R., Bairaktaris I., Frangedaki E., Dimitriadis P , Iliopoulou T., Koutsoyiannis D. and Lagaros N., Wildfires vs. Sustainable Forest Partitioning, Conservation 2022, 2, 195–218.

[189] Spanos, I., Meliadis, I., Platis, P., Mantzanas, K., Samara, T., Meliadis, M. (2015) Forest Land Ownership Change in Greece. COST Action FP1201 FACESMAP Country Report, European Forest Institute Central-East and South-East European Regional Office, Vienna. 31 pages. [Online publication].

Ministry of Environment and Energy. The main objective is the protection, promotion and development of forest ecosystems, so that forests become truly sustainable by applying modern scientific knowledge and technological achievements in protection and management.

Reforestation –drone seeding as a promising innovation

Though several large wildfires have occurred worldwide in recent years and humanity may seem defenseless against future natural hazards that are beyond mitigation, technological innovations give space and hope for improvement in forest management practices and policies.

Anti-erosion protection and reforestation of disturbed forest areas, especially after forest fires, is more than necessary especially in sensitive ecosystems and landforms. Traditional methods are enhanced by new ones resulting in a more effective and faster restoration of the affected land. Areas that present strong morphological gradients and a geological background that favors erosion, need soil protection with anti-erosion plant species as their reforestation is considered a necessary procedure for the sustainability and preservation of the ecosystems and a moral obligation towards the environment for the next generations.

However, the tens of thousands of hectares of burned land cannot be reforested and anti-erosion measures cannot be implemented in a short period of time. Unmanned aerial vehicles (drones) come to provide a solution. Drones are rapidly evolving with new flight capabilities and flexibility so that they are able to »*sow*« dozens of seeds of anti-corrosive plants and seeds of forest regeneration species on a daily basis, covering, in a short time, very large areas, as well as areas which are particularly difficult to access.

The project »*Study of the Adjacent Environment and Characteristics of the Selected Areas for Drone Seeding*«[190] aims at reforestation and anti-erosion protection of disturbed forest areas, especially after forest fires. This pilot project and its outcomes, along with a series of similar public-private partnership programs regarding environmental management and pioneering initiatives and technologies are expected to be examined in the forthcoming parliamentary period by the Special Permanent Committee on Research and Technology of the Hellenic Parliament.[191]

The proposed method is an innovative reforestation technique that uses drone seeding. The selected seeds and the seeding plan are crucial for the success of the project and requires advanced technologically procedures in order to achieve the set goals. The objectives of the project are:

- The reforestation of areas that have not regenerated sufficiently due to natural conditions (lack of suitable soil conditions, adverse climatic conditions, etc.) after two years since the fire.

[190] Karavitis C., Psomiadis E., Papanikolaou I, Liaros M., Misialis K., Alexiou S., Mpenou K., Stafanakis D., Karetsos G., Solomou A., Avramidou E., Paitaridou D., Fragkou S., Anti-Corrosion and Regeneration Seeds Using Unmanned Aerial Vehicles (Drone Seeding) – The project is financed by Motor Oil Hellas (MOH) which commissioned Agricultural University of Athens to study and implement it, with the assistance of UCANDRONE, the Ministry of Environment and Energy, ELGO DIMITRA and the Megara Forest Office.

[191] www.hellenicparliament.gr

- The reforestation of areas that are either extensive that manual sowing is not feasible or are inaccessible.
- The anti-corrosion protection of areas that are immediately at risk of severe corrosion and loss of soil material after the fire.

Also, several characteristics of the selected areas will be identified with a simultaneous assessment of the positions in terms of the prevailing conditions (including climatic and hydrological-hydrographic conditions), topography, soil, geological- geomorphological features, possible difficulties or obstacles (pastures or similar socio-economic issues, etc.).

The selection of these areas was carried out by assessing the following factors:

- The need for reforestation (e.g. if there is natural regeneration in progress).
- The suitable conditions for reforestation.
- Types of plants that should be selected and the availability of suitable seeds.
- The reforestation method to be preferred (in relation to probability of success, cost, etc.).
- The proper preparation of the seeds (in a capsule or in pellets).
- Design and construction of the seeding unit that will be integrated into the drone.
- The schedule of reforestation.
- The maintenance measures during the first stages.

After the assessment, two areas were selected, the first one for seeding due to lack of natural regeneration and the second one for anti-corrosion seeding due to the special conditions presented with steep slopes and particularly erosive geological background (marls).

Drone seeding is an innovative process of reforestation and anti-corrosion protection for the Greek area and its success will create a new technological breakthrough, both for the environment and the restoration of the ecosystem, as well as for humans. There are certainly areas that planting by hand is absolutely the right approach, but, in other cases, drones can be a very effective tool for planting the right seed, at the right time, to achieve maximum protection of forest life. The nature and complexity of forest ecosystems in the Mediterranean region and in Greece indicate the necessity for robust and integrated policies, strategies, and special measures to meet with climate change challenges and sustainability.[192]

Outlook

In the next decades, increased fire risk is expected in the Mediterranean. 95% of fires are due to human activities (i.e. agricultural practices) or negligent behavior and arson. It is, therefore, necessary to increase public perception and awareness of the risks of wildfires and their impact on soil and water resources. Local communities are vital parts of forest ecosystems and they should not be excluded from decisions that play a crucial role in their existence. The participatory model should be a fixed regulation in policy planning and decision-making. A bottom-up participatory model with the

[192] »Target 6.6: By 2020, protect and restore water-related ecosystems, including mountains, forests, wetlands, rivers, aquifers and lakes.« and »Goal 15: Protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reverse land degradation and halt biodiversity loss«.

engagement of multilevel stakeholders could serve as a barometer for the quality of environmental decisions. This is the mean for achieving ambitious goals and ensuring that the planned policies are realistic enough to implement.[193]

The debate about post-fire measures benefits and shortcomings is yet open, which hinders the development of proper restoration strategies as reluctant local communities always need time to adapt and cooperate. Understanding the interactions of the different measures will definitely help to establish new forest management procedures. The use of efficient tools to properly plan and evaluate the effects of these procedures sets a path for optimizing economic and human resources.[194]

Thus, it is necessary to create an appropriate legislative framework and more flexible and timely decision-making process. There is also a need to support investments and entrepreneurs in forest sector by promoting policy measures characterized by an overall circular concept. The development of strategic interactions between scientists and policy-makers is necessary, along with the establishment of transparent procedures for the inclusion of all interested and affected parties in the management of forests. The inclusion of information and communication technologies (ICT) and the use of innovative forest monitoring tools could serve as the means to bridge the gap between scientific knowledge and forest policy.[195]

[193] Andrea V., Mediterranean forest policy beyond the Paris Climate Agreement, Land Use Policy 112 (2022) 105797

[194] Gonzalez-Romero J., Lopez-Vicente M., Gomez-Sanchez E., Pena-Molina E, Galletero P., Plaza-Alvarez P., Fajardo-Cantos A., Moya D., De las Heras J., Lucas-Borja M.E., Post-fire management effects on hillslope-stream sediment connectivity in a Mediterranean forest ecosystem, Journal of Environmental Management 316 (2022) 115212.

[195] Bocher M., Advanced approaches for a better understanding of scientific knowledge transfer in forest and forest-related policy, Bocher M., Forest Policy and Economics 114 (2020) 102165.

Japan – Research and Legislative Reference Bureau (RLRB), National Diet Library (NDL)

Marine Plastic Pollution

Yoshinori Suzuki and Hiroko Azuma

What is it about?

Surrounded by the ocean, Japan has had a serious problem with marine litter, which primarily consists of plastic waste, since around 2000. Roughly 27,000 to 55,000 tons per year[196] of marine litter was collected in Japan during the five years from FY2015 to FY2019. The damage from such large amounts of marine litter includes an increased burden on the marine environment, obstruction to vessel navigation, and losses in the fishing and tourism industries.

Recent studies have revealed the true extent of marine pollution caused by tiny plastic particles, or microplastics, and concern about adverse effects on ecosystems and human health continues to grow. Field surveys of microplastic concentrations around Japan show that the average concentration of pelagic microplastics near the ocean surface in the East Asian seas around Japan is 3.7 pieces m-3, which is significantly higher than in other waters. (Table 1) For this reason, the East Asian seas around Japan are regarded as hot spots for pelagic microplastics.[197]

Table 1 – Observed concentrations of surface microplastics

Oceans	Concentration (pieces m-3)
East Asian seas	3.70
N. Atlantic (accumulation area)	1.70
Seto Inland Sea	0.39
Arctic polar waters	0.34
Mediterranean Sea	0.15
N. Pacific	0.12

Source: Prepared by the author based on Isobe, A. et al., »Microplastics in the Southern Ocean,« Marine Pollution Bulletin, volume 114, Issue 1, 2017.1.15, p.624. https://doi.org/10.1016/j.marpolbul.2016.09.037

Plastic waste discharge and disposal in Japan

Total plastic waste discharge in Japan for 2020 was 8.22 million tons, including 3.9 million tons (47.5%) from containers and packaging, 1.57 million tons (19.1%) from electrical and electronic equipment, 730,000 tons (8.9%) from household articles, and 590,000 tons (7.1%) from building

[196] Japan N.U.S Corporation, Report on Comprehensive Examination Work on Grasping Actual Conditions of Marine Litter and its Biological Effects in FY2020, pp.III-29-III-31. (in Japanese), https://www.env.go.jp/content/900543555.pdf

[197] Isobe, A. et al., East Asian seas: A hot spot of pelagic microplastics, Marine Pollution Bulletin, volume 101, Issue 2, 2015.12.30, pp.618-623. https://doi.org/10.1016/j.marpolbul.2015.10.042

materials.[198] The plastic packaging waste discharge per capita generated in Japan in 2014 was estimated to be just over 30 kg, less than the United States but slightly more than the EU 28 and China.[199]

Plastic waste disposal methods in Japan during 2020 include material recycling[200] at 1.73 million tons[201] (21%), chemical recycling[202] at 270,000 tons (3%), energy recovery such as incineration with power generation at 5.09 million tons (62%), simple incineration at 660,000 tons (8%), and landfill at 470,000 tons (6%).[203] Due to the country's small land area and shortage of landfill sites, waste in Japan is commonly disposed of by incineration. For this reason, plastic waste is often disposed of by energy recovery.

Japan formerly exported large amounts of plastic waste to China and other foreign countries. But since the 2017 tightening of restrictions on plastic waste imports in China as well as similar restrictions on plastic waste import elsewhere worldwide, export volumes of plastic waste have dropped significantly in recent years.[204] This has led to a rapid increase in the amount of plastic waste sent for disposal in Japan. As a result, a lot of untreated plastic waste is temporarily accumulated in Japan.

Recent measures against plastic waste

(a) Resource Circulation Strategy for Plastics

Given the situation, the Japanese government formulated a *Resource Circulation Strategy for Plastics*[205] in May 2019 to promote plastic resource circulation in Japan.

The strategy sets forth the basic principles such as 3R+Renewable, which comprises (1) reducing single-use plastic containers and products, (2) promoting alternatives to plastics such as recycled materials and renewable resources (e.g., paper, biomass plastics), (3) using plastic products for as long as possible, and (4) thoroughly sorting and collecting used plastic products and utilizing them effectively (reusing or recycling them if possible, or if not, incinerating them for energy recovery).

[198] Plastic Waste Management Institute, Material flow diagram of the status of production, discharge, disposal and recovery of plastic products 2020, 2021.12, p.4. (in Japanese) https://www.pwmi.or.jp/pdf/panf2.pdf

[199] UNEP, SINGLE-USE PLASTICS: A Roadmap for Sustainability, 2018, p.5. https://wedocs.unep.org/bitstream/handle/20.500.11822/25496/singleUsePlastic_sustainability.pdf?sequence=1&isAllowed=y

[200] Material recycling is a technology to process plastic waste into pellets and flakes, which are then used as raw materials to make other plastic products.

[201] Of this amount, 740,000 tons (42.7%) is exported overseas, 620,000 tons (35.8%) is processed into pellets, flakes, and other materials for export, and only 370,000 tons (21.4%) is recycled domestically. See note (3) above, p. 5.

[202] Chemical recycling is a technology that chemically breaks down plastic waste and reuses it as raw materials for chemicals.

[203] See note (3) above, pp. 2-3, 11.

[204] From 2010 to 2016, Japan exported 1.5–1.7 million tons of plastic waste per year, which decreased to about 600,000 tons in 2021. Trade Map – International Trade Statistics (Database). https://www.trademap.org/tradestat/index.aspx

[205] Consumer Affairs Agency, et al., Resource Circulation Strategy for Plastics, 31 May 2019. Ministry of the Environment website (in Japanese) https://www.env.go.jp/content/900513722.pdf

The strategy also establishes six milestones to be achieved in the future. (Table 2) This strategy includes specific measures such as mandatory charging for plastic shopping bags and thorough reduction of microbeads usage.

Table 2 – Milestones in the Resource Circulation Strategy for Plastics

Reduce
1. Cumulative 25% reduction in single-use plastics emissions by 2030
Reuse/Recycle
2. Reusable or recyclable design for all plastic containers and packaging by 2025
3. 60% rate of recycling for plastic containers and packaging by 2030
4. 100% effective utilization of all used plastics (reusing or recycling them if possible, or if not, combusting them for energy recovery) by 2035
Use of recycled material/biomass plastic
5. Doubling the use of recycled plastic by 2030
6. Introducing about 2 million tons of biomass plastic by 2030

Source: Prepared by the author based on *Summary of the Resource Circulation Strategy for Plastics*, 2019.5.31. Ministry of the Environment website (in Japanese) https://www.env.go.jp/content/900513721.pdf

(b) Mandatory charging for plastic shopping bags

Based on the Resource Circulation Strategy for Plastics, mandatory charging for plastic shopping bags started in July 2020. Specific details of the charging system include: (1) retailers using plastic shopping bags are subject to the system, (2) plastic shopping bags with handles are charged, and (3) plastic shopping bags that are more than 50 μm thick, 100% marine biodegradable plastic, or more than 25% biomass material are exempt, and (4) the price is set by the retailers themselves.

Although some customers complained about the system at first, it has been evaluated as effective to a certain extent, as the percentage of shoppers who requested no plastic bags increased from 57.21% in March 2020 to 80.26% in March 2022 at supermarkets[206] and from 28.3% in March–June 2020 to 74.6% in July 2020–February 2021 at convenience stores.[207]

(c) The Plastic Resource Circulation Act

In Japan, the Plastic Resource Circulation Act (Act No. 60 of 2021), which includes measures to promote circulation of plastics by all stakeholders involved in whole lifecycle of plastics, from designing products to disposing plastic waste, was enacted in June 2021 and took effect April 2022.

Based on the Act, measures have been established at each stage of (1) design and manufacturing, (2) sales and provision, and (3) discharge, collection, and recycling. The main measures of the Act include: (1) developing guidelines for Design for the Environment for manufacturers and establishing

[206] Environmental Initiatives of the Japan Chain Stores Association, Japan Chain Stores Association website (in Japanese) https://www.jcsa.gr.jp/topics/environment/approach.html

[207] Efforts to Reduce Plastic Bags, Japan Franchise Association website (in Japanese) https://www.jfa-fc.or.jp/particle/497.html

a mechanism to certify products designed in accordance with the guidelines, (2) requiring retailers and service providers to set targets for reducing single-use plastics and take action such as reviewing the provision method, (3) promoting separation, collection and recycling of plastic waste by municipalities, voluntary collection and recycling of used products by manufacturers and retailers, and waste reduction and recycling by plastic waste generators. The main measures of the Act encourage voluntary efforts by businesses and regulations on their activities under the Act are not strict.

The measures at the sales and provision stage require retailers and service providers that provide 12 single-use plastic products[208] free of charge to set targets for reducing these products and take actions to achieve the targets. Retailers and service providers themselves are required to choose ways to reduce single-use plastic products from a list proposed by the government, such as charging for the items, grant benefits to those who decline the items, use thinner and lighter products, or use products made with alternative materials. At present, concerns about losing customers have resulted in few businesses charging for the items, while many others have chosen to use thinner and lighter products or to use products made with alternative materials.

Discussion of plastic waste management

(a) Basic policy for Promotion of Plastic Resource Circulation

As mentioned above, the Japanese government has set forth the basic principle of 3R + Renewable as well as six milestones for the promotion of plastic resource circulation. Criticism of this approach includes (1) the government assumes mass plastic production and disposal without taking steps to drastically reduce excessive plastic production, (2) rapid expansion of production of alternative materials may have adverse effects on the environment and society, such as environmental destruction due to land use change and competition with food, and (3) the criteria for »when recycling is difficult«[209] are unclear, which may lead to continued easy promotion of energy recovery that goes against climate change countermeasures.

(b) Regulation of single-use plastic products

Some have questioned the effectiveness of regulation of single-use plastic products under the Act, since the number of items subject to its regulation is limited and enforcement of the regulation is left largely to voluntary efforts of businesses. Some environmental groups call for more extensive and stronger regulations, such as requiring that not only 12 items but also plastic containers and packaging, such as Styrofoam food trays and plastic packaging for vegetables and fruits, either be subject to mandatory charging or prohibited from use.[210]

[208] Plastic forks, spoons, table knives, muddlers, drinking straws, hairbrushes, combs, razors, shower caps, toothbrushes, clothes hangers, and clothing covers.

[209] As mentioned above, the basic principle of 3R + Renewable requires that used plastic products are reused or recycled if possible, or if not, incinerated for energy recovery.

[210] NGO Network for Realizing a Plastic-Reducing Society, Joint Proposal for the Government Ordinance on the Plastic Resource Circulation Act 2022.1.14. (in Japanese)

Role of TA in the debates

The Research and Legislative Reference Bureau (RLRB) of the National Diet Library, Japan (NDL) publishes a journal entitled *The Reference* with content that is intended to support Diet deliberations. *The Reference* is provided directly to Diet members and is also publicly available on the NDL website. The February 2020 issue features content on marine plastic litter, including the results of international and domestic studies on the actual state and effects of marine plastic pollution as well as the current status of measures taken by some countries. This special issue comprises the following three papers: »Current Status of and Countermeasures for Marine Plastic Pollution,«[211] »Overview of Municipal Solid Waste Management and Current Status of Single-use Plastics Regulation in the United States,«[212] and »Trends of International Trade in Waste Plastics.«[213]

As previously mentioned, Japan has initiated a variety of measures, such as reducing the amount of single-use plastic products, promoting the use of alternatives to plastics, promoting the re-use of plastic products, and regulating single-use plastic products, but addressing the issue of marine plastic pollution will require further scientific research and technological development.[214] Plastic products have been available worldwide for a long time, and as waste plastics entered the oceans, microplastics appeared in oceans around the world. In addition to preventing further influx of plastic waste into the oceans, we must survey both the effects of plastic waste on the marine ecosystem and the volumes of plastic waste accumulated in the deep sea as well as further develop technology for marine biodegradable plastic.

According to an opinion survey on environmental issues conducted by the Cabinet Office in August 2019,[215] 89% of the general public are concerned about marine plastic pollution. People have also shown willingness to embrace measures that contribute to not exacerbating the problem, carrying reusable bags so as not to use plastic bags whenever possible, not dumping waste illegally, and sorting waste correctly according to recycling rules.

Since plastic products are indispensable in our social lives, a wide range of discussions to build a social consensus to address the issue of marine plastic pollution are necessary, therefore the role of TA becomes important.

[211] Yoshinori Suzuki, »Current Status of and Countermeasures for Marine Plastic Pollution,« The Reference, vol.70 no.2, February, 2020, pp.3-28. (in Japanese) https://dl.ndl.go.jp/info:ndljp/pid/11451656

[212] Satoshi Iwasawa, »Overview of Municipal Solid Waste Management and Current Status of Single-use Plastics Regulation in the United States,« The Reference, vol.70 no.2, February, 2020, pp.29-59. (in Japanese) https://dl.ndl.go.jp/info:ndljp/pid/11451657

[213] Masahiro Endo, »Trends of International Trade in Waste Plastics,« The Reference, vol.70 no.2, February, 2020, pp.61-72. (in Japanese) https://dl.ndl.go.jp/info:ndljp/pid/11451658

[214] Ryota Nakajima, »Efforts for Deep-sea Plastic Research at the Japan Agency for Marine-Earth Science and Technology (JAMSTEC),« Kanrin, vol.102, May, 2020, pp.6-9. (in Japanese)

[215] Overview of the opinion survey on environmental issues, The Cabinet Office Website (in Japanese) https://survey.gov-online.go.jp/r01/r01-kankyou/gairyaku.pdf

Switzerland – Foundation for Technology Assessment (TA-SWISS)

Negative Emission Technologies

Bénédicte Bonnet-Eymard

What is it about?

Climate change is a s symptom of the increase of greenhouse gas (GHG) emissions, mainly carbon dioxide (CO_2), in our atmosphere. As stated in the 6th Intergovernmental Panel on Climate Change (IPCC) report, climate change is unequivocal human induced and the scale of the recent changes is unprecedented over many centuries to many thousands of years.[216] The disruption of a tempered climate over thousands of years puts nature as well as human kind under pressure.

To minimize climate change and its negative consequences, Switzerland has ratified Paris Agreement's long-term temperature goal targeting a maximum of 1.5 °C global warming compared to the pre-industrial area and has committed to reach net zero GHG emissions by 2050 in 2019. The Federal Council proposed a roadmap in 2021 to achieve these objectives.[217] A ramp down of all possible emissions is planned. However, some emissions from agriculture, waste incineration or cement production are technically hard-to-abate. To offset these residual emissions, so called negative emissions technologies (NETs) can be used. These technologies can remove CO_2 from the atmosphere and store it sustainably through biological and technical processes or use it as feedstock. According to the swiss roadmap, removing the hard-to-abate emissions would eventually mean removing around 7 million metric tons of CO_2 equivalents annually from 2050 onward.[218,219,220] To achieve this, Switzerland is considering five technologies:

- CO_2 sequestration in the form of biomass by means of afforestation, forest management and wood growth with subsequent long-term wood use
- CO_2 sequestration and storage in the form of carbon via soil management as humus or plant carbon
- CO_2 capture from biomass flue gas with subsequent storage (BECCS)
- Direct air CO_2 capture with subsequent storage (DACCS)
- CO_2 removal from the air by accelerated weathering of rock and concrete.

These methods vary in terms of their maturity, removal process, time scale of carbon storage, storage medium, mitigation potential, cost, co-benefits, risks and governance requirements. Moreover,

[216] IPCC, Sixth Assessment Report, Groupe 1

[217] Swiss climate strategy 2050, https://www.bafu.admin.ch/bafu/en/home/topics/climate/info-specialists/emission-reduction/reduction-targets/2050-target/climate-strategy-2050.html

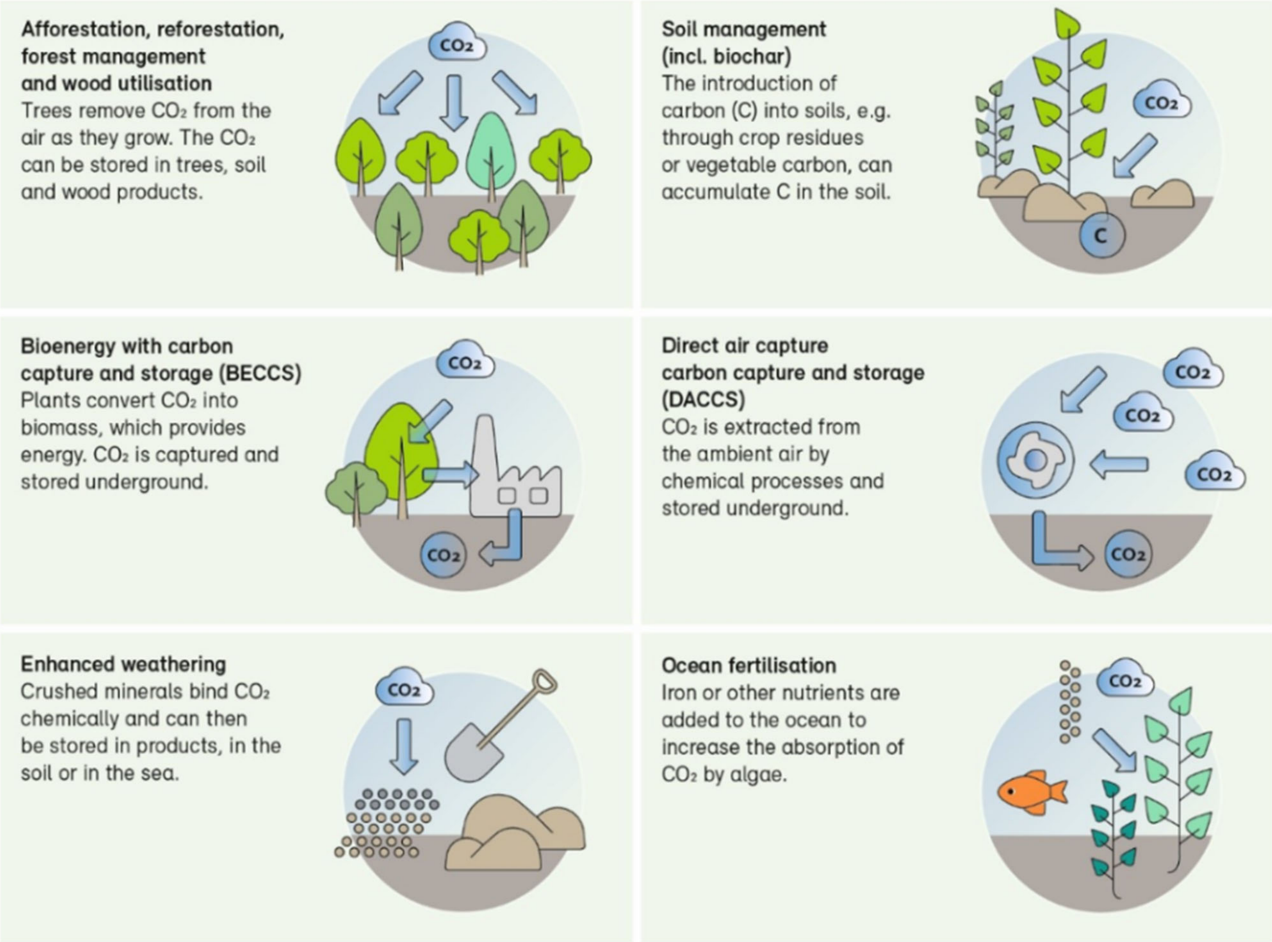
[218] In 2019, Switzerland produced greenhouse gases amounting to 46.2 million metric tons of CO2 equivalents.

[219] https://www.bafu.admin.ch/bafu/en/home/topics/climate/info-specialists/emission-reduction/negative-emissions-technologies.html (in German)

[220] In 2050, 5 million metric tons of CO2 should be avoided with carbon capture and storage (CCS) on top of the 7 million by NET.

the impacts of NETs deployment for ecosystems, biodiversity and people will be highly variable depending on the method, site-specific context, implementation and scale. The political strategies for the deployment of NETs are also still open and the role of the State, private companies and individuals remains to be discussed. Many unknowns currently remain for these technologies and they the general public has barely started debating them.

Figure 1 – Considered approaches for negative emissions in Switzerland



Afforestation, reforestation, forest management and wood utilisation
Trees remove CO_2 from the air as they grow. The CO_2 can be stored in trees, soil and wood products.

Soil management (incl. biochar)
The introduction of carbon (C) into soils, e.g. through crop residues or vegetable carbon, can accumulate C in the soil.

Bioenergy with carbon capture and storage (BECCS)
Plants convert CO_2 into biomass, which provides energy. CO_2 is captured and stored underground.

Direct air capture carbon capture and storage (DACCS)
CO_2 is extracted from the ambient air by chemical processes and stored underground.

Enhanced weathering
Crushed minerals bind CO_2 chemically and can then be stored in products, in the soil or in the sea.

Ocean fertilisation
Iron or other nutrients are added to the ocean to increase the absorption of CO_2 by algae.

Source: Federal Office for the Environment, Switzerland

Ongoing debate

Besides the specific opportunities and risks for each technology, the very concept of these negative emissions is controversial.

Their isolated role is recognized as beneficial for the climate and even necessary to achieve climate goals. And yet, their possible consequences on the motivation of each individual to reduce his or her greenhouse gas emissions and on the policies chosen are decried: first, at the psychological level, these technologies constitute according to some a demotivation to reduce emissions and may lead to a real decrease in emissions reduction: »If technologies can offset my footprint, why should I consume less, pay more for energy or stop flying to limit my CO_2 emissions?«. Second, these technologies could lead to a political gamble. Indeed, for example, the IPCC scenarios almost all use the

BECCS technique, which for some is neither proven nor even credible. More broadly, the implications of large-scale deployment of these technologies have yet to be defined more precisely.

Societal, human and ethical issues are intertwined with these aspects. First, the perception and acceptance of NETs by the Swiss population remains open. The crucial question of how much effort each citizen would be willing to make to reduce his or her emissions is then also raised, as well as the link between this effort and the perceived risks of NETs. How our regional lives will be impacted by these technologies (e.g. the consequences of living next to a DACCS or BECCS installation, above a CO_2 storage area, etc.) still needs to be answered, as well. Furthermore, the ethics of these technologies have been studied by international groups and its mapping has identified many potential areas of conflict (e.g. justice, harm prevention as well as regulatory competencies).[221] The spatial and temporal separation of CO_2 emission and disposal increases the ethical implications, especially in terms of inter- and intragenerational justice. Nevertheless, if the consequences of a global warming above 1.5 °C are well assessed, should these technologies not be considered an ethical obligation, as a »we must« and not as a »we should«? The question of »What happens if we don't put these technologies into practice?« ought to be considered.

Furthermore, the economic opportunities and risks are also aspects to be considered. Some expect the market size to be as large as today's oil market in 40 years[222], and the swiss implications of the development of a global CO_2 market are currently not well understood.

How the swiss population stands on these aspects is not yet clear and the debate must be started.

Selected controversies and consequences for specific technologies

Concerning the individual technologies, we would like here to point out four important specificities. First, BECCS has often been the focus of attention for NETs because it is present in 97% of the IPCC Integrated Assessment Model scenarios for limiting warming to 2°C.[223] Indeed, from a theoretical point of view, this technique is attractive because it not only reduces CO_2 but also produces energy. However, the feasibility of this technique in a large-scale deployment is an open question, due to technical and societal aspects. For example, it will represent a significant change in land use, with competition between land used for bioenergy and food, or for other land-based mitigation actions (reforestation and afforestation). This potentially impacts food security, water systems, air quality but also civil society. It will also create a global biomass market, with the need for trade and transport of biomass feedstocks, linking the land available to produce the biomass resource to available energy infrastructure and storage sites, potentially on an intercontinental scale. At the environmental level, the different stages of BECCS also have their positive or negative consequences. [224] The regulatory framework

[221] Buck H. J., Rapid scale-up of negative emissions technologies: social barriers and social implications, Climatic Change, vol. 139(2), pages 155-167, 2016

[222] SwissRe

[223] Low S., Schäfer S., Is bio-energy carbon capture and storage (BECCS) feasible? The contested authority of integrated assessment modeling, Energy Research & Social Science, Volume 60, p. 10136, 2020, ISSN 2214-6296

[224] Gough, C., Mander, S. Beyond Social Acceptability: Applying Lessons from CCS Social Science to Support Deployment of BECCS. Curr Sustainable Renewable Energy Rep **6,** 116–123 (2019).

must also be put in place. Second, carbon storage in trees and surface soils involves reversing deforestation, reforestation, increasing soil carbon levels, and enhancing wetlands. It is seen at this point by EASAC, the European Academies' Science Advisory Council, as the only viable and competitive NET technology.[225] This topic opens up great debates on the implementation of these practices for agriculture and land use. Interestingly, in Switzerland, agriculture is today not subject to carbon pricing. Third, DACCS is contentious due to the large amount of renewable energy needed for its operation, as the availability of green electricity is very limited. Finally, it should be noted that BECCS and DACCS are only possible if CO_2 storage sites are available. But then, where to store it? If abroad, the liquified CO_2 will need to be transported and infrastructures developed.

TA-SWISS contribution to this topic

These technologies and their implementation are at the heart of a political debate in Switzerland, which will be voted earliest in 2023. A very controversial issue concerns the use of domestic storage sites only or the possibility to use storage sites abroad. The first option, proposed in a popular initiative (The Glacier Initiative) in November 2019, would limit the amount of hard-to-abate emissions well below the 7 million metric tons planned by the Federal Council. The second option is the direct counter-proposal of the Federal Council announced in 2021, which allows the use of abroad storage sites. This on-going debate then includes the definition of a »hard-to-abate« emission and which quantity of residual emission should be acceptable.[226] Furthermore, the CO_2 Act and relates Ordinance that will be revised next year and by 2025 should be totally revised. It should provide further information and directives for implementing NETs.

To support the political debate, TA-SWISS has mandated in 2021 a TA study on NETs to the Öko-Institut, a german research institute and the EMPA, the swiss federal laboratories. The central part of the interdisciplinary TA-SWISS study is a systematic survey of stakeholders and groups in Switzerland who are familiar with the technologies or their impacts; the survey aim is to pool existing knowledge and provide an overview of the various opinions on the opportunities and risks of NETs. The LOTA (Landscape of opinions for Technology Asessment) methodology is used, which enables a rational sustainability discourse in the transdisciplinary research process.[227]

The study will form the basis for an early, fact-based evaluation of existing knowledge and of knowledge gaps with regard to NETs. Despite current uncertainties surrounding technical aspects of these technologies, the study is designed to shed light on the potential of the new technologies in Switzerland and their possible consequences and side effects from various societal perspectives. Overall, the process encourages open and unbiased debate on the hopes and fears associated with NETs. The study should be published in spring 2023.

[225] EASAC, Negative emission technologies: What role in meeting Paris Agreement targets?, EASAC policy report 35, 2018

[226] Parallelly to this national debate, the Federal Council has started negotiations with other countries to reach agreements to store CO2 abroad.

[227] Mader, Clemens & Hilty, Lorenz & Som, Claudia & Wäger, Patrick. (2019). Transparenz normativer Orientierungen in partizipativen TA-Projekten – Ein Software basierter Ansatz. TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis. 28. 58-64. 10.14512/tatup.28.1.58.

Switzerland – Foundation for Technology Assessment (TA-SWISS)

Substitute products for meat and milk

Adrian Rüegsegger

What is it about?

Since the emergence of the climate debate, environmental aspects also play an important role in nutrition, because agriculture contributes significantly to the emission of greenhouse gases. The production of meat and milk requires a lot of resources and causes large-scale emissions of carbon dioxide (CO_2) and methane. In Switzerland, agriculture accounts for less than one percent of the gross domestic product[228], but it is responsible for about 16 percent of the greenhouse gases emitted by the economy.[229] Dairy products are a very important factor in Swiss agriculture. Swiss cheese is also well-known abroad, and 82,470 tonnes of it were exported in 2021.[230]

Climate-conscious consumers

According to surveys by life cycle assessment specialist Niels Jungbluth of the Swiss consulting firm ESU-Services, a vegan diet can reduce the environmental impact of food by a good 30 percent.[231] There are also precisely stated »CO_2 footprints« for individual foods. The Swiss organisation Eaternity develops a solution for the food industry to measure exactly and efficiently the environmental footprint of food products. The database already includes around 500 products and ingredients. A poster lists them in an overview according to their CO_2 footprint.[232] Consumers can take this information into account when making their purchasing decisions. Around five per cent of Swiss people eat a vegetarian diet, and just under one per cent eat a vegan diet. This leaves a large group of people who regularly or occasionally eat meat and dairy products. Many are prepared to limit their consumption of dairy products and meat.

The ever-growing range of substitutes for meat and milk offers consumers new opportunities. A study[233] by the Swiss Federal Office for Agriculture (FOAG) concludes that sales of meat substitutes in Switzerland will continue to grow. However, the share of 2.2 percent of sales in the meat market in 2020 was still low for substitute products, even though sales doubled between 2016 and 2020 to 117 million Swiss francs per year. Moreover, an ecological advantage only results if less meat is con-

[228] www.eda.admin.ch/aboutswitzerland/en/home/wirtschaft/uebersicht/wirtschaft---fakten-und-zahlen.html

[229] www.bfs.admin.ch/bfs/de/home/statistiken/raum-umwelt/umweltgesamtrechnung/luftemissionen.html

[230] www.schweizerkaese.ch/fileadmin/content/switzerland/Medienmitteilungen/MM_Schweizer_Käseexporte_31-1-2022_DEF.pdf

[231] Regionalität wird überschätzt. Bei Lebensmitteln sind die Transportwege oft nicht der wichtigste Aspekt für die Ökobilanz. Matthias Benz, Neue Zürcher Zeitung, 1.10.2021

[232] www.dietchangenotclimatechange.com/de/2021/10/29/lebensmittel-im-klimacheck-poster-von-eaternity-zum-kostenlosen-download/

[233] Bereits jeder sechste Burger ist fleischlos. Matthias Benz, Neue Zürcher Zeitung, 18.5.2021

sumed at the same time. This cannot yet be observed. Many consumers are rather critical of substitute products, as an online survey with 534 participants from Switzerland showed.[234] They doubt that the substitute products can contribute to climate protection.

Highly processed substitute products

Vegetarian or vegan products have a reputation for being natural and healthy. But not all substitutes are as simple as tofu. When it comes to »recreating« the minced meat for a hamburger from vegetable components, the latest food technology processes are used. This is all the more true the more the imitation is supposed to have the characteristics of real meat. Vegan imitations are among the most processed foods, so it is controversial whether they are equivalent to the original from a nutritional point of view. For example, most »milk drinks« made from plants contain significantly less protein than cow's milk. Those who pay close attention to health are thus best off consuming fresh or only slightly processed alternatives to meat and milk. One might ask whether a diet without meat and milk would not also be possible without imitations, since there is a centuries-long tradition of vegetarian nutrition, especially in other cultures such as India, which has meanwhile also produced very popular dishes in the West.

Opportunities for the food industry

For Switzerland, the new trends in nutrition could be an opportunity from an economic point of view, given its great experience in the fields of biotechnology and food technology, both in research and production. With the Swiss Protein Association (SPA), there is a recently founded organisation that is committed to promoting high-quality and competitive production of alternative protein sources along the entire value chain and to creating favourable conditions in Switzerland.[235] There are successful specialised companies in many countries, some of which are also present on the stock exchange, for example the Swedish company Oatly, which produces oat milk, and the American manufacturer of plant-based burgers Beyond Meat. The German sausage producer Rügenwalder Mühle is also successful with substitute products and has announced that in July 2020, for the first time, it made more sales with substitute products than with meat products. Internationally renowned Nestlé, Danone and Unilever are also active in the market with plant-based alternatives to meat and dairy products.

But the plant-based substitutes today are usually even more expensive than the original. Because of the high costs, there is also no in vitro-grown meat on the market yet. But the first products have at least been announced. The Swiss company Mirai Foods is researching the production of meat in the bioreactor and wants to bring it to market first in Singapore, and in a few years also in Europe. In the longer term, it should be possible to produce the in vitro meat much more cheaply. According

[234] Consumers' evaluation of the environmental friendliness, healthiness and naturalness of meat, meat substitutes, and other protein-rich foods. Christina Hartmann et al., Food Quality and Preference, Vol. 97 (2022), published online, 3 December 2021

[235] Schweizer Hersteller alternativer Proteinquellen schliessen sich zusammen. Medienmitteilung der Swiss Protein Association (SPA) vom 15. September 2021

to a study by the market researcher AT Kearney, in twenty years only 40 percent of meat could still come from animals.[236] In Switzerland, the major retailer Migros is leading the way in the development of artificial meat.[237]

Open questions for agriculture in Switzerland

A move away from milk and meat production would have far-reaching consequences for agriculture in Switzerland. Without dairy farming, the cultivation of alpine pastures would hardly be possible at certain altitudes for climatic and/or topographical reasons, and there are also other areas that cannot be used for arable farming. An alternative use or the cessation of production would, not least, profoundly change the landscape so typical of Switzerland. Consideration is already being given to which plants could be grown in Switzerland as raw materials for meat substitute products, so that protein-rich plants such as soya would no longer have to be imported on a large scale.[238] However, a complete turn away from meat and milk production is not to be expected, because animal husbandry also has an ecological benefit. For example, it contributes to biodiversity if it is sustainable and extensive.

Eating habits also have a cultural component and animal husbandry is an essential element of agriculture in Europe. A rapid reduction in meat consumption is not to be expected, especially as demand in emerging countries continues to rise from a low level as a result of increasing prosperity. A report by the Food and Agriculture Organisation and the OECD forecasts a global increase in meat consumption of 14 per cent by 2030, with saturation or a slight decline expected in the wealthiest countries, not least due to the availability of substitute products.[239] Thanks to more efficient production methods, the report assumes »only« a five per cent increase in greenhouse gas emissions in agriculture by 2030, which is nevertheless worrying for a sector that is one of the world’s largest emitters.

Ethical and regulatory considerations

A report commissioned by the Swiss Federal Ethics Committee on Non-Human Biotechnology (ECNH) discusses ethical issues relevant to the interface of climate change, climate protection measures and agriculture.[240] It notes that animal-based food production accounts for around half of the food system’s emissions, despite contributing less than a fifth of the world’s calorie supply. The report stresses the need for climate-friendly agriculture and food industries. However, this raises

[236] Hier wächst Wurst. Investoren pumpen Milliarden in pflanzliche Esswaren und Laborfleisch. Franziska Pfister, NZZ am Sonntag, 4.10.2020

[237] Migros und Coop kooperieren für das Fleisch der Zukunft. Edith Hollenstein, Tages-Anzeiger, 16.9.2021

[238] Pflanzliche Proteine als Fleischersatz: eine Betrachtung für die Schweiz. Daniel Heine et al., Agrarforschung Schweiz, Vol. 9(1), S. 4-11, 2018

[239] OECD-FAO Agricultural Outlook 2021-2030, S. 166; OECD Publishing, Paris, 2021

[240] Dietary transition. Teea Kortetmäki, In: Agriculture and climate change. Ethical Considerations. Federal Ethics Committee on Non-Human Biotechnology ECNH and Ariane Willemsen (eds.), Bern, 2022: www.ekah.admin.ch/inhalte/ekah-dateien/dokumentation/publikationen/Buchreihe_Beitraege_zu_Ethik_und_Biotechnologie/Buch_15_Inhalt_Agriculture_and_Climate_Change.pdf

other ethical issues as well as concerns – a balancing of interests and a public debate are therefore likely to be needed to find viable solutions that will stand up in a democratic system. Processed plant-based substitutes are also addressed in the Ethics Committee's report. These could be acceptable »imitates« for many who do not want to give up meat for culinary reasons. However, there is also the caveat that the substitute products are unnatural due to their high degree of processing.

The food sector is heavily regulated – from agriculture to processing to trade. The regulations are primarily intended to ensure the safety and health of consumers. In addition to the legally binding regulations, there are labels that are not mandatory but are intended to provide guidance for consumers. The best known is the »Nutri-Score«, which is already established in some countries and is now increasingly being used in Switzerland. It is a five-point colour scale that indicates whether a product serves a healthy diet or rather not. However, the health benefits of such labels are controversial. The question now is whether such labels would be useful to indicate the climate balance of food. A report[241] by the European Academies Science Advisory Council (EASAC) on the UN Food Systems Summit 2021 mentions labelling as one of several options to promote sustainability in the area of nutrition. However, the liberal think tank Avenir Suisse warns against paternalism in this context, which aims to prevent »bad« behaviour.[242]

Politics and the role of technology assessment

The topic of a sustainable, more plant-based diet is also on the minds of the relevant Swiss authorities and politicians. The Swiss Nutrition Strategy 2017-2021 of the Federal Department of Home Affairs (FDHA) mentions in the category of meat that the daily consumption of an average of 110 grams per person is three times too high.[243] In its statement[244] on the parliamentary interpellation by National Councillor Mike Egger, the Federal Council points out with regard to the aspect of a balanced diet that, according to Swiss dietary recommendations, meat consumption should be reduced and meat should be partially replaced by other protein-rich foods. With regard to health, however, the statement also says that some of the substitute products for meat are highly processed foods that are not optimally composed in terms of nutritional physiology.

The way we eat can contribute significantly to reducing greenhouse gas emissions. However, there are many open questions in this context that concern us all. The possibilities for action also depend on the options that exist and how these are perceived by the population. Nutrition is a particularly

[241] The Role of Science, Technology, and Innovation for Transforming Food Systems in Europe. Food Systems Summit Brief. Claudia Canales, Robin Fears, EASAC, April 2021, www.easac.eu/fileadmin/PDF_s/reports_statements/Food_Security/FSS_Brief_IAP_Europe.pdf

[242] Kann uns der Staat vor Übergewicht retten? Avenir Suisse warnt vor Paternalismus wie der Zuckersteuer. Simon Hehli, Neue Zürcher Zeitung, 28.1.2022

[243] Geniessen und gesund bleiben. Schweizer Ernährungsstrategie 2017-2021. Bundesamt für Lebensmittelsicherheit und Veterinärwesen BLV (Hrsg.), Juni 2017

[244] Keine einseitigen Massstäbe bei der Beurteilung von Fleisch und Fleischersatzprodukten. Interpellation Nr. 21.3915, eingereicht von Mike Egger (SVP) im Nationalrat am 18.6.2021 und Stellungnahme des Bundesrates vom 18.8.2021

multifaceted topic in the area of tension between the factors of environment, health, consumer habits, agriculture and industry. TA-SWISS will therefore conduct an interdisciplinary study on the topic of »Substitute products for meat and milk« from the end of 2022. The study should show what contribution these products can make with regard to a more climate-friendly food system.

Wallonia – SPIRAL research centre – University of Liège

The July 2021 floods in Wallonia: How our TA practices enriched the debriefing

Catherine Fallon and Aline Thiry

Drastic and destructive: this was the nightmare lived by several thousands of citizens facing dramatic level of water flow within the Vesdre valley on July 14-15 2021. Not only was the cost of life very high, also the cost to the built environment and the impact in terms of water and soil pollution is still dramatically high. This massive destruction was used as an opportunity by the analysts to put on the agenda the reforms necessary to better manage the risks of sudden water flow and particularly flush overflow.

Can TA be presented as a building stone for the political and social handling of such disruptions?

The recurring questions from the population were: how is it possible that a rain can cause such a disaster? If the dams located upstream of the valley are supposed to hold back the water, why did they release the water at the height of the crisis? The General Flood Risk Plan (GFRP) in Wallonia had already highlighted the vulnerability of this valley, so how come the local authorities had never built a crisis procedure to deal with such an announced event? Why did the information available from the weather offices not alert those in charge of river management? The event was qualified as exceptional: such heavy stationary rains could happen again in our regions and the question is then: how to prepare for it in the face of climate change?

Can a dam be described as a critical infrastructure »whose failure must be prevented at all costs«?[245] The protection against natural hazards or manmade threats is one among many essential tasks for operators of such large critical infrastructures. On the one hand, they have to meet challenges such as climate change, demographic change or urbanization. On the other hand, they have to face a drastic decrease in funding for public investments, even concerning infrastructure maintenance. The decline in public investment is regularly denounced in European countries, where the management of public budgets is subject to European pressure and international control in order to meet the requirements of rating institutions. In such conditions, many infrastructures are under threat of major failures: from highways to tunnels and dams. Decisions about public investments needed to maintain critical infrastructure are under strong pressure in most European countries, not only Belgium.

What is it about?

A dam is a hydroelectric facility equipped with a reservoir, capable of storing relatively large quantities of water and keeping water in reserve to be released when the flow of the river is lower. There

[245] The European Programme for Critical Infrastructure Protection (EPCIP) does not include « dam » in the list.

are ten large dams in Wallonia; their main function is to store drinking water, water for touristic activities or agriculture and water for industry (such as the wool industry in Verviers in the 19th century). They also provide the necessary water support to regulate the flow of rivers: a river like the Meuse would not be navigable without the presence of dams upstream. On the Vesdre river, four large dams have been built and are managed for flood management and flood control.

Another advantage of dams is the production of green, renewable energy. In Wallonia, in terms of installed capacity, hydroelectricity is at 110 megawatts (MW), i.e. less than 1% of the total installed capacity in Belgium, but with a load factor of 75%. Within the framework of the various European plans for renewable energy production, Wallonia aims to increase the productivity of existing infrastructure. The cost of this infrastructure is estimated at 1 billion euros.

The major problem of a dam is the risk of a dam accident, especially for the large reservoir dams which can cause much greater flooding downstream. The La Gileppe dam on the Vesdre was built in 1878; between 1930 and 1990 the largest hydroelectric dams in Belgium were built and put into operation, four of which are linked to the Vesdre valley. Since 2 February 1993, jurisdiction over waterways and their dependencies has been transferred from the federal state to the regions. Some dams are now managed directly by the regional administration (e.g. La Gileppe and Eupen): the operator must take into account the demands of the various stakeholders in order to trade off these water demands. Other dams are placed at the disposal of an industrial company specialised in electricity production (Engie, for Butgenbach and Robertville) which must arbitrate between external demands for water storage and production and the production of electricity which ensures an operating yield.

Ongoing debate

Flood risk analysis in Wallonia

Floods are a recurrent risk in Wallonia: since 1967, more than 60% of Walloon municipalities have experienced at least four floods resulting in damage to homes. Between 1967 and 2008, Wallonia was affected by seven major events recognised as public disasters and covering more than a third of its territory.

In 2003, the Walloon government set up a an expert group (»Groupe Transversal Inondations«, GTI) made up of civil servants from the Walloon public service, provincial administrations and university scientists. The administration has benefited from the expertise of the academics and the on-the-ground knowledge of the provincial departments, which are familiar with the flood risk management challenges facing municipalities. This group defined the PGRI 2022-2027[246] but it operates without addressing the issue of crisis management with the actors on the ground. Few municipalities are developing an emergency plan that specifically considers the risk of flooding, even though they are involved in the PGRI. As an example, for the Vesdre, the draft PGRI 2022-2027 (p.211) raises many concerns about improvements to be made in terms of risk management and highlights

[246] General Flood Risk Plan imposed under Directive 2007/60/EC of the European Parliament and of the Council of 23 October 2007 on the assessment and management of flood risks.

the particular risk of the Vesdre basin: it is a densely populated basin, including in the high flood risk zones. This very long document did not attract the interest of local authorities.

Dam safety issues

Nowadays, the operation of hydroelectric power plants is carried out automatically, thanks to advances in the fields of information technology, sensors and communications, which makes it possible to improve the efficiency of the plants.[247] Maintenance and upkeep is a real challenge, because this work must be carried out by highly qualified specialists in the fields of welding and grinding, who can intervene in order to make these infrastructures more reliable and thus improve their performance.

The maintenance of a hydroelectric power plant, as with any industrial process, must be programmed to ensure that each component is serviced or repaired so that it can perform its defined function.[248] There are different types of maintenance: that which corrects detected defects and failures, and that which aims to guarantee the reliability of equipment in operation in order to anticipate an accident or breakdown.[249] Finally, the objective of evolutionary maintenance is to compensate for technological obsolescence or new operating requirements, for example in terms of regulation or safety. The more advanced level of maintenance is based on risk analysis to continuously improve the management of the site and to deal with recurring or emerging problems.

If the monitoring and maintenance of infrastructure is neglected, major risks can arise, such as overflow and rupture during a flood (33% of accidents in France), due to poor flood management. Or the degradation and ageing of installations (20% of accidents in France), due to poor site monitoring. The ageing of infrastructure and its monitoring are permanent challenges. A permanent assessment of the mechanical (creep, shrinkage, swelling of concrete, consolidation of embankments, etc.) and hydraulic (clogging of drainage, loss of efficiency of injection curtains, entrainment of materials, etc.) characteristics is necessary to ensure the proper functioning of hydroelectric infrastructures.[250,251]

An operator is responsible for the quality of the works, compliance with laws and regulations, monitoring activities, and safety device controls. This activity is fundamental to the safety of the dams

[247] GUICHON Pierre, Rapport des machines à EDF Service de la production hydraulique « Méthode de contrôle et d'entretien préparé », 1989, Lyon, p.3

[248] Comité Français des Barrages et Réservoir, « Diagnostics d'ouvrages par vecteurs aériens et sous-marins », in Colloque – Méthodes et techniques innovantes dans la maintenance et la réhabilitation des barrages et des digues, 27-28 novembre 2018, Chambéry, p.13

[249] Ibid.

[250] Comité Français des Barrages et Réservoir, « Retour d'expérience sur les membranes d'étanchéité pvc en parement amont de barrages », in Colloque – Méthodes et techniques innovantes dans la maintenance et la réhabilitation des barrages et des digues, 27-28 novembre 2018, Chambéry, p.204

[251] POUPART M., ROYET P., « Surveillance et maintenance des barrages à électricité de France » in Colloque technique du CFGB, 10-11 mai 2001, Aix, p.8

and the control of downstream flow variations is also essential to the safety of the structures.[252] The maintenance of a public site entrusted to a private operator is the latter's responsibility: he must organize annual control visits by an independent approved body and provide regular feedback on the follow-up. Until 2022, the dams managed by the Walloon Public Administration (Service Public de Wallonie – SPW) were not subject to this type of control.

Under the aegis of the International Committee on Large Dams (ICOLD) founded in 1928, the Belgian Committee on Large Dams (CBGB) was created in 1929. It was initially an advisory committee for »the construction and operation of large dams, from the point of view of navigation, energy production, flood water drainage, agriculture, water distribution, hygiene, etc.« The CBGB is composed of managers, engineering specialists (attached to the universities and the regional administration) and must give advice to the government. For example, in 2016, the CBGB implemented the creation of flood maps downstream of structures in the event of failure (dam failure, overflow, etc.). However, there is no legal framework for the management and safety of dams in Belgium with regard to external inspection and control. The dams managed by ENGIE have their own control authority that submits the expert reports to the SPW: there is no legal framework requiring the Mobility and Infrastructures division of SPW to give feedback on these inspections.

In their article »*Out of order: understanding repair and maintenance*« [253], Graham and Thrift (2007) point to the place and consideration given to maintenance, repair and upkeep of ageing physical infrastructure networks: it sometimes takes a shock to realize the flaws in a system that is supposed to be running smoothly.

SPIRALs contribution to the topic

Our research group has recognised expertise in emergency planning and crisis management in Wallonia. When the Minister in charge of dam management in Wallonia requested a study on the July 2021crisis, a Swiss engineering firm (Stucky) specialised in the monitoring and management of the safety of large dams submitted a draft project for evaluation work in partnership with the University of Liège. In the report »Independent analysis on the management of waterways during the bad weather of the week of 12 July 2021«[254], we coordinated the study of the administrative management of flood risk and emergency planning, as well as the administrative management of dams, river monitoring and flood monitoring.

Our participation had a particularly important impact because the engineers (Stucky) had a lot of expertise in terms of dams and hydrological modelling, while our group brought a specific expertise

[252] OLIVER Jean-Louis, « Les barrages hydro-électriques français », Archives orales du Ministère de la Transition écologique et solidaire, 19 septembre 2003, p.6-7

[253] Graham, S., & Thrift, N. (2007). Out of Order: Understanding Repair and Maintenance. Theory, Culture & Society, 24(3), 1–25.

[254] Zeimetz L., Launay M, Bourqui P., Calixte E., Fallon C., Teller J., (2021), Analyse indépendante sur la gestion des voies hydrauliques lors des intempéries de la semaine du 12 juillet 2021, Rapport à l'attention du Cabinet du Ministre Philippe HENRY, Ministre Wallon du Climat, de l'Energie et de la Mobilité, 30/9/2021, Stuky 5875/4001, Chef de projet : Michaud T.

that was essential to analyse this crisis within the context of Wallonia. Among the central issues that we raised are:

- How are the competences organised between the administration and the field (dams) and local (municipalities) managers?
- How are flood risk maps and emergency plans constructed?
- How is the follow-up of weather alert information (European and federal level), water level alert (navigable and non-navigable rivers) organized?
- How are the crisis managers informed?
- What are the prevention measures?
- Can we talk about a risk culture in valleys identified with a high flood risk?

The Spiral research centre was able to open the scope of investigation to include technical issues in the Walloon context and the Belgian federal and regional administrative structures; to insist on the need to consider emergency planning and crisis management structures in the report; to further open the perspectives and lines of investigation to include local/provincial actors.

The researchers of Spiral were associated with the Swiss team in all interviews, as well as on site (in the dams sites), down the Vesdre valley and with the public servants and university researchers working on these issues. Although Spiral does not really specialize in »dams« and »flood management«, the socio-technical TA approach was a huge guarantee of the quality of the conclusions drawn from this work.

The analysis work had a significant impact. Not only was it discussed with the administrations concerned, who all validated it, but it was also presented to the Minister concerned. It was also presented to the special parliamentary commission of inquiry of the Walloon Parliament dedicated to the analysis of the floods. Among the recommendations formulated in the final report of the Parliament[255], a certain number of recommendations emerge from this work of objectivation, not only for the technical questions but also for the socio-technical questions.

[255] Rapport de la Commission d'enquête parlementaire »Inondations», Parlement de Wallonie, 31 mars 2022, https://www.wallonie.be/fr/inondations/commissariat-special-la-reconstruction-csr/rapport-de-la-commission-denquete-parlementaire-inondations