Dutch debate on 5G needs more substance

Message to parliament

In July 2020, the first section of 5G frequencies was auctioned in the Netherlands and its first applications were launched. Critics are concerned about digital security and health effects. Supporters point out the many technical possibilities. The debate threatens to become polarised. As a result, relevant questions about risk assessment and cyber resilience are being sidelined. The Rathenau Instituut has provided the Dutch House of Representatives with five points of attention to add substance to the debate. These points will be useful in preparation for the *Schriftelijk Overleg* (Written Consultation) for the *Telecomraad* (Telecom Council) on 14 and 15 October 2020.

The five points of attention in short:
1. Continue to monitor health effects closely.
2. Give broader concerns and interests a voice in the decision-making process at an early stage.
3. Continue to invest in the cyber-resilience of the Netherlands.
4. Strengthen digital autonomy.
5. Start preparing for 6G now.

What is 5G?

The term 5G stands for fifth generation mobile communication. It is not a revolutionary new technology, but the successor to 4G. The current 4G network is reaching its limits due to the constantly growing demand for connections and data. A future 5G network will be able to process data faster, with less delay and more capacity. Less delay is especially important in , sending data back and forth, for example to control an operating robot. More capacity means that more devices can connect to the network at the same time and maintain a fast connection. The expectation is that 5G can be used for a range of applications: from surveillance with drones above a football stadium and sensors in agriculture, to supporting augmented reality on a container ship for virtual inspections.

5G, like 4G and its precursors, uses spectrum bands. At European level, three spectrum bands have been designated for 5G: low, medium and high. Each band has different characteristics and is suitable for different applications.

- The low band (700, 1400 and 2100 MHz) is suitable when there are many users and relatively little data transmission. This is the case, for example, with smart energy meters. The antennae for low frequencies have a range of several hundred metres to several kilometres. This band can achieve national coverage and was recently [auctioned in the Netherlands](#).
- The medium band (3500 MHz, 3.5 GHz) can achieve highspeed data on a local level and is suitable for high-quality image applications such as virtual reality. The antennas have a range of a few dozen to a few hundred metres. The frequency is comparable to the current WiFi signal (2.5 GHz and 5 GHz). Good coverage in buildings is difficult to achieve with the medium band, because the signal has more difficulty with penetrating through walls and windows. Because the antennas have a shorter range, many antennas are needed for proper coverage. The medium band will be auctioned in the Netherlands in 2022.
- The high band (26,000 MHz, 26 GHz) is most suitable for very highspeed data on a local level. For camera surveillance at a football stadium, for example. The antennas have a range of a few metres. That is why many set-up points are needed and why a nationwide network is difficult to realise. The high band will be auctioned last.

Public debate about 5G

In the Dutch public debate, supporters and opponents often express one-sided advantages or disadvantages of 5G. Supporters point out that the technology enables applications with a certain futuristic characteristics, such as self-driving cars and remote-controlled operating robots. The government sees 5G as indispensable to the Dutch economy. Opponents raise questions about the possible harmful health effects. There is also debate about digital security and the possibilities for surveillance.

The government indicates that the measured exposure does not exceed the prescribed limits. At the same time, organisations such as RIVM and the *Gezondheidsraad* (Dutch Health Council), in its recent report of 2 September, say that there are various uncertainties, making it important to keep a close eye on the situation.

In the spring of 2020, 5G was the subject of disinformation campaigns in the Netherlands: transmission masts were set on fire and citizens filed lawsuits against the state. Because resistance is growing, relevant questions about risk assessment and cyber resilience are at risk of being ignored. The Rathenau Instituut therefore presents five points of attention for Parliament.

Health

1. Continue to keep a close eye on health effects

Electromagnetic fields from antennas can heat up the body. This can potentially be harmful and therefore limits are set on how much the general public can be exposed to electromagnetic radiation. These limits are based on recommendations of the International Commission on Non-Ionizing Radiation Protection (ICNIRP) from 1998. The Netherlands has established a limit that is fifty times as strict as the international commission. Research by the Agentschap Telecom (Radiocommunications Agency) and the RIVM (National Institute for Public Health and the Environment) shows that the exposure effects of separate antennas and devices for 5G are another ten times lower than the Dutch limit.

However, it is expected that the number of radiation sources will increase as more devices and applications are developed, which are used simultaneously or for longer periods of time. Think of a family together in one room watching Netflix on a tablet, playing a game with VR glasses and watching videos on their phone. It is unknown how the exposure to radiation will increase in the future. That is why the RIVM, the Agentschap Telecom and the Gezondheidsraad conduct follow-up research.

For lower spectrum bands, for example, more insight is needed into the actual use of 5G. Which devices are used and how? These tests must take place with realistic test rigs. The Gezondheidsraad (Dutch Health Council) advises further research into the influence of radiation on certain diseases and disorders. [1] Although the link between radiation and disease has not been demonstrated in humans, a possible connection cannot be ruled out.

For the highest band, there are more unknown factors. The Gezondheidsraad (Dutch Health Council) therefore recommends to auction this frequency band only when the health risks have been investigated. The Dutch House of Representatives can see to it that the government further investigates the health effects and continues to monitor them closely.

---

1   They include cancer of the male reproductive organs, reduced fertility and birth defects, www.gezondheidsraad.nl/documenten/adviezen/2020/09/02/5g-en-gezondheid.

Broader concerns

2. Give broader concerns and interests a voice in the decision-making process at an early stage

Although follow-up research is necessary, Rathenau Instituut's research on how scientific knowledge is used in policy making, shows that technological developments, such as 5G, always involve scientific uncertainties. More research can shed light on those risks, but often cannot eliminate all uncertainties. Public controversies about such developments often involve broader societal concerns and major interests (Rathenau Instituut 2014). For example, in the debate on 5G, in addition to health risks, there are discussions about spatial planning due to the positioning of antennas, and concerns about surveillance due to the expected increase in sensors. This requires policymakers to give broader concerns and interests a voice in the decision-making process.

Furthermore, with 5G, the connection between national and local policy is important. This is because Dutch municipalities are involved in the launch of 5G and have to deal with local protests. Various municipal councils have paused the launch of 5G in response to protests. However, the new Telecommunicatiewet (Telecommunications Act) compels municipalities to cooperate in the installation of antennas. This puts municipalities in a difficult position, especially if there is little local support. The Rathenau Instituut argues that the Dutch House of Representatives should make a case for clear frameworks that give municipalities more room to accommodate the concerns of citizens.

Digital security

3. Continue to invest in the cyber resilience of the Netherlands

The discussion on digital security focuses on possible links between suppliers and countries with an offensive cyber programme aimed at the Netherlands. In particular, the use of equipment from market leader Huawei is the subject of much debate. Since 5G networks will be part of the vital infrastructure, they could become a target for sabotage, espionage and terrorism. The Dutch government will therefore, in line with the policy of the European Commission, impose additional requirements on telecom providers. The government can, for example, force a telecom provider not to use a particular supplier for components of the 5G network. Further conditions have also been laid down for access control, security updates (patching) and the detection of incidents. It is important that the Dutch House of Representatives continues to closely monitor the government's actions in this area. It already does this, in part, through private briefings because of confidential information about critical parts of the network.

It is also important, when discussing security, not to focus only on Huawei or 5G. Every form of ICT, be it 5G or a satellite connection, contains vulnerabilities, regardless of the provider. Or, as the Rathenau Instituut said in 2017: 100% security does not exist (Rathenau Instituut 2017).

In other words, the security threat does not disappear by excluding specific suppliers. Moreover, vulnerable situations arise not only through deliberate disruption, failure or misuse, but also, for example, through a software update with unforeseen effects,

through human error or through a combination of factors. As society continues to digitise, and more and more devices become interconnected, dependencies grow and the risk of manipulation, failure or disruption increases.

Given this vulnerability, a broad range of measures to make our digital society more resilient remains essential. These might include a combination of better use of existing technology (such as encryption), better anticipation of new technologies (such as machine learning and post-quantum cryptography[2]) and investment in active enforcement and supervision (Rathenau Instituut 2020). The Netherlands can also make further efforts to de-escalate the international cyber conflict. This can be done, for example, by making international agreements on sabotage and espionage (Rathenau Instituut 2019).

4. Strengthen digital autonomy

An overall concern is the growing dependence of the Netherlands and the EU on foreign suppliers for the design and protection of digital systems, particularly from the United States and China. To reduce this dependence, the Netherlands can stimulate - preferably through European cooperation - its own IT activity. This can be done, for example, by stimulating the innovation climate, by setting specific standards and by demanding stricter purchasing conditions (Rathenau Instituut 2020). At the moment, however, there is a chronic shortage of the necessary expertise. The Dutch House of Representatives can ask the government to invest more in the necessary expertise, to bring more focus to the *Nederlandse Cyber Security Research Agenda* (Netherlands Cyber Security Research Agenda) (NCSRA), and to create more attractive contracting procedures for start-ups.

Prepare for the future

5. Start preparing for 6G now

The international standardisation process for 6G, the successor to 5G, is already underway. In those standards, all kinds of characteristics of the technology are laid down that have consequences for new possibilities and risks. It is therefore important to link the wishes arising from the debate on 5G with the standardisation process for 6G and for subsequent generations of mobile

---

2   *Machine learning* can help in automatically detecting and fixing vulnerabilities in software. Post-quantum cryptography should enable data encryption that can withstand attacks using the processing power of a quantum computer. These technologies are under development and have only limited application.

communication technology. These standards are primarily shaped by the industry, but governments can exert influence. For example, by monitoring the process, by contributing to the development of safer protocols and encryption and by paying attention to possible health risks. With a view to future cyber resilience, it is important that the Dutch government and the EU involve themselves more emphatically in decision-making concerning international standards (Rathenau Instituut 2020).

Relevant publications of the Rathenau Instituut

Rathenau Instituut (2020) Cyber resilience with new technology. An opportunity and a necessity. www.rathenau.nl/en/digital-society/cyber-resilience-new-technology

Rathenau Instituut (2019) Cyberspace without conflict. The search for de-escalation of the international information conflict. www.rathenau.nl/en/digital-society/cyberspace-without-conflict

Rathenau Instituut (2017) A never-ending race. On cyberthreats and strengthening resilience. www.rathenau.nl/en/digital-society/never-ending-race

Rathenau Instituut (2014) Contested science. Public controversies about science and policy. www.rathenau.nl/en/kennisgedreven-democratie/contested-science