Update on the implications of the Dutch Temporary Cyber Operations Act

read more ⋮ 5-7 minutes ⋮ 5/16/2024

Discussion Prompt: The Dutch Temporary Cyber Act: Necessary measure or disproportionate expansion of power?

See all contributions to this question.

The Dutch Parliament now allows its intelligence services to intercept internet traffic more easily in the fight against foreign cyber attacks. What exactly this means in practice remains unclear.

In the Netherlands, a Temporary Cyber Operations Act was enacted in March 2024. This new law makes it easier for the Dutch secret services to conduct hacking and cable tapping operations, which they say is urgently needed in the fight against cyber attacks from countries such as Russia and China. Others, however, fear that this law will create a digital dragnet. In 2022, the technical expert of the TIB intelligence operations review committee resigned for this reason.

The Cyber Operations Act complements the current Intelligence and Security Services Act of 2017 (Wiv 2017), which, among other things, enabled bulk interception of Internet traffic. After a small majority spoke out against this law in an advisory referendum in 2018, it was stipulated that such interception should always be “as targeted as possible”.

In practice, this and some other legal requirements proved to hinder effective and flexible operations. Therefore, the new law makes it easier for the secret services to access computers and servers of Dutch citizens and companies when they have been hacked by, for example, the Russians or the Chinese. The most controversial part is the introduction of an exploratory phase that precedes the bulk interception as regulated by the Wiv 2017.

The purpose of this exploratory phase is to determine which data streams qualify for actual bulk interception. As this is an exploratory phase, the “as targeted as possible” requirement has been dropped. Concerns were also raised that the wording of the new law is so broad that data in this phase may theoretically be intercepted and stored for 6 months. Moreover, this data may be shared with foreign partner services, which was strongly opposed by the Council of State.

There could have been a robust parliamentary debate on this, but for many members of parliament the issue proved too complicated. In addition to the already complex Wiv 2017, the Temporary Cyber Operations Act makes this topic almost impenetrable. Added to this, the cabinet only provided clarification when the parliamentary questions were very precise, but for this the parliamentarians lacked the necessary background knowledge. This is a result of the fragmentation of the political landscape and the large number of new members of parliament, which means that much experience in this field has been lost.

Unlike the House of Representatives, the Dutch Senate managed to get some new information from Interior Minister Hugo de Jonge. The temporary law, for example, does not only apply to Russia, China, Iran, North Korea and other countries designated by the cabinet, but also when it is not yet certain whether cyber attacks can be attributed to one of these countries. Furthermore, bulk interception does not mean that entire neighborhoods will be wiretapped, but rather the networks of Internet and other communications providers. The Interior Minister confirmed that data from the exploratory phase can also be shared in bulk with foreign partner agencies.

Other issues, however, have not been clarified. According to a report by the oversight commission CTIVD, the exploration has so far been carried out by taking a “snapshot” of a data stream for only two hours a day. Because this was not explicitly asked in parliament, we do not know whether this will be the case in the future, even though it makes a significant difference compared to continuous interception as allowed by the wording of the law.

Data from the exploratory phase that is shared with foreign partners may not be used by them for further intelligence research. But what exactly they are allowed to do with it and what the added value is for them has not been clarified either. Does this sharing involve the exchange of digital threat information, or will that take place at a later stage?

After all, such exchange is important to counter cyber attacks, which is what the temporary law is specifically aimed at. In general, the issue of cyber defense was almost completely ignored during the parliamentary debate, even though it has a different methodology than the more offensive gathering of intelligence on other countries. For cyber defense, it is important to have a broad view on data streams, but how this relates to the legal requirement of proportionality has never been clarified.

The case of the Temporary Cyber Operations Act shows that all parties involved have a lot of work to do to be well prepared for the proposed general revision of the Wiv 2017 which will take place in just a few years from now. Members of parliament, journalists and interest groups will have to thoroughly familiarize themselves with this matter, just as they did in the run-up to the 2018 referendum.

The cabinet and the secret services need to be more open and forthcoming about how the legislation relates to current and, preferably, future practice. This is not only to allow the people and parliament to make the best possible assessment of necessity, risks and safeguards, but also to ensure that this time the law will be more workable and sustainable.

Previous Chapter Next Chapter