

Referentienummer: NWP2231654

Datum: 18 juli 2023

Spreektekst M. Moussault bij PEGA Commissie dd 24 januari 2023

First of all, I would like to thank you for inviting me to appear for your committee. I understood that the purpose of this hearing is that I explain about the general legal framework in the Netherlands in regard to the oversight on the intelligence agencies. It's my pleasure to do so.

Since I am the chair of the body that is charged with the ex ante review of special investigatory powers, the focus of my presentation will be on that part of the oversight. However, I'm afraid that there are some limits to what I can tell you. In the Netherlands, the technical means or tools of the intelligence agencies are considered state secrets in two different ways. First of all, the fact that special means are used is state secret, but also the fact that certain means are not used is considered a state secret. That maybe seems not logical, but I will explain it with an example.

Imagine there are two special tools to hack of a computer. The one with the name Neptune. And the other one which is named Caesar. Now, Neptune would be used in the Netherlands and Caesar not, and I would say, I'm sorry, I'm not allowed to say if Neptune is used in the Netherlands, but I can inform you that we do not use Caesar. It would be clear, I think, for everybody that Neptune is used in the Netherlands. This is why I cannot inform you about any means used and not used by the services. I do realise that on this point my French colleague was in the hearing with you two weeks ago had more liberties to inform you. Well, I'm sorry. There are differences between countries.

However, I can explain you about the oversight, but not about the means that are used. The powers of the intelligence and security services in the Netherlands are regulated by the Intelligence and Security Services Act 2017 or in short the ISS Act. The oversight on the intelligence services is regulated in the same act. Roughly, the oversight is divided between the three bodies. The District Court of the Hague, that is more practical. The examining magistrate, the review committee on the Intelligence and Security Services, in Dutch CTIVD. But here after the review committee. And last but not least, the Investigatory Power Commission in Dutch TIB, we call it the TIB.

First of all, it is important to mention that in general the services can only act within their legal task and their task is described in the acts I just mentioned. The tasks of the general services are to conduct investigations with regard to organisations and persons who give cause for serious suspicion that they pose a threat to the continued existence of the democratic legal order, or to the security or to other vital interests of the state. That is the main task, and the main task of the military services is to conduct investigations into the potential and the armed forces of other powers for the purpose of a balanced composition and effective use of power. So the Dutch Armed forces. The exercise of special investigatory powers needs an ex ante review. And for special investigatory powers, not for all investigatory powers, the services need the minister's authorisation. Special powers are, for example, intercepting telephone communication, hacking and the interception of satellite or cable communication. The Investigatory Powers Commission is charged with reviewing the lawfulness of the authorisation granted by the Minister. The exercise of a special investigatory power against a journalist or a lawyer or if it concerns opening a letter is permitted only if the District Court of The Hague has granted authorisation. There is also general oversight on the services, and the review committee is charged with general oversight on the lawfulness of actions of the services. Their task is not limited to special investigatory powers. The review committee has access to all documents, all information systems, etc. of the services. However, their oversight is not binding. Part of the review committee is the complaint department, and the judgement of the complaint department are, unlike to the review committee, binding.

Now back to the Investigatory Powers Commissions. This commission has three members of whom at least two need to have six or more years experience in the judiciary. The third member does not have to meet these requirements. The ISS Act offers room to appoint a member with technical expertise and technical expertise has proved to be very important. The Investigatory Powers Commission performs an ex ante review of the lawfulness of the authorisation to use special powers that are granted by the Minister to the Services. The Commission is an independent commission. And equally important, the rule is binding. That means that if the Investigatory Powers Commission rules and authorisation to be unlawful, that special power may not be used. The Minister's authorisation is based on a written request, and the request comes from the services. So in practice, the Investigatory Powers Commission refused the written request from the services. Their request should contain all relevant information to review the granted authorisation. The Investigatory Powers Commission does not have access to the information system of the services to obtain additional information. However, the Commission can ask additional questions and in that way obtain all the required information.

The review of the Investigatory Powers Commission is not a marginal test. I will subsequently discuss four elements that are considered in the Investigatory Powers Commission's assessment. Each assessment. First of all, is a necessity. A request must substantiate the necessity to use an investigatory power. The Commission does not make its own evaluation of a presented threat, but reviews whether the threat that is presented in the request has been sufficiently substantiated and forms a reason to use the requested investigatory powers. Secondly is subsidiarity. As you all know, subsidiarity means reviewing whether the least invasive investigatory power is used to attain the aims. In more complex operations, particularly in hacking operations, technical expertise is frequently required to be able to review if the least invasive means will be used. Fortunately, we have this expertise in our commission. Thirdly, is the element as targeted as possible? The criterion itself is stated but not explained in the ISS Act. So the Commission had to define this criterion in practice and we defined it as follows: „The extent to which the acquisition of information that is not strictly necessary for the investigation is restricted to a minimum. Given the technical and operational circumstances of the case.“ Some people may argue that this criterion is redundant, given the test of necessity and proportionality and subsidiarity. But that's a separate discussion altogether. And that brings me to the last element of our assessment, which is proportionality.

In the case of proportionality, the importance of the investigatory power to be used is considered against the detriment the use will cause to the parties involved. Most often, the latter relates to the infringement of privacy. The Investigatory Powers Commission is of the opinion that everything that is known contributes to the balancing of these interests must be considered in the proportionality test. That means, for example, that in the case of a large threat, the use of more invasive investigatory powers is more likely to be justified than in the case of a lesser threat. But on the other hand, everything that contributes to the infringement of privacy must also be taken into consideration.

These four elements necessity, subsidiarity, as targeted as possible, and proportionality, are elements that are reviewed on each request. Also on request considering hacking. Now hacking is a special investigatory power that is allowed by the Intelligence and Security Services Act. The website of the General Intelligence and Security Service explicitly states that hacking is one of the special investigatory powers. So this is not a secret. It states that the service can hack a computer or smartphone or any digital device to gather information for their investigation. If one of the services want to hack a target, they have to address a request to the minister. If authorisation is granted by the minister, that is followed by a review by the Investigatory Powers Commission. There is general oversight by the review

committee. This committee can, for instance, check whether the information provided to the Minister and the Investigatory Powers Commission was adequate or can check whether the better information was stored securely.

Now, what does hacking include? I must warn you, the article considering hacking itself covers two full pages. So I'm afraid that is too many details for this hearing. What is important is that the power shall also include the power to penetrate any security features to introduce technical provisions in order to undo the encryption of data stored or processed in the automatic information systems. And it also can introduce technical provisions in connection with the actual exercise of the power referred to in other articles with other means, and to copy data stored or processed in the automated information system. Now, unfortunately, I have to return to my introduction. In the Netherlands, the technical means or tools of the intelligent agencies are considered a state secret, so I cannot tell you that much more about hacking. And I do have to end my presentation here. Thank you for your attention.