Committee of Digital Vulnerabilities in Society – Summary

Official Norwegian Report (NOU 2015: 13) to the Ministry of Justice and Public Security
30. November 2015

In recent decades digitalisation has led to radical social changes. It has improved work efficiency for most of us, so that fewer people are needed to carry out the same amount of work. Digitalisation has changed the way in which we control processes, so that complex operations and infrastructures can now be controlled from one or a few central locations. It has provided the population with a wide range of new services, such as mobile cashless payment systems, electronic interaction with public authorities and real-time traffic information, which allows us to find the most suitable route between two places. It has also revolutionised the way in which we communicate, with mobile phones, social media and collaboration support tools now being a key part of everyday life. Norway is a world leader in the use of ICT. This makes Norwegian industry more competitive and enhances society's overall productivity and innovativeness. To enhance further efficiency, society must have confidence that the technology is safe to use.

The major technological changes pose a few challenges. We see that key services, such as payment and telecommunications, are challenged by international organisations that provide services in Norway without the Norwegian authorities having the legal authority to regulate these. Our ability to keep information confidential, and thus also protection of privacy, is also challenged. Many organisations also face real threats of their computer systems being attacked and as a result becoming partly controlled by unauthorised persons. There is therefore significant technological pressure that can challenge key social values.

A particularly important observation is that critical societal functions have become dependent on long and complex value chains, which generally span over several sectors and countries. Therefore, the vulnerability of say a mobile payment service will be determined by legal provisions and supervisory regimes in the energy sector, the electronic communications sector, the financial sector and within industry regulation. A sub-contractor who has outsourced key parts of the operations to another country could inherit vulnerabilities from the corresponding sectors in the country in question.

We find such complex, cross-sectoral value chains in all the critical societal functions discussed in this report. This has implications for how we should respond to intentional and unintentional incidents. The consequences of a cyber security incident may lie in a different sector from the incident itself, and the knowledge that sector boundaries pose no obstacle to an attacker challenges our ability to manage live situations in an efficient or expedient manner.

One effect of the digital development is a sharp change in society's risk and vulnerability profile. We experience new threats, e.g., that machines and infrastructure in Norway may be attacked by anonymous players who are located in other countries. We have new vulnerabilities to deal with, such as programming errors in one

component that may cause a major mobile network outage. Through digital value chains, our societal functions are exposed to events in new and previously unknown ways. For example, a fault in the telecommunication networks can lead to road tunnels having to be closed and doctors not having access to patient files.

Just as digitalisation has changed the vulnerability status in society, the way we deal with these vulnerabilities will have a bearing on the society we create for the future. In a general societal perspective, proper vulnerability risk management will be crucial to maintaining the constitutional government and the democracy's fundamental values. At the same time, these same values may come under pressure when facing other, challenging digital opportunities, such as surveillance of individuals or of the population as such.

Norway is regarded as one of the most digitalised countries in the world. This has given us major efficiency and modernisation benefits, but it has also meant that we are one of the countries where the change in the risk and vulnerability profile has progressed furthest. One of the challenges of having come this far is that there is usually a lack of clear examples from other countries to use as a reference. This change requires that, as a society, we develop and change the way we relate to vulnerabilities. Yet it is clear that many of the challenges we are now facing can only be solved in an international context. For a small country such as Norway, it will be very important to participate actively in the international arenas where relevant issues are discussed.

In this report we have presented the steps we believe Norwegian society should take. Our most important recommendations are given below.

- *Reduce the criticality of Telenor's core infrastructure.* Telenor's core infrastructure is a component of virtually all digital value chains. Therefore, an outage in this infrastructure has serious and simultaneous consequences in most areas of society, and for the critical societal functions discussed in this report. Telenor's core infrastructure is well-developed, professionally operated and historically has very high stability. Nevertheless, it could be paralysed by human error, failure to follow procedures, sabotage, terror or disloyal personnel. In the view of the committee, the sum of the social values this network carries is unacceptably high. Therefore, the committee will recommend working toward a target state where at least one additional player has a nationwide core network, which is on the same level as Telenor's as regards coverage, route diversity, redundancy and independence.
- *Ensure the balance between protection of privacy and a safer society through studies and public debate.* The committee has noted that the interests of public safety lead to proposals to introduce new and intrusive surveillance methods. Examples of this are proposals to introduce digital border surveillance and the Norwegian Police Security Service's desire to register utterances on social media and to analyse information from open channels. The committee acknowledges the police and intelligence agencies' needs behind such proposals, but believe that the proposals are of such an intrusive nature that they should not be introduced

without prior public debate. Such a debate should be prepared through an official report that discusses these types of measures in full. Intelligence needs, technological expertise and protection of privacy must be safeguarded and a thorough report must be made on the technological, legal and social issues the cases raise.

- *Use of cryptography should not be regulated.* There is international debate on whether use of strong cryptography should be regulated. It is extremely difficult - perhaps impossible - to develop systems that safeguard legitimate needs for protection and monitoring at the same time. It is reasonable to believe that limitations in the lawful use of cryptography will affect Norwegian citizens, businesses and authorities. However, such limitations will not deter dishonest players from using cryptography and therefore not solve the police and the intelligence services' problem either. That is why the committee believes that use of cryptography should not be regulated or banned in Norway, that the Norwegian authorities should work actively against regulation or prohibition internationally and that new investigation methods must be developed to ensure efficient police and intelligence work.
- *Strengthen the inter-sectoral measures of the Ministry of Justice and Public Security in the area of cyber security.* No sector can control its own digital vulnerability alone. The value chains mean that all sectors inherit vulnerabilities from other sectors and sector boundaries are no obstacle to attackers. At the same time, the committee has also observed that at times the sectors have difficulty agreeing on implementation of cross-sectoral measures. The committee agrees that in many cases the various sectors are very different and may need specific adaptations. However, this is not in contrast to cross-sectoral solutions if these state a lower limit, so that the sectors are free to define stricter requirements. The committee finds that development of cross-sectoral mechanisms will be necessary over time, and that an efficient cross-sectoral public policy system will be necessary to deal with society's cyber vulnerabilities. The ability of the Ministry of Justice and Public Security to implement cross-sectoral measures should therefore be strengthened.
- *Establish a comprehensive framework for cyber security incident management.* The committee has noted that public and private organisations that are exposed to serious cyber attacks experience uncertainty and inadequate coordination between the government agencies that are responsible for combating cyber attacks. Therefore, the committee believes that the Ministry of Justice and Public Security must take the initiative to establish a comprehensive framework to clarify the efforts between relevant stakeholders in incident management and prosecution. The framework should be established and practised in close cooperation with the Ministry of Defence.
- *Strengthen police ability to combat cybercrime by establishing a new Cyber Crime Center.* The committee observes that among businesses and individuals there are low expectations as regards the assistance the police can provide to the victims of cybercrime. This means that only a small percentage of cybercrime is reported. Therefore, the committee would like to support the proposal to

establish a new national centre to prevent and investigate complex and cross-sectoral cybercrime. The centre should be organised under the National Criminal Investigation Service (NCIS, Kripos), and it should have a national technical responsibility for the prevention and investigation of serious and complex cybercrime. It should also have a separate assistance function to support the police districts both with respect to police tactics and prosecution.

- *Clarify a regulatory responsibility for Norwegian space activities.* Through digital value chains, most areas of society are more or less dependent on digital satellite-based services. These services may be position, navigation, precise indication of time, communication, earth observation, etc. Governance related to this area is complex. Regulation of the space activities is sanctioned by many different laws and regulations and the responsibility for monitoring the space sector has been decentralised. The need to clarify the regulatory responsibility for Norwegian space activities involves raising awareness about the vulnerabilities of the various areas of society, identifying dependencies and setting requirements for and the supervising space activities.
- *Strengthen cyber security skills in several supervisory authorities.* The committee sees an increasing digitalisation rate within most sectors and the supervisory authorities will be faced with many more or less new and complex issues. There will therefore be an increasing need to strengthen cyber security skills within more supervisory authorities. In the short-term it will be important to have joint resources, so that expertise may be supplied to various supervisory authorities from, for example, the Norwegian National Security Authority (NSM) in individual cases. In the long-term, technological development indicates that sectors and businesses must establish their own cyber security expertise. Most sectors will face similar challenges related to cyber security and it will be appropriate to establish common platforms for exchange of experience and dialogue between sector supervision and cross-sectoral supervision. In connection with the introduction of cyber security requirements, function-based regulations and supervision should be considered. This is in order to be able to keep up with fast technological changes and to facilitate security measures that are tailored to each activity.
- *Establish a general national skills strategy within cyber security.* The committee has seen that there is a challenging situation as regards cyber security skills at most levels of society. The curricula for primary and secondary schools include teaching objectives related to the subject, but it is unclear whether the actual learning outcome covers the cyber security knowledge each of us must have in order to be able to protect our digital life. The committee believes that the objective of a general strategy should be that a minimum of cyber security must be included in all bachelor degree programmes in ICT. A cyber security master's degree programme must be established and be in proportion to the competence needs in the public and private sector and a long-term plan should be drawn up for development and maintenance of Norwegian research capacity in this field.

In addition to the proposed measures we have highlighted here, we propose measures within each of the topics of electronic communication, satellite-based services, energy supply, oil and gas, water supply, financial services, health and care services, transport, research and education, management and crisis management, detecting and dealing with cyber attacks, joint components and cross-sectoral issues.