Roadmap for

Digital Hard- and Software Security

Roadmap for

Digital Hard- and Software Security

Ministry of Economic Affairs and Climate Policy
Ministry of Justice and Security

The Hague, April 2018


09:41
smart home
DEVICE
GROUP
SCENE
add new
preferences
speaker
lights
heating
power
doors
locks
OFFICE
LIGHT

Table of Contents

Foreword

At first glance, teddy bears, washing machines, thermostats and motion sensors might seem to have little in common. However, all of them can be connected to the Internet: teddy bears to help learn a language; washing machines that only run when the wind turbines are turning; and thermostats that learn when to turn themselves down. Sensors – depending on the devices and apps to which they are connected – can keep homes safe, or notify emergency services in the event of an accident. While still in its infancy, the Internet of Things is growing at an alarming rate. It brings ease and enjoyment to our lives, while also presenting unique opportunities and problems. It is precisely the increasing interconnectedness between the digital and physical worlds that makes the potential consequences of digital weaknesses so important. Imagine spy equipment disguised as children's toys, or smart thermostats in the Netherlands used to initiate DDoS attacks elsewhere in the world – unbeknownst to anyone. This Digital Hard- and Software Security Roadmap aims to prevent such scenarios.

The digital security of hard- and software demands a strategy that is both flexible enough to adapt to new developments and robust enough to remain effective, and an approach that clarifies risks and solutions and helps shape standardisation and mandatory certification, including risk-awareness campaigns – an approach that clearly shows what action consumers themselves can take. This approach aims to let providers, users and other stakeholders know where they stand, and contributes to confidence in the process of digitalisation. In so doing, the Roadmap contributes not only to digital security, but also to reaping the benefits of advancing digitalisation.

The present Roadmap is a collection of measures intended to bring about significant improvements to the digital security of hard- and software. This does not imply that we know all there is to know – the problems are still too new and too complex. Some processes are still at the exploratory stage, and we are aiming to collaborate with all the relevant parties (which are quite numerous, when it comes to digital devices) to decide how to proceed. The above applies to the development of a security monitor and innovative solutions for ensuring the security or proper disposal of hard- and software, and also to issues surrounding liability and supervision. This Roadmap is a living document. Updates will be issued as necessary, along with an annual summary of the developments.

I look forward to our journey together, as we move towards digitally secure hard- and software.

Mona Keijzer
State Secretary for Economic Affairs and Climate Policy


Station 2
Montagestation

Summary

Digitalisation increases our dependency on ICT. Although there are many associated advantages, this also makes us vulnerable to threats such as data theft, business sabotage or extortion. Because interconnected devices are increasing in number, digital security is a concern not only for individuals, but also for society as a whole. Many parties, including the Dutch government, are currently taking measures to promote the security of digital products. However, due to poor cohesion as well as market and behavioural failure, these measures are still lacking in effectiveness.

The Digital Hard- and Software Security Roadmap offers a cohesive set of measures for eliminating security gaps in hard- and software, detecting vulnerabilities and mitigating their consequences. All stages of the product life cycle are covered; digital security must be promoted from beginning to end, from product design and production right through to use and disposal. Effective examples include strong passwords, timely updates and deletion of data at the end of a product's life. Joint responsibility is also important in this respect, as it is not only the suppliers of a product, but also the users who have a part to play in digital security. The Dutch government is investing in various instruments aimed at promoting hard- and software security, to which other parties, such as sector organisations and universities, can also contribute.

Whatever the stage, the aim is to strike the right balance between security, freedom and economic growth. A one-sided focus on security can potentially undermine other public values, such as human rights and innovation, despite the fact that innovative products can actually help reinforce security in the long term. This Roadmap aims to counteract these threats and protect fundamental rights and values, while also taking full advantage of the opportunities offered by digitalisation. It also leaves room for complementary measures in specific domains or sectors, as relevant risk assessments and associated measures can vary greatly.

This Roadmap proposes the following measures:

Standards and certification. The application of standards in both the design and use of a product is important in order to reduce vulnerabilities. Standards can also be used to increase the demand for secure products. Most efforts in this regard are aimed at coordinating various initiatives that seek to create standards for retaining cost/other effectiveness and make an active contribution to European negotiations in the field of standards and mandatory certification.

Monitoring the digital security of products. Detecting and sharing information on vulnerabilities allows manufacturers to modify non-secure products. Retailers can consider removing products from the shelves and users can decide to patch or deactivate their products. The Dutch government intends to cooperate with the private sector and other relevant stakeholders to develop a monitoring mechanism offering information on the digital security of products, with a specific focus on devices that are part of the Internet of Things. This monitoring will also include experiences in the international arena.

Cleaning up infected user products. Internet service providers can play a major role in increasing hard- and software security. The Dutch government plans to initiate discussions with Internet service providers, to explore how they can help combat non-secure IoT devices (analogous to their successful approach to mitigate botnets.

Testing for digital security. Testing for vulnerabilities is necessary at various stages of the product life cycle. To gain experience and find out what a shared testing platform has to offer, a pilot is under development using a range of sector-based use cases.

Cybersecurity research. Innovation is indispensable when it comes to hard- and software security, which is why the Netherlands invests in research on innovative solutions to tackle security problems.

Liability. Liability legislation enables users to claim damages resulting from a lack of digital security, which acts as an incentive for providers to keep their hard- and software secure. The Dutch government is currently in dialogue with stakeholders and specialists regarding areas for attention and improvement when it comes to liability for insufficient digital security of hard- and software. The Netherlands is also actively taking part in the expert group on liability and new technologies. In the EU negotiations on the European Commission's proposal for a directive on digital content and digital services, the Dutch government is proposing mandatory security updates for software products supplied to consumers.

Statutory requirements, supervision and enforcement. Setting minimum security requirements can serve to keep non-secure products off the market. The Dutch government is investigating which minimal security requirements can be made applicable to devices under the EU's Radio Equipment Directive.

Awareness campaigns and empowerment. As part of the cybersecurity awareness campaigns run by the website https://veiliginternetten.nl, the Dutch government will be launching one or more public campaigns to support policy-making for digitally secure hard- and software. Awareness campaigns will tie in with the above-mentioned measures where necessary, in order to raise awareness and increase resilience among consumers and SMEs.

National government procurement policy. National governments are major hard- and software users. They can include digital security criteria in their procurement policies, in order to both set a good example and foster demand for digitally secure products. The Dutch government will investigate which additional measures are necessary or desirable in national government procurement to ensure digitally secure hard- and software.

1. Introduction

Ongoing digitalisation and rapid developments in ICT offer the Netherlands major opportunities for economic growth and social development. Thanks to new technologies, we are able to disseminate knowledge and information at heretofore unthinkable scales and speeds. The importance of ICT is expected only to increase as time goes on – a full quarter of the economic growth over the last decade was attributable to ICT, for example. This development is often referred to as the 'digital revolution', and many claim that this is only the beginning.

Ongoing digitalisation is increasing our dependence on ICT, which makes it even more important for people to be able to trust the digital products they use. This is essential not only for the digital security of individuals, but also for society as a whole. Hard- and software vulnerabilities can give malicious users easy access both to a single device and to the network to which it is connected. This can have potentially far-reaching consequences, such as hacking smart thermostats for DDoS attacks, the ability to sabotage appliances or entire production processes and theft of data that is stored on digital devices.

Policy challenges

A wide range of parties, including the Dutch government, are taking measures to ensure the digital security of their hard- and software.[1] Although 100% digital security is not possible, the optimum level of digital security in society has not yet been reached. Reasons for this include a lack of coordination between the various measures[2] and market as well as behavioural failure. Industry does not always take into account the security risks presented by digital processes and products, for example. It is also difficult for consumers to assess the security level of digital devices, or comprehend the long-term effects of their decisions when it comes to digital security.

The challenge is to formulate the right combination of measures for this complex arena. New, different and potentially stricter policy and other measures may be required to promote digitally secure hard- and software. A range of parties at various levels (e.g. national, European and international) can contribute to this process.

It is important to have a comprehensive understanding of the supply chain, applicable existing or new instruments and the solutions they can offer.

1 For a non-exhaustive summary of various instruments already in use by various parties to promote digitally secure hardware and software, see the 2017 study by the Netherlands Organisation for Applied Scientific Research (TNO) titled Digitaal Veilige Hard- en Software [Digitally Secure Hardware and Software].

2 TNO study (2017).

Digital Hard- and Software Security Roadmap

The Digital Hard- and Software Security (DHSS) Roadmap aims to provide the necessary coordinated approach that will allow the Netherlands to act as a leader in the field of digital hard- and software security. The Roadmap is dynamic in character in that it is both sufficiently flexible to take advantage of new developments and sufficiently robust to afford investments in long-term measures.

The DHSS Roadmap contributes to the implementation of the Dutch Cybersecurity Agenda,[3] and incorporates the findings and recommendations from the TNO report titled Digitaal Veilige Hard- en Software [Digitally Secure Hard- and Software]. The Roadmap also takes into account European developments[4] and the recommendations of the Cybersecurity Advisory Council of the Dutch government on the subject.[5]

Work-in-progress

The Roadmap will always be a 'work-in-progress', and the Dutch Ministries of Economic Affairs & Climate Policy and Justice & Security wish to continue to develop and implement it in conjunction with relevant stakeholders. This version presents the initial building blocks. General principles have been formulated, with an attempt to produce a comprehensive set of measures for promoting digital security in a balanced fashion, involving the responsibilities of relevant stakeholders. The above does not eliminate the need for complementary measures, which may be required in specific sectors and domains.

3 Dutch Cybersecurity Agenda 'Nederland digitaal veilig' [Dutch Digital Security], Ministry of Justice and Security (2018).

4 https://ec.europa.eu/digital-single-market/en/policies/cybersecurity#usefullinks.

5 CSR2017, 'Naar een veilig verbonden digitale samenleving: Advies inzake de cybersecurity van het Internet of Things (IoT)' [Towards secure connections in a digital society: Cybersecurity recommendations for the Internet of Things (IoT)].

Internet of Things

The 'Internet of Things' (IoT) is a key driver of the digital revolutions. More and more products are becoming connected to the Internet, and the IoT is an expanding paradigm of technical, social and economic significance. It is an emerging concept that consists of a broad ecosystem of interconnected services and devices, such as smart everyday household items, cameras, cars and health monitors. A typical aspect of this technology is the collection, exchange and processing of data via the Internet. In 2017, 8.4 billion devices were connected to the Internet worldwide – 31% more than in 2016. This number is expected to increase to 20.4 billion by 2020, at least 63% of which will be consumer devices;[1] the remaining 37% will be used by industry.

Threat

Recent years have seen warnings by various security experts regarding the increasing threat presented by IoT. In general, IoT devices have poor digital protection. This is partly due to the use of standard passwords, the lack of encryption or the absence of software updates to eliminate security vulnerabilities and fundamental design flaws. Such vulnerabilities have been exploited multiple times in recent years, and IoT devices have been used as a means to initiate attacks. Devices have also been hijacked to listen in on users, or manipulate their environments, including their business processes.

IoT in the Netherlands

Over 92% of Dutch residents have multiple IoT devices in their homes – devices that are attractive to cybercriminals. Despite the fact that 82% of Dutch residents are aware that devices connected to the Internet are susceptible to hacking, nearly three-quarters (71%) have taken no measures against cybercrime.[2] This causes increasing problems, for third parties as well as the users themselves. Mirai malware has been used to hack IoT devices (such as smart thermostats and TVs) in order to bring the Internet to a standstill, with around $110 million of damage in North America and Europe as a result. Dutch IoT devices have also been infected by that malware.

1 https://www.gartner.com/newsroom/id/3598917.

2 BIT 2017, Internet Eigenwijs [Internet Your Way].

Terms

This Roadmap uses various terms, such as ‘hardware’, ‘software’ and ‘digital products and services’. Figure 1 illustrates these terms, using the example of a smart washing machine. The difference between **hard- and software** can be expressed in two ways:

1: Hardware is a collective term for the physical components in digital devices, while software is the collective name for the intangible programming carried out on digital devices. Devices rely on the interaction between hard- and software to function effectively. Hardware, for example, has certain performance limitations. If the demands of the software exceed these limitations, the device will not work properly.

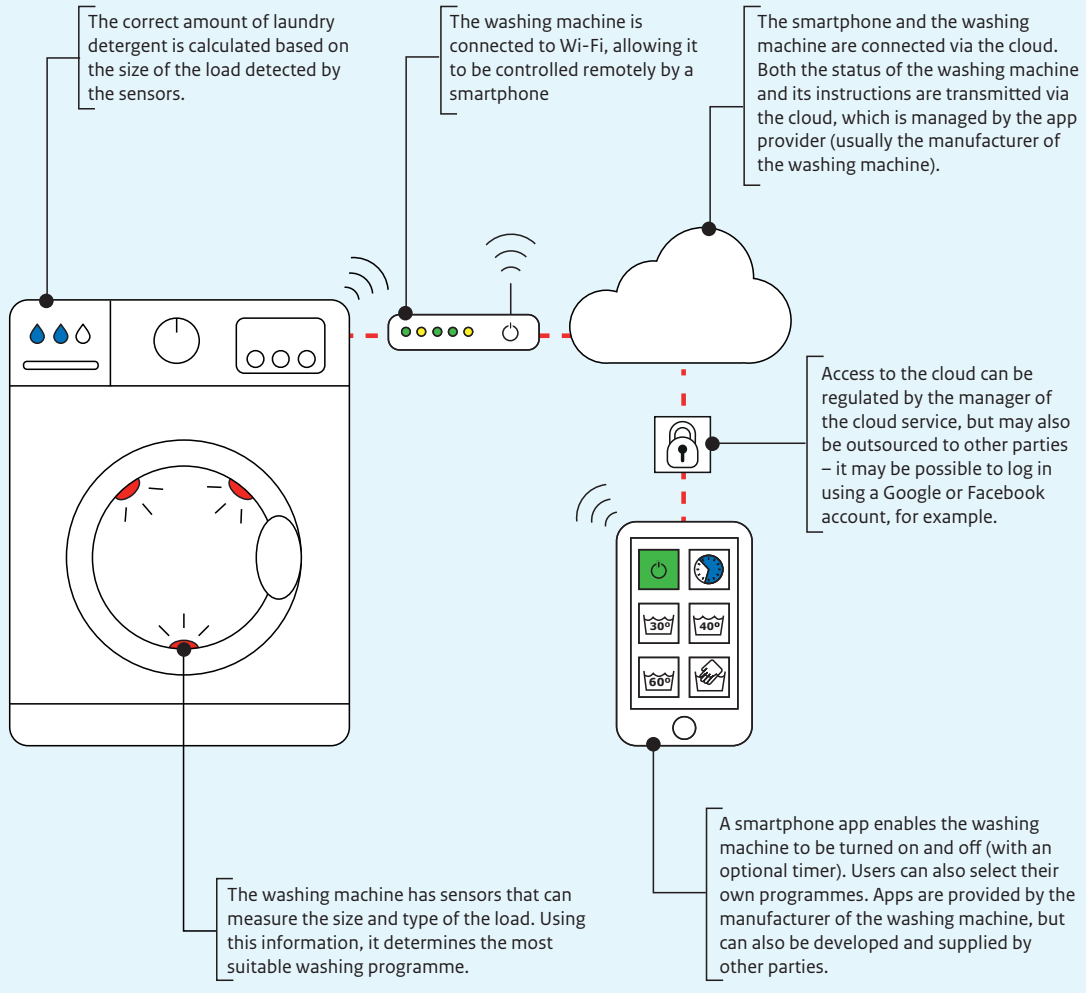
2: The difference between hard- and software can also be expressed in terms of variability. In this sense, hardware can be viewed as the parts of a device with fixed functionality that cannot be changed, and software as the part that can be more easily modified, replaced or removed. This distinction is not black-and-white, however. Certain software is pre-programmed into the hardware by the manufacturer, and is very difficult for users to modify or remove. Examples of this kind of software include ‘firmware’ (which controls the hardware at a very deep level) and ‘embedded software’ (which has been designed specifically for certain hardware and is often the only software present on the device in question). Moreover, the functionality of hardware is not unchangeable, as it can always be altered by changes to the software. The physical characteristics of the hardware will not change, however.

Digital products are products with a software component. They may also include hardware components, but this is optional. A **digital service** is a service offered via electronic means. Examples of these types of services include software updates and subscriptions to digital products.

Figure 1 *The terms 'hardware', 'software', 'digital product' and 'digital service' can be illustrated using a smart washing machine, which uses sensors in the drum to select the correct programme and quantity of laundry detergent. It can also connect to a smartphone through a Wi-Fi network, enabling it to be operated remotely using an app via a cloud service.*

All the mechanical and electronic components of the washing machine and the smartphone are classified as 'hardware' (e.g. the machine drum and the sensors and chips in the washing machine and smartphone). All of these components, in both the washing machine and the smartphone, are controlled at a deep level by firmware. At a higher level, they are controlled by specific software: the software in the washing machine was pre-installed by the manufacturer (embedded software), while the software on the smartphone can be downloaded by the user in the form of an app.

The washing machine is a digital product, because it contains software elements. A digital service is also linked to it (the cloud service). If the washing machine was not purchased but rented, the machine itself can be regarded as a digital service as well.



2. Basic principles

The DHSS Roadmap is based on five principles that govern the current and future development and implementation of an approach to digitally secure hard- and software. They are set out in greater detail below.

2.1 Product life-cycle approach

All stages in the product life cycle can play a role in improving the digital security of hard- and software. There are three stages, roughly speaking: pre-use, during use and disposal. When considering hard- and software security, it is easy to gravitate towards setting product design requirements. Where digital products are concerned, however, the usage stage is equally important, as these products are frequently accompanied by a digital service (often a cloud service) that is updated on an ongoing basis. During this stage, it is not only product manufacturers, but also the users who are responsible for ensuring digital security, by changing passwords, installing updates, etc. (see principle 2, 'Joint responsibility'). Once the manufacturer has decided to stop updating the software, the user may still continue to use the product. The disposal stage is therefore also explicitly included in the set of measures.

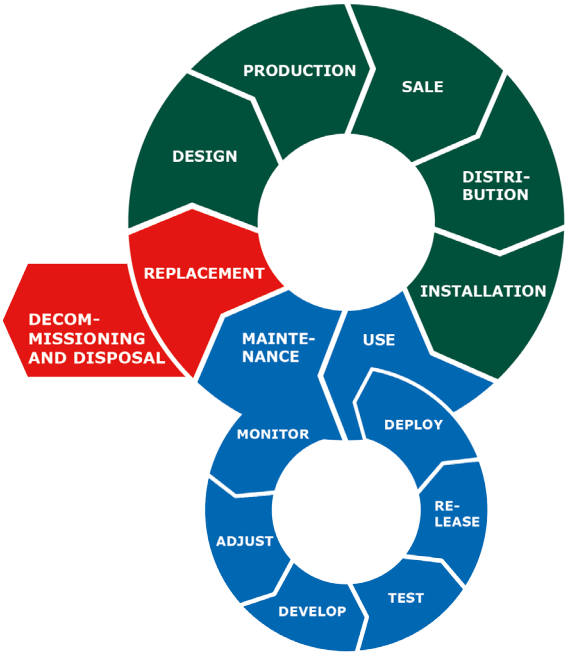


Figure 2 All stages in the product life cycle are important for improving the digital security of hard- and software. A distinction can be drawn between the pre-use stage (green), the usage stage (blue) and the disposal/ replacement stage (red).

2.2 Joint responsibility

The parties involved have various responsibilities and roles, based on the premise that digitally secure hard- and software requires a concerted approach. These parties are very diverse in nature, however, ranging from consumers, SMEs and multinationals to scientists, civil society and supervisory authorities. Although each party has its own roles and responsibilities, more can generally be expected from larger, professional parties than from their smaller counterparts. The following general distinctions can be drawn, where the finer details will be partly determined by both the context (e.g. relationships such as B2B, C2B, C2C, critical/non-critical infrastructure) and the party type (e.g. professional vs. non-professional).

Providers (manufacturers and retailers): providers are mainly responsible for the digital security of the hardware, software and associated services they offer. They are the initial link in the chain, the point at which digital security can be anchored in the design, production and sale of hard- and software.

Users (from consumers and SMEs to multinationals): users can create demand for digitally secure hard- and software, and can also play a part in the maintenance of hard- and software. The limited rationality of users must be taken into account, however: it is harder for users to assess the impact of digital security risks, and they will lose sight of the bigger picture if swamped with too much information.

Government (including supervisory authorities): the government is responsible for upholding public values, and can do so using various policy instruments, such as incentive schemes, behavioural experiments and legislation. As a user and outsourcing party, the government can also help bolster the demand for digitally secure hard- and software.

Other parties (e.g. sector/consumer organisations, intermediaries and scientists): in addition to thoselisted above, there is a diverse group of other parties that can contribute to digitally secure hard- and software. It is important that these parties also be included in the Roadmap.

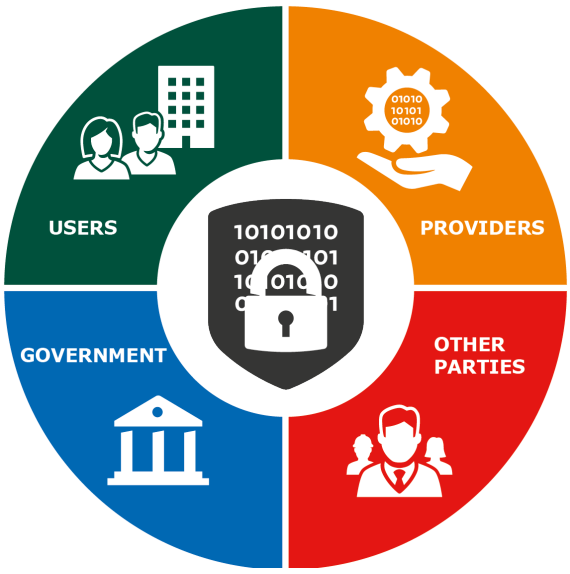


Figure 3 All stakeholders must be involved in promoting digital hard- and software security.

2.3 Balancing public values

A dynamic balance between security, freedom and economic growth is essential when promoting digital hard- and software security. Digital security is key in order to take full advantage of the economic potential of digitalisation. However, a one-sided focus on security can potentially undermine other public values, such as human rights and innovation. A set of measures that fails to take the innovation climate into account, for example, may adversely affect the innovative capacity of the Netherlands – an undesirable scenario. Innovative products, after all, can actually help enhance digital security. The Dutch government and its partners are therefore investing in a free, safe and open cyber domain where the opportunities offered by digitalisation are fully utilised, threats are countered and fundamental rights are protected.[1] This can be achieved through a constant open dialogue between all stakeholders, both national and international.

1 See, among others, the Dutch Cybersecurity Strategy 2 (2013) and the International Cyberstrategy 'Building Digital Bridges' (2017).

Weighing up public values

Determining the right balance of public values is a complex task, a fact illustrated by the system used in the report titled 'Balancing interests in developing cyber policy: A conceptual framework', which was commissioned from PwC and Clingendael by the Ministries of Economic Affairs & Climate Policy, Justice & Security and Foreign Affairs. Many dimensions covered by the fields of economic growth, freedom and security are necessary to ensure these public interests. An example of this is users' freedom to decide whether to install a software update. Should users always be free to make this decision themselves, or are there conceivable situations in which software updates should be installed automatically? The answer to this question can also affect other public values. For example, automatic software updates may have a positive effect on digital security, but at the cost of individual freedom.

Core public interests	Dimensions of intervention	Key policy dilemmas
Freedom	Ethical	• Paternalism vs. individual responsibility • Human vs. computer
	Economic	• Protective vs. reactive • Monopolies vs. competitive market
Prosperity	Legislative	• Transnational vs. national • Regulation vs. 'laissez faire'
	Administrative	• Centralized vs. decentralized • Private vs. public
Security	Diplomatic	• Transparency vs. secrecy • Digital sovereignty vs. international cooperation
	Protect & enforce	• Offensive vs. defensive • Known vs. unknown enemy

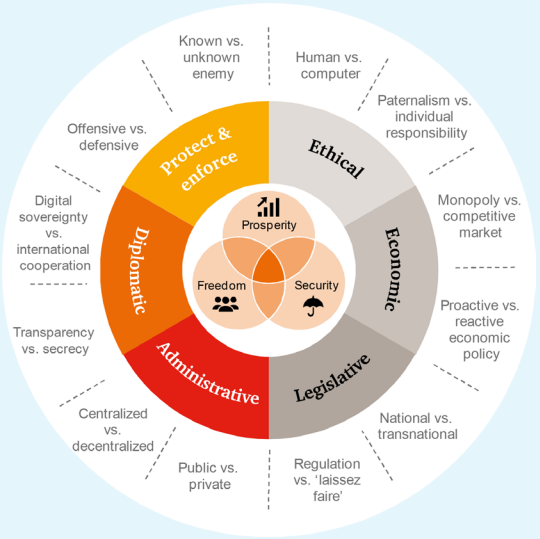


Figure 4 A conceptual framework for balancing the public values of freedom, security and prosperity in the cyber domain. Source: 'Balancing interest in developing cyber policy; A conceptual framework' (PwC and Clingendael, 2017)

2.4 Portfolio approach

Promoting digitally secure hard- and software requires a broad spectrum of instruments. The digital product ecosystem is complex, and vulnerabilities can emerge at various stages of the product life cycle (as outlined above). The various components of digital products can also result in security risks, each with its own impact. A range of national and international parties are involved in the different stages and in the production of the various components, meaning that the risks cannot all be combated with a single instrument. Several instruments are necessary in order to promote digitally secure hard- and software in a balanced and dynamic manner. It is also important to look at how the different instruments interrelate: where might frictions emerge, and where can synergies be created? In this respect, the Dutch government has a steering role in upholding digital security as a public value. It can do so by means of 'softer' instruments, such as education and incentive schemes, or using 'hard' measures, such as legislation.

Prevention, detection and mitigation

The measures in this Roadmap can be further subdivided into three categories: prevention, detection and mitigation (see Figure 5). Prevention measures are implemented to limit the scope of the security risks, such as by setting standards or encouraging innovation in the field of digital hard- and software security. Given that 100% digital security is not a reasonable expectation, other instruments are also used to detect security risks, such as the active testing of digital systems. Lastly, measures are taken to mitigate the effects of security incidents, liability law being one such instrument. This mix of instruments will be outlined in greater detail in the following section.

Figure 5 *Promoting digital hard- and software security requires a broad spectrum of instruments.*

Basic principles of digital hard- and software security

Given the government's steering role in upholding the public value of digital security, it is worthwhile to consider the extent to which it is possible to create a set of basic principles applicable to digital hard- and software security. Such a set of principles would represent a group of elements and features that the government, in conjunction with public and private parties, wishes to maintain or exclude when it comes to digitally secure hard- and software. These may include non-default passwords, transparency on data usage and the objectives of algorithms, and clarity regarding the frequency of security updates. Any set of basic principles developed will tie in with existing initiatives. The aim is to counteract a potentially fragmented approach by using shared standards and to promote harmonisation. This set of basic principles could also serve as the basis for potential supplementary, sector-specific measures (see principle 5 below) and for a pro-active attitude within Europe. Our goal is to work with stakeholders to create principle descriptors that are shared at national level, and are effective and efficient.

2.5 Room for a complementary (differentiated) approach

The DHSS Roadmap offers a foundation for the Netherlands to lead the way in promoting digital hard- and software security. It offers the initial building blocks, and attempts to create a balanced set of measures that satisfy the basic principles listed above. Complementary measures will still be required, however, as making well-considered risk decisions and determining appropriate measures will remain necessary in each domain and each sector. Consumer products will be subject to different considerations than critical infrastructure or industrial processes, for example, and measures appropriate to one domain will not always be transferable to another. This Roadmap (and other frameworks) will therefore need to leave room for complementary domain/sector-specific measures wherever they are necessary or desired.

3. Measures

3.1 Standards and certification

Standards and certification can help improve digital hard- and software security throughout the product life cycle, from design to disposal. They reduce the number of vulnerabilities during the development stage, and can also help resolve them during the usage stage. Certification of hardware/software devices or their providers makes it clear to users exactly what they can expect from a device or provider. Such certification by an independent, expert organisation can help purchasers make the right choice and boost demand for secure products.[1] Standards and certification can also be used to demonstrate compliance with statutory requirements (see Section 3.7).

The Netherlands wishes to harmonise the various standardisation and certification initiatives as much as possible. Many such initiatives are currently underway,[2] which confuses businesses as to which standard they should apply, and confuses procurers regarding what a standard or certification actually entails. This reduces the effectiveness of standardisation and certification. Fragmented initiatives also mean high costs for many parties in terms of both time and money. This is especially problematic for SMEs, as they often have limited resources for implementing standards and are, partially for this reason, often dependent on the wide-ranging requirements of dominant procurers.

In order to increase the adoption rate of standards that contribute to digital security, the Netherlands is making an active contribution to standards and certification with broad national and Europe-wide acceptance, thus helping to combat fragmentation and disruption of the level playing field. Reciprocal acknowledgement of standards and certifications can also help reduce transaction costs, increasing the affordability of digitally secure IoT devices.

Actions

» As part of the EU negotiations, the Netherlands is insisting on the rapid adoption of the Cybersecurity Act (CSA) and the active development of a European Cybersecurity Certification framework for ICT products and services. Moreover, the Dutch government supports the swift adoption of mandatory certification for specific product groups, i.e. products that present the greatest risk or the most problems in practice. In the long term, mandatory certification or compliance with a CE marking for all products with Internet connectivity should be implemented through gradual expansion (see Section 3.7, 'Statutory requirements, supervision and enforcement').

1 Netherlands Bureau for Economic Policy Analysis (CPB) Policy Brief 2018/1, Knelpunten op de markt voor cyberveiligheid [Problem Areas in the Cybersecurity Market].

2 See also, among others, the TNO study (2017).

EU Framework: Security Certification of ICT Products and Services

The proposed Cybersecurity Act (CSA) is the European Commission's attempt to create, amongst others, a harmonised framework for the cybersecurity certification of ICT products and services within the EU. The absence of reciprocal agreements on standards and certification systems forms a barrier to creating a European market for cybersecurity products and services. It limits the scale for providers, and reduces choice and creates increasing uncertainty for procurers. This can be changed through common European certification of products and services, indicating that they are resilient (at a specified security level) to threats to their availability, authenticity, integrity and reliability of data or of the functionalities and services being offered. The CSA aims to target fragmentation and foster the harmonisation and reciprocal acknowledgement of cybersecurity certification at European level. Once a European certification framework has been adopted for a product or service, national government schemes will become redundant and Member States will no longer need to develop their own certification programmes.

Partnering Trust

The aim of Partnering Trust is to bring uniformity to the criteria for online and other ICT services, enabling providers to clearly specify the security and reliability of their product range and to provide a uniform demonstration of the quality of services (e.g. for auditing and certification purposes). Partners in Germany (Trusted-Cloud), France (Labelcloud) and the Netherlands (Zeker-Online) focus on online services. These include cloud services, which are essential for supporting new digital services, as they supply the necessary data storage and computing facilitiesr. It is for this reason that the European Commission has included cloud services as a priority in its memorandum on normalisation practices. As part of Partnering Trust, the Netherlands works in conjunction with Germany, France and the European Commission, among others, to give this priority due attention.

Secure Software Alliance

The aim of the Secure Software Alliance is to further develop the Secure Software Framework (SSF) for secure software development, and guarantee its quality. The framework essentially aims to guarantee software security at the earliest possible stage, by addressing potential vulnerabilities at every point in the product life cycle. The alliance also aims to bring hard- and software developers and their customers closer together. Especially where customisation is required, this relationship (and the distribution of responsibility) is of crucial importance. The certifications that attest to process quality are a key component in this regard. The Secure Software Development (SSD) framework of the Dutch Center for Information Security and Privacy (CIP) addresses both contractors and clients, proceeding from a baseline framework of standards that safeguard the quality of the end product.

Smart Industry

In order to help the Dutch production industry take advantage of the opportunities offered by digitalisation, the Smart Industry Standardisation Platform was launched in 2018 as part of the broader Smart Industry standardisation action agenda.

The Dutch government will also argue for the above in the European Council. [3]

- Promotion of standards/certification: in preparation for the CSA, the Netherlands has already launched initiatives in a number of key fields to promote the adoption of international standards and the formation of partnerships and frameworks, such as Partnering Trust, the Secure Software Alliance and the Smart Industry Standardisation Platform. Concerning existing and potentially new initiatives, leading up to the CSA, the Netherlands will actively seek cooperation with other European countries. Market incentives for encouraging the application of standards and certification will also be investigated. Insurers and government procurement policy are examples of key avenues in this respect.
- Clustering of standardisation and certification initiatives: The Netherlands aims to pro-actively forge links with global standardisation and certification initiatives via the NEN standardisation platform, which can play an important role in streamlining Netherlands-based activities in the various international standardisation institutions. This approach can ensure that Dutch interests are represented, creating a broad support base for international standards and certification programmes.
- The Netherlands will invest in multilateral collaboration in the field of IoT standardisation, through global platforms such as the Global Forum on Cyber Expertise (GFCE). Potential partners include countries in the top 10 of the World Economic Forum's Global Competitiveness Index, which are leaders in the production and early adoption of hard- and software.

3.2 Monitoring the digital security of products

As stated above, 100% digital security is not a viable objective. There is an unavoidable chance that non-secure products will end up on the market, products may become non-secure during use and that updates for a product may cease to be provided. Manufacturers, retailers and users alike all benefit from transparency regarding the quality and security of digital products. A monitoring mechanism that provides information on the security of digital products can be of great value, as it enables manufacturers to modify their products in response to identified vulnerabilities, and potentially to recall them from the market in the event of clear security threats. This information can also help them continue to develop secure products. Retailers can decide to stop selling certain products, and users can opt to have their products patched or deactivated for their own security.

Where possible, it is preferable to adopt an international approach in this regard, given the highly international character of the digital product market. Further study with regard to this concept of monitoring is required to determine exactly what information is relevant and who should receive it. This study will also incorporate international experience with this kind of monitoring.

Action

- The Dutch government intends to collaborate with parties from the public and private sectors to develop a monitoring mechanism offering information on the digital security of digital products, with a specific focus on IoT devices. This mechanism will also include experiences gained in the international arena.

3.3 Cleaning up infected user products

Internet service providers can play a major role in combating digital vulnerabilities. As managers of Internet connections, they can alert users to any non-secure devices identified on their networks, representing a potential contribution to digital security during the usage and disposal stages of the product life cycle.

Abuse Hub

The Abuse Information Exchange manages a centre (Abuse Hub) that provides its members with regular reports on the level of botnet malware infections on the computers of its end users. The members cover over 90% of the fixed-line broadband Internet connections in the Netherlands; these connections are also where we would expect to find the vast majority of IoT devices used in a domestic or small-business context. Abuse Hub has proven its worth, since the proportion of infected computers among affiliated providers dropped from 80% in 2010 to 60% in 2016. Expanding the reports to include infected IoT devices could improve things even more. The Abuse Information Exchange is currently investigating the feasibility of increasing the scope to include IoT devices.

3 This campaign will put into effect the motion to argue for mandatory certification for products with Internet connectivity put forward by Paternotte et al. (Parliamentary Paper 21501-30, No. 422).

A dialogue with Internet service providers and the Abuse Information Exchange is currently underway to determine how they can help keep non-secure IoT devices off the Internet, along with ways of informing their subscribers and recommending a course of action whenever devices are found to be vulnerable or compromised. This can make a significant contribution to combating non-secure devices.

Action

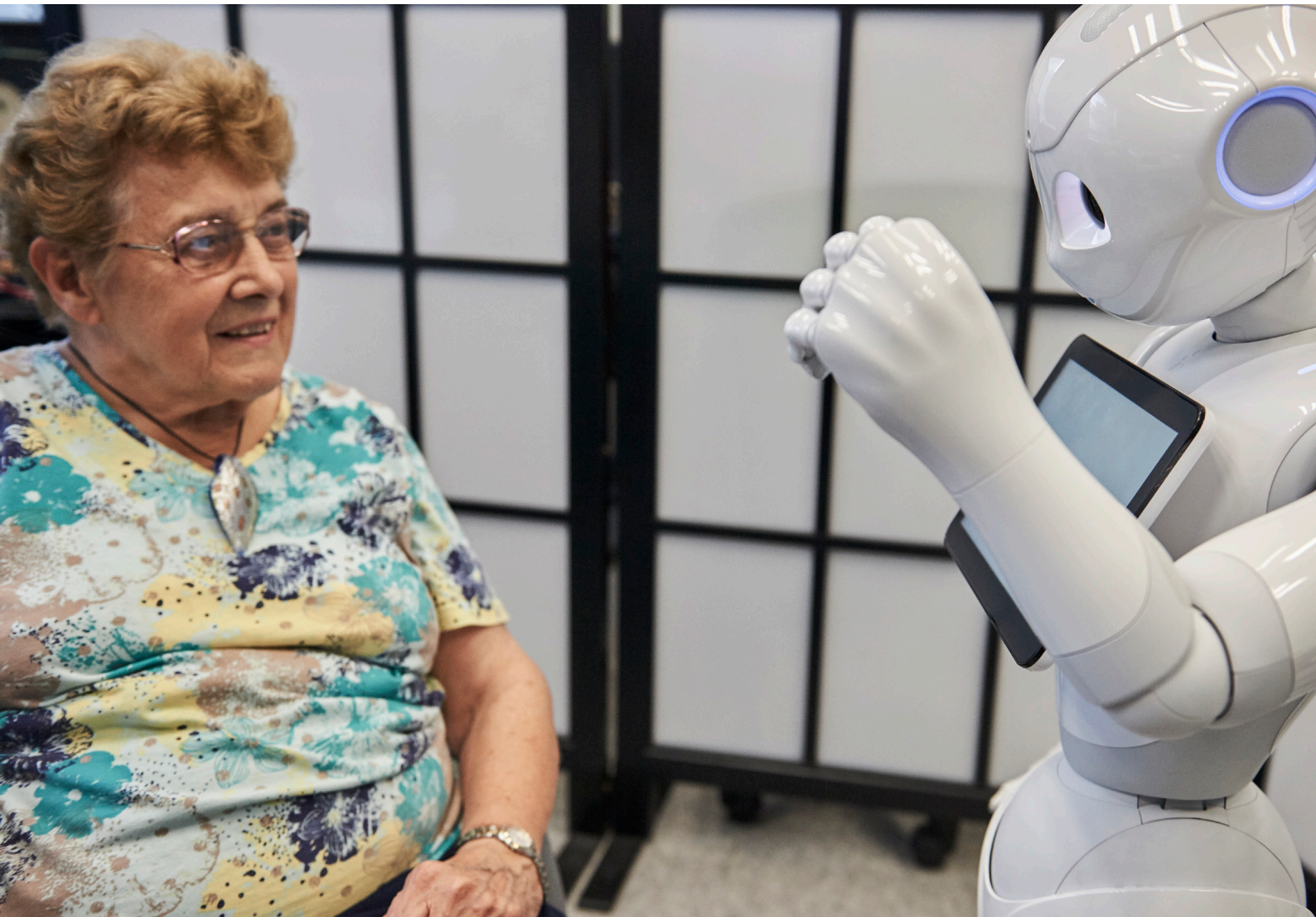
» The Dutch government plans to initiate discussions with Internet service providers to explore how they could help combat non-secure IoT devices (analogous to their successful approach to mitigate botnets).

3.4 Testing for digital security

Product testing is essential in order to attain a level of certainty regarding digital security. Providers test products (e.g. during development), and businesses and organisations regularly evaluate the digital security of their internal ICT environments. There are many ways to test products, services and systems for digital security, including cybersecurity scans, red team assessments, penetration tests and ethical hacks (for responsible disclosure or coordinated vulnerability disclosure purposes). A cybersecurity market is emerging that caters to the growing demand for testing, with wide-ranging and differentiated supply and demand. The market is also dynamic; cybercriminals are always coming up with new ways of attacking products and systems, to which providers must be ready to respond. In conjunction with TNO and industry, the Dutch government aims to launch a pilot to determine the potential value of a shared testing platform for organisations when testing more accessible sections of the supply chain (or the entire chain of which their product is a part), and to facilitate knowledge exchange.

Action

» A pilot will be launched using a range of sector-specific use cases, to gain experience with a shared testing platform and explore its possibilities.



Cross-Sector Cyber Testbed

Testing may become more accessible and knowledge exchange more effective if a testing platform or parts thereof can be shared across multiple sectors (a 'Cross-Sector Cyber Testbed', or CSCT). A testbed of this type ought to enable businesses to test sections of the chain (or the entire chain of which their product forms a part), involving multiple parties from the relevant chain. The ability to test 'across the chain' is unique, and can be of great value to providers and users of ICT products and services. The test results are important to all parties involved in the task of maintaining the desired level of digital security protection. These results can also serve as input for both existing standards and those yet to be developed. Opportunities also exist for creating links to education, where testing facilities can be used in education and research programmes to not only generate, safeguard and disseminate new knowledge, but also to facilitate ongoing mutual learning. The potential benefits of collaboration with existing national and international testing platforms is also under consideration.

3.5 Cybersecurity research

The development and market maturity of innovative solutions can make a significant contribution to the digital security of hard- and software. Innovation requirements differ at each stage of the product life cycle, which means that entirely new solutions are necessary for the disposal stage, to facilitate the safe deactivation and removal of hard- and software. Product design, manufacturing and usage require not only the development of new technological and other solutions, but also research on influencing behaviour (among users especially) and more intensive collaboration in order to strengthen the overall knowledge base.

The ministries of Education, Culture & Science, Justice & Security, Defence and Economic Affairs & Climate Policy plan to strengthen their involvement with the cybersecurity knowledge base.[4] This decision has been prompted by both the growing dependence on foreign suppliers of cybersecurity products and services, and a rising need for knowledge and expertise in the field of digital security. Cybersecurity – which includes the development of the digitally secure hard- and software knowledge base – is one of the themes addressed by the Safe Society Societal Challenge programme. [5] This initiative focuses on research into secure and reliable systems (including crucial infrastructure and communication); defence and management of systems and crucial/other infrastructure; helping citizens and organisations develop digital skills and awareness; socio-economic factors and the ethics of cybersecurity; privacy, identity and participation; and public administration and law enforcement.

The Netherlands is also investing in the development of cybersecurity research and the application of the Small Business Innovation Research (SBIR) instrument, to promote research contributing to innovative solutions, digitally secure hard- and software and beneficial external effects, such as knowledge spillovers.

In addition, the Netherlands aims to foster the development of encryption software that will improve the digital security of hard- and software. As part of the aforementioned National Cyber Security Research Agenda III (NCSRA III), an additional €410,000 will be earmarked to encourage research initiatives and projects in the field of cybersecurity, especially those that feature encryption as a key aspect.

The Dutch government plans to organise dialogue sessions with relevant stakeholders to generate new innovative solutions for the disposal stage. Research shows that there is a lack of focus on instruments applicable to this stage, while developing relevant instruments would create opportunities for providers, users and society as a whole. Consider new business models such as software-as-a service, in which consumers pay to use a product rather than purchasing it outright. This offers advantages to providers and users alike, including a more clearly delineated set of responsibilities, where providers are responsible for installation, maintenance, management, timely automatic remote updates and upgrades, and backups. By aiding the sustainable use of products, this business model therefore also contributes to a sustainable society.

4 2017 – 2018 session, appendix to the proceedings, 664.

5 Refer to the 'safe society' challenge in the Kennis- en Innovatieagenda 2018-2021: Maatschappelijke uitdagingen en Sleuteltechnologieën [Knowledge and Innovation Agenda for 2018–2021: Social Challenges and Key Technologies]. https://www.topsectoren.nl/publicaties/publicaties/ rapporten-2017/december/11-12-17/kia-2018-2021.

National Cybersecurity Research Agenda III (NCSRA III)

The third National Cybersecurity Research Agenda (NCSRA III) is currently under development, and offers a framework for a broad and multidisciplinary cybersecurity study. The implementation of the agenda aims to help coordinate cybersecurity research efforts in both the public and private sectors. One of the agenda's five pillars is 'improved design', which encompasses all usage-stage software-development activities.

Small Business Innovation Research (SBIR)

The SBIR programme harnesses the creativity of the business community to solve problems, and urges entrepreneurs to develop and market new products. To do so, it uses a phased innovation competition, in which businesses that submit the best offers are awarded the contract to conduct a feasibility study. The businesses with the most promising feasibility studies will be commissioned to develop their products further in a testbed environment or pilot; later on, these solutions will stand a good chance in government tender procedures.

Actions

- Dcypher will release a new National Cybersecurity Research Agenda (NCSRA III) in Q2, seeking to coordinate research efforts addressing the design of secure systems and services, among other topics.
- The Cybersecurity SBIR currently includes tenders in the research and development stage, which focus on the security of IoT hard- and software and will be completed by mid-2019.
- The Dutch government is encouraging open-source encryption by earmarking additional funding as part of the NCSRA III.
- The Dutch government will organise dialogue sessions on innovative solutions for application in the disposal stage of hard- and software.

3.6 Liability

Liability law not only gives users recourse to claiming damages resulting from a lack of digital security, but also encourages providers to take measures in order to prevent or control damage. Liability acts as an important financial incentive for providers to both ensure and maintain the security of hard- and software, and encourages them to consider possible negative external effects in the development and marketing of digitally secure hard- and software. As such, liability law contributes to the digital security of hard- and software throughout the product life cycle.

The Dutch government will discuss the liability model with stakeholders and experts and ask them to contribute ideas for optimising the preventive effect of liability law. The central question concerns the issues parties are confronted with in reality. What damage results from non-secure hard- and software, and who are the victims? Are businesses and consumers aware of their options for claiming damages under existing liability law, including the relevant product liability? What problems might they encounter when trying to claim damages?

The discussions held to date have revealed that liability law in and of itself would seem to offer sufficient recourse to options for claiming damages. However, the discussions also showed that improvements are possible through a more precise definition of 'error' or 'fault'. At present, it is not always clear when software contains an 'error' or is 'faulty', and it is therefore not always immediately apparent whether the provider is responsible for the shortcoming. This could be remedied outside liability law itself, by formulating product and minimum requirements that clarify exactly when software can be considered to contain an error or fault. If the software does not meet these requirements, it becomes easier to demonstrate that it is faulty and to claim damages (see also Section 3.7). Some predict that such requirements will be more effective than modifications to liability law, due in part to the fact that product and minimum requirements are more effective against negative external effects, as software that does not meet the requirements cannot enter the market. This helps avoid losses suffered by individual consumers and businesses, but also prevents damage caused to society by DDoS attacks and the like.

Actions

- The Dutch government is currently in dialogue with stakeholders and scientists regarding areas for attention and potential improvements and solutions in the field of liability for a lack of digital hard- and software security. Based on these discussions, the government will establish possible future steps in conjunction with public and private parties.

European developments in liability

The digital security of hard- and software is inherently a cross-border concern. The European Commission evaluated the EU Directive on product liability in 2017: the results, which are expected to be made official in Q2 2018, present a good opportunity for an EU exchange of ideas regarding whether (and if so, how) product liability regulations should be modified with regard to technologies such as IoT devices and software. In view of this, it is important that the Netherlands participate in the European Commission expert group on liability and new technologies, which will also look at the Product Liability Directive. To date, national discussions and the literature have already proposed extending product-liability regulations to software as well, along with broadening the definition of 'damage' to also include purely financial loss (currently, the definition is essentially limited to damage due to death or injury). The Dutch government will include this aspect in its evaluation of the results of the aforementioned evaluation, and in its participation in the expert group.

The following development will affect the liability of retailers of digital content and digital services (e.g. software, e-books, films, music streaming) to consumers. Negotiations are currently underway regarding a proposed EU Directive 'on certain aspects relating to supply contracts for digital content'. Such a Directive is intended to regulate the rights of buyers and sellers, such as the contractual requirements applicable to the provision of digital content, and legal recourse for consumers if retailers fail to fulfil the contract. Put briefly, the proposal to which the Member States have jointly agreed obliges retailers to issue security updates. The only time when this obligation will not apply is if the consumer has been expressly informed that no updates will be issued, and has given their express agreement. Under this obligation, a provision in the general terms and conditions is insufficient. The Netherlands wishes to provide greater assurance of security updates to consumers. This benefits not only them as individuals, but society as a whole, as non-secure hardware or software being used by one or more consumers can result in significant damage to third parties. It is for this reason that, in the negotiations on the proposal for an EU Directive, the Netherlands has proposed obligatory security updates across the board. The Netherlands is currently trying to garner support for this proposal in Brussels. The negotiations between the Council and the European Parliament are still underway.

- The Netherlands is an active participant in the EU liability and new technologies expert group, in which it incorporates input by Dutch stakeholders.
- In the EU negotiations on the European Commission's proposal for a directive on digital content and digital services, the Netherlands is proposing mandatory security updates for all software products supplied to consumers.

3.7 Statutory requirements, supervision and enforcement

Setting minimum security requirements can serve to keep non-secure products off the market. The Netherlands has initiated EU investigations into the possibility of using the Radio Equipment Directive (RED), which governs devices that connect wirelessly to the Internet (a fast-growing segment of the IoT), to set minimum digital security requirements. Products that fail to meet these requirements would then be removed from the market.

Oversight and enforcement give providers an incentive to comply with legislation. Depending on their mandate, supervisory authorities and regulators may intervene at certain stages of the product life cycle. To strengthen enforcement, the Dutch government aims to promote national and international cooperation between the various supervisory authorities. Various such authorities have a partial enforcement responsibility concerning digital hard- and software security. The Authority for Consumers & Markets (Autoriteit Consument & Markt) supervises a significant portion of consumer protection, while the Dutch Data Protection Authority (DPA) supervises compliance with privacy regulations. In addition, there are supervisory authorities for specific sectors, such as health care, transport and energy, which often have international counterparts.

Actions

- The Dutch government is investigating which minimal security requirements can be made applicable to devices under the European Radio Equipment Directive.
- The Dutch government is organising a national dialogue session for regulators and supervisory authorities to explore their role in promoting digitally secure hard- and software over the period ahead, to create synergy among the authorities' various efforts and to investigate potential improvements to their mutual collaboration.

Radio Equipment Directive (RED)

The RED sets out the requirements that devices must meet in order to carry the European CE mark. Radiocommunications Agency Netherlands is the relevant supervisory authority in the Netherlands. To date, the provisions cover matters such as user-friendliness, the prevention of interference and vulnerability to breakdowns. However, the RED also offers an option for setting (post-activation) minimum digital security requirements for the devices it covers. Harmonised European standards and certification (see Section 3.1 of this Roadmap) could offer support in complying with these statutory requirements.

3.8 Awareness campaigns and empowerment

Awareness campaigns and empowerment are elements that can be deployed throughout the product life cycle. Designers can be made more aware of the importance of applying security-by-design; purchasers can be alerted to reliable/unreliable products; and users can be encouraged to maintain the digital security of their products.

The Netherlands will employ awareness campaigns and empowerment in the field of digital hard- and software security principally to raise the impact of existing and new measures. The primary objective of awareness campaigns is to make consumers and SMEs aware of the digital security risks of IoT devices, how they can be addressed and which government measures can help them do so. Insights from the behavioural sciences and from behavioural experiments will also be used to ensure that users know what they must do (what their options are) to make the right purchase decisions and use hard- and software correctly.

The campaigns will tie in with the website https://veiliginternetten.nl (the online platform for cybersecurity information), which is also used for other cybersecurity campaigns. The Netherlands also wishes to bolster awareness and empowerment during the product development stage. Providers can address this internally and large companies can assist smaller businesses in doing so. Cyber essentials[6] can also help businesses enhance their internal digital security.

6 Cyber essentials are guidelines that help businesses lay a solid security foundation. The Digital Trust Centre (currently under formation) will also offer information and recommendations via its digital platform.

Action

» As part of the cybersecurity awareness campaigns run by the website https://veiliginternetten.nl, the Dutch government will be launching one or more public campaigns to support policy for digital hard- and software security.

3.9 National government procurement policies

The procurement policy of the national government can serve to promote digital security throughout the entire product life cycle. The inclusion of relevant criteria in procurement policies will force potential national government suppliers to meet requirements, which can cover all stages of the life cycle.

Given its position as a major user, the national government can use its procurement policies to bolster demand for digitally secure products, creating an incentive for providers to bring such products to market. In doing so, the national government also sets a good example, encouraging everybody to consider the digital security of hard- and software before making a purchase. Of course, the national government also believes it is important to be able to rely on the hard- and software it procures, and therefore wishes to investigate which additional measures are necessary.

Action

» The Dutch government will investigate which additional measures are necessary/desired to ensure the digital security of hard- and software within its procurement procedures.

This report is published by:

Ministry of Economic Affairs and Climate Policy
PO Box 20401 | 2500 EK The Hague
The Netherlands

Ministry of Justice and Security
PO Box 20301 | 2500 EH The Hague
The Netherlands

www.government.nl

April 2018