National Cyber Security Centre
Ministry of Justice and Security

Cyber Compass 2019

Distribution permitted by TLP: WHITE
(Traffic Light Protocol)

The Cyber Compass has been given the label TLP: WHITE. It is distributed by the Dutch National Cyber Security Centre (NCSC-NL). The NCSC-NL uses the Traffic Light Protocol (TLP) to define clearly and unambiguously what may be done with the information it provides. If information has a TLP designation, you will know with whom you may share it. This is described in the FIRST standard (www.first.org/tlp). Recipients may share the information in the Cyber Compass both within and outside of their organisation, while information may also be published.

We welcome your responses at info@ncsc.nl.

Cyber Compass 2019

Introduction

In this rapidly changing society, it is important to maintain digital resilient. Developments in the digital domain move at a sharp pace with increasing complexity. Obtaining an insight in the challenges we face is therefore crucial.

The Cyber Compass is developed for this purpose. The objective is to shape the response of organisations based on eight themes and related expectations. It is an interactive instrument that gives insight, raises awareness and offers perspective for action.

This allows organisations to anticipate the digital challenges ahead and the cybersecurity issues facing.

The Cyber Compass distinguishes eight themes with predictions for future developments. The themes have been divided further into a number of specific expectations. Each theme has a description, accelerators and decelerators.

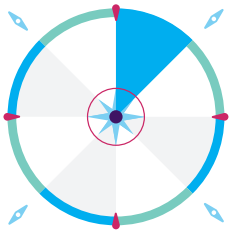
The expectations are described in detail. The expected relevance and the expected moment of breakthrough for each expectation is listed. To conclude, indicators that point to a breakthrough are specified.

You can find a graphic representation of the Cyber Compass as an appendix of this publication.

Theme

Digitisation of every aspect of society

Everyday processes such as living, working, relaxing, travelling, shipping goods and communicating increasingly depend on digital technology. This dependence is expected to keep increasing in the future. In many cases, analogue alternatives are no longer available. Moreover, the application of digitised processes extends beyond national borders.



Examples

Smart devices and sensor-based applications. Wearables for banking and travel. Off-the-shelf apps and software for mobile phones. The use of international cloud services.

Accelerators

Pressure of commercial interests, economies of scale.

Decelerators

Fragile infrastructure, privacy considerations, legislation.

Expectations

Dependence on streaming

Data storage media are increasingly replaced by streaming services, leading to an increased dependency on electricity and digital infrastructure. This puts pressure on availability and reliability. User data is used for profiling, with much information being stored outside the user's national borders.

- Potential consequences: storing personal data on third-party hardware entails a risk of loss of control over this data. In the case of a public cloud, a standard service offered to a wide target audience, it is usually unclear who exactly has access to your data – particularly for data being stored in a country with legal obligations to share data tacitly with the police and investigative services.
- Expected relevance: low.
- Expected breakthrough: 2021.
- Indicators that point to a breakthrough: reports in the media about profiling by streaming services.

Complications surrounding data ownership

As a consequence of new methods to process and store data, it has become more difficult to control access to information. For instance, data stored using a cloud service is stored on third-party hardware. In addition, data is stored all around the world, while the exact location is not always under the data owner's control.

- Potential consequences: loss of confidence in digital technology. Increased number of lawsuits against major technology firms. New legislation and regulations.
- Expected relevance: average.
- Expected breakthrough: 2020.
- Indicators that point to a breakthrough: mounting social unease about data processing by apps and underlying services.

Increased opportunities for 24-hour access to knowledge and services

The increased digitisation of information has made knowledge more accessible to a wider audience at a lower price. Information sources that used to be accessible only in physical form (e.g. libraries and archives) are now available to more people. Furthermore, Massive Open Online Courses (MOOCs) that are available to a wider audience also offer access to knowledge.

- Potential consequences: autonomous interpretation of a medical status without the intervention of a medical specialist, leading to incorrect diagnoses. Possibility of patients being monitored remotely on an ongoing basis and health insurers offering lower premiums in exchange for information derived from wearables.
- Expected relevance: low.
- Expected breakthrough: 2020.
- Indicators that point to a breakthrough: use of wearables by health insurers and care providers.

Increased use of wearables for medical assistance

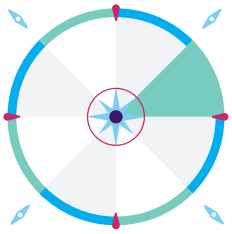
Wearables are used more frequently and offer ever more opportunities to monitor health. It will become common for some indicators to lead to the emergency services being alerted and for multiple indicators to provide an outline of the user's medical status.

- Potential consequences: storing personal data on third-party hardware entails a risk of loss of control over this data. In the case of a public cloud, a standard service offered to a wide target audience, it is usually unclear who exactly has access to your data – particularly for data being stored in a country with legal obligations to share data tacitly with the police and investigative services.
- Expected relevance: low.
- Expected breakthrough: 2022.
- Indicators that point to a breakthrough: reports in the media about profiling by streaming services.

Theme

Increase in legislation and regulations

Legislation and regulations regarding cybersecurity aspects will be expanded. As the relevance of cybersecurity to society increases, so will the urgency of related challenges. This will lead to a greater need for frameworks, guidelines and regulation. Due to market mechanisms, legislation and regulations may also affect areas outside of their scope of application. When confronted with diverging regulations in multiple countries, most multinationals and globally operating businesses will elect to meet the most demanding standards.



Examples

Legislation and regulations including PSD2, the Network and Information Systems Security Act, the EU Cybersecurity Act, the Computer Crime Act III and the GDPR.

Accelerators

International support and consensus.

Decelerators

Differences in insights, competing interests, lobbying efforts.

Expectations

International regulation continues to lag behind technological developments

The opportunities offered by digital technology are rapidly expanding. Consider, for example, Internet of Things applications or applications that increasingly blur the line between fact and fiction. It is imperative to guard against misuse of these opportunities. The call for international regulation is growing ever louder. As those with malicious intent will always find new and more ways to exploit vulnerabilities, legislation is expected to fall ever further behind, leading to a growing discrepancy.

- Potential consequences: exploiting vulnerabilities will remain an appealing prospect for those with malicious intent. This may lead to an increase in cybercrime in the broadest sense. Because of a lack of legal frameworks, organisations do not find it sufficiently urgent to further improve their resilience.
- Expected relevance: average.
- Expected breakthrough: 2020.
- Indicators that point to a breakthrough: because of competing interests, European and global partnerships will become harder to realise, making it more difficult to introduce international regulations.

Status of cybersecurity professionals will be boosted further

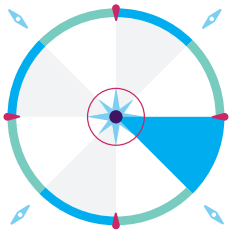
Due to an increase in national and international regulations over the past few years, more organisations will need to step up their efforts to meet statutory requirements. This will require the employment of additional data protection professionals, both now and in the future.

- Potential consequences: an awareness of the role of cybersecurity in the continuity of organisations will lead to cybersecurity professionals becoming increasingly involved in strategic decision-making.
- Expected relevance: high.
- Expected breakthrough: 2020.
- Indicators that point to a breakthrough: the role of cybersecurity in the continuity of organisations will become a more frequent topic on the agenda of upper management and supervisory authorities, leading to a greater demand for cybersecurity professionals. Maintaining cybersecurity will become increasingly formalised, for example by giving government bodies the authority to intervene in organisations that are insufficiently compliant.

Theme

More intelligent mobility

Significant developments are taking place in the field of systems designed to support autonomous mobility and intelligent systems that support this mobility, for example through infrastructure and traffic control systems. Technology plays a central part in this, in combination with social, societal, legal and ethical aspects.



Examples

Self-steering vessels, self-driving vehicles, autonomous drones, driverless trains, smart infrastructure, etc.

Accelerators

Legal framework, improved technology (e.g. with regard to safety) and cost efficiency, social acceptance.

Decelerators

Accidents, lack of a legal framework, ethical considerations. Lack of standards, differences in communication standards and protocols.

Expectations

Full dependence on electricity for internet and technology will put pressure on critical infrastructure

To a growing extent, intelligent mobility is powered by electricity, replacing fossil fuels. As more data is stored, data centres will continue to gain a bigger share in the total power consumption. It is to be expected that newly developed products will be powered by electricity as well, leading to an even greater dependence on electrical power. As a result of the increasing prevalence of solar and wind power, the supply is expected to fluctuate to a greater extent. This will put further pressure on the electricity grid, increasing the risk of distribution capacity shortages and outages.

- Potential consequences: disruptions to critical infrastructure with a social impact, e.g. vehicle or vehicle technology outages and malfunctions or shortages at vehicle charging stations and traffic control systems due to a failure to meet demand. Increased use of alternative and sustainable energy carriers such as hydrogen, biogas, batteries and other types of decentralised energy storage systems.
- Expected relevance: high.
- Expected breakthrough: 2021.
- Indicators that point to a breakthrough: growing frequency and prolonged duration of electricity grid outages.

Increased focus on cybersecurity aspects of intelligent mobility systems

The social relevance of cybersecurity measures in mobility systems is gaining importance to both vendors and consumers. Among other things, this will give rise to a need to identify vulnerabilities in the technology used for such systems.

- Potential consequences: expansion of response & disclosure policies, more statutory requirements when it comes to secure mobility, increased certification of information security systems in mobility systems, more mobility systems that incorporate security by design.
- Expected relevance: average.
- Expected breakthrough: 2021.
- Indicators that point to a breakthrough: rising demand for cybersecurity professionals, higher 'bug bounties', awareness of vehicle hacking.

Standardisation will offer opportunities for greater protection of critical infrastructure

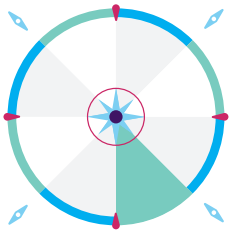
As autonomous vehicles become increasingly common, the corresponding critical technology will become more standardised. This will offer opportunities for the development of standards that mitigate yet unforeseen infrastructure vulnerabilities.

- Potential consequences: both regular and self-driving vehicles may become safer.
- Expected relevance: low.
- Expected breakthrough: later.
- Indicators that point to a breakthrough: expansion of legislation and regulations, adoption of standardised technologies by the mobility industry.

Theme

Homogenisation of the digital landscape

Increasingly, the same solutions (including technological ones) will be applied on a large scale.



Examples

Certain types of chips and reference architectures are commonly used in a wide range of applications, so the impact of such a component proving vulnerable could be enormous.

Accelerators

Buying off the shelf is cheaper than developing new technologies or solutions.

Decelerators

Incidents may prompt a growing demand for alternative solutions. Geopolitical tensions may lead to heterogeneity.

Expectations

Desire to reduce mutual dependence (on power blocks) will lead to greater variety in technologies

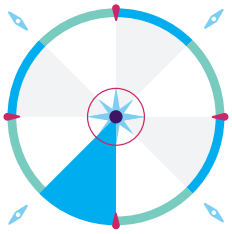
To reduce the dependence on power blocks, e.g. in the case of popular software produced by large market parties, a conscious decision will be made to use other types of technology.

- Potential consequences: increased costs.
- Expected relevance: average.
- Expected breakthrough: 2021.
- Indicators that point to a breakthrough: directives that seek to reduce mutual dependence and hence homogeneity.

Theme

Monopolisation of the digital domain

A small number of large market parties dominate almost the entire digital market. A small group of suppliers delivers services used in almost every chain.



Examples

Almost all organisations use the services of the Big Five.

Accelerators

Lobbying efforts and a technology push in which technological potential is driven by the supply side. Misuse of existing monopolies, vendor lock-in that prevents customers from changing suppliers easily.

Decelerators

Government intervention through legislation and/or competition measures, break-up of monopolies. Geopolitical developments.

Expectations

Economies of scale will lead to uniform security mechanisms

Large organisations are not only able to develop new technology to improve security more easily themselves, but are also in a position to demand security mechanisms when using the services of third parties. On account of their size, the costs of developing new security mechanisms are relatively low. Due to economies of scale even the tiniest improvement has a positive effect.

- Potential consequences: by demanding security mechanisms, organisations can nullify the effectiveness of simple techniques to hack systems.
- Expected relevance: high.
- Expected breakthrough: 2020.
- Indicators that point to a breakthrough: increased use of two-factor authentication and biometrics. Offer of cybersecurity measures as part of the service.

Data protection will be key to remaining competitive

Gathering and protecting data is an important consideration when it comes to competitiveness. The more unique the data remain, the higher their value for market parties. Security incidents have a negative effect on an organisation's image. As a result, an organisation's cybersecurity reputation has become a more significant criterion for customers when deciding with which organisation to do business.

- Potential consequences: organisations may invest more in cybersecurity and use it to gain a competitive edge. Organisations may actively attack each other to enhance their own competitiveness.
- Expected relevance: average.
- Expected breakthrough: 2021.
- Indicators that point to a breakthrough: effect on a number of users following scandals that involved the violation of user privacy.

Dependence on a limited number of parties will put pressure on resilience

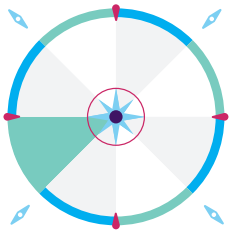
Because of the dominance of a small number of parties, an entire sector or even the entire critical infrastructure may suffer the consequences of a supplier being affected by a cybersecurity incident.

- Potential consequences: expansion of regulations and legislation to improve the resilience of these parties, so that incidents have a less dramatic impact. Measures to reduce dependence and provide access to alternatives.
- Expected relevance: average.
- Expected breakthrough: 2021.
- Indicators that point to a breakthrough: past incidents, such as the fuel supply problem at Schiphol in 2019.

Theme

Increased incident response complexity

Due to a focus on core activities and the transition away from owned servers to software in the cloud, the number of organisations involved and technologies used in a delivery chain will increase. This will lead to a greater need to coordinate information and responsibilities as well as access to all relevant information in the event of an incident.



Examples
Growing use of encryption for data traffic.

Accelerators
More encryption, rise of disinformation and fake news, shortage of adequately trained staff.

Decelerators
Standardisation of security solutions, improved coordination between stakeholders

.

Expectations

Root cause analysis and detection will become more difficult

Root cause analysis and detection will become more difficult, as not all information in the chain is available in real time.

- Potential consequences: greater risk of disruptive incidents, as they can be detected neither accurately nor in time. Incidents may last longer. Improved cooperation between chain partners. Responses may need to become more specific.
- Expected relevance: low.
- Expected breakthrough: 2020.
- Indicators that point to a breakthrough: repeat of past incidents, e.g. (Not)Petya, where a leak in foreign accounting software spread rapidly and partially shut down the primary process in the port of Rotterdam.

Detection will become more difficult due to more 'black boxes' in the chain

Chains will increasingly contain 'black boxes', whose operation and impact on the rest of the chain is not transparent. This will render detection complex, as not all information will be available.

- Potential consequences: greater risk of disruptive incidents, as they can be detected neither accurately nor in time. Incidents may last longer.
- Expected relevance: average.
- Expected breakthrough: 2021.
- Indicators that point to a breakthrough: large-scale adoption of technologies such as DNS over HTTPS; these encrypt the process of looking up the domain name that goes with an IP address.

t

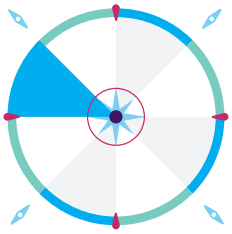
Having become more aware of the importance of data protection, organisations will take measures to better protect their data. This may lead to attacks in which the attackers weaponise data protection technology for their benefit. Such attacks are harder to trace.

- Potential consequences: security products may lead to reduced security.
- Expected relevance: average.
- Expected breakthrough: 2021.
- Indicators that point to a breakthrough: those with malicious intent adopt technologies such as DNS and VPN over HTTPS, using their encryption aspects to their advantage in order to make attacks more difficult to detect.

Theme

Decline of the human factor

Decision-making in processes will become increasingly automated. Where humans used to decide based on the available information, own insight and experience, this role is now being taken over by artificial intelligence using algorithm-based software. Although the algorithms were designed by humans, the decisions are being made autonomously. It will also become possible for software to improve itself through machine learning on the basis of pattern recognition. This will lead to the ongoing decline of the human factor in decision-making and production process chains.



Examples

Bureaucratic tasks such as taxes, subsidies, insurance, payment transactions and logistical processes.

Accelerators

Labour costs, shortages on the labour market, human error, competition, market demand, technological developments and reliability requirements.

Decelerators

Legislation, initial investments, serious incidents caused by algorithms, fear and mistrust of algorithms and robots, ethical considerations.

Expectations

Reduction of the number of security incidents caused by human error

Processes driven by algorithms are less error-prone. Naturally, this also depends on the technology used and potentially the quality of the algorithm in question. After all, computers make decisions based on information rather than instinct. All decisions made and actions taken should therefore be predictable, making processes less susceptible to errors.

- Potential consequences: fewer errors made by humans. As software and machines that take autonomous decisions (and have the potential to be self-learning) become more important to the decision-making process than humans, those with malicious intent will shift their focus towards influencing the algorithms or hardware involved in the decisions. This development makes it relatively straightforward to achieve economies of scale, thereby increasing the impact.
- Expected relevance: high.
- Expected breakthrough: 2021.
- Indicators that point to a breakthrough: more incidents as a result of algorithms that are incorrect or have been manipulated deliberately by those with malicious intent.

Human ability to improvise challenges to computer-made decisions will diminish

As 'closed' algorithms become increasingly prevalent in decision-making processes, the way decisions are made will become more of a 'black box'. Because algorithms are human-made, such a black box will inevitably contain bias. In a democratic society, it is important to know how this black box works.

- Potential consequences: increased demand for transparency regarding the algorithms in question, with regulations or guidelines assuming greater importance. Reduced confidence in AI due to a sense of losing control.
- Expected relevance: average.
- Expected breakthrough: 2020.
- Indicators that point to a breakthrough: discussion in the media of developments such as a transparency lab to increase transparency. Legislation aimed at ensuring detailed insight into decision-making processes.

Negative consequences of the lack of human judgement will become more visible

Because artificial intelligence (AI) involves making decisions on the basis of information within a specific context, there is no room for correction based on human insights or additional details that do not seem relevant until later. AI is easier to deceive with false input than humans. Lack of insight knowledge will make it harder for humans to judge the validity of decisions. This may lead to wrong decisions being made.

- Potential consequences: decisions that prove incorrect in the context of broader social interests or from an ethical point of view. Decisions may be challenged more often.
- Expected relevance: average.
- Expected breakthrough: 2022 and beyond.
- Indicators that point to a breakthrough: more frequent research into ethical dilemmas regarding AI.

Tampering with control and master data will lead to mistrust of AI

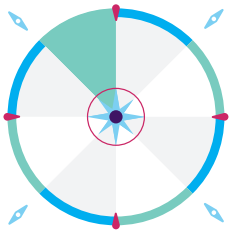
Certain organisational or external interests may lead to an increased likelihood of tampering with master data. This may result in the deliberate or unintentional contamination of control and master data and the manipulation of outcomes.

- Potential consequences: mistrust may lead to resistance against AI, with the potential result of reducing the use of AI for decision-making processes in sectors where outcomes are challenged more often (e.g. insurance). AI systems that generate fake content may become more prevalent. Such content may include computational propaganda and deep fakes, which involves the use of AI to generate fake video footage that is almost indistinguishable from the real thing.
- Expected relevance: average.
- Expected breakthrough: 2021.
- Indicators that point to a breakthrough: incidents such as the Cambridge Analytica scandal, which involved the illegal manipulation of the data of millions of Facebook users.

Theme

Reduced freedom to choose suppliers

A variety of factors will lead to a narrower choice of suppliers due to security considerations.



Examples

The freedom to choose suppliers will come under pressure in the telecoms sector in particular.

Accelerators

Geopolitical tensions and security requirements that prevent new players from entering the market. Protectionism, more stringent legal frameworks. Industry politics.

Decelerators

The use of security as a selling point. Basic security standards that guarantee a level playing field. Lobbying efforts on the part of businesses.

Expectations

Due to the increased relevance of privacy and other legislation, suppliers are increasingly assessed more critically for compliance (with these frameworks).

European legislation has established high privacy and data protection standards. In addition, security considerations have given rise to mounting unrest about the use of suppliers based in countries where businesses may have a statutory obligation to cooperate with cyber attack programmes, such as cyber espionage and acts in preparation of sabotage.

- Potential consequences: supervisory authorities may impose fines for failure to comply with legislation. Emergence of new (smaller) businesses that are able to comply with legislation. Exclusion of actors.
- Expected relevance: average.
- Expected breakthrough: 2020.
- Indicators that point to a breakthrough: increased legislation and regulations to exclude or prescribe suppliers.

Appendix

Cyber Compass figure

National Cyber Security Centre
Ministry of Justice and Security

Cyber compass 2019

Insight in the challenges ahead is important for organizations to remain digitally resilient. With foresights on the eight themes provided by the cyber compass, organizations gain a tool to anticipate and act on these challenges and better prepare for cyber issues.

The National Cyber Security Centre (NCSC-NL) works with businesses, government bodies and the academic world to increase the resilience of Dutch society in the digital domain.

Background

This product is based on a general observation of trends, publicly accessible sources and the NCSC-NL's tactical and operational expertise. In its preparation, the NCSC is grateful to make use of the expertise brought to bear by representatives of the following parties during a meeting of experts:

Centric, Clingendael, Defence Cyber Expertise Centre, DNB, Fox-IT, The Hague Centre for Strategic Studies, The Dutch Ministry of Economic Affairs and Climate Policy, the National Coordinator for Security and Counterterrorism, the Netherlands Forensic Institute, Privacy Company, the National Police, the Rathenau Institute, SIDN, Surfnet, the Netherlands Organisation for Applied Scientific Research, Delft University of Technology

The input of these parties, united in the National Security Analysts Network (ANV), contributed to the substantive quality of the Cyber Compass 2019.

Publication
National Cyber
Security Centre (NCSC)
PO Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague,
the Netherlands
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

November 2019