Lessons learned from 130-year of car and road traffic safety

The Haddon matrix

A model for cyber safety measures

Master thesis Executive Master in Cyber Security

Cyber Security Academy

Leiden University

Supervisors:

Prof.dr. Bibi van den Berg
Daan Weggemans MSc

Jeroen Kasbergen
S2239132

January 2020

Content

Acknowledgement

It has been an epic 'road trip' and journey to complete these two year of the Executive Master in Cyber Security program at Leiden University. In retrospective these two years was a constant endurance race divided in start, continue and finish combinations. The exams, papers and group assignments were linked in a chain of modules that led to this thesis.

Although combining a working career and a master's study is hard work, the revenue is enormous. I found the intellectual challenge, introduction to a new field of science and getting insights in new theories and thought lines highly valuable. I especially enjoyed the holistic approach on cyberspace. The great variety in subjects, from legal to technical and everything in between, combined with the insights in some of the major cyber events was something I really appreciated. Also, the (guest) lecturers stimulated critical thinking. However, was it all great? I do believe that any experience has highs and lows, however, even in lesser times, this whole journey added to my understanding of cyberspace.

I would like to give a big thank you to all the people that supported me during this two-year long journey. The first thank you goes out to the Cyber Security Academy, Leiden University, TU Delft and The Hague University of applied Sciences. Their holistic approach to cyber security, which started with the guidance of Jan van den Berg and continued with Bibi van den Berg (no relatives), proved to be a way of thinking I can very much relate to. Thank you for your directions through these two years. Furthermore, I would like to extent my thanks to my current employer, the Dutch ministry of Economic Affairs and Climate policy, represented by my program manager at the Digital Trust Center, Michel Verhagen. Michel took me abord in my first year of this master program. He provided me with a relevant working environment and facilitated the combination of work and education by setting the right conditions.

Also, a big thank you to all of my fellow students. All of you that started on the 1st of February 2018, from each and every one of you I have learned. You provided different viewpoints and we had our lively interactions. We'll keep in touch and work on that much needed network of holistic cyber security 'experts' to tackle the societal challenges ahead.

Furthermore, I would like to thank my family. The last two years were a challenge. The combination of this education, having young children, both being working parents and trying to maintain a social life proved to be a big challenge at many times. Selma, Teun and Gijs, for the next years I will give you the much-needed attention that you deserve and that I deprived you of during this program. I will first enjoy finishing this milestone and then we will look at what needs to be done from the mile-long list of things to do. I am sure that these things to do will include rides in the MGB!

Finally, a specific, warm and very special thanks goes out to Selma. She stood next to me during these busy times. Thank you for the support, holding the fort during stressful times towards the end of each and every module. Thank you for keeping things on track during the weeks and weekends and for your confidence in the good outcome. There is no way I could have done it without you and your support!

Jeroen Kasbergen

January 2020

Abstract

Cybercrime, threats, hacks, ransomware and viruses, that is what is controlling the news on cyberspace. Hacks and ransomware cases show that we are not digitally secure. A typical reaction in cyber security is: who did this and how did they compromise our networks? Important as it is, a whole field of science and cyberspace events is not covered by cyber security. The impact of cyberspace on our society is growing. Events in cyberspace are no longer just having consequences in cyberspace but also affect people in the physical world. Not being able to e-mail is a nuisance. Not being able to reach the emergency services makes that people's lives are at stake. First response by many will be: was it an accident or an attack? But does that matter for the harm done to people? Should the primary focus not be to keep people safe from harm? By making a historical review of a typical safety domain, that of car and road traffic safety, this thesis analyses the difference between safety and security for cyberspace. It identifies proven safety insights and concepts from 130-year of car and road traffic development, with one aim: to identify possible ways to protect people and reduce physical harm via cyberspace.

1. Introduction

During the second day of the One Conference 2019 in The Hague, the then Director General of the Dutch General Intelligence and Security Service, Dick Schoof, spoke on the importance of cyberspace for our society. *"All this new technology is changing the way we live, work, even wage war. The best analogy with the past, perhaps, is the invention of the internal combustion engine and the automobile. These, too, changed our way of life, our work. We had to do everything possible to make sure these changes were safe. Today, we follow clear traffic rules, wear seat belts, and in case of a collision we are protected by airbags. So how can we ensure that we remain safe with all this new technology? What are the threats to this digital society?" (Schoof, 2019, p.3 - 4).* Throughout society, digital and connected services and devices are used and society is more and more relying on them (WRR, 2019). As a society we want to be safe and secure in this digital era. However, with the growth of cyberspace, interconnected devices, the digitalization of society, we become more dependent on computers, devices and automated stuff. This also means that more of these devices, computers and automated staff can cause harm. Harm that can't be imagined or can it? To give a list of what ifs: what if the dikes are opened in the Netherlands? What if medicines are dispensed wrongly via a medicine pump? What if bridges open without warning? What if self-driving cars malfunction and crash? What if the automatic landing system of an airplane fails to work or gives the wrong information? What if…? The answer is that in any of these situations people can get hurt. Keeping people safe from harm is studied in safety science. As stated by B. van den Berg & Prins the aim of safety scientists is: *"…protect humans, first and foremost, rather than take away the causes of harm…"* (Van den Berg & Prins, 2018, p.11).

Cyberspace is new and complex but that was also true for car and road traffic 130-year ago. When the first cars appeared, they were preceded by a person waving a flag. The car soon proved to have safety challenges for society. Deaths and injuries in car crashes became more frequent and over time safety measures were developed to reduce the physical harm to people. Cyberspace is new development and new threats and dangers are emerging in or via cyberspace. So, what can be learned from 130-year of car and road traffic safety development and see to what extent these learnings can be a template for the prevention of harm via cyberspace?

1.1 Context

As argued by Jan van den Berg, cyberspace is the realm in which cyber activities are conducted (J. van den Berg, 2018). With the growth of cyberspace, a new security industry emerged. This cyber security industry works on the prevention of DDOS attacks and viruses, installs firewalls, tries to keep hackers and ransomware out of the computer networks and systems. The Dutch National Cyber Security Centre (NCSC) creates a yearly report on the cyber security of the Netherlands. The 2019 report, the Cyber Security Overview of the Netherlands (CSBN), speaks of threats in the following categories: states or state liaisons, criminals, terrorists, hacktivist, cyber squatters and script kiddies, insiders and finally a category of unintentional acts (CSBN 2019). These categories are focussing on who caused the incidents. The 2019 WRR report, 'Preparing for Digital Disruption' also looks at the sources of disruption. It addresses the criminal intent and intentional breaches, but also refers to accidents and unintentional disruptions as follows: *"Although cyber-attacks are an important cause of incidents, human error, broken servers, software issues or external factors such as cable breaks or power failures can also have a major impact on the functioning of digital infrastructure."* (WRR, 2019, p.5). With this quote the WRR is acknowledging the existence and influence of incidents in cyberspace but still focusses on the nature of the cause of an event. The harm that is caused by an event is most of the time quantified in money or unavailability of systems. But what about the harm it causes to people?

In this thesis the concept of cyber safety will be introduced next to the concept of cyber security. Cyber safety and cyber security are not opposing themes, but they are different. This thesis will go into the basic definitions of safety and security. This thesis will also try to deepen the field of cyber safety, and takes car and road traffic safety as an inspiration to come up with insights and measures to reduce physical harm to people via cyberspace.

1.2 Relevance of the comparison between safety in cyberspace and car and road traffic

The invention of the car started humans to explore, travel and go other places. It opened up new possibilities in travel and enabled the exchange of ideas, people, goods and therefore stretched the boundaries of our world. The internet and cyberspace do that also in a virtual way. With the introduction of the internet people spoke of the digital highway. The digital highway gave access to resources anywhere in the world at the click of a mouse button. The libraries of Leiden University and the library of the University of California are just as close in cyberspace. The introduction of the car also reduced distance in the physical world. Families that lived apart for hundreds of kilometres, no longer needed to travel for days by foot or horse. The car reduced travelling distance from days to hours. The internet and cyberspace now make it possible to connects families at the push of a button in virtual space.

The choice to look at cars and road traffic was primarily fuelled by the notion that this is a safety driven industry. Preventing incidents, reducing the impact of accidents and reducing the harm to people is key focus in the development of cars and the traffic safety. Another reason is that both cyberspace and car and road traffic are manmade globally used complex systems. In that respect they are more or less similar. Reinventing the wheel is not really useful, so it would be better if lessons learned from one field of science would be used in another field of science. As Esbester and Wetmore say it on the topic of car and road traffic safety: *"Better understanding of the temporally and geographically contingent nature of mobility technologies and practices, and of how accidents, safety, and risks are co-constructed and co-produced, could offer us insights into how we might reduce deaths and injuries in the future – surely a manifestation of a useable past if ever there was one. And that is the broader challenge this issue lays down to historians, not just of (auto)mobility, but of technology: while recognizing in its own right the value and importance of producing studies of the past, we can also find ways to make our work useful to non-historians in shaping the world of tomorrow." (Esbester & Wetmore, 2015, p.316).* This quote is in essence what this thesis entails. To learn from car and road traffic safety development and to see how to prevent harm to people via cyberspace.

1.3 Cyber safety: the research question

As pointed out, the cause of cyber incidents is deemed very important in cyber security research. Both the CSBN and the WRR reports handle predominantly on categorizing threats and classifying perpetrators. In both reports, harm in general or specifically to people is, besides the mentioned societal disruption, not addressed. Both reports do mention that a disturbance of cyberspace can lead to physical repercussions in society. The CSBN concludes that for instance in the energy sector, which is highly digitized, manual alternatives are no longer available but leaves it with that. The consequences of what this means for the physical safety of people is not mentioned. That events in cyberspace are able to inflict harm in the physical world to humans has been proved in a couple of cases. On the 23rd of December 2015 in parts of the Ukraine the lights went out (SANS Institute, 2016). People were left in the cold and dark. Who knows what harm has stricken these people? In the SANS report and in hardly any news coverage the actual harm to people is mentioned. It is possible that no harm is done, but some people did not have electricity for six hours. It is hard to imagine no harm is caused at all. A more recent example can be found in the 2019 outage of the emergency services telephone number 112 in the Netherlands. In the aftermath of this crisis, the media reported on the possible deaths of two people because the emergence services were not reached on time (RTL Nieuws, 2019). In both cases the event took place in cyberspace and had real world consequences. However, the Ukraine incident, which was a hack, took the turn of focussing on the cause and the finding the responsible hacker(s). As with the emergency telephone number 112 outage, the response was on how to prevent future harm to people by such an outage (KPN, 2019). To summarize, up until now there is much attention to fighting cybercrime in cyberspace, but with the growing interwovenness of cyberspace in today’s society, physical harm can be inflicted when events occur in cyberspace. There is only limited research into the physical harm via cyberspace. This can be caused because it is never researched, or it can be that physical harm is only now emerging. Nevertheless, there are two reasons why there should be research conducted to the harm to people via cyberspace. First of all, as said with the interwovenness of cyberspace into our daily lives, there will be physical consequences to people caused by events in cyberspace. Secondly, as illustrated with the Ukrainian power outage, current research into these events in cyberspace look at these events from a whole different angle. That angle, being the angle of finding the cause, attribute the event to a perpetrator and come up with measures to prevent that event to happen again, is not reducing the physical harm to people. This thesis is a first step on the road to not only look at the cause of a cyber event, but also reduce the impact of such an event on persons in the physical world. It does so by answering the following main question:

To what extend can lessons learned from 130-year of car and road traffic safety development help in the prevention or reduction of physical harm inflicted to people via cyberspace?

To come to an answer to this question additional questions need to be answered. A first question that needs to be answered is *"How did car and road traffic safety develop?".* A second question that needs to be answered is "*What is cyberspace?*". It is also important to look at the concepts of safety and security, what is meant by them and how this is relevant for cyberspace, this is done by answering the question: *"What is the difference between safety and security in cyberspace and how does this relate to harm to humans?"*

1.4 Thesis layout

To answer the main question this thesis is structured as follows. Chapter two will explain the method of research chosen to answer the main- and sub-questions. It will also elaborate on how the research was conducted. Furthermore, chapter two will address the way the comparison between cyberspace and car and road traffic should be perceived.

Chapter three will contain the theoretical framework that this thesis will build on. In short, the following models and theories will be used: the Haddon matrix will be explained as it is the leading model in car and road traffic safety science to reduce physical harm in an event. Furthermore, the three-layer model of cyberspace by Jan van den Berg will be introduced. With this model and also based on the work of Dunn Cavelty, cyber security is briefly touched upon. Finally, the concepts of safety and security will be explained based on the work of Aven, Waldron and B. van den Berg et.al.

The fourth chapter, describes the development of car and road traffic safety. Furthermore, this chapter contains a filled Haddon matrix with examples of measures for improving car and road traffic safety. The chapter ends with general observations and restrictions in the use of the Haddon matrix.

The fifth chapter, is in the same structure as the fourth chapter, after a general introduction, which contains more details of how the Haddon matrix fits cyberspace, the identified measures in chapter four are transposed to cyberspace. This chapter also ends with general observations and limitations in the use of the Haddon matrix for cyberspace.

Chapter six will give a final summary of the research done and answer the main question. Final remarks will be dedicated at future research suggestions.

2. Research method

This chapter describes the method of research for this thesis. It explains the starting point of the research and also goes into the details of the research, it's scope and the challenges and limitation of the research.

2.1 Thesis form

This thesis is a design science thesis. That means that this thesis will deliver an artefact. An artefact is a product of the research conducted. Such a product can consist of a model, a process, code, or a practical solution to a problem. The problem that is being addressed in this thesis is the lack of attention for physical harm to people via cyberspace. By the application of the Haddon matrix, a model derived from car and road traffic safety, to cyberspace, this thesis delivers an artefact that can help in the prevention or reduction of physical harm to people via cyberspace. The goal of the Haddon matrix is to prevent harm to people in car and road traffic incidents. In addition to this artefact, additional results of this thesis will be an overview of the characteristics and general observations on the effectiveness of measures in car and road traffic safety. This overview can serve as a template for future measures in cyber safety.

2.2 Desk research

The chosen method to answer the research question is twofold. The first research method is desk research. The second part is the application of the Haddon matrix to reduce physical harm to people via cyberspace. This form of research is chosen because it suits the research question. The information on car and road traffic safety, cyberspace, cyber safety and harm to people via cyberspace can be found by looking at relevant literature and (peer) reviewed articles. Furthermore, the composition of the Haddon matrix, both for car and road traffic safety and cyber safety can be done based on the information available from the desk research.

The desk research into car and road traffic safety was conducted simultaneous with the research into the car and road traffic history. The research started with three books describing the history of the car. The research was extended to peer reviewed papers available via the online University Leiden Library. One of the search terms used to come up with relevant papers was the exact search term 'car safety'. This exact search term was limited to the title and was completed with the words ‘road traffic’ anywhere in the body. Another search term included the exact title ‘road safety’, and containing the term ‘history’ and ‘research’. In addition to these search queries, selected articles also referred to other relevant articles. This snowball effect was also utilized to create the general overview of car and road traffic safety development. These sources are supplemented with publications by the European Union (EU), the organisation on Scientific Research on Traffic Safety (SWOV) and the Organisation for Economic Cooperation and Development (OECD). These three organisations proved to be important in the safety of car and road traffic, either by setting standards, share information or advice government on the approach on this issue.

The desk research on cyberspace, cyber safety, harm and security, proved to be challenging on the subject of cyber safety and the harm in and via cyberspace. These concepts are not broadly researched, and consequently there is not much literature or publications available. The concepts of cyberspace and cyber security are mature in this respect. Finally, there is the research on the difference on safety and security. The basic definitions are on the one hand based on the standard books in safety and security science with the starting point in ‘Contemporary security studies’ by Alan Collins. These starting points then led to more specific articles on the theoretical framework for cyberspace, cyber safety and cyber security.

2.3 Scope of the desk research

The first element that determined the scope of the desk research is that of the car and road traffic safety. The online dictionary Merriam-Webster defines traffic as: “*the vehicles, pedestrians, ships, or planes moving along a route*” (Merriam-Webster, 2019). The scope in this thesis is that only the (passenger) car and road traffic will be researched. The reason for this scope is that, first of all, the car was developed first in the development of individual transport. It was used on a large scale and by individual users. Furthermore, all other road traffic participants using for instance trucks, lorries or busses are a derivate of the car. That makes their safety development similar and therefore not of additional value to this thesis. Diving in the car and road traffic safety, there is a limitation to what is necessary to explain on the working of a car. For the subject of this thesis, it is needed to understand the basic concept of a car and what types of safety measures are developed. There is therefore, no need to go into the exact technical details of each and every measure.

3. Theoretical framework

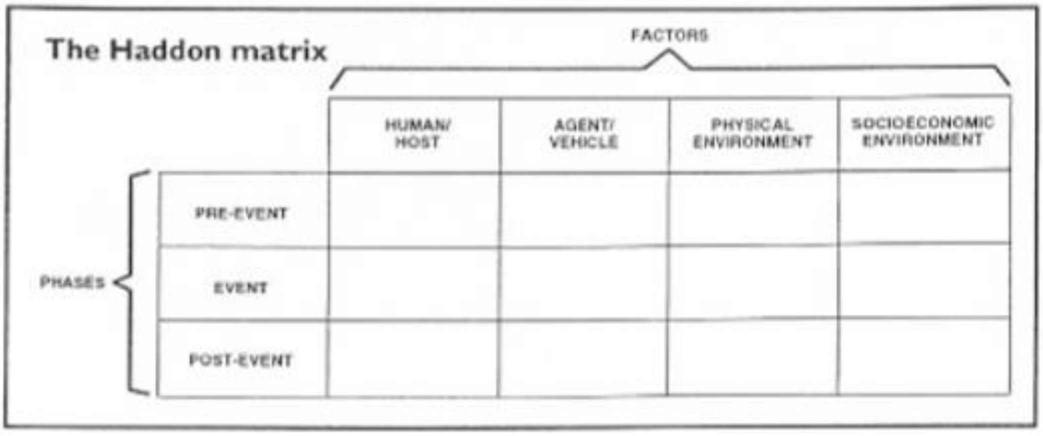
To address lessons learned from car and road traffic safety, first the right context must be created. This chapter describes the theories that are being used in this thesis. This overview of theories is the result of desk research. The theories chosen will first explore the Haddon matrix, a model used to categorize measures to improve car and road traffic safety. Then the concept of cyberspace is addressed. Finally, the concepts of safety and security will be explained in relation to each other as well as in relation to harm in and via cyberspace.

3.1 The Haddon matrix

From the desk research there is one specific finding that stood out in car and road traffic safety. There is an important theoretical model behind the safety improvements in car and road traffic which is called the Haddon matrix. In the article: 'Landmarks in the History of Safety', Michael Guarneri explains the significance of the Haddon matrix. The Haddon matrix is created by William Haddon Jr. who was a pioneer in car and road traffic safety (Waggoner, 1985). Haddon came up with a conceptual model that created the possibility to look at other measures then influencing the drivers behaviour when trying to diminish physical harm to people in car and road traffic crashes (Williams, 1999). Haddon, who was a physician by trade, focussed on analysing the injuries inflicted in a crash, and thought on ways to reduce the severity of that harm (Waggoner, 1985). With this changed focus, Haddon opened up a whole new range of technical, environmental and socioeconomic measures that were not considered in a structural way before. The Haddon matrix in that sense is a conceptual model to plot different approaches to reduce harm (Williams, 1999). The Haddon matrix is not a decision-making model. The choice of what measures are being introduced is left to the lawmaker, car manufacturer or others that play a role in improving car and road traffic safety.

The Haddon matrix distinguishes three phases in any event. These three phases are: the pre-event phase which is the period before any incident will occur; the event phase which is when the actual incident takes place and the post-event phase which is the aftermath of the incident. Measures to prevent events from happening are in the first phase. Measures to reduce the impact of an event are in the second phase and measures to reduce the secondary impact and the consequences of an event are in phase three.

In addition to these three phases the Haddon matrix contains four factors of influence. These four factors are: the driver who is the person behind the wheel; the agent which is the vehicle that the person is driving; the physical environment, the road the car drives on including all the peripheral items like trees, lamps etc and finally the socioeconomic environment which is the whole of society that plays a role in car and road traffic safety (Newman, 2004; Williams, 1999). In figure 1, the three phases and four factors are shown in what is called the Haddon matrix.



The Haddon matrix

		FACTORS			
		HUMAN/ HOST	AGENT/ VEHICLE	PHYSICAL ENVIRONMENT	SOCIOECONOMIC ENVIRONMENT
PHASES	PRE-EVENT				
	EVENT				
	POST-EVENT				

Figure 1: The Haddon matrix (A. F. Williams, 1999)

Measures can be divided over the three phases of an event, which is the first dimension of this matrix. However, the Haddon matrix contains a second dimension, the factors that play a role in an event. By combining these two dimensions, the matrix consists of twelve points of intervention in reducing harm to people.

Guarnieri explains that this concept of Haddon influenced the content of the US National Traffic and Motor Vehicle Safety Act of 1966. That act marked a break with the traditional thought patterns on car and road traffic safety. Guarnieri states that up until that point: *"…people were responsible for their own safety, and the victim shared the guilt for his or her injury."* (Guarnieri, 1992, p.152). This was an exponent of military doctrine that stated that whenever adhering to orders no accidents would happen. In other words, accidents will happen when orders are not followed through completely (Guarnieri, 1992). 'The landmark' that Guarnieri describes is the societal mind shift from blaming an event on the driver, third parties or an outside element of chance, to the use of the sciences of engineering and medicine to understand the causes of an event (Guarnieri, 1992). By using statistics, as done by engineers and epidemiologists, scientists in the field of car and road traffic safety built their understanding of when and what inflicted the actual harm in events (Williams, 1999).

In the field of cybersecurity governance, Lawrence Lessig is an authority on how to regulate the behaviour of people. He also developed a model, that includes four way to regulate behaviour in cyberspace and these are the law, norms, the market and architecture (Lessig, 2006). It is interesting to see that there is some resemblance in the Haddon matrix and the model of Lessig, although they emerged from a totally different background and in a totally different time period. For this thesis the model of Lessig is noted, but will not be used further.

3.2 What is cyberspace?

There are multiple scientific definitions of cyberspace. For this thesis three concepts are worth mentioning. These three concepts together create a better understanding of what cyberspace entails. As will become clear the concepts will gradually broaden the concept of cyberspace. These three concepts are selected because they illustrate the growing understanding of cyberspace. The first definition by Dunn Cavelty is based on the technical foundations of cyberspace. The definition of Jan van den Berg has a broader concept of cyberspace and the difference between the technical foundations and the actual use of cyberspace is becoming clearer. Also, his three-layer model introduces the concept of governance of cyberspace, by encapsulating the technical and socio-technical layer. This is relevant for this thesis because, as will become clear later, the governance plays an important role in car and road traffic safety. It is therefore likely that this will be very relevant for cyber safety too. In the third concept the understanding of cyberspace is also broad. However, in addition to the broad concept of B. van den Berg & Kuipers, their concept is also the foundation of the cyber harm model that will be discussed later.

The first definition of cyberspace is given by Dunn Cavelty *"Cyberspace (a portmanteau word combining "cybernetics" with "space") connotes the fusion of all communication networks, databases, and sources of information into a vast, tangled, and diverse blanket of electronic interchange."* (Dunn Cavelty, 2012, p.4). This definition focusses on the electronic exchange of information. One could say that this definition focusses on the underlying information technology components of cyberspace. It does recognize that cyberspace consists of electronic communication of information supported by an infrastructure of networks and

databases. A clear extension of the definition by Dunn Cavelty is the three-layer model of Jan van den Berg. This model contains a conceptualization of cyberspace (J. van den Berg, 2018). The model has a core that is made of the IT components, a second layer that consist of the activities done by users and a final layer that encapsulates the other two, the governance layer. In the concept of J. van den Berg these three layers in total define cyberspace.
These three layers, as shown in figure 2, will subsequently be described in more detail. The first layer, the core of the model, is the technical layer. This layer comprises of the ICT components, either devices or networks. According to J. van den Berg (2018) this is the enabling technology that drives our digital society. The second layer of the model is the socio-technical layer. This is the layer in which cyber activities are conducted (J. van den Berg, 2018). These cyber activities are enabled by the core technical layer. In this concept there is a clear difference between the hard and software, networks and protocols that create the internet that is driving cyberspace, and that is what the user does while using this technology. The socio-technical layer contains a variety of cyber activities. An important characteristic of any cyber activity is that they are performed to achieve a goal. J. van den Berg distinguishes three types of activities: basic activities that include communications, receiving information and consuming broadcasts; advanced cyber activities that include searching, performing transactions and performing social interaction in online communities. Finally, there are less favourable activities such as criminal activities, espionage and war in cyberspace. It is important to note that J. van den Berg also signals that society is depending more and more on the cyber activities and therefore the proper working of the underlying IT services is crucial. To ensure the proper working J. van den Berg argues that there is a final layer of the model: the governance layer. This layer contains the measures that govern the cyber activities and the technical enablers. The function of the governance layer is, in his words: *"here acceptable risk levels should be fixed and appropriate measures taken to reduce*

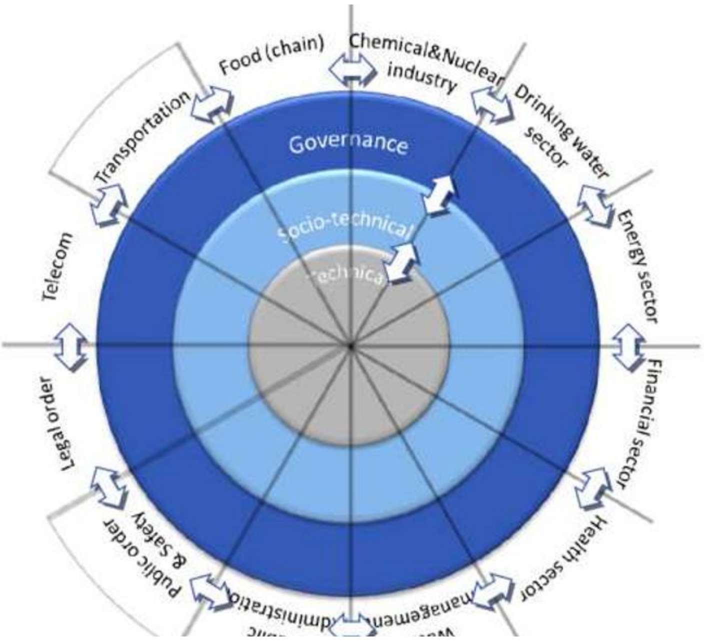


Figure 2: Conceptualization of cyberspace, J. van den Berg (2018)

the identified cyber risks to acceptable levels." (J. van den Berg, 2018, p.4). He divides the measures into two parts. First there are the measures to govern the IT-security which are based on the confidentiality, integrity and availability of information and systems. Secondly, the cyber activities are governed by measures defined in a risk-based approach. J. van den Berg introduces the bow-tie as the process to assess the risks associated with the cyber activities. The bow-tie model starts with identifying critical cyber activities, the risks that are associated with these activities, setting a level of risk you want to take, agreeing on what you want to do about it, executing the measures you decide on and seeing if these measures work. These measures typically either reduce the likelihood a threat emerges or reduce the impact of an emerging threat. Both can lead to an acceptable risk level. In this model, it is crucial that both the critical cyber activities are known and that threats are identified. To take measures to mitigate unidentified threats is not included in this method.

Finally, there is the concept of cyberspace as introduced by B. van den Berg and Kuipers. They state that there is no universal definition of cyberspace. They continue and argue that it would make sense to see what is common in all the definitions to get a set of characteristics that defines cyberspace (B. van den Berg & Kuipers, 2020). Their research is based on the research done by Kuehl and his definition of cyberspace which states that cyberspace is: *"a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."* (Kramer, Starr, & Wentz, 2011, p.4). B. van den Berg & Kuipers distinguish six characteristics of cyberspace in two sets. These two sets consist of the physicality of cyberspace on the one hand and the use of cyberspace on the other. The physicality set consists of the fact that cyberspace is an ecosystem, containing digital technologies that are interconnected in a network. The set containing the use of cyberspace involves actors and behaviours in cyberspace that create,

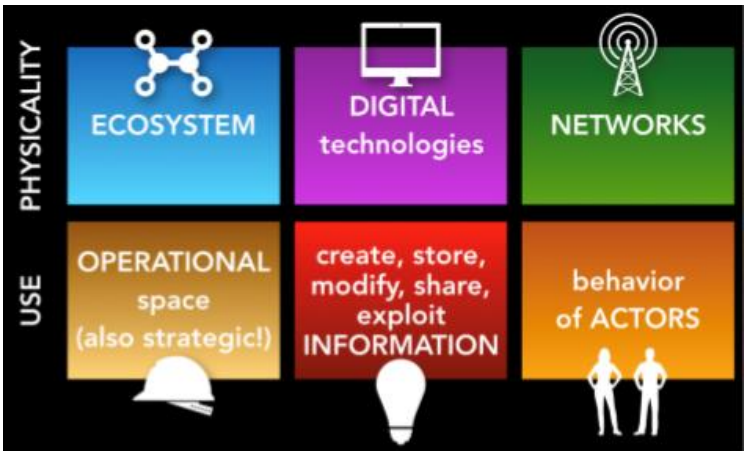

PHYSICALITY
USE
ECOSYSTEM
DIGITAL technologies
NETWORKS
OPERATIONAL space (also strategic!)
create, store, modify, share, exploit INFORMATION
behavior of ACTORS

Figure 3: Six elements of cyberspace, B. van den Berg & Kuipers (2020)

store, modify, share and exploit information to a certain goal. In addition to that, B. van den Berg and Kuipers also see cyberspace as a space in which one can perform these actions as a space next to and intertwined with the physical world (B. van den Berg & Kuipers, 2020). These two sets are very similar to the technical and socio-technical layer in the three-layer model of J. van den Berg. The physicality is embedded in the technical layer of the three-layer model. Also it contains the goal-setting in the use of cyberspace. Actors behave in cyberspace with a certain goal, either in the physical world or in cyberspace.

There are also two relevant differences between the three-layer model and the concept of these six elements of cyberspace. The first is the prominent role of the ecosystem in the overview of B. van den Berg and Kuipers. J. van den Berg does mention an ecosystem, but in this six elements of cyberspace model, the ecosystem is more important. Secondly, the three-layer model clearly defines the governance of cyber space which is not adressed in the overview of the elements of cyberspace by B. van den Berg and Kuipers. They do mention that governments and others do play a role in challenges that cyberspace holds but do not define the governance function as a defining criterium of cyberspace.

For this thesis all three definitions are relevant. First of all, they are relevant to establish the understanding that cyberspace research is evolving rapidly. The above-mentioned descriptions of cyberspace are only eight years apart. Secondly, cyberspace is more than IT services and systems. Cyberspace is an ecosystem, both in the way the technical layer is interconnected and dependant on all individual elements, as in the fact it is an ecosystem of cyber activities in which the users of these activities pursue goals and form a new digital society which is very much interwoven which now also has effect in out physical lives. Finally the relevance of the third definition is that it is laying the foundation for what needs protecting in cyberspace, which will be explained more in depth in the next paragraphs.

3.3 Safety and security

Safety and security are two different fields of science. On the one hand there is safety science and on the other hand there is security studies. The aim of safety sciences it to keep people safe, either through prevention or reduction of physical harm. A major topic in safety science is child safety. Child safety is the protection of children from physical harm. Security studies is the domain of states and the territorial, military and diplomatic relations between states and international bodies. A clear subject of study in that respect would be the creation of the Transport Security Administration in the USA weeks after 9 / 11. Their task is to ensure security and to prevent deliberate attacks on planes. As the TSA state it themselves: *"On the morning of September 11, 2001, nearly 3,000 people were killed in a series of coordinated terrorist attacks in New York, Pennsylvania and Virginia. The attacks resulted in the creation of the Transportation Security Administration, designed to prevent similar attacks in the future."* (TSA, Mission, 2016). Security studies focusses on the who caused the event and how can this be prevented in the future.

However, it is important to note the nowadays safety and security are not always clearly divided anymore. Waldron ask: "*What is the relation between security and personal safety? A person is safe to the extent that she is alive and unharmed. Is a population more secure simply by virtue of people being safer, i.e., simply in terms of a diminution in the prospect of their being killed or harmed?"* (Waldron, 2012, p.461). Waldron reaches the conclusion that safety and security are very much related and intertwined. His argument continues by stating that security is a concept that is wider than safety. His perspective is that security is the protection of not only humans but also material property. However, he also limits the meaning of security by stating that security is: the protection delivered by security against threats and the fear of threats (Waldron, 2012). This conclusion is supported by the work of Aven (2014). Aven's definition of safety science is that it is the study of safety of human beings. However, Aven questions if that scope is still valid because he states that: *"It is common to distinguish between safety and security, where security relates to intentional situations and events (terrorist attacks, burglary, etc.) in contrast to safety, which covers the accident type of situations and events."* (Aven, 2014, p.17)**.** Aven then continues to argue that the notion of safety could or should also include intentional harm. This follows from the argument of Aven that risk can be seen as a neutral concept (Aven, 2014). However, there are others that disagree on that point. For instance, in the work of Slovic, it is being argued that the perception of risk is an important element in the way individuals and society treats risks (Slovic, Fischhoff, & Lichtenstein, 2005). Therefore, risk is not as neutral as Aven states. At the end of his argument, Aven makes it clear that in his opinion, regardless of the common ground in the risk approach, there is a reason to separate these notions: *"Nevertheless, it may be attractive in some cases to highlight when security issues are addressed in contrast to accidental events, and then use the term 'security'"* (Aven, 2014, p.17). The reason for such a difference could very well be because of political or judicial reasons. Whenever something is an intentional event, it can lead to criminal charges. In such a case the perpetrator is an important factor. In case something is a safety incident, there is not so much attention to who is to punish but the focus will be more on how to prevent a similar event in the future.

So, from the work of Waldron and Aven alike, safety and security are different subjects but they do have similarities. An answer to how these two concepts relates, in particular in cyberspace, comes from B. van den Berg et al. They state that security and safety alike revolve around the prevention of harm (B. van den Berg et.al., 2019). So, B. van den Berg et al. state that: *"The complex, often global challenges that we face today all reveal that security and safety aspects are interwoven to such a degree that these notions cannot be isolated anymore."* (B. van den Berg et.al., 2019, p.9). At this point in time, this is not yet the case in cyberspace. Security is the predominant factor and safety is not yet addressed. Therefore, in this thesis to successfully introduce a model for cyber safety these concepts should be treated independently. At a later point in time an integrated approach as proposed by B. van den Berg et.al., as shown in figure 4 can be pursued.

The top section of the cyber harm model is where physical harm is plotted. Both examples mentioned earlier on the Ukrainian power outage and the emergency telephone services outage in the Netherlands are examples of harm to society via cyberspace.

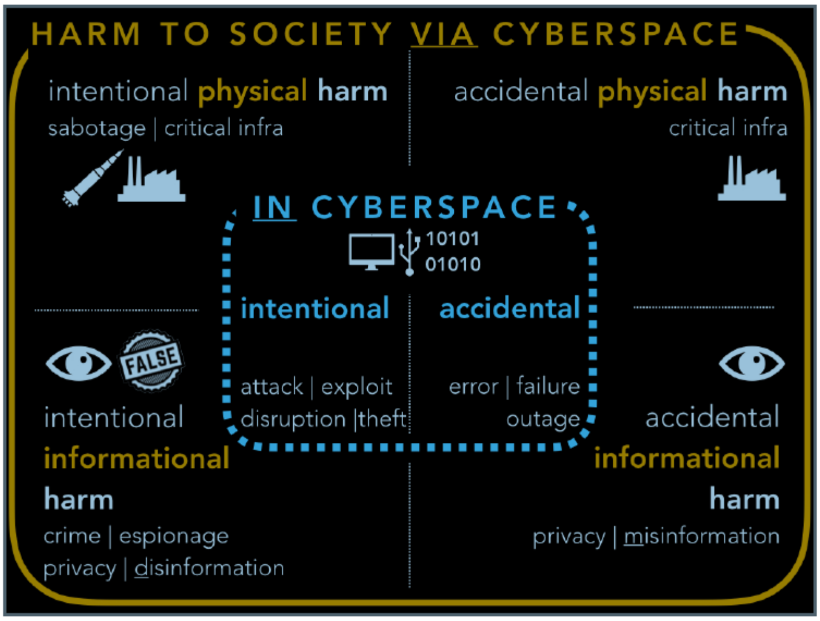


Figure 4: cyber harm model (B. van den Berg & Kuipers, 2020)

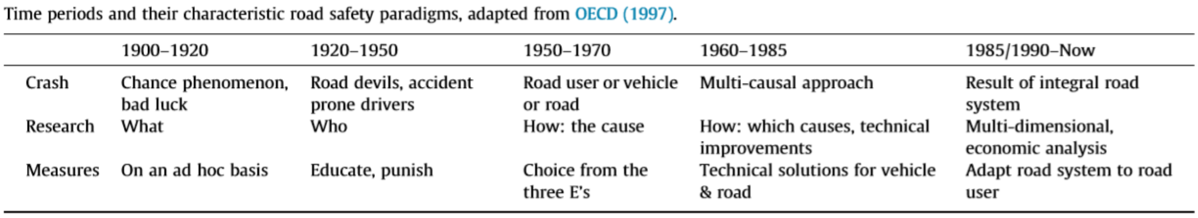
To summarize the relevance of the above-mentioned models, definitions and theories: cyberspace evolved from a technical environment used to exchange data, into an ecosystem in which people form relations, perform activities and on which society is depending more and more. Even more so, society and cyberspace are to a large extent integrated. In the early days of the internet, it was important to look at security to reduce threats. Nowadays, because of the interwovenness of the real world and cyberspace there is a growing need to also look at the safety implications of cyberspace. Since events that take place in cyberspace, can transgress into the real world and cause physical harm. Looking at the cyber harm model safety is in the upper part of the model. For this thesis, the first step is to use the original definition of safety. By doing so there is a clear definition of the harm that needs to be reduced, the physical harm to people. That is also best linked to how this is perceived by car and road safety. It is left for future research to see to what extent cyber safety models and theories can be interwoven with cyber security models and theories.

4. The car and road traffic safety

In this chapter car and road traffic safety is described to such an extent that it can be used to identify measures plotted in the Haddon matrix. There is much that can be said about the history and development of car and road traffic, but as indicated before, this thesis is about the learnings that can be taken from car and road traffic safety and not about the full history of the car. The first paragraph in this chapter gives a general overview of car and road traffic safety paradigms over time. Subsequently, there is an overview of car and road traffic safety measures per factor as defined in the Haddon matrix. These insights will then be used to inspire the cyber safety measures to in the next chapter.

4.1. Historical development of car and road traffic safety

The historical overview is based on the work of Hagenzieker et al. (2012). They give an overview of the 130-year period of car and road safety development. To structure the development over the 130-year period, five specific time periods can be distinguished, each with their own characteristics. These periods are shown in figure 5. These time-periods reflect the nature of the measures for car and road safety, the science on car and road safety and the prevailing safety beliefs in these periods.



Time periods and their characteristic road safety paradigms, adapted from OECD (1997).

	1900–1920	1920–1950	1950–1970	1960–1985	1985/1990–Now
Crash	Chance phenomenon, bad luck	Road devils, accident prone drivers	Road user or vehicle or road	Multi-causal approach	Result of integral road system
Research	What	Who	How: the cause	How: which causes, technical improvements	Multi-dimensional, economic analysis
Measures	On an ad hoc basis	Educate, punish	Choice from the three E's	Technical solutions for vehicle & road	Adapt road system to road user

Figure 5: Time periods and their characteristic road safety paradigms, adapted from OECD (1997), (Hagenzieker et al, 2012, p.151)

It is clear, when one examines this diagram, that the road safety paradigms evolved over the years. Car and road traffic safety follows a path of growth. The development starts in the first time period. In this first period only ad-hoc safety measures were taken and there was no structural research on road safety. The first steps taken during this period are mainly gathering data and trying to understand what happened during an accident (Hagenzieker et al., 2014). In the second time period, based on the insights from the first period, the focus was on accident-prone drivers. Based on the information from the first period, one found that only a small number of drivers was actually involved in accidents. This led to interventions focussing on the behaviour of these drivers. Measures varied from punishment to educating these specific drivers (Hagenzieker et al., 2014). In the third time period, the main focus of prevention was understanding the cause of an event. The measures were designed to mitigate the cause of the event and were typically applied to one of the factors in the road system, either the driver, the vehicle or the road. Measures in this time period were typically drawn from the three E's. The three E's stand for educating people, enforcing the rules and engineering the car or road (Hagenzieker et al., 2014). In the fourth period, the main focus of preventing events was on the road and the vehicle. Technical improvements were dominant strategies to increase the safety. New in this period is the introduction of the Haddon matrix, described earlier. In this period the understanding grew that an event could have more than one cause. This multicausal paradigm led to technical measures to the car and the road and also paid attention to the interaction between these two (Hagenzieker et al., 2014). In the fifth and final period, the paradigm shifted towards an integrated approach on car and road traffic safety. It became clear, based on measurements and statistics, that car and road traffic safety can only be improved if approached in a systematic manner and that the interaction between the driver, the vehicle and the road is crucial. As an addition to that, it was also recognized that each factor has its limitations. In general, these limitations are most prominent with the driver. Each and every driver is acting differently. Measures in this time period are measures that improve the interaction between the factors in the system (driver, car and road) and try to get them to work together and assist or correct the limited capabilities of the driver (Hagenzieker et al., 2014).

4.2. The four factors in the Haddon matrix

In this paragraph the four factors from the Haddon matrix will be described in more and relevant historical detail.

4.2.1 The human / driver

The human can have multiple forms and roles in car and road traffic. It can be the driver, a passenger or another traffic participant. For this thesis the driver is chosen as the object of study as it is the driver that is actually controlling the car in traffic. Therefore, what makes it consistent with the information found in the literature, is that the driver is the factor as meant by the human or host in the Haddon matrix.

4.2.2 The car

The car is the agent as defined in the Haddon Matrix. The first real automobile was introduced around 1886. Karl Benz created a tricycle car called the Benz Patent-Motorwagen (Parissien, 2014; Rae, 1965). This car was equipped with an internal combustion engine, which was smaller, lighter and stronger than the up until then available steam engines. A major improvement to the combustion engine was the electronic starter which was introduced in 1912. Before this invention, the car needed to be started by turning over the engine with manual force and had the tendency to recoil, making it a dangerous procedure. The electric starter made the car safer and user-friendly to start which contributed highly to the popularity and usability of a car equipped with such a system (Rae, 1965). Besides the electronic starter, safety was not top of mind in these early days. Sometimes, safety was present in practical additions to the car, for instance, in the presence of lighting. Lights help to enhance the sight on the road and the visibility of cars in traffic (Chapman, 2018). Another addition to safety and practicality is found in the introduction of the pneumatic tire by John B. Dunlop in 1888. The pneumatic tyre provided a smoother ride, better shock absorbing qualities and increased durability then wooden cart wheels. With these qualities the car became easier to drive. The skillset of drivers could be lowered which made controlling the vehicle reachable for more drivers (Rae, 1965). Over time the car evolved, a closed monocoque design improved the protection of car occupants. Technical measures such as air conditioning improved driver conditions in the car. A recent development is the rise of the electric car, stimulated by government incentives and the growing concern for the environment (Niestadt & Bjornavold, 2019). The electric car comes with its own safety issues. One can imagine that an electric car crash must be treated differently by firefighters than when a gasoline car has a crash. Other concerns are that quietness of electric cars is unsafe in the interaction with pedestrians (Cocron & Krems, 2013). The electric car and the safety implications are so new that this thesis will signal their existence and leave this for future research.

The basic overview of a car is shown in figure 6. A car has a steering wheel (1) to direct the car in the right direction. A car has an exhaust system (2) when it is equipped with an internal combustion engine. A car needs to stop and therefore is equipped with brakes (3). The brakes will slow down and stop the wheels (4). Seats will make sure that driver and passenger(s) are comfortable and are equipped with headrests and seatbelts. Mirrors, both on the side and a rear-view mirror in the car (6), will provide line of sight behind the car. Windscreen wipers (7) will remove rain and snow and a heater/blower (8) will clear sight on the windscreen when it’s cold and wet. The engine (9) will drive the car and be fuelled by the appropriate source. Lamps (10) will provide light to see and to be seen and finally a badge (11) will show the cars registration to the outside world.

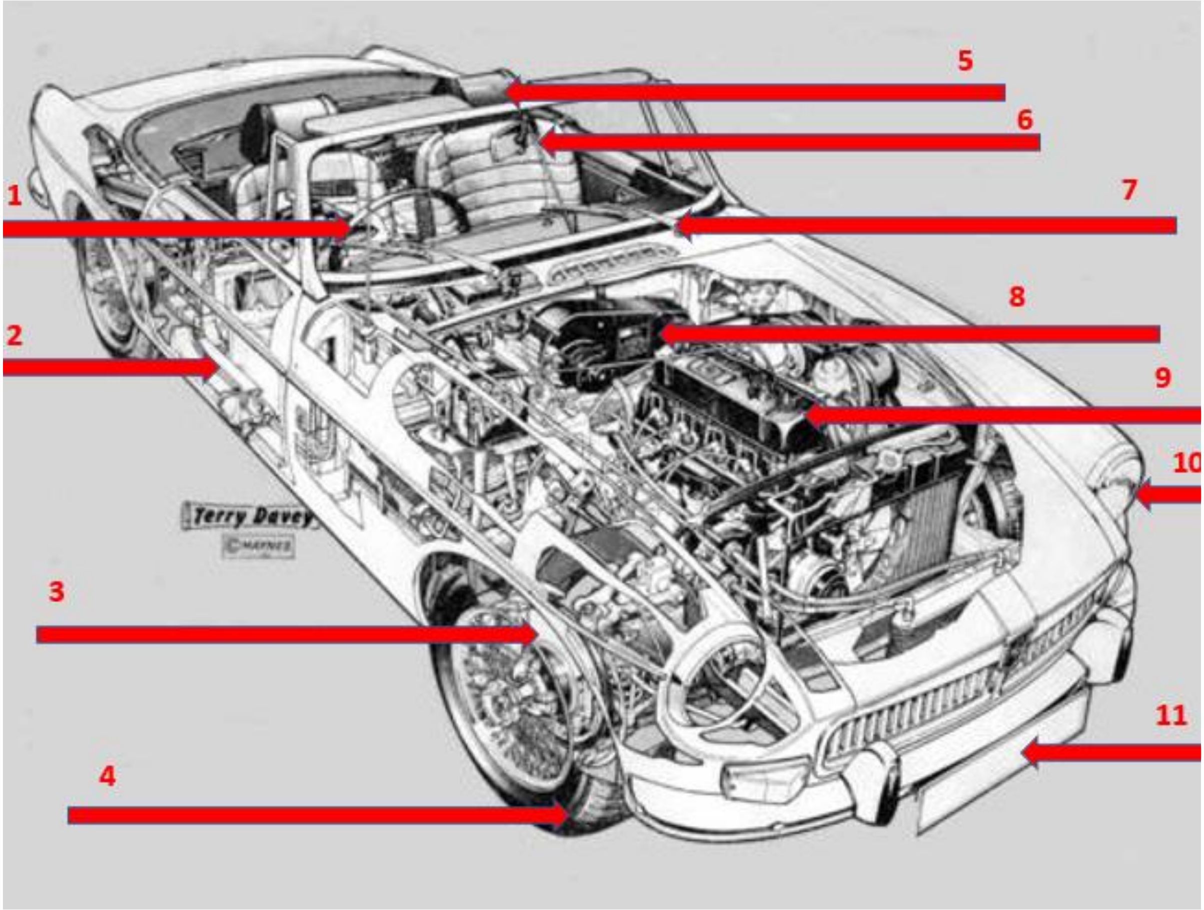


Figure 6: key components of a car, imaged adapted from (Haynes, 2016)

In addition to these basic systems that are present in any car, there are numerous additional features that can be present in a car, varying from in-car entertainment, satellite navigation, interior lights, air-conditioning, gauges and displays to provide information to the driver, camera’s to give a view of the surroundings of a car and of course the various dashboard control lights to inform a driver on any failure in the car’s system. Key safety features in the car, as defined in the overview, include: seat belts, pneumatic tires, airbags, crash absorption zones, monocoque structure, air-conditioning, fuel interruption system on collision and advanced driver assistance systems such as anti-locking brake system (ABS) (Chapman, 2018; Rae, 1965).

4.2.3 The physical environment

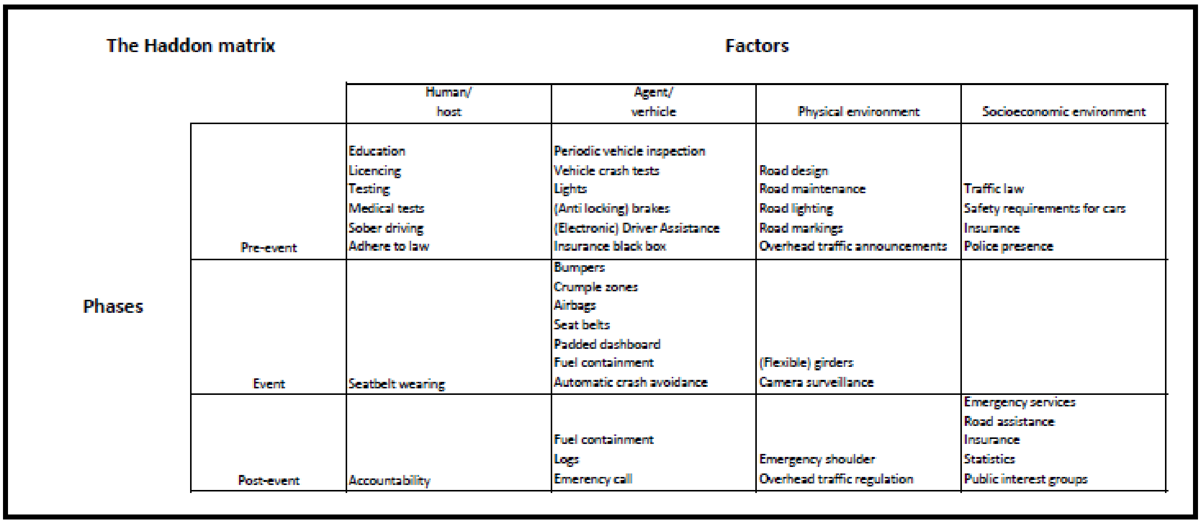
The physical environment is the space in which the car and other traffic moves. Over the years this has become a vast network of paths, tracks, roads, high and freeways spanning the world. In highly populated areas more space is dedicated and needed for vast amounts of traffic, whereas in rural areas this infrastructure will be spread out more thinly. The road has evolved from being a dirt road or mule path into highly sophisticated specially designed roads. This however needed considerable financial and engineering efforts. The first roads for cars were the existing roads and paths. However, these were never created with high speed vehicles in mind. This changed in the US with the introduction of the specifically designed toll roads providing smooth flow of traffic across long distances (Rae, 1965). Nowadays, roads can contain a diverse range of safety measures, varying from dedicated lanes for the separation of types of traffic, girders, electronic sensors, camera surveillance and dynamic traffic control systems all aimed at a smooth flow of traffic, preventing accidents and improve road safety (OECD, 2008).

4.2.4 The socioeconomic environment

Within the Haddon matrix the definition of the socioeconomic factor is society as a whole. Specifically, these are the stakeholders in car and road traffic safety. This can be the obvious ones like car manufacturer and governments, but also includes insurance companies, the consumers and public interest groups. The importance of the socioeconomic environment is recognized in the work of Esbester and Wetmore. They state that cars and road traffic is and was: *"… a technology that was increasingly becoming a crucial component of transportation, the economy and daily life."* (Esbester & Wetmore, 2015, p.311). They signal that society is changing its attitude towards injuries in car and road traffic. A specific reference is made to the concept of 'Vision Zero'. 'Vision Zero' is the initiative of the Swedish government to strive to zero deaths in Swedish traffic (Esbester & Wetmore, 2015). Esbester and Wetmore also refer to the work of Claes Tingvall. Tingvall emphasizes that public interest groups are vital to achieve any change in car and road traffic safety (Esbester & Wetmore, 2015). This confirms the role of safety advocates such as Ralph Nader. However, there are other parties that also played a role in this socioeconomic environment. One that needs to be mentioned here are the insurance companies. They proved to be of vital interest to improving safety. Just from an economic standpoint, they benefit from fewer accidents because this reduces the amount of damage payments they have to make. However, the insurance companies were a driving force behind the statistics on accidents because they needed to know what caused an accident for liability purposes so they analysed the data in a structured way. The availability of these structured accident statistics, as discussed earlier in relation to the identification of 'the second crash', fuelled the Haddon matrix with the information it needed.

4.3 The phases of a car and road traffic safety incident

In this paragraph each one of the phases of the Haddon Matrix will be addressed in more detail. Within each phase the measures to improve safety and reduce harm will be discussed per factor. The aim of this overview is to identify per phase what safety measures entail, why they are effective and how they work. By no means this overview will strive to be a complete set of measure ever taken in car and road traffic safety. However, these exemplary measures serve the purpose to sketch the nature of these measures. This broad overview of measures will be transposed to see if and in what form and under what condition they can improve safety in cyberspace. The Haddon matrix that is being used for this analysis is based on desk research as discussed earlier.



The Haddon matrix		Factors			
		Human/ host	Agent/ verhicle	Physical environment	Socioeconomic environment
Phases	Pre-event	Education Licencing Testing Medical tests Sober driving Adhere to law	Periodic vehicle inspection Vehicle crash tests Lights (Anti locking) brakes (Electronic) Driver Assistance Insurance black box	Road design Road maintenance Road lighting Road markings Overhead traffic announcements	Traffic law Safety requirements for cars Insurance Police presence
	Event	Seatbelt wearing	Bumpers Crumple zones Airbags Seat belts Padded dashboard Fuel containment Automatic crash avoidance	(Flexible) girders Camera surveillance	
	Post-event	Accountability	Fuel containment Logs Emerency call	Emergency shoulder Overhead traffic regulation	Emergency services Road assistance Insurance Statistics Public interest groups

Figure 7: Haddon matrix: car and road traffic safety

4.3.1 The pre-event phase

The pre-event phase is the phase before an incident happens. Since road and traffic safety is typically a domain of accident prevention the vast amount of measures can be plotted in the pre-event phase.

In the **pre-event** phase, much attention goes out to the **driver**. One of the key elements of car and road traffic safety is driver-training. Driver-training takes many forms as there are

theoretical and practical training options. The goal of driver-training is threefold, according to Assailly (Assailly, 2017). The three elements are the theoretical part, skills and attitude. These three elements are, as Assailly describes, part of the concept of road safety education. The theoretical part is to learn the rules in traffic and gain insight into how to handle in a specific traffic situation. Secondly, the practical training is there to educate the driver in how to actually drive a car and participate in road traffic. The final part of the education is aimed at behaviour. What unwritten rules are there in traffic, what behaviour is expected and how does a driver interact with other traffic (Assailly, 2017). So, road safety education is about knowing how to drive, actually being able to drive and understand how to behave in traffic.
The formalisation of the road safety education is the driving exam and the driver's licence. Many countries use the starting age of 18 years for qualifying for a driver's licence, although 16 can also be found around the world. Countries can pose limitations on the age until a driver's licence is valid, or requiring additional medical checks for people over a certain age.
Car and road traffic education is started at an early age. Children are introduced into the world of traffic in small steps. They start participating on foot, later by bike and when they are eligible for a driver's licence, they can start training. Learnings from road safety education are that successful road safety education is depending on four specific conditions (Assailly, 2017). These four conditions are: the pedagogical objective, the competency of the trainer, the method adapted and testing the one that is being taught. These four conditions are internally connected in such a way that a change to one of them would require recalibration of the others. Assailly also concludes that education does not stop once it is mastered. There is a need to periodically train and improve the skill. Such repetition of education fits the post licencing improvements that Shinar defined, as discussed earlier.
In the Netherlands drivers follow a regulated route to obtaining a driver's licence. They need to take lessons at a certified driving school. These trainers and schools need to comply to standards. Furthermore, they are supervised by a national authority. In the Netherlands there is an independent organisation appointed to conduct this process. This Central Bureau of Driving ability (CBR), is the only organisation in the Netherlands that is allowed to test and certify persons and to examine if someone is eligible to obtain a driver's licence. In the research done by David Shinar in which he deals with the human factor in road safety, he identifies four elements of safety improvement of the driver. These four are driver

education, driver licensing, the enforcement and post-licensing driver improvement (Shinar, 1978).

Other measures to improve car and road traffic safety are aimed at influencing driver's behaviour. A major issue in this respect is the use of alcohol and drugs. To positively influence this behaviour, awareness campaigns are designed to convince people to change to not drink or do drugs when one needs to drive Also, the police regularly performs checks on drivers to see if they are under the influence of alcohol and/or drugs. While drinking and driving remains a problem, the emergence of new technology develops into new dangers for drivers. The car phone, mobile phone, modern autonomous driving features in cars, the rise of the smartphone and apps prove to be a whole new category of distractions for drivers. If one is preoccupied with other stuff, this reduces car and road safety (NHTSA, 2016). These new challenges are and will continue to be the subject of awareness campaigns to change the driver's behaviour.

In the **pre-event** phase, there is a variety of measures that can be taken to increase the safety of the **car**. These measures are aimed at the prevention of a crash, for instance anti-locking brakes enable easier and shorter stopping, thus improving the chances to avoid a collision. Lights improve visibility for the driver and make the car more visible for other traffic. Especially electronic driver assistance features also known as Advance Driver Assistance Systems are specifically designed to assist the driver in controlling the car and driving it safely. These systems are becoming more advanced and with computer assistance are developing toward the possibility of a self-driving car (Gifei & Salceanu, 2017). These systems are the systems directly involved in the minutes or seconds before an event and are not in the way of the user. For instance, the anti-locking breaks are only activated when the driver is braking hard. In that sense this is a passive measure, only active when needed and it requires no other activation by the driver than the regular breaking.
Other measure that are important are the vehicle crash tests. By industry or governmental standards that set norms, cars are tested to see how they perform before they are allowed to go on the road. Combined with universal type approval, by for instance the EU, the actual product safety pushes manufacturers to keep on producing safer cars. Not only because manufacturers want and need a car to pass such test, some car manufacturers even made zero accidents their aim.

Finally, a major contribution to safety has been made by the system of periodic vehicle inspections. Such a yearly or bi-yearly basic check of individual cars is making sure that the car inspected is still safe to drive or that repairs need to be made. The owner of a car is obliged to have his car inspected, failing to do so will result in a fine and prosecution. Also, failing to comply will risk losing the coverage by the insurance in case of an accident.
A fairly new phenomenon is the monitoring of the car by, for instance, the insurer of a car or the fleet-owner, in the case of a lease-car. This monitoring, with the knowledge of the driver via a black-box, is aimed at influencing the behaviour of the driver with two motives. The first motive is to enhance economical driving, which is in the best interest of the fleet owner and secondly to drive safely, which is primarily an insurers motive.

In the **pre-event** phase, there is much attention to the design, creation and maintenance of the **physical infrastructure**. Safety measures start with this proper design, construction and maintenance of the roads. If a road surface is cracked, full of potholes or other defects, it will require more skill of the driver to drive safely and it will put strain on the car to keep driving properly. An example of this can be found in the introduction of the toll roads in the US. Toll roads are paid-per-use highways that were designed for speed and long-distance driving. They proved to have a substantial impact on the number of accidents. As Rae states: *"The important lesson of the toll roads has been that properly designed highways make possible high-speed movement of traffic with a minimum of accidents."* (Rae, 1965, p.185). The ways these toll-ways were designed later inspired the US federal government to roll out the interstate highway network that was designed such that they would be safe to drive. Other specific measures in the physical infrastructure are the lighting of the road at night and the markings on the road surface. If a situation is unclear, the environment will require more attention of the driver therefore increasing the possibility of making an error and causing an accident.
In recent years a new feature has appeared over spanning the road. Overhead information signs, combined with dynamic traffic systems, are able to inform the drivers about specific situations, upcoming traffic jams and other potential dangers. These systems can also instruct drivers to adjust their speed or keep off a specific lane.
A final word on preventive measures embedded in the road or physical environment are speed traps or trajectory speed controls. Speed traps will check drivers on speeding at a

specific point. Trajectory speed controls will check the average speed of a car between two or more fixed points. Both enforcements contribute to an increased safety level since speeding is one of the important causes of accidents.

In the **pre-event** phase, the measures in the **socioeconomic environment** that actually reduce harm mostly take the form of laws. These laws improved car and road traffic safety enormously. There are national traffic laws that regulate maximum speed, the do's and don'ts on the road, on which side of the road you drive and which levels of alcohol or other substances are forbidden. However, there are also laws, on a supra-national level such as the EU, that set as basic safety level for cars. The EU is working on new legislation that will oblige new cars to be equipped with a wide range of new technologies such as the fore-mentioned black-box and warning sensors for driver distraction (European Commission, 2019). There are also laws on the earlier mentioned periodic vehicle inspection, the licensing of drivers, seatbelt wearing, accountability insurance and so on and so forth (Wegenverkeerswet, 1994). As described above, insurance companies or the insurance itself also play a role in the prevention of accidents. Finally, there is the police that needs to ensure the enforcement of these rules. If the chances of getting a fee for a traffic violation is high, drivers will most of the time try to avoid getting a fine. That leads to adherence to the law and leads to safer car and road traffic.

4.3.2. The event phase

In the **event phase**, measures the **driver** can undertake are very limited. If the event happens it will happen. The measure that does mitigate harm during the event is wearing a seatbelt. When the driver wears his seatbelt, the driver is restrained in the seat on impact. The seatbelt was invented in 1958. This invention, by Volvo engineer Nils Bohlin (Chapman, 2018), was specifically aimed at absorbing energy that is released during in a crash. Although a clear technical intervention, the seatbelt is included in the human factor of the Haddon matrix. The reason for this is that it is every individual human that should actively put on the seatbelt when driving. Putting the seatbelt on when crashing is clearly not feasible and not a realistic scenario. In the USA automatic seatbelts were tried for some time. By automizing the seatbelt, the driver did not have the choice of wearing thus transforming the measure from an active measure to a passive measure. There is a distinct difference in the use of passive and active measures in the effectiveness of car and road safety measures. The passive measures, which are things that do not need an activation, according to Williams, surpass active measures in effectiveness as he states: *"The advantage of passive measures is that once in place they apply to virtually everyone, whereas active measures must be implemented by each person."* (A. F. Williams, 1999, p.16). As described, the seatbelt is an active measure. In other words; each and every driver still needs to be persuaded to wear the seatbelt (Newman, 2004). So other factors in the Haddon matrix are involved too, like awareness campaigns and the education of the drivers and the enforcement of the rule by the police.

In addition to the measures mentioned there are also a range of measures that are included in the **car** to help during the **event phase**. These measures are typically aimed at absorbing the energy that is released during a crash and they too are based on the ground breaking work of Haddon. In the article: 'Landmarks in the History of Safety', Michael Guarnieri explains the significance of two scientists in this context. Both scientists, Gibson and Haddon, came up with the same formula to improve safety: *"… injury prevention depended on the control of energy*" (Guarnieri, 1992, p.151). The first measure to be taken in this context is the padded dashboard. This measure was a direct consequence of the shift in focus from the change of the driver's behaviour to studying the cause of the harm sustained in a crash. This research specifically uncovered 'the second crash'. This notion of 'the second crash' proved to be an eye opener for many in the industry. The discovery of 'the second crash' was based on statistics by epidemiologists. In the prevention of harm in a car crash the first impact cannot be prevented in all circumstances. However, by investigating the sustained trauma by the driver, it was found that the 'second crash', that is for instance smashing into the dashboard or windshield, caused major trauma. By applying measures to decrease the impact of 'the second crash', a drastic harm reduction was achieved (Newman, 2004). An important notion in this case is that the measures are specifically effective where the driver and the car physically collide. A technological advancement to mitigate the harm sustained in 'the second crash' is the airbag. This device that is implemented that is in the steering wheel is specifically designed to cushion the head when a car is abruptly stopped in a crash. In contradiction to the seatbelt the airbag has the advantage that the driver does not need to do anything to benefit from the airbag. This is a passive measure that will be there when needed but is not bothering the user when not needed.

The car also contains structural measures such as crumple zones and bumpers. These measures are less refined as the airbag but are still very useful in dampening the impact of the sudden energy displacement when a car is in crash. Bumpers have the particular function to absorb energy. Crumple zones are also for absorbing energy and are specifically placed on positions in the car where they can do their work without harming the driver. Finally, there is one very specific measure in car safety that needs to be discussed. This is the fuel containment measures in a crash. A well-known safety scandal was the fuel tank issue of the Ford Pinto. Because of economic reasons, Ford designers shortened the rear-end of the Pinto, leaving the fuel tank vulnerable in a crash. The Pinto was nicknamed the *'the barbeque that seats four'* (Parissien, 2014, p.270). Preventing fuel to be spill in a crash, triggered the redesign of fuel tanks and integrated designs of the car to shield the fuel tank during a crash.

In the **event phase** there are only limited measures in the **physical environment** that can reduce harm. One of the most eye-catching measures are the girders along the highway. These girders are designed to absorb the impact of a car sliding of the road. That car and road safety is a complex issue becomes clear when one sees the comments of motorcyclists on girders. Motorcyclists consider girders as dangerous because they can cause harm to them when they slide underneath them. This also goes for trees along many local and rural roads. Originally these trees had the purpose of keeping the users of the road cool whereas nowadays these trees prove to be obstacles that can cause harm to cars and motorcyclists in a crash.

In the **event-phase** no **socioeconomic measures** are found.

4.3.3 The post-event phase

In the **post event** there is only one measure the **person** can actively execute. That measure making sure the person has insurance. Insurance is not only mandatory for operating a car but it also pays for damages to others when one is involved in an event. The accountability by law that is covered by the insurance is a measure to ensure that drivers themselves are not burdened by the (financial) harm and consequences of an accident. This collective system is something that needs to be taken care of by every individual car owner. So, this can be classified as an active measure. To counteract non-compliance to this rule, government has issued regulation and enforcement by for instance the public prosecutor. In the Netherlands out of the 8.5 million cars in 2019 (CBS, 2019), a mere 1% is not insured (Openbaar Ministerie, 2020). Several times a year the databases of the car registration and the insurance registration in the Netherlands are being compared, leading to fines for not having insurance (Openbaar Ministerie, 2020).

In addition to covering the damages whenever one is involved an accident, there is another safety stimulating effect to drivers of cars. Insurance companies influence the car and road safety by a market mechanism. That economic mechanism is pricing. Insurance companies give incentives to their clients for safe driving. Whenever you drive safely and do not cause an accident in the course of a year, your premium will be lowered. This price incentive is improving individual driver's behaviour.

The **post-event** safety measures in a **car** are relatively limited. As an addition to the above-mentioned fuel containment systems, a post-event system is the automatic detection of a crash and the consequent cut-off of the fuel supply to the engine. This specific measure contributes to not spilling fuel if in the crash fuel lines are broken. Furthermore, this system will shut down the engine. The latter will stop the car from running out of control and secondly it will create a safe working environment for people that come to the aid.

In the **post-event** phase, the **physical environment** on, for instance, highways and freeways is equipped with a shoulder or even designated emergency safe harbours. These facilities are used both for cars involved in an accident to safely stop and assess the damage but equally important they limit the obstruction for other drivers.

The same goes for the above-mentioned overhead traffic announcements. In a post-event situation, they will inform others to be careful which will prevent additional accidents happening in the same location.

In the **post-event** phase, there is again a role for the insurance companies form the **socioeconomic environment**. The statistics that are being compiled on the accidents prove to be valuable for the analysis of future preventive measures.

There is also great value in the availability and capabilities of the emergency services such as firefighters, emergency medical staff and the police that can respond to an accident. Other parties also play a role in this. Effective road assistance clearing the road after an event will limit the disturbance of traffic which will prevent consequential accidents to happen.

Finally, there is the role of the public interest groups in society. One of the turning points in the development of car and road safety can be credited to Ralph Nader. In his book, titled “Unsafe at any speed”, Ralph Nader (1972) described the development of the safety ecosystem of car manufacturers in the 1950’s. General Motors (GM) and Ford were competing to become the biggest in the US automobile market. In 1955 Ford started a campaign focussed on the safety of Ford cars. GM argued that the public did not want to pay for safety. At the Ford factory, however, the seatbelt and padded dashboard were by far the most popular options chosen by buyers. Nader (1972) stated that: *“Henry Ford II perpetuated the myth that motorists would reject safer cars and that sales strategies and safety don’t mix”*. Nader (1972) continues his reasoning line with the statement that for decades the automobile industry was occupied with styling instead of safety. This all changed 1966 after Nader appeared in a public hearing before US congress. Car and road safety were more and more analysed by means of statistics provided by for instance insurance companies. It provided an insight into the cause of accidents and the cause of the consequent harm. It became clear that not only the driver but also other factors contributed to the infliction of harm. Ralph Nader triggered public awareness of the dangers of driving a car and the specific role of the manufacturers in it. Nader concluded that the development of the car and road traffic safety come in three stages*: “The regulation of the automobile must go through three stages – the stage of public awareness and demand for action, the stage of legislation, and the stage of continuing administration.”* (Nader,1972, p.343). As a result, in that year the National Traffic and Motor Vehicle Safety Act came into effect with a clear goal: *“That Congress hereby declares that the purpose of this Act is to reduce traffic accidents and deaths and injuries to persons resulting from traffic accidents.”* (Public Law 89-563, 1966, p.718). Nader continued to administrate accidents and the causes, time and time again informing the public on safety issues and forcing the car industry to continuously improve the safety of the cars.

4.4 Additional remarks and observations

The layout of the Haddon matrix can be read field for field and the content of each and every field can be valued individually. This however does not use the potential of the Haddon matrix to the fullest. As pointed out, the example of the seatbelt proves that by the mere design of this measure physical harm to the driver is not prevented. The seatbelt should be introduced in the car, the driver needs to be persuaded to wear it, either by education, awareness or enforcement. This means that measures to improve safety can also be linked to multiple factors in the Haddon matrix. To be effective in harm reduction there is a need of an integrated approach on a system level (Newman, 2004). The effect of the different factors also needs to understood. For instance, the law in the case of the seatbelt is threefold. Legislation was put into place to oblige manufacturers to design, produce, test and install seatbelts in cars. But there was also legislation obliging people to wear the seatbelt, a law that is enforced by the police. Finally, the seatbelt became a part of the certification process of a new car and seatbelt checks were included in the yearly technical check of every single car. To summarize, the seatbelt as a technical intervention would not reduce that much harm, but with the support of the other factors in the Haddon matrix the value to car and road safety is very much increased. Such an integrated approach, also known as a safe system approach, is also proposed by the Dutch ‘Foundation on Scientific Research of Road Safety’ (SWOV). In their outlook, 'Vision Sustainable Safe Road Traffic 2018-2030’, they have identified requirements that need to be met to improve safety. First of all, there are technical solutions such as in the road design, in the environment around the rand and in cars. These technical measures need to be in line with what humans can understand and process. Secondly, road users need to be informed, educated and trained in such a way that they can safely participate in road traffic. Thirdly, the government takes measures to put laws in place, checks and enforces these rules. Finally there is a system of care that can assist after an accident (SWOV, 2018).

A development that needs mentioning also is the goal of what is called ‘Vision Zero’. This vision was presented by Sweden in an attempt to reach zero deaths in traffic. This mission has been adopted by the EU and is to be achieved in 2050 (Belin, 2012; European Commission, 2019). This long-term goal underlines that car and road traffic safety is a wicked problem. Regardless the efforts of governments such as Sweden, society as a whole still uses the car and somehow seems to accept these deaths and injuries of individuals. This observation can also have consequences for how safety and cyberspace need to be perceived.

5. The Haddon matrix to improve cyber safety

The aim of this chapter is to see whether the use of the Haddon matrix, by extrapolating measures from car and road safety to cyberspace, may result in the reduction or prevention of physical harm via cyberspace, and if so to what degree and under what conditions. First there is an introduction on an abstract level to see to what extent the Haddon matrix fits cyberspace. On this abstract level the similarities and difference of the car and road safety and cyberspace are discussed. Based on the insights from the previous steps potential challenges and limitations are identified. The second part of this chapter describes the factors in the Haddon matrix and transposes them to cyberspace. The third part will be the analysis of the measures as defined in car and road safety and transpose them to cyberspace. The fourth part, the filled matrix, will display possible measures to improve the physical safety of humans in relation to a cyber event. Based on the above-mentioned aim of applying the Haddon matrix to cyberspace, the overview of measures must be valued in that light. In no way may it be seen as the full and complete list of measures to reduce harm to people via cyberspace, it however will give an overview of possible measures their benefits and limitations. At the end of this chapter there will be a summary of the insights on the use of the Haddon matrix to improve safety via cyberspace.

5.1 The Haddon matrix and cyber harm

The Haddon matrix is a tool specifically designed to plot potential measures to reduce harm to humans. Measures are divided over the four factors and three phases: before, during and after an event. This approach has a physical focus. As discussed, the harm in cyberspace varies. Harm can take different forms, it can be harm in cyberspace to systems, but also harm via cyberspace to information or manifest in a physical form. As discussed, the cyber harm model by B. van den Berg and Kuipers accommodates these all. This leads to the identification of the first difference between car and road safety and cyber safety. Car and road traffic safety is primarily a matter of life and death. Consequences of an event in traffic are very much physically felt by people. Up until recently, the digital world of the internet, the technical base and our activities on the internet, were limited to this electronic space. With the concept of the cyber harm model, there is now the possibility to also look at physical harm via cyberspace. A very tangible example of an event in cyberspace that caused physical harm is the outage of the emergency telephone number in the Netherlands in 2019. The Dutch telecom operator KPN plays an important role in the organisation, sustaining and supplying emergency telephone services to the national emergency number 112 (Ministerie van Justitie en Veiligheid, 2019). On the 25th of June 2019 the emergency number 112 could not be reached. The cause of the outage has been determined as an accident. A code flaw caused a problem in the system that routed calls to the right destination. Three backup systems did not function, they suffered from the same problem, resulting in an outage of several hours (Trouw, 2019). Days later the physical consequences of this event became clear. Media reported that probably two people did not receive medical assistance on time during the outage and consequently passed away (RTL Nieuws, 2019). The unavailability of 112 caused physical harm to people via cyberspace and therefore can be plotted in the upper part of figure 4. Although the outage was in the technical components, the consequences of this event were felt in the physical world. In the aftermath of the event it becomes clear that two people died. To be clear, these people died because of a medical condition. However, this medical condition was not treated in time because the emergency services could not be reached, and when reached arrived too late. To summarize, the event, that started as a failure of a routing system, caused the unavailability of digital systems in cyberspace, but transgressed into the physical world causing harm to people. This real tragedy proves that harm to people via cyberspace is no longer only digital, but now affects people also on a physical level.

The Haddon matrix is based on the assumption that events will happen. It is used to plot potential measures on the various factors and phases of an event. However, as pointed out in the theoretical framework, the Haddon matrix is not a decision-making model. If measures improving the physical safety of people have been identified, it is still a responsibility of the stakeholders to decide which measure will be the most opportune, effective or reasonable. With this observation, the decision-making process is out of scope of this thesis.

The Haddon matrix is best used when a specific physical harm is identified. By understanding the nature of the harm and how it is inflicted, it is possible to come up with measures to counter or minimize that specific harm, before, during or after the event. This is a different approach than that of risk management. As pointed out by J. van den Berg, risk management methods are leading in ensuring security in cyberspace (J. van den Berg, 2018). Risk methods reason from vulnerabilities or threats that can either be accepted, ignored, mitigated, reduced or completely solved. This method is to a large degree focussed on the use of the identified vulnerabilities. Referring back to the CSBN report, there is not much attention to events that have a physical impact on the safety of humans. The Haddon matrix potentially fills a gap in that respect in not discriminating in the cause of an event. In addition to this, the method propagated by Haddon presumes actual events that inflict physical harm derived from injury reports and statistics. This model, with the three phases, does resemble the idea of cyber resilience that has been recently introduced in cyberspace science. In the Haddon matrix, in the safe system concept and in cyber resilience, it is assumed that events will occur. As mentioned by Fredrik Björck et.al. cyber resilience is for the first time discussed at the 2012 World Economic Forum in Davos. According to Björck et.al., the definition of cyber resilience is: *"Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events."* (Björck et al., 2015, p.2). Within this definition there are three important elements. These elements are: continuous ability, intended outcome and adverse cyber events. Looking into these three elements in more detail, the continuous delivery refers to a state in which the object is able to keep on doing what is needs to do without interruption. The intended outcome, refers to the fact that the goal of a function is to perform a certain task and that stays the same. Finally, the element of adverse cyber events refers to occurrences, that regardless its cause, have impact on the integrity, confidentiality or availability of systems, networks or information. When compared to cyber security, Björck et.al. come up with a set of characteristics that they identify as differences between these two concepts. One of the aspects is the intention or goal of both concepts. According to Björck, the intention of cyber security is to ensure that systems become fail-safe. Whereas the intention of cyber resilience is safe-to-fail. The first is trying to create systems that will never fail. The latter assumes that events will happen and system will be subject of these events. The difference is that these systems are designed in such a way they are safe-to-fail, powered by their capability to adapt and recover (Björck et al., 2015). This leads to the continuous delivery of the intended function. To that extent the theory of cyber resilience is very much in line with the safety ideas expressed in the Haddon matrix and the safe system approach. Another similarity is the multi-facetted approach. Cyber resilience is achieved by taking measures on different levels much like the Haddon matrix does. Training a person, enabling a device, supported by an infrastructure, covered by law or insurance, are interconnected and supportive layers. Together these elements create a resilient system.

To summarize, cyber resilience and the Haddon matrix, as opposed to risk management, are focussed on reducing harm regardless where it comes from. Since we have seen that cyberspace and the physical world are interwoven, there is a need in methods and tools to improve safety in an integrated manner. The Haddon matrix does this and in that way can be seen as a tool to improve cyber resilience. In the next paragraphs this addition and potential limitations of the Haddon matrix is further explored.

5.2 What is the harm in or via cyberspace?

The Haddon matrix is based on the prevention of harm or more specific; physical injuries in car and road traffic accidents. This is a very clear and precise goal. That clear and precise goal is something that needs to be investigated when the Haddon matrix is applied to cyberspace. As seen in the KPN example, in which the business goal is to deliver continuous access to the emergency service access, the harm is inflicted to the systems and availability of the emergency services. As discussed, the harm via cyberspace events can (eventually) harm people. With car and road traffic safety the harm to humans is the primary focus. Although, insurance companies also want to take measures to reduce harm to objects, because also that is covered in the insurance. What the cyber harm model and the Haddon matrix both not do is define specific the actual harm. Input from real events is needed to make use of both models. The concept of the Haddon matrix emerged when, after statistical research it became clear that most injuries in car accidents were caused by specific head trauma that was inflicted in 'the second crash' (Williams, 1999). This insight triggered the introduction of specific measures such as the padded dashboard and airbag. So, what is needed to make cyberspace safer is insight in the harm that is inflicted to humans to tailor the measures.

5.3 Haddon matrix and cyber equivalent factors

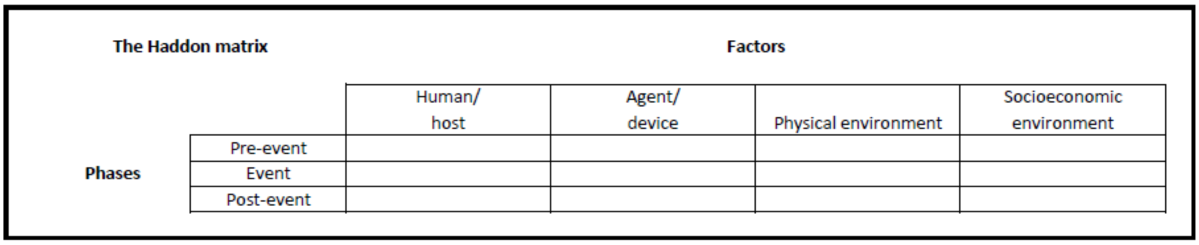
The use the Haddon matrix for cyberspace safety measures needs modification to fit cyberspace. The factors, now related to car and road traffic, need to be converted to their cyber equivalents.

The first factor is the **human**. The human is still a person, also when one applies this model to cyber safety. The human is the person conducting the cyber activities as defined by J. van den Berg. These cyber activities are the actions one performs to achieve a certain goal. Regardless the complexity of these activities, the person wants to perform them without

getting harmed in the process. This makes the person the first factor in the Haddon matrix.
The cyber equivalent of the **agent** is more complex than the definition of the person. The definition of the agent in the Haddon matrix is the car. The car is the object that is being used by the driver to achieve its goal. Following that definition, the vehicle of the person to perform cyber activities is a digital device. Such a device can either be a mobile device such as a laptop, a (smart) phone, a tablet, but also stationary devices such as desktop computers, terminals and all kind of devices for specific functions, for instance parking meters, medical devices and industrial control systems. As done with the car, devices can be described in a general manner. They also come in all kind of brands, types, configurations, colours, shapes and sizes, just like cars. They have a way to communicate via for instance a network (internet) connection, they have most of the time a user interface, processing power and memory to store and run software and some sort of operating system. To summarize, the person that performs a cyberactivity does so by using any type of digital device. That defines the second factor in the Haddon matrix.

The **physical environment** of cyberspace is a point in which car and road traffic and cyberspace differ in complexity. In the concept of the three-layer model of J. van den Berg, there is the physical layer that enables the cyber activities. This layer is broad and it encloses all the used ICT components including the earlier defined devices. In the concept of cyberspace by B. van den Berg and Kuipers, the set of physical characteristics contains the networks used in cyberspace, the digital technologies such as the devices and the ecosystem concept. The networks are definitely part of the physical infrastructure as meant by Haddon. Probably there is also a part of the digital technologies part of this environment too. The ecosystem part will be excluded for now. That specific concept doesn’t seem to fit in the physical environment factor of the Haddon matrix. However, the complexity of the physical environment between a road and the physical layer driving cyberspace is enormous. This complexity of the ICT that enables cyberspace, the vast number of digital components such as protocols and software, in addition to physical components, such as servers, routers and cables make that these two are incomparable on thar operational level. However, on an abstract level, both the road and the physical layer are there to accommodate movement. This makes that with understanding of the difference of complexity these two notions fit.

Finally, there is the factor of the **socioeconomic environment**. The socioeconomic environment is just as with car and road traffic, the whole of society, its norms and ways of doing things. For cyberspace the norms are formed by the consumers of the products and services, the manufacturers of the devices and services, the public interest groups, insurance companies and last but not least the government. The role of the government in car and road traffic and cyberspace differs fundamentally. Governments are in control over the physical environment of roads. They can impose and enforce laws and regulations on car manufacturers, road contractors and set specific requirements on how a driver is allowed to drive. This doesn't work in cyberspace. The complex ecosystem of worldwide interconnected networks and services is a huge issue when it comes to the jurisdiction of states, governments and police. The internet and cyberspace are world spanning virtual environments. In addition to that, while roads, high and freeways are in general built and maintained or paid for by governments, the creation, design, setup and maintenance of the internet and cyberspace is done by a variety of individuals, NGO's such as ICANN, ISOC, IETF and a long list of commercial companies providing the networks, the internet exchanges and all kinds of other services. As stated by Foster et.al.: *"The Internet is governed by the complex interaction of consumers, businesses, researchers, and governments throughout the world"* (Foster et al., 1997, p20). So, if the government is struggling with its role, responsibility and control over the internet, this issue will be a challenge when the same government wants to reduce harm in this same space. The process and effectiveness of laws in this context will need to be closely examined.



The Haddon matrix **Factors**

		Human/ host	Agent/ device	Physical environment	Socioeconomic environment
Phases	Pre-event				
	Event				
	Post-event				

Figure 8: Haddon matrix for cyberspace

To summarize this paragraph, the Haddon matrix for harm to humans via cyberspace is displayed in figure 8. This matrix will serve as the template for the filled matrix at the end of this chapter.

5.4 Measures to improve safety in cyberspace

In this paragraph the examples of car and road traffic safety measures are extrapolated to sketch cyber security safety measures. As with the measures in car and road traffic safety these measures will be discussed per phase in the Haddon matrix.

5.4.1 Measures in the pre-event phase

The clearest and most pregnant measure in the **pre-event** phase in car and road traffic safety is the education of the **driver**. With the speed of development of the internet and the rise of cyberspace, there was only little attention to education. To be more precise, besides awareness campaigns and professional training, there is only limited basic training for persons on the safe use of cyberspace. Although there is no doubt on the value of training a person (as one of the measures to reduce harm) the cyber driver licence as a concept needs to be directly acquitted. Such a driver licence would only work if persons are obliged by law to obtain such a licence, that persons receive certified training, practice in a controlled environment and are tested. In addition to that, the actual possession of a cyber driver licences should be checked and enforced. This is all not going to happen.

The consequences of little or no training leaves people in danger. One can go online and participate in cyber activities, in forming online relationships and communities, in creating new ‘spaces’, with limited knowledge of what cyberspace entails or how to behave safely in it. This leads to harm. Such harm is already being inflicted, not only as in the mentioned telephone outage of the Dutch emergency telephone number 112, but there are more examples. An infamous example of the transgression of an online event leading to physical human harm is the Project X Haren in the Netherlands in 2012 (Dijk et al., 2013). A birthday invitation by an underage girl via Facebook triggered the visit of thousands of people to the village of Haren. The Dutch authorities gave the advice not to come to the party but people did anyway. In the end there was chaos, violence and arrests. To summarize, a simple digital invitation to a birthday party resulted in people getting harmed in the real world.

The need to educate young people in digital skills is acknowledged in The Netherlands. There is an initiative that introduces an integrated education plan aimed at improving the digital skills and knowledge of children. This education plan starts in primary school and continues up until graduation from secondary school. This plan, as part of a broader educational reform, titled curriculum.nu, will be introduced in 2021 (Curriculum.nu, 2019). The educational plan is to train children in digital skills, how to behave safely and create understanding of the consequence’s digital media, and unsafe online behaviour, have. This is of course a start, but this is not fully covering the issue. Youngsters that will start basic education from 2021 will be educated, but the rest of the users of cyberspace will lack this education. Even for these children, although this lays the foundation of understanding what cyberspace is and how to behave safely, future training is still needed since cyberspace will keep on evolving at a fast pace. The basic elements of the education to improve skills, theoretical knowledge and attitude, will need to be more intense, quick and not only supplied to future generations. There should be plans to educate the vast majority of people that is already engaged in cyber activities and give them the possibility to gain theoretical knowledge, gain skills and change their attitude in behaving safe in cyberspace. To operationalize such an education, one could develop theoretical courses in the form of e-learnings and create online quizzes to test the understanding. Creating virtual sessions and letting people behave in a simulated world would build the practical skill set of people. The hard part will be to convince people to take these courses. As discussed, the obligation of a cyber driver licence is not going to work. With the growing digitization of society, it is no longer a choice to perform cyber activities, people are constantly exposed to cyber activities, even in daily routines. There could be possibilities to train people via employers, through municipalities or other societal organisations. However, it would be best if people would be interested in taking such training because they feel they would need to. The harm via cyberspace is for that just not big enough. The sustained events in cyberspace are apparently not at such unacceptable levels that public opinion will support demand training. To conclude this measure, education in cyber safety will work and is needed. A cyber driver licence is, however, an unachievable and unrealistic option. Other measures will need to be implemented besides education to ensure the safety of people via cyberspace.

The **pre-event** measures in **devices** open up a range of possibilities. As drawn from the car and road safety analysis, the role of the manufacturers of the cars stands out. As pointed out by Ralph Nader, the responsibility for producing safe car lies with the car manufacturers. This can be transposed directly to cyberspace. The devices that are being used by the persons conducting cyber activities are currently designed for speed, usability and style. However, these devices are more and more becoming autonomous. For instance, a self-driving Uber car was involved in a lethal accident in 2019 (BBC News, 2019). The safety of these devices is not a unique selling point. Looking at the measures of car and road traffic safety the pre-event measures in the car are either aimed at assisting the driver, to ensure that the car is safe to operate or absorb energy in a crash. In the devices the autonomous decision making however make it harder to understand and control the actions of a device. The lessons that can be derived from these measures are as follows. The way a device is maintained by its user, but also how the device is designed, constructed and maintained with updates by a manufacturer, and how the device is tested for safety contributes to improving safety. If we take the smart phone as an example, manufacturers spend time and money on the design of the smartphone, on the software, utilities and on the technical specifications such as memory, processing power and the size and resolution of the screen. It is in the power of manufacturers of devices to include safety features in a smartphone. The safety measures in the prevention phase should be based on the harm that people will sustain when an incident occurs via their smartphone. As derived from the measures in the car, these measures should be built into the device. So, the preferred type of measures will be passive measures. The person should not be bothered with controlling, authenticating or installing these kinds of measures. Safety features should be present in a device, updated or installed without effort for the user. From a functional standpoint these measures should only emerge when they are really needed. Much like the anti-locking breaks or Advanced Driver Assistance Systems, these features should support the person using the device and help to avoid harm. Nevertheless, things will happen as can be derived from the example of Marines that published their whereabouts on Strava, consequently uncovering their routines and military bases around the world (Hern, 2018). This also proves that users are not always aware of the dangers associated with the use of cyberspace and that brings us back to the importance of training.

The last measure to be discussed is the insurance black box in cars. Such a box, installed on a device, monitors behaviour with the goal to reward safe use. Users of a car that is equipped with such a device are economically motivated to behave safely. The issue with this is that there is a bias in this system. The economic choice will be that users that are already sure that they behave safely will opt for such a monitoring system. People that would need such a device to change their behaviour would probably not opt for such a monitoring system. Installing a black box on for instance a smartphone, this issue is extended even more. The privacy implications of monitoring a smartphone that is used to perform cyber activities are far greater. That makes that measures like these need to overcome numerous technical, legal and societal issues. So, such a safety measure will probably not emerge soon.

To summarize, the tests, design, maintenance and inspection of devices would contribute to cyber safety. These measures are only effective if they do not interfere with the person's day-to-day activities and protect the device and its user from identified harm as soon as it is about to happen. Last but not least there is a role for the legislator in this, because without the obligation to change, manufacturers will continue the way they are going now. The role of the legislator will be further discussed in the pre-event phase of the socioeconomic environment.

The **pre-event** measures in the **physical environment** are complex. Again, the most important input to design safety measures in the physical environment is the definition of which actual harm you want to reduce. If the harm is that people can't access information, a measure and cyber resilient approach would be to make sure that there are always alternatives available to access data. That the need of information is necessary to prevent or reduce harm can be learned from the 2015 Ukrainian power grid failures. Just before Christmas the lights went out in some regions in the west of the Ukraine. The operators at the control room where also affected, not only the region's power supply was cut, the power to the control room was disabled too and the supporting systems were unavailable. Literally blind, the harm to people was being cold for several hours (SANS Institute, 2016). The prevention of such harm can be achieved by creating resilient data storage, alternative routes to transport data or by opening alternative data stores. These alternatives, however, should, as with the device, be transparent for the user without putting the burden of these measures on the users. The complexity of cyberspace will also be a challenge in this respect. The enormous amount of different parties involved in the physical layer will make that implementing measures via this route very hard. On a business level scale this is complex, let alone on a wider scale. However, this doesn't mean it is impossible. That is because it is in the best interest of the suppliers of the physical environment, either integrated or supported by cyberspace, to keep these systems safe to use for its users. ICANN, IETF, ISOC, but also the commercial parties as ISPs, big tech companies such as Google, Facebook and Amazon, don't want the internet to break or cyberspace to become unsafe to use.

Another challenge in the physical environment lies with the role of governments. In the real world they are in control of the physical infrastructure. In cyberspace they are really struggling over what and how to control. Since cyberspace is crossing borders, jurisdiction is a difficult concept. Also, the internet is designed as an open and global network. There are only a few countries in the world that try to achieve a form of far reaching control over (their part of) cyberspace. If governments aren't in control over the physical environment the only alternative is to take measures via the socioeconomic environment: change norms, create laws or just trust companies to do the right thing.

To summarize the possibilities for cyber safety via the physical environment there is potential. To introduce measures is within the reach of the parties involved in the physical environment. However, it is up to the collective of stakeholders to convince parties to step up and take the responsibility in ensuring that harm via cyberspace to people is prevented or reduced.

The **pre-event** measures in the **socioeconomic environment** are the measures mostly related to influencing the other three factors. One of the most important instruments that comes directly from car and road traffic safety is the use of laws and regulation. States and supra-state institutions like the EU play an important role in improving safety in car and road traffic. As briefly touched upon in the physical environment, the nature of the internet and the global presence of both the internet and cyberspace make that the design and implementation of effective laws and regulations is a challenge for individual states. But this doesn't mean that laws will not make a difference. In 2018 there was a big rise of awareness on the topic of online privacy. The general public and business were suddenly confronted with privacy, via the introduction of the GDPR within the EU (European Union, 2020). The goal of the GDPR is on the one hand to give individuals privacy rights and on the other hand regulate the way businesses handle the (online) privacy of these individuals. The higher goal of this legislation was to harmonize the EU's single market. The same goes for more stringent rules on the products that are used in wireless communication. The EU is forcing manufacturers of connected devices to comply to a set of minimum requirements that are formulated in the Radio Equipment Directive (European Commission, 2016). A final example that really touches on the safety of humans is the online sales of medicines. The EU has set standards and created a means to recognize approved online medicine reseller (European Medicines Agency, 2018). All three sets of regulation tackle two specific issues that were formulated earlier in this research, the first one being the global span of cyberspace, by regulating on a supra national level, and the issue of what harm is prevented by addressing specific issues such as privacy, product safety or regulating the EU single market. To elaborate on that: the GDPR, RED and Directive on 'falsified medicines for human use' are valid for the whole of the EU, which surpasses the state boundaries. With the (economical) size of the EU, big (tech) companies' behaviour is also influenced. From an economic standpoint, they all want to have an EU presence to have access to the EU's single market. Secondly, these sets of rules either improve the privacy of individuals or improve product safety. If this approach would be extended to other areas in which harm via cyberspace is identified, this could really hold value for improving safety. But, as learned from car and road traffic safety, laws need enforcement. Without the proper enforcement, organisations, individuals and others will not likely to be compliant with these rules. The question is how and how effective will the enforcement of these European regulations be? At least in the Netherlands the first reports are promising. The amount of reported privacy issues is on the rise (Autoriteit Persoonsgegevens, 2019). In itself the rise is not a good thing, but at least is shows that insight in the harm and the size of the problem is gained.

Another measure derived from car and road traffic safety is the role of public interest groups influencing the public opinion. As described, the role of Ralph Nader was crucial in the public views of the safety in car and road traffic. Such an advocate, that literally gives the wake-up call on safety issues, can be of big help in ensuring that safety in cyberspace will become a priority. Still, the effectiveness of such an advocate depends on the severity of the harm that needs to be reduced. In car and road traffic security that harm was clear.

A final role within the socioeconomic environment is there for insurance companies. In car and road traffic safety they provided the much-needed statistics on the harm in crashes. It was exactly that data, combined with other sources, that found the major sources of harm in the energy transfer between the driver and the vehicle in an accident which led to the notion of 'the second crash'. Within cyberspace the role of insurance companies is on the rise. They are not yet in such a position to provide, let alone act on, the insights they have on the harm to humans via cyberspace. Also, not everyone agrees on the role of insurance companies in making cyberspace both safe and secure (Woods & Moore, 2019). The obvious difference between cyberspace and car and road traffic in this respect is that one is legally obliged to have car insurance. This is not the case in cyberspace. If that would be the case

this would automatically lead to more statistics on the damage claims from the insurance clients and then also give more insight in the harm that is suffered in cyberspace. It is well possible that whenever more and more people get harmed in or via cyberspace the role of insurance will change. If there is a need of an insurance policy the market will demand it. Then if there is a market, insurers can influence changes in the behaviour of their clients. Insurance companies will formulate entry criteria to get an insurance policy. They can demand certain skills, device configurations or basic safety measures to be in place, to be eligible for compensation in case of harm.
To summarize, the socioeconomic environment has in the pre-event phase a major role in reducing harm in cyberspace. That role is complicated because of the complexity of cyberspace. But by combining efforts by these parties and combining measures in the other factors, they are a major contributor to cyber safety improvements.

5.4.2 Measures in the event phase

The event phase starts when harm is done to humans via cyberspace.

The **event phase** measure to keep the **person** safe that is mentioned in car and road traffic is the wearing of the seatbelt. For the seatbelt to have effect it has to be worn at the moment of a crash. Cyber safety measures that keep the human safe in an event are just as limited as the measures in car and road traffic safety. What is clear is that the measure is something the person should have done before the event and is a harm reducing measure during the event. This measure is something a person needs to actively do and that is putting the burden on the person. As already established the additional actions will most likely make this not a measure that would actually work for the users. Then we are back at the point of what is the harm that needs to be prevented. If there is a more detail understanding of the physical harm that is likely to emerge, specific measures can be designed to reduce the impact of the event on a human.

The **event phase** measures in **devices** can be helpful. In various ways the manufacturers of devices can improve the safety of the devices. That is because the devices can process information and if connected, the devices can receive new information and instructions during their life time. First of all, devices can, if that is an appropriate measure, stop all processes on the device and for instance only leave emergency capabilities available. From car and road safety it is found that the fuel should be stopped as soon as possible after a crash because of its explosive nature. Consequently, there were fuel containment systems installed. Also, the airbag proved to have substantial benefit for the car's occupant. Both measures are passive measures that only emerge on the moment they are needed during an event. For cyber safety, to stop harm to humans, a measure could be found in stopping an unwanted effect of a device. It is important to exactly define what these unwanted effects are. In the case of a pacemaker, a device to control your heart rhythm, does it need to send out pulses when it fails or does it need to shut down instead? Another example can be the electronic locks in an office building. There is a choice to deactivate the locks in case of a fire to let people leave the building without having to unlock. Or the other way around, are there physical alternatives whenever the digital lock system fails. Do the door locks freeze or unlock during a system failure and is there resilience in the system? The turning side of these kind of device specific measure is that they need to be thought thru to the point in which they are the most effective in reducing harm. A prerequisite in any of these measures is that they should be passive, not bothering the user in day-today use, and active at the event in which they are designed to reduce harm.

The **event phase** measures in the **physical environment** to mitigate damage are scarce. As stated in chapter 4, it is the girders that for instance absorb energy of a car crash and keep the car sliding of the road. For cyber safety this is much more complicated. Although it is possible to route traffic through the network in a particular way, doing it in such a manner that this increases safety or reduces harm is hard to conceptualize. However, following the resilience way of thinking, measures to protect humans from harm should be based on the continuation of delivery of the intended business goal. Remotely controlling bridges for instance is something that is common in the Netherlands. There are a lot of waterways and having bridge managers stationed at every bridge is proving to be expensive. So, bridge managers do their work more and more from a remote location. Based on sensors, camera's and other information they open and close their bridges. This will sometimes harm people as described in a case in Zaandam in which nor the systems, nor the bridge manager, detected people on the bridge. The bridge opened and people got hurt (Onderzoeksraad, 2016). Measures to stop harm in this event could be found in connected sensors or automated movement detection. The information they provide could assist the bridge manager in deciding to stop the opening or closing of a bridge when there are people still on it.

Automatic detection seems to be a good alternative. The big challenges in the design of those kind of solutions is always finding a way to prevent harm and to prevent misuse of the system.

The **event phase** measures in the **socioeconomic environment** are just as at car and road traffic safety not present.

To summarize the measures in the event phase. The measures that hold value need to be measures that on the one hand do not limit the usability of the device or that of cyber activities and, therefore, are the most effective if they are passive and only become active when there is an event. The area with the most potential for measures is by far the device. Devices are the most appropriate factor from the matrix to impose measures on, while it contains not only processing power that can intervene during an event, but it is also the interface between the person conducting cyber activities and the physicality of cyberspace. The latter, especially with the rise of the technology of connected sensors, the infrastructural environment also has vast opportunities to introduce passive measures to take measures during an event.

5.4.3 Measures in the post-event phase

The post-event phase is the phase in which an event occurred and this is the area in which the reduction of harm via consequence management is important. In car and road traffic the most measures for harm reduction are positioned in the socioeconomic environment.

The **post-event** phase measures that can be undertaken by a **person** are of course aimed at reducing the harm in the aftermath of an event. In car and road safety that is primarily covered by insurance. Every driver has to have insurance to at least cover for damages caused by that driver to others. By being obliged to have such insurance the harm done to another is minimized in terms of economic value. At this time the chances are little that a private person hurts someone physically via cyber space. However, this is relevant for companies and organisations using cyber physical systems. These systems, for instance that are controlling the railways, could become unavailable. If train systems then cause trains to be stranded somewhere in the countryside this can cause harm to people. Imagine a hot summer day, no air-conditioning, no water and no windows to open. The train will turn into an oven within minutes. Claims from these people, can be covered by a liability insurance. By

the increasing dependency on the digital services to do or provide business, more and more events can harm people via cyberspace. Insurance could be helpful.
The only real alternative is to decrease the dependency on cyber activities. An example is the growing dependency on electronic payments. Banks forced people to use electronic payment measure. But without keeping some cash money available buying groceries during an outage of bank systems will prove to be challenge. Again, resilient thinking is such a case will help for both individuals and organisations. So, to limit harm after a cyber event, keeping some (analogue) alternatives available could very well be a real measure.

The **post-event** phase measures in **devices** can also provide the valuable statistics as above-mentioned. Furthermore, just as with modern cars can have a black box or have a data connection with for instance the manufacturer of a car or an emergency room, devices can also report events automatically. In a way this already happens with certain software components. Programs sometimes ask permission to send out error logs when a piece of software malfunctions. If such functionality is extended to also include hardware or the combination and it would include services in cyberspace, these reports can help build an overview of signalling potential harmful situations. But also, this kind of functionality can inform emergency services (as will be discussed in the measures by the socioeconomic factor) that can step in and help to reduce the harm.

The **post-event** phase measures in the **physical environment** need to be found in the monitoring of events happening in the physical environment of cyberspace. Large scale monitoring of activities in cyberspace could help detecting events when they have occurred. These events could then be responded to and the data of it used for future more accurate detection. Improvements on this monitoring and analysis could be made with the use of sensors and the analytic capacity of AI. In the long run these capacities could possibly even built real-time and predicting capabilities. If so, these measures could also move up in the event phase to in the event or even before the event-phase. But it is also very conceivable that there would be real societal resistance to the idea that there would be large-scale monitoring. A solution to that could be pattern recognition of events without analysing the content. For smaller organizations and networks this would be well possible. However, if one wanted to do something like this in the whole of the internet or cyberspace, the issue is that there is not one single owner. Currently there is not one authority that can be assigned such a task. Governments have limited influence on the infrastructure of cyberspace. Other organizations have a role, the fore-mentioned ICANN, ISOC and IETF are a part of this environment but also many, many more. Practically, such a large-scale measure would not work as long as the responsibilities to maintain cyberspace are as it is.

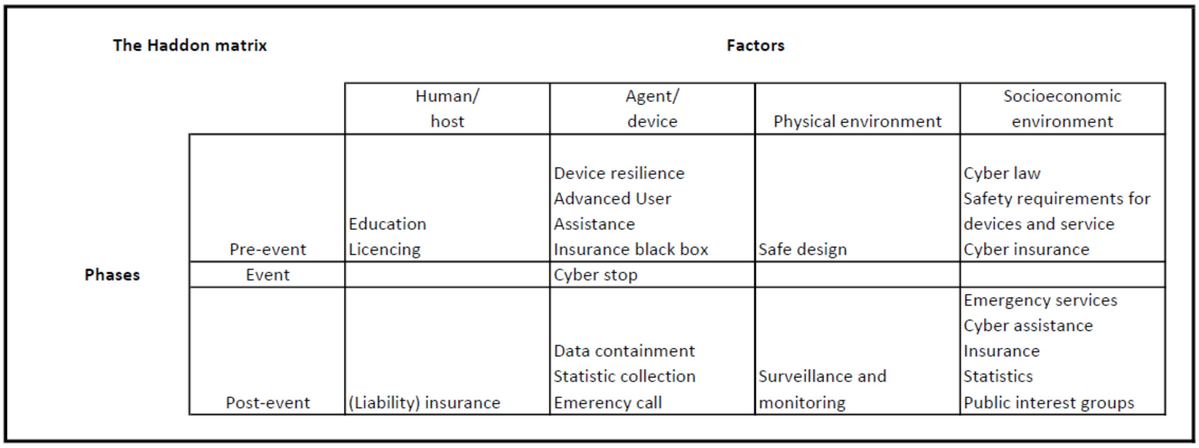
The **post-event** phase measures by the **socioeconomic environment** are more numerous than in the event phase. To minimize harm after the event, emergency services such as digital firemen and digital road assistance can be helpful. This kind of services, just as in road traffic, should be specialized in delivering first aid in the post-event phase of a cyber event. To elaborate on this, the capabilities of these kind of emergency services should range from retrieving data that was presumed to be lost, repair or restore configurations, software or hardware. But these emergency services could also play a role in assessing the damages sustained in the real world by the event. As a result, this would also feed the very much needed statistics to assess the harm of cyber events. Finally, such a service could even contribute more to cyber safety by providing advice what measures to take to mitigate the harm in future. A service like this needs funding, capacity and structure. In line with car and road traffic safety these services might find a place in the fore-mentioned insurance policy. Insurance companies do supply support in a wide range of fields of service. Other parties could also provide these kinds of services in addition to their existing services. This could be companies in the digital services like ISP's or telecom providers. Adding this kind of services seems logical since they are an economical extension of their products. However, there are more possible organizations that might be logical candidates to accommodate this kind of services. There are organizations that already have cyber incident response capabilities. Cyber Security Incident Response Teams are formed to help and support organizations if they are involved in a cyber event. There are (inter)national organisation, sectoral organisation and there are even commercial services provided by cyber security corporations. Currently these response units focus foremost on cyber security. To extend their task to events that cause harm via cyberspace will prove to be a leap. That is, because the digital domain is then left and that is a big step. If for instance a critical infrastructure organisation is reporting a cyber event at the National Cyber Security Centre in the Netherlands, they will receive assistance. This assistance is however not for non-critical organisations and definitely not for private citizens. The other way around, other

organisations also struggle with cyber events in the physical world. This is illustrated by the very specific instructions for towing a malfunctioning Tesla (Tesla Motors, 2020).
Finally, there is also a role for public interest groups. As described in car and road traffic safety, the safety of cars was highly promoted by Ralph Nader. A similar cyber safety advocate can stand up and speak out on the lack of interest in the issue of cyber safety. Demand for safe and resilient products and services would be very much in line with the development of car and road traffic safety. Such an advocate for safety would of course highly benefit of spectacular examples, maybe the emergency services disruption of 2019 in the Netherlands can be used in this context to prove the value of cyber safety measures.

To summarize, in the post-event phase, there is again a role for insurance companies. Not only to reduce the harm to third parties, in for instance paying for damages, but also a role in providing emergency services to private persons and companies. This kind of services should of course be aligned with existing initiatives such as CSIRTS and other authorities.

5.5 The Haddon matrix for reducing harm in cyberspace

Based on the above-mentioned theoretical measures to improve cyber safety the Haddon matrix as shown in figure xx is composed. The matrix contains the measures that are inspired on the car and road traffic safety measures. Although the measures are theoretical, they show that using the Haddon matrix can be a valuable addition to the existing body of knowledge on cyberspace in general and cyber safety science in particular.



The Haddon matrix		Factors			
		Human/ host	Agent/ device	Physical environment	Socioeconomic environment
Phases	Pre-event	Education Licencing	Device resilience Advanced User Assistance Insurance black box	Safe design	Cyber law Safety requirements for devices and service Cyber insurance
	Event		Cyber stop		
	Post-event	(Liability) insurance	Data containment Statistic collection Emerency call	Surveillance and monitoring	Emergency services Cyber assistance Insurance Statistics Public interest groups

Figure 9: Haddon matrix for reducing cyber harm

5.6 General observations in defining cyber safety measures

The first observation is that the Haddon matrix as shown in figure 9 can be used in categorizing cyber safety measures that can prevent or reduce physical harm to people. Education and measures in the technology of both the device and physical environment can be helpful, but specific measures as a cyber airbag will only help if the physical harm wants to prevent is defined properly. There is also a lot of potential in the socioeconomic environment.

The second observation is that it is hard to come up with actual measures to increase cyber safety without specific cases of harm. As shown in different examples such as the emergency services telephone outage the transition to physical harm is there. But without a structural registration, in depth research to what this harm entails, measures will be theoretical. As pointed out by B. van den Berg and Kuipers there is a definite need in gaining knowledge and insight in the field of cyber safety. Defining the harm, quantifying the harm and prioritizing which harm to tackle first are all unknown now.

The third observation is that the defined safety paradigms in car and road traffic safety could be used as guidance to what or where the attention should be focussed on to improve cyber safety. As shown in figure 5 there is gradual growth and integration of measures. First, safety measures are focussing on one factor such as the person or the car. Later in its development the safety measures become more interwoven. The interaction between the factors in the Haddon matrix can finally lead to cyber safe systems approach.

The fourth observation is, that for this thesis the focus is on physical harm to people via cyberspace. By using the Haddon matrix, there were times that almost automatically, harm in cyberspace of informational harm was touched upon.

To summarize, learnings from the effectiveness of car and road traffic safety in comparison to cyber safety are that, education, although doubted in effectiveness is still needed. Passive measures are more effective than active measures. If you know what is exactly causing harm the measures can be found in multiple factors, before, during or after an event. Finally, the combination of measures over all factors increases the effectiveness of measures.

6. Conclusion

This thesis set out to see what could be learned from car and road traffic safety for physical harm to people via cyberspace. With conducting this research light has been shed on different facets of cyberspace. This thesis used conceptualizations of cyberspace and of harm in or via cyberspace, to give insight what cyber safety might entail. To see what can be learned from car and road traffic, an overview was made from the development of car and road traffic safety and landmarks in this development. Finally, the Haddon matrix was used to see if that specific model would help in identifying measures to reduce or prevent physical harm to persons via cyberspace.

This all was not at all easy, not only because car and road traffic and cyberspace are different technologies, the stakes are also different and they address a different subject in human society. But these technologies are also remarkably the same: both are global, complex and connecting people.

Having said that, let’s return to the main question of this thesis:
To what extend can lessons learned from 130-year of car and road traffic safety development help in the prevention or reduction of physical harm inflicted to people via cyberspace?

To answer this question: insights from car and road traffic safety development can definitely help in the prevention or reduction of physical harm inflicted to people via cyberspace. They can help to the extent that they show a path of growth in safety measures that can be transposed to cyber safety. Also, some of the car and road traffic safety measures can be used to inspire cyber safety measures. The Haddon matrix as composed in chapter 5, proves that this model works for cyberspace and cyber safety. That same Haddon matrix can also be taken as a starting point for future cyber safety measures. In more detail the working of the model with pre-event, event and post-event phases, the education of users, the possibilities the device and environment hold and most important the influence the four factors have on the working of each of the measures can be very beneficial for improving cyber safety. A very practical learning is that the Haddon matrix is entirely based on the identified harm. It is specific harm that opens the door for the composition of measures spread over the Haddon matrix. The identification of harm to people via cyberspace, or even broader, getting statistics on event in and via cyberspace is needed to really advance in cyberspace. To summarize: the Haddon matrix with its three event-phases and four factors of measures, proves to be a suitable model to use to identify measures on cyber safety.

As pointed out there is not much attention for safety in cyberspace research. Cyberspace is currently mainly focussing on the security of cyberspace. By not looking at the safety aspects of cyberspace things will be missed and people can get hurt. The situation of cyberspace is in that sense the same as in the early days of car and road traffic safety. People got hurt and everyone was focussing on just a single aspect of the problem, the driver. Solutions given by this thesis come as parallels from car and road traffic safety. People need to be aware of the fact that events will happen and that society needs to be able to cope with that. Secondly the continuous development of safety systems in cars teaches us that absolute safety in car and road traffic is still far away. A cyber resilience approach can in that respect be an addition to the use of the Haddon matrix. Ambitious plans as 'Vision Zero' are brave and will hopefully once be achieved. However, it teaches us for cybersecurity that there is still a long way to go.

So how to proceed? The following pointers can help: as seen with car and road traffic safety, investigating the cause of the harm is key. Keeping track of events could provide insights into the cause of the harm. Also, quantifying harm is something that is necessary. Only then, one can identify things like 'the second crash' in cyberspace. For now, measures seem mostly theoretical, the question is for how long they will remain that. As seen harm is inflicted to people via cyberspace. Better to act now, than to wait until loads of people will be harmed.

Conditions that are relevant for successful cyber safety measures are: measures should be integrated and supported by all stakeholders; measures that improve resilience prove to be invaluable; passive measures proof to be better than active measures; start educating all users of cyber activities on how to use them safely; continue the education of users of cyber activities since there is continuous change in cyberspace and ways to be harmed; prevent harm by the second crash in a cyber event; get manufacturers to introduce passive safety measures in the technology of cyberspace (both in products and services); especially for active measures, use the whole spectrum of factors in the Haddon matrix; create and update measuring points and statistics on what causes the harm and what the cyber harm is; civil society should speak up and demand safety in cyberspace; finally a safety advocate, with the actual facts of events, will help the cause of cyber safety.

6.1 Final remarks and reflection

One of the main observations from this research that puzzles is that the car has been around for 130 year. Only halfway its 130-year existence, car and road traffic safety came along. So, safety was added to the product only after society woke up and did not accept the casualties anymore. Even now, regardless the efforts such as 'Vision Zero', individuals and society still seem to accept that harm and injury is present in the use of the car. People still die in accidents. In comparison; the cry in cyberspace for zero cybercrime is out and very loud about! Apparently, the advocates of cyber security do something good. However, where is the cry for cyber safety? Cyber safety as an addition to cyber security should focus on the prevention of harm to people and we have enough examples of harm via cyberspace but are they recognized?

The above-mentioned lessons of car and road traffic safety can also be beneficial for the safety of systems or information. This would be an obvious field for future research. Not only because the Haddon matrix could also be transposed to these subjects, but also every day and do nothing on cyber safety, the complexity of the issue grows and more and more chances that people will get hurt via cyberspace. In that sense, it was sometime hard to limit this thesis to only look at physical harm to people via cyberspace. The Haddon matrix and potential measures to improve safety in cyberspace and to cyberspace are also valuable. The examples of physical harm to people were sometimes hard to find, is that because we are just not looking for them? Examples of harm in cyberspace such as privacy, data-leaks, or hacks of systems, defacement of websites, crashes of systems or databases are more easy to find. But with the focus on harm to persons it must be said, the stakes are way higher. Devices can be swapped, data can be gathered, human lives can never be replaced and the prevention or reduction of harm should get undivided attention in the coming years.

References

Assailly, J. P. (2017). Road safety education: What works? *Patient Education and Counseling*, *100*, S24–S29. https://doi.org/10.1016/j.pec.2015.10.017

Autoriteit Persoonsgegevens. (2019). *Cijfers datalekken 2019*. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2019

Aven, T. (2014). What is safety science? *Safety Science*, *67*, 15–20. https://doi.org/10.1016/j.ssci.2013.07.026

BBC News. (20th of November, 2019). Uber self-drive crash “mostly due to human error”. *BBC News*. https://www.bbc.com/news/technology-50484172

Belin, M.-Å. (2012). *Public Road Safety Policy Change and its Implementation—Vision Zero a road safety policy innovation*. Inst för folkhälsovetenskap / Dept of Public Health Sciences. http://openarchive.ki.se/xmlui/handle/10616/40987

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Red.), *New Contributions in Information Systems and Technologies* (pp. 311–316). Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_31

CBS. (19th of December 2019). *Over 200 times more passenger cars than in 1927* [Webpagina]. Statistics Netherlands. https://www.cbs.nl/en-gb/news/2019/51/over-200-times-more-passenger-cars-than-in-1927

Chapman, G. (2018). *Drive: The definitive history of motoring,*. DK. https://www.libris.nl/boek/?authortitle=giles-chapman%2fdrive--9780241317662

Cocron, P., & Krems, J. F. (2013). Driver perceptions of the safety implications of quiet electric vehicles. *Accident Analysis & Prevention*, *58*, 122–131. https://doi.org/10.1016/j.aap.2013.04.028

Curriculum.nu. (2019). *Digitale geletterdheid – Curriculum.nu*. https://www.curriculum.nu/voorstellen/digitale-geletterdheid/

Dijk, J. A. G. M. van, Boeschoten, T., Tije, S. ten, & Wijngaert, L. van de. (2013). *De weg naar Haren: De rol van jongeren, sociale media, massamedia en autoriteiten bij de mobilisatie voor Project X Haren : Deelrapport 2*. https://research.utwente.nl/en/publications/de-weg-naar-haren-de-rol-van-jongeren-sociale-media-massamedia-en

Dunn Cavelty, M. (2012). *Cyber-Security* (SSRN Scholarly Paper ID 2055122). Social Science Research Network. https://papers.ssrn.com/abstract=2055122

Esbester, M., & Wetmore, J. M. (2015). Introduction: Global Perspectives on Road Safety History. *Technology and Culture*, *56*(2), 307–318. https://doi.org/10.1353/tech.2015.0059

European Commision. (26th of March, 2019). *Road safety: Commission welcomes agreement on new EU rules to help save lives* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1793

European Commission. (5th of July, 2016). *Radio Equipment Directive (RED)* [Text]. Internal Market, Industry, Entrepreneurship and SMEs - European Commission. https://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en

European Commission. (19th of June, 2019). *EU Road Safety Policy Framework 2021-2030—Next steps towards "Vision Zero"*. https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/move-2019-01178-01-00-en-tra-00_3.pdf

European Medicines Agency. (17th of September, 2018). *Buying medicines online* [Text]. European Medicines Agency. https://www.ema.europa.eu/en/human-regulatory/overview/public-health-threats/falsified-medicines/buying-medicines-online

European Union. (2020). *EU data protection rules* [Text]. European Commission - European Commission. https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en

Foster, W., Rutkowski, A., & Goodman, S. (1997). Who Governs the Internet? *Commun. ACM*, *40*, 15–20. https://doi.org/10.1145/257874.257877

Gifei, S., & Salceanu, A. (2017). Integrated Management System for quality, safety and security in developing autonomous vehicles. *2017 10th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, 673–676. https://doi.org/10.1109/ATEE.2017.7905041

Guarnieri, M. (1992). Landmarks in the history of safety. *Journal of Safety Research*, *23*(3), 151–158. https://doi.org/10.1016/0022-4375(92)90018-5

Hagenzieker, M. P., Commandeur, J. J. F., & Bijleveld, F. D. (2014). The history of road safety research: A quantitative approach. *Transportation Research Part F: Traffic Psychology and Behaviour*, *25*, 150–162. https://doi.org/10.1016/j.trf.2013.10.004

Haynes. (2016). *MG MGB Roadster (1962—1980) Repair Manuals*. Haynes Manuals. https://haynes.com/en-us/mg/mgb-roadster/1962-1980

Hern, A. (28th of January, 2018). Fitness tracking app Strava gives away location of secret US army bases. *The Guardian*. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

KPN. (25th of June, 2019). *KPN stelt verhoogde dijkbewaking in voor 112 en wil nog meer waarborgen voor bereikbaarheid*. KPN Corporate NL. https://overons.kpn/nl/nieuws/2019/kpn-stelt-verhoogde-dijkbewaking-in-voor-112-en-wil-nog-meer-waarborgen-voor-bereikbaarheid

Kramer, F. D., Starr, S. H., & Wentz, L. K. (Red.). (2011). *Cyberpower and National Security*. Potomac Books. https://doi.org/10.2307/j.ctt1djmhj1

Lessig, L., & Lessig, L. (2006). *Code* (Version 2.0). Basic Books.

Merriam-Webster. (2019). *Definition of TRAFFIC*. Last accessed Geraadpleegd 12 december 2019, van https://www.merriam-webster.com/dictionary/traffic

Nader, R. (1972). *Unsafe at any speed: The designed-in dangers of the American automobile* ([Expanded ed.].). Grossman.

Newman, G. R. (2004). *CAR SAFETY AND CAR SECURITY: AN HISTORICAL COMPARISON*. 33.

NHTSA. (8th of September, 2016). *Distracted Driving*. NHTSA. https://www.nhtsa.gov/risky-driving/distracted-driving

Niestadt, M., & Bjornavold, A. (2019). *Electric road vehicles in the European Union*. *European Parliamentary Research Service*, 11.

OECD. (28th of September, 2008). *Towards Zero: Ambitious Road Safety Targets and the Safe System Approach* [Text]. https://www.oecd-ilibrary.org/transport/towards-zero_9789282101964-en

Onderzoeksraad. (28th of January, 2016). *Accident at Den Uyl Bridge, Zaandam*. http://www.onderzoeksraad.nl/en/page/3748/accident-at-den-uyl-bridge-zaandam

Openbaar Ministerie. (2020.). *Verzekering*. Openbaar Ministerie. Last accessed 20th of January 2020, https://www.om.nl/onderwerpen/verkeer/handhaving-verkeer/apk-verzekering/verzekering/

Parissien, S. (2014). *The life of the automobile: The complete history of the motor car* (First U.S. edition..). Thomas Dunne Books, StMartin's Press.

Rae, J. B. (1965). *The American automobile: A brief history*. The University of Chicago Press.

RTL Nieuws. (28th of June, 2019). *Hulpdiensten vertraagd, ook dode in Twente tijdens 112-storing*. RTL Nieuws. https://www.rtlnieuws.nl/nieuws/nederland/artikel/4761936/hulpdiensten-vertraagd-ook-dode-overijssel-tijdens-112-storing

SANS Institute. (22nd of March, 2016). *SANS Industrial Control Systems Security Blog | E-ISAC and SANS Report On The Ukrainian Grid Attack | SANS Institute*. https://ics.sans.org/blog/2016/03/22/e-isac-and-sans-report-on-the-ukrainian-grid-attack

Schoof, D. (2019). *Speech Dick Schoof One Conference 2 oktober 2019.pdf*. https://www.aivd.nl/documenten/toespraken/2019/10/02/speech-dick-schoof-bij-one-conference-2-oktober-2019

Shinar, D. (1978). *Psychology on the road: The human factor in traffic safety*. Wiley.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (2005). *Facts and Fears: Understanding Perceived Risk* (Vol. 39). https://doi.org/10.1007/978-1-4899-0445-4_9

SWOV. (2018). *DV3—Visie Duurzaam Veilig Wegverkeer 2018-2030*.

Tesla Motors. (2020). *Tesla Motors*. http://assets.teslastatic.com/

Trouw. (25th of June, 2019). *Hoe heeft het zo mis kunnen gaan met 112?* Trouw. https://www.trouw.nl/gs-b67dd3ea

TSA. (9th of December, 2016). *TSA website*. Transportation Security Administration. https://www.tsa.gov/about/tsa-mission

Van den Berg, B., Hutten, P., & Prins, R. (2019). *Security and safety: An integrative perspective*.

Van den Berg, B., & Kuipers, S. (2020). *Vulnerabilities & cyberspace: A new kind of crisis?*

Van den Berg, B., & Prins, R. (2018). Security and safety: A conceptual analysis. *Under review*.

van den Berg, J. (2018). Cybersecurity for Everyone. In M. Bartsch & S. Frey (Red.), *Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden* (pp. 571–583). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21655-9_40

Waggoner, W. H. (1985, maart 5). William Haddon Jr., 58, Dies; Authority on Highway Safety. *The New York Times*. https://www.nytimes.com/1985/03/05/us/william-haddon-jr-58-dies-authority-on-highway-safety.html

Waldron, J. J. (2012). Safety and Security. *Civil Liberties, National Security and Prospects for Consensus: Legal, Philosophical and Religious Perspectives*, 55. https://doi.org/10.1017/CBO9781139035286.003

Wegenverkeerswet. (1994). *Wegenverkeerswet*.

Williams, A. F. (1999). *The Haddon matrix: Its contribution to injury prevention and control* (R. McClure, Red.; pp. 15–16). Centre of National Research on Disability and Rehabilitation Medicine, School of Medicine, University of Queensland. https://eprints.qut.edu.au/10081/

Woods, D., & Moore, T. (2019). Does Insurance Have a Future in Governing Cybersecurity? *IEEE Security & Privacy*, 0–0. https://doi.org/10.1109/MSEC.2019.2935702

WRR. (2019). *Preparing for Digital Disruption*.