Security risk assessment: Exploring real-life praxis

de Wit, J.J.

DOI
10.4233/uuid:303fcd6f-622f-42ca-bd91-7b84b6237548

Publication date
2024

Document Version
Final published version

Citation (APA)
de Wit, J. J. (2024). *Security risk assessment: Exploring real-life praxis*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:303fcd6f-622f-42ca-bd91-7b84b6237548

SECURITY RISK ASSESSMENTS: EXPLORING REAL-LIFE PRAXIS

Johan de Wit

TECHNISCHE UNIVERSITEIT DELFT
MDCCCXLII

To Evrie,

the inspiration of my life.

TECHNISCHE UNIVERSITEIT DELFT • MDCCCXLII •

Financial support for the printing of this thesis was kindly provided by Delft, University of Technology

ISBN: 978-94-6366-826-2

The studies in this thesis were financially and in-kind supported by Siemens Smart Infrastructure.

Cover design: Johan de Wit
Printing: Ridderprint, the Netherlands

An electronic copy of this dissertation is available at TU Delft Repository

SECURITY RISK ASSESSMENTS: EXPLORING REAL-LIFE PRAXIS

Dissertation

for the purpose of obtaining the degree of doctor

at Delft University of Technology

by the authority of the Rector Magnificus

Prof.dr.ir. T.H.J.J. van der Hagen

Chair of the Board for Doctorates

to be defended publicly on

Tuesday 12 March 2024 at 15:00 o'clock

by

Johannes Jacobus DE WIT

Master in Security Science & Management,

Delft University of Technology, The Netherlands

born in Rotterdam, The Netherlands

This dissertation has been approved by the promotors.

Composition of the doctoral committee:

Rector Magnificus, chairperson	
Prof.dr.ir. P.H.A.J.M. van Gelder,	Delft University of Technology, promotor
Prof.dr.ir. W. Pieters,	Radboud University Nijmegen, promotor
Independent members:	
Prof.dr. M.J.G. van Eeten,	Delft University of Technology
Prof. A.S. Hassoldt,	Delft University of Technology
Prof.dr.ir. M.F.W.H.A. Janssen,	Delft University of Technology
Prof.dr. S.L. Kuipers,	Leiden University
Dr. C. Liesener,	Siemens Smart Infrastructure Switzerland

Powered by SIEMENS

The research leading to this dissertation is made possible by the financial and in-kind support from Siemens Smart Infrastructure.

TECHNISCHE UNIVERSITEIT DELFT
MDCCCXLII

CONTENTS

PART 1: INTRODUCTION

PART 2: SCIENTIFIC PUBLICATIONS

PART 3: PROFESSIONAL PUBLICATIONS

PART 4: CLOSING

‘While risk is often portrayed mathematically, our response is more often instinctive.

Understanding the factors that drive how we think about and act upon risk is critical’

General Stanley McChrystal,

US Army, retired[1]

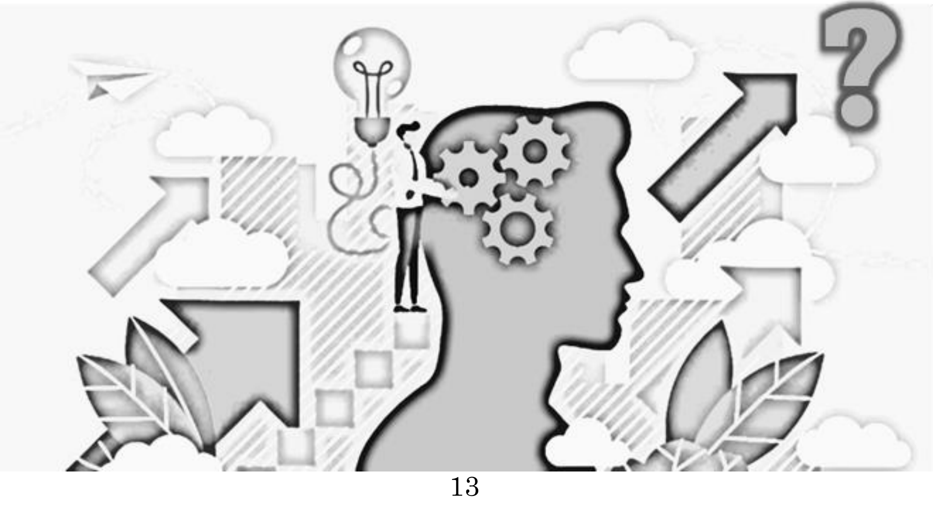
[1] Stanley A. McChrystal, Risk, a user's guide (New York: Penguin business, 2021).

SUMMARY

Facing a (security) threat, what is the best thing to do? The overall research questions driving this study are about how security professionals assess, reason, and decide about security risks, and where their justification is founded on. The presented results are explorative, based on trying primarily to understand individual professional judgment and secondary, if possible, to explain the reasons behind this judgement. This work will not answer all the questions, it is, however, a valuable start to understand the difficult task the professionals in this domain are facing: preparing for, and thus predicting possible security threats.

Security threats originate from malicious human intention. The behavior resulting from this intention is meant to circumvent security measures and is often concealed (at least the preparation). In other words: its meant to be unpredictable. This is just the single thing that organizations need to do: prepare to face these threats. Threats are in this work defined as a possible cause of a risk. A (security) threat can become a (security) risk if the likelihood of it passes a certain threshold and if the consequences of it materializing are considerable. Whether a threat is perceived as potential risk is depending on the context and can vary over organisations.

Many organizations have implemented a security function, often separated for physical and cybersecurity domains, that is in charge to analyze security threats and deal with potential security risks. As the future is unpredictable by nature, and, in the specific case of security threats/risks, often detailed information is lacking, security risk assessments and security risk decision making is commonly based on predictive expert judgement.



So how do the professionals tasked with predicting and preparing for possible threats/risks exactly do that?

The research presented in this dissertation has focused on this phenomenon for little over 7 years. It is conducted as an external PhD research process. It is very much related to the day to day activities and conversations of the PhD candidate with the practitioners in the field.

Studying risk assessments, containing activities for identification of risks in a certain context, analyzing these risks, evaluating them and finally treating them, led this research to cross various scientific domains.

The introduction presents the overall research questions and the journey to answer them. The introduction starts with some theoretical background on risk. A risk is defined as the effect of uncertainty on objectives. This defection contains the two most common recognized elements of risks in general: likelihood and consequences. Likelihood reflect the uncertainty of future events. Studying uncertainty led to the development of the 'scale of uncertainty', a graphical model of the balance between information and uncertainty. If about a risk in a given situation *all* information would be available there would be no uncertainty. As a risk is defined as the effect of uncertainty on goals, without uncertainty there is no risk. As risks deals with a certain state in the future this is a hypothetical situation. On the other end of the scale are situations where no information is available, often referred to as unknown unknowns. This is the situation with unlimited uncertainty. In real life we are somewhere in between. To guide the discussions about risks, a general term that usually encompasses different levels of uncertainty, three levels of uncertainty are proposed. Starting from the hypothetical certainty the first is a situation of 'risk'. The uncertainty at this level can be computed based on evidence. In the proposed scale of uncertainty risk is, thus, narrowly defined to the description above. The next level is a situation of 'uncertainty'. In these situations little to no evidence is available but experts can nevertheless estimate the uncertainty. This is the level where expert judgement is the primary source of information. The third level is a situation of 'ambiguity'. In these situations so little and or vague, doubtful or obscure, that even experts cannot form a judgement and can only guess. Security risks are primarily positioned in the levels uncertainty and ambiguity as will be presented in this dissertation.

Overtime several processes are developed to manage risks. They all consist of a series of subsequent steps like: establish context, risk assessment containing identification, analysis and evaluation of risks and finally risk treatment. As will be stated in the introduction and in Part 1 Chapter one, these steps each involve a number of decisions that the risk manager need to make. So although risk management processes might seem objective, they are driven by decisions of actors that can be considered subjective. So in fact risk assessments can be defined as subsequent decision making by actors.

The remainder of the introduction presents the theoretical background of some of the most prominent theories on decision making. As these are often developed in separated scientific domains, they overlap and complement each other. An attempt is made to combine these valuable theories into an overarching comprehensive decision model. This model, combined with the scale of uncertainty, offered a framework to explore real life security risk decision making. The model consists of two main parts: so called system 1 and system 2 thinking. System 1 thinking is fast and intuitive while system 2 thinking involves conscious reasoning. Within these two main components the subsequent phases in decision making are detailed. Several parts of this model and phases are studied in detail to start to understand the conscious and unconscious reasoning of security professionals.

Part 1 of this dissertation contains four chapters, each presenting a paper as published in peer reviewed journals (the paper presented as Chapter 4 is under review).

Chapter 1 presents a study to identify if security professionals, confronted with choices with predefined options, would be vulnerable to known biases. The experiments set up to test this are offered to a convenience sample of professionals via an online survey. The first part of the survey consists of a replication of well-known experiments that founded the Prospect Theory. In the second part of the survey these experiments, which involve options based on monetary win or loss, are reformulated in security risk decisions. The results significantly show that security professionals are as vulnerable to decision biases as lay people. Security risk decisions are driven by these biases of almost three out of four security professionals. The consequences of these findings are that security risks might not be treated to a maximum extend. In their decisions the professionals are guided more by reducing consequences rather than reducing likelihood. As reducing likelihood is related to prevention and reducing consequences to mitigation, it can be concluded that security professionals seem to have their focus on mitigation. These findings also identify so called probability ignorance. This will be further explored in Chapter 3.

In the next chapter security professionals are asked, via a survey, to describe their preferences when assessing a risk: what aspects of a risk do they consider. This study starts with an open question. The answers to this question can be considered 'on top of mind' and reflect a system 1 consideration. In the next parts of this study the respondents are asked to rate and rank security risk aspects. In the latter they are forced to perform compensatory decision making that is considered to reflect system 2 thinking. The answer are compared and differences analyzed. The most prominent difference is safety of employees and customers/visitors. Only 24% of the respondents had this aspect 'on top of mind'. In the end, after offering them this aspect, three in four of them put this in their top 10 of most important. It is safe to conclude that there is a difference of considered risk aspects between system 1 and system 2 reasoning. The aspect likelihood is only ranked in the top 10 of 34% of the respondents and didn't make it into the overall top 10. A second indication for probability ignorance in this domain of practice.

Chapter 3 presents the results of a study into the level of available security information of the professionals when assessing security risks, their confidence in their risk assessments and the influence of more detailed information on professional risk assessments. The professionals indicated to have detailed risk information available in only half of their risk assessments. When asked if they can assess a risk, even if they do not have exact information, they indicate that only sometimes they can't. They indicate, on average, to be confident about their assessments most of the time. The findings identify overconfidence of security professionals which seems to grow with experience.

Confronted with real life security cases, and asked to assess the likelihood of these, the respondents show a broad range of answers, an indication for so called noise. Based on the exact same information, professionals with comparable expertise reach very different likelihood assessments. Finally the conjunction fallacy is tested. This fallacy shows that more detailed information raises the assessed likelihood while logic reasoning should lead assessors to the opposite results. The consequences of the research presented in this chapter for the security domain are vast. First it shows that professionals, tasked to manage security risk in organisations and society, do this often without detailed or exact information. This rules out proper system 2 reasoning and leads them to depend on their own expertise and system 1 decision making, of which we by now know that this is prone to be influenced by biases (sees Chapter 1). More experienced professionals show less need to retrieve more information, even when they are aware information is imperfect.

They seem to rely on their expertise more. This Chapter clearly shows that professionals with comparable background can reach very different outcomes of their risk assessments. This might lead to different risk exposure of comparable organisations in our society. Finally it is shown that more detailed information of a case leads to significant higher likelihood assessment of such a case. Well informed professionals might assess a higher likelihood to a case opposing logic reasoning. This might lead to a less efficient allocation of resources.

The final Chapter of this part presents a study on the sources of security risk information. Possible sources as applied by security professionals are identified, their perceived quality is assessed and their application in daily praxis is collected. The quality of information sources is assessed by applying the NATO system or admiralty code. In this study a novel assessment criterion is proposed: source intention. This new criterion helped to explain some of the observed difference between perceived quality of certain sources and their application in praxis. Most prominent example of this is the source science/scientific publications. The quality of this source is perceived high (rank 3) but it's application is only ranked 9. This can be explained by the relatively low perceived source intention (rank 7). The respondents indicate that they doubt if the intention or aspiration, goals and objectives between science and praxis are in line. By now it might not come as a surprise that the source personal experience is ranked second, close to the highest rank source: experts. This study discovered the most important sources of security risk information for the individual professionals working in this domain.

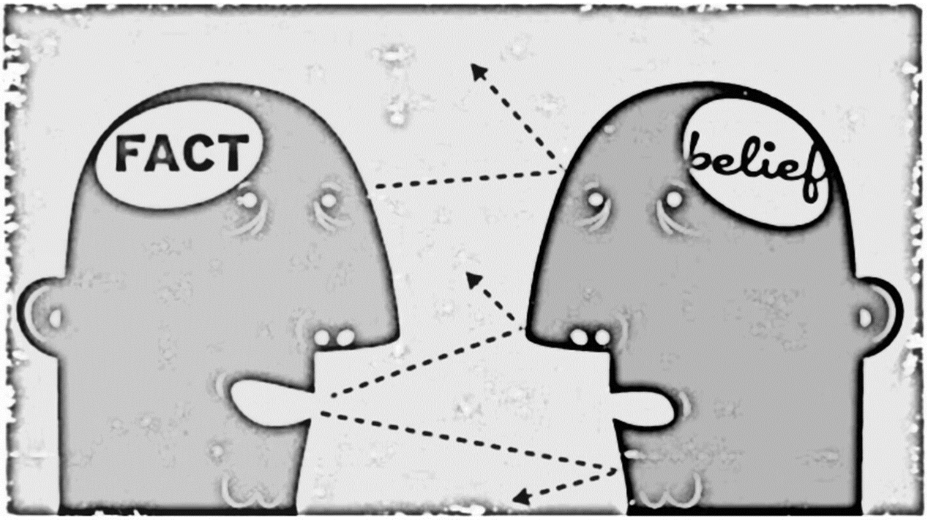
Over the course of this PhD journey the professional security domain has shown interest in this topic and received the results via several presentations at conference as are listed in the concluding Chapter of this dissertation. In Part 3 two professional publications are included in this dissertation. They might not be considered of scientific value, although they are both peer reviewed, but they show the attention this research got in the professional domain.

Chapter 5 present a cover article that is published in Security Magazine, the official publication of ASIS, the world's largest association for security professionals with 36.000 individual members worldwide. This article presents a summary of the results of the previous chapters with the purpose to raise awareness in the professional domain for flaws in judgement, decision making and risk assessments. As one of the most obvious questions in an professional environment, almost always direct following awareness, 'now what?', this article contains some possible recommendations to circumvent these possible flaws. This article turned out to become the fifth most read online article of this magazine in 2022.

The second professional publication is a peer reviewed contribution for the project Platform Influencing Human Behaviour, commissioned by the Royal Netherlands Army. The Hague Centre for Strategic Studies (HCSS) is bringing together academic experts and policymakers from different parts of Europe to explore ethical, legal and military-strategic issues and boundaries involved in information-based behavioural influencing in the military context. Our contribution consist of a brief summary of the results of our studies compiled in two main topics:

1. the information on which assessments are based (identify sources, how much security risk information is available, how does this influence confidence)
2. biases and heuristics influencing the interpretation and perception of this information (study of vulnerability for known biases, conjunction fallacy, availability/on top-of-mind study, system 1 and 2 thinking)

This paper is included in this dissertation as Part 2 Chapter 6. It is published online at the HCSS website at 12 June 2023.



This dissertation ends with a concluding chapter. This chapter is presenting all the results and conclusions of the previous chapters but combines them in a discussion like style. The conclusions are already summarized in this summary and elaborated in more detail in the sections of the individual chapters and are as such not repeated. The first part starts with the scale of uncertainty. On the left is the 'certainty area' which represents 'facts'. On the far right is the 'unknown unknown area' which represents 'belief'. This part elaborates on real world implications of 'facts vs belief'.

The second main part of the concluding chapter is discussing probability ignorance in risk decision making which was identified in several of the performed studies. As one of the main components of risk and risk management, ignoring this might reduce risk assessments to impact assessments and risk management to mitigation of impact leaving out prevention.

Finally the concluding chapter addresses the impact this study already had and might have on the professional security community. The attention this research generated and the combination of surprise and enthusiasm it provoked is briefly described.

At the end of this dissertation an epilogue is added, containing some individual observations and perceptions on the science and professional community.

This summary hopes to encourage both other scholars and professionals, to read the other parts of this dissertation. Both can find their 'own style' of publications in this dissertation, but taking the remarks of the epilogue in mind, the author hopes both sides will take the effort to read and appreciate the papers for 'the other side'.

SAMENVATTING

Beoordeling van beveiligingsrisico's ontrafeld: Studie van de praktijk

Wat te doen met een potentiële beveiligingsdreiging? De onderzoeksvragen die de basis vormen van dit onderzoek hebben betrekking op de wijze waarop beveiligingsprofessionals beveiligingsrisico's beoordelen, beredeneren, erover beslissen en waarop hun beoordeling is gebaseerd. Het in deze dissertatie gepresenteerde onderzoek is onderzoekend van aard, primair gericht op een poging om de individuele beveiligingsrisicobeoordeling van professionals te begrijpen. Secundair om de bron van deze beoordeling te verklaren. Het gepresenteerde onderzoek zal niet alle mogelijke vragen beantwoorden, maar is een waardevolle start om de moeilijke taak te begrijpen waarmee professionals in dit domein worden geconfronteerd: het voorbereiden op en daarmee het voorspellen van mogelijke beveiligingsdreigingen.

Beveiligingsdreigingen komen voort uit opzettelijke en kwaadaardige menselijke bedoelingen. Het potentiële gedrag voortkomend uit deze bedoelingen is gericht op het omzeilen van beveiligingsmaatregelen en wordt vaak heimelijk uitgevoerd en verborgen gehouden (althans de voorbereiding). Met andere woorden: het is bedoeld om onvoorspelbaar te zijn. Zoals hierboven aangegeven is dat nu juist de opgave voor beveiligingsprofessionals. Ze worden geacht zich voor te bereiden deze bedreigingen het hoofd te bieden en ze dus te voorspellen.

Veel organisaties hebben een beveiligingsfunctie geïmplementeerd die verantwoordelijk is voor het beoordelen en beheersen van deze beveiligingsrisico’s. Aangezien de toekomst van nature onvoorspelbaar is en er in het specifieke geval van beveiligingsdreigingen vaak gedetailleerde informatie ontbreekt, worden beveiligingsrisicobeoordelingen en beslissingen meestal gebaseerd op het subjectieve oordeel van beveiligingsprofessionals.

Hoe doen deze professionals die belast zijn met het voorspellen van, en voorbereiden op, mogelijke dreigingen dat precies?

Het promotieonderzoek zoals gepresenteerd in deze dissertatie heeft zich iets meer dan 7 jaar op deze vraag geconcentreerd. Het is in deeltijd uitgevoerd als een extern promotieonderzoek. De vraagstelling heeft een directe relatie tot het dagelijks werk van de onderzoeker die werkzaam is in dit beveiligingsdomein.

Dit onderzoek, gestart met het bestuderen van risicobeoordelingen, bestaande uit risico-identificatie, risicoanalyse, risico-evaluatie en uiteindelijk het nemen van maatregelen, bleek uiteindelijk te leiden tot een zoektocht door verschillende wetenschappelijke domeinen.

De introductie van deze dissertatie start met een theoretische beschouwing over risico's. Een risico wordt gedefinieerd als het effect van onzekerheid op doelstellingen. Deze definitie, afkomstig uit de NEN 31000, bevat de twee meest algemeen erkende elementen van risico's: waarschijnlijkheid en gevolgen. Waarschijnlijkheid representeert de onzekerheid van toekomstige gebeurtenissen. Het bestuderen van onzekerheid leidde tot de ontwikkeling van de ‘scale of uncertainty’, een grafische weergave van de balans tussen informatie en onzekerheid. Als over een risico in een bepaalde situatie alle informatie beschikbaar zou zijn, zou er geen onzekerheid zijn. Aangezien een risico wordt gedefinieerd als het effect van onzekerheid op doelen bestaat er zonder onzekerheid geen risico. Aangezien risico's betrekking hebben op een mogelijke toekomstige toestand is dit een hypothetische situatie omdat de toekomst per definitie onzeker is. Aan de andere kant van de schaal bevinden zich situaties waarin geen informatie beschikbaar is, zogenaamde unknown unknowns. Dit is de situatie met onbeperkte onzekerheid. In het echte leven zitten we er meestal ergens tussenin. Als leidraad voor de discussies over risico's worden tussen deze twee uitersten drie niveaus van onzekerheid voorgesteld. De eerste is de zone ‘risk’, de onzekerheid op dit niveau kan worden berekend op basis van beschikbare objectieve informatie. Het volgende niveau is de zone ‘uncertainty’. In deze situatie is er weinig tot geen objectieve informatie voorhanden maar experts kunnen de onzekerheid inschatten op basis van expertise. Dit is het niveau waarop het oordeel van deskundigen de primaire informatiebron is. Het derde niveau is de zone van ‘ambiguity’. In deze situaties is de aanwezige informatie zo beperkt, vaag, twijfelachtig of duister dat zelfs deskundigen er geen gefundeerd oordeel over kunnen vormen. Beveiligingsrisico's worden voornamelijk gepositioneerd in de zones ‘uncertainty’ en ‘ambiguity’.

In de loop der tijd zijn voor het beheersen van risico’s verschillende processen ontwikkeld. Ze bestaan uit een reeks opeenvolgende fases: vaststellen van de context, risico identificatie, risico analyse, risico evaluatie en ten slotte risico behandeling. Ieder van deze fases omvat een aantal beslissingen die de professional risicobeoordelaar neemt. Hoewel risicobeheerprocessen wellicht objectief ogen bestaan ze feitelijk uit een serie beslissingen door actoren die als subjectief kunnen worden beschouwd. Risicobeoordelingen kunnen dus in feite worden gedefinieerd als volgordelijke besluitvorming door professionals.

De introductie vervolgt met een theoretische beschouwing van enkele van de meest prominente theorieën over besluitvorming. Omdat deze vaak in gescheiden wetenschappelijke domeinen zijn ontwikkeld overlappen ze elkaar en vullen ze elkaar aan. In deze dissertatie wordt getracht deze theorieën te combineren tot een overkoepelend alomvattend beslismodel. Dit model bood, in combinatie met de schaal van onzekerheid, een raamwerk om de besluitvorming over veiligheidsrisico's door professionals in het beveiligingsdomein te onderzoeken. Het besluitvormingsmodel bestaat uit twee hoofdonderdelen: het zogenaamde systeem 1 en systeem 2 denken (termen die zijn geïntroduceerd door de Nobelprijs winnaar Daniel Kahneman en die nader worden uitgelegd in de introductie). Systeem 1 denken is snel en intuïtief, terwijl systeem 2 denken bewust redeneren omvat. Binnen deze twee hoofdcomponenten worden de verschillende besluitvormingsfasen gedetailleerd beschreven.

Deel 1 van deze dissertatie bevat vier hoofdstukken met elk een wetenschappelijk artikel zoals gepubliceerd in een peer-reviewed wetenschappelijk tijdschrift.

Hoofdstuk 1 presenteert een onderzoek om vast te stellen of beveiligingsprofessionals, geconfronteerd met keuzes met vooraf gedefinieerde opties, kwetsbaar zijn voor bekende biases. De experimenten die zijn opgezet om dit te testen zijn via een online enquête aangeboden aan een gelegenheidssteekproef van professionals. Het eerste deel van het onderzoek bestaat uit een replicatie van bekende experimenten die aan de basis lagen van de Prospect Theory. Hierin worden aan de respondenten keuzes voorgelegd met twee opties ieder met een monetaire winst of verlies. In het tweede deel van het onderzoek zijn deze experimenten geherformuleerd tot keuzes gerelateerd aan beveiligingsrisico’s. De significante resultaten laten zien dat beveiligingsprofessionals net zo kwetsbaar zijn voor biases in hun beoordeling en besluitvorming als leken. Bij bijna drie op de vier beveiligingsprofessionals blijken beslissingen over beveiligingsrisico’s te worden beïnvloed door deze biases.

Het gevolg van deze beïnvloeding is dat beveiligingsrisico's mogelijk niet maximaal worden beheerst. Daarnaast blijkt dat de professionals zich bij hun beslissingen meer laten leiden door het verkleinen van de gevolgen van een dreiging dan door het verkleinen van de waarschijnlijkheid van het optreden ervan. Aangezien het verminderen van waarschijnlijkheid verband houdt met preventie kan worden geconcludeerd dat beveiligingsprofessionals hun focus meer lijken te hebben op mitigatie dan op preventie. Deze bevindingen wijzen ook op het bestaan van het zogenaamde probability ignorance. Dit fenomeen wordt tevens geconstateerd uit de resultaten van het onderzoek gepresenteerd in hoofdstuk 2.

In het volgende hoofdstuk worden beveiligingsprofessionals via een enquête gevraagd naar de aspecten van beveiligingsrisico's die ze overwegen bij het beoordelen van een beveiligingsrisico: welke aspecten van een risico nemen zij in overweging. Dit onderzoek begint met een open vraag. De antwoorden op deze vraag kunnen worden beschouwd als 'on top-of-mind' en een 'systeem 1' beoordeling. In de volgende delen van dit onderzoek wordt de respondenten gevraagd om de veiligheidsrisicoaspecten te voorzien van een waardering (hoe belangrijk vinden ze een aspect) en daarna te rangschikken in een top 10. In het laatste geval worden ze gedwongen om compenserende besluitvorming uit te voeren wat kan worden beschouwd als 'systeem 2' beoordeling. Deze antwoorden zijn met elkaar vergeleken en de verschillen geanalyseerd.

Het meest opvallende verschil is het aspect: 'veiligheid van medewerkers en klanten/bezoekers'. Slechts 24% van de respondenten had dit aspect 'on top of mind'. Uiteindelijk hebben drie op de vier van hen, nadat ze dit aspect kregen aangeboden, dit in hun top 10 van belangrijkste aspecten geplaatst. Hieruit kan geconcludeerd worden dat er een verschil bestaat tussen beoordelingen via systeem 1 en systeem 2. Het aspect 'waarschijnlijkheid' staat slechts in de top 10 van 34% van de respondenten en heeft de overall top 10 niet gehaald. Dit is een duidelijke tweede indicatie voor probability ignorance in dit praktijkdomein.

Hoofdstuk 3 presenteert de resultaten van een onderzoek naar het niveau van beschikbare informatie over beveiligingsrisico's dat professionals beschikbaar hebben bij het beoordelen ervan. Tevens is onderzocht of de beschikbare informatie invloed heeft op het vertrouwen dat ze hebben in hun risicobeoordeling. Tot slot is onderzocht wat de invloed is van meer gedetailleerde informatie op professionele risico-inschattingen. De professionals gaven aan in slechts de helft van hun risicobeoordelingen gedetailleerde risico-informatie beschikbaar te hebben. Op de vraag of ze een risico kunnen inschatten, zelfs als ze niet over exacte informatie beschikken, geven ze aan dat ze dit vrijwel altijd kunnen. Daarnaast geven ze aan meestal vertrouwen te hebben in hun risicobeoordeling. Deze resultaten wijzen op een bovenmatig vertrouwen in eigen oordeel door beveiligingsprofessionals, dat lijkt toe te nemen met de ervaring. De beveiligingsprofessionals is vervolgens een aantal realistische veiligheids-casussen voorgelegd en hen is gevraagd een oordeel te geven over de waarschijnlijkheid ervan. De resultaten tonen een (zeer) brede spreiding van deze beoordelingen, een indicatie voor zogenaamde ruis. Op basis van exact dezelfde informatie komen professionals met vergelijkbare expertise tot zeer verschillende waarschijnlijkheidsbeoordelingen. In dit onderzoek wordt tenslotte de conjunction fallacy getoetst. Deze fallacy laat zien dat meer gedetailleerde informatie de ingeschatte waarschijnlijkheid verhoogt, terwijl logisch redeneren de beoordelaars tot de tegenovergestelde resultaten zou moeten leiden. De gevolgen van het in dit hoofdstuk gepresenteerde onderzoek voor het veiligheidsdomein zijn groot. Ten eerste blijkt dat professionals die belast zijn met het beheersen van beveiligingsrisico's in organisaties en de samenleving, dit vaak doen zonder gedetailleerde of exacte informatie. Dit sluit correct systeem 2 redeneren uit. Dit leidt ertoe dat ze afhankelijk zijn van hun eigen expertise en systeem 1 besluitvorming, waarvan we inmiddels weten dat deze vatbaar is voor beïnvloeding door vooroordelen (zie hoofdstuk 1).

Meer ervaren professionals hebben minder behoefte om meer informatie te verzamelen, zelfs als ze zich ervan bewust zijn dat beschikbare informatie onvolledig is. Ze lijken meer op hun expertise te vertrouwen. Dit hoofdstuk laat duidelijk zien dat professionals met een vergelijkbare achtergrond tot zeer verschillende uitkomsten van hun risicobeoordelingen kunnen komen. Dit kan leiden tot een andere risicoblootstelling van vergelijkbare organisaties in onze samenleving. Ten slotte wordt aangetoond dat meer gedetailleerde informatie over een risico leidt tot een significant hogere waarschijnlijkheidsbeoordeling van een dergelijk risico. Goed geïnformeerde professionals zouden een hogere waarschijnlijkheid toekennen dan logische redenering toestaat. Dit kan leiden tot een minder efficiënte allocatie van middelen.

Het laatste hoofdstuk van dit deel bevat een onderzoek naar de bronnen van informatie over beveiligingsrisico's. Mogelijke bronnen zoals toegepast door beveiligingsprofessionals zijn geïdentificeerd, de gepercipieerde kwaliteit ervan is gevraagd en hun toepassing in de dagelijkse praktijk is geanalyseerd. De kwaliteit van informatiebronnen wordt beoordeeld door toepassing van het NAVO-systeem of de admiraliteitscode. In deze studie wordt een nieuw, aanvullend, beoordelingscriterium voorgesteld: bronintentie. Dit nieuwe criterium geeft een verklaring voor het waargenomen verschil tussen de gepercipieerde kwaliteit van bepaalde bronnen en hun toepassing in de praktijk. Het meest in het oog springende voorbeeld hiervan is de bron wetenschap/wetenschappelijke publicaties. De kwaliteit van deze bron wordt als hoog ervaren (positie 3) maar de toepassing ervan staat slechts op positie 9. Dit kan verklaard worden door de relatief lage gepercipieerde bronintentie (positie 7). De respondenten geven aan te twijfelen of de intentie of aspiratie, doelen en doelstellingen tussen wetenschap en praktijk met elkaar in overeenstemming zijn. Inmiddels is het misschien geen verrassing dat de bron persoonlijke ervaring op de tweede plaats staat, dicht bij de bron met de hoogste rang: experts. Dit onderzoek heeft de belangrijkste bronnen van informatie over beveiligingsrisico's blootgelegd voor de individuele professionals die in dit domein werkzaam zijn.

Dit promotieonderzoek heeft de afgelopen jaren de aandacht getrokken van het professionele beveiligingsdomein. De (tussentijdse) resultaten zijn gedeeld via presentaties op verschillende professionele conferenties, zoals vermeld in het afsluitende hoofdstuk van dit dissertatie. In deel 3 zijn twee professionele publicaties opgenomen. Ze worden wellicht niet als wetenschappelijk beschouwd, hoewel ze beide door vakgenoten zijn beoordeeld, maar ze tonen de aandacht die dit onderzoek kreeg in het professionele domein.

De eerste wordt als hoofdstuk 5 gepresenteerd. Het betreft een coverartikel dat is gepubliceerd in Security Magazine, de officiële publicatie van ASIS, 's werelds grootste vereniging voor beveiligingsprofessionals met wereldwijd 36.000 individuele leden. Dit artikel geeft een samenvatting van de resultaten van de voorgaande hoofdstukken met als doel het bewustzijn in het professionele domein te vergroten voor gebreken in beoordeling, besluitvorming en risico-inschattingen. Als een van de meest voor de hand liggende vragen in een professionele omgeving, bijna altijd direct volgend op het bewustzijn, 'wat nu?', bevat dit artikel enkele mogelijke aanbevelingen om deze mogelijke tekortkomingen te omzeilen.

De tweede professionele publicatie is een peer-reviewed bijdrage voor het project Platform Beïnvloeding van Menselijk Gedrag, in opdracht van de Koninklijke Landmacht. Het Haags Centrum voor Strategische Studies (HCSS) heeft academische experts en beleidsmakers uit verschillende delen van Europa samengebracht om ethische, juridische en militair-strategische kwesties en grenzen te onderzoeken die te maken hebben met op informatie gebaseerde gedragsbeïnvloeding in de militaire context. Onze bijdrage bestaat uit een korte samenvatting van de resultaten van de eerder genoemde onderzoeken gebundeld in twee hoofdonderwerpen:

1. De informatie waarop beoordelingen zijn gebaseerd (identificatie van bronnen, beschikbaarheid van informatie over beveiligingsrisico's, invloed op vertrouwen)
2. Biases en heuristieken die de interpretatie en perceptie van deze informatie beïnvloeden (onderzoek naar kwetsbaarheid voor bekende biases, conjunction fallacy, beschikbaarheid/on top-of-mind-onderzoek, systeem 1- en 2-denken)

Dit artikel is opgenomen in deze dissertatie als deel 2, hoofdstuk 6. Het is online gepubliceerd op de HCSS-website op 12 juni 2023.

Deze dissertatie wordt afgesloten met een afsluitend hoofdstuk en een epiloog. In het afsluitende hoofdstuk worden de conclusies niet één op één herhaald. De conclusies zijn in deze samenvatting al in algemen zin gepresenteerd en in de afzonderlijke hoofdstukken in nader detail uitgewerkt. Het afsluitende hoofdstuk combineert de resultaten in een discussieachtige stijl.

Het eerste deel begint met de schaal van onzekerheid. Aan de linkerkant is het gebied 'certainty' dat staat voor 'feiten'. Uiterst rechts bevindt zich het gebied van de 'unknown unknows' dat staat voor 'geloof'. Dit deel van het concluderend hoofdstuk gaat dieper in op de implicaties van 'feiten versus geloof' in de echte wereld.

Het tweede deel van het afsluitende hoofdstuk omvat een beschrijving van het begrip ‘probability ignorance’, het negeren van waarschijnlijkheid of kans bij het nemen van risicobeslissingen. Dit fenomeen is geïdentificeerd in verschillende van de eerder genoemde onderzoeken. Als een van de belangrijkste componenten van risico- en risicobeheer kan het negeren van waarschijnlijkheid risicomanagement feitelijk omzetten in impactmanagement waarbij het risico bestaat dat preventie uit het oog wordt verloren. Ten slotte gaat het afsluitende hoofdstuk in op de impact die deze studie heeft gehad en nog kan hebben binnen de professionele beveiligingsgemeenschap. De aandacht die dit onderzoek reeds heeft getrokken en de combinatie van verbazing en enthousiasme die het teweegbracht wordt kort beschreven.

In de epiloog worden ten slotte enkele persoonlijke observaties over de wetenschappelijke en professionele gemeenschap gedeeld opgedaan tijdens deze interessante reis.

Deze samenvatting hoopt zowel andere wetenschappers als professionals aan te moedigen om de andere delen van deze dissertatie te lezen. Beiden kunnen hun 'eigen stijl' van publicaties vinden, maar de epiloog indachtig, hoopt de auteur dat beide partijen de moeite zullen nemen om de artikelen voor 'de andere kant' ook te lezen en te waarderen.

PREFACE & ACKNOWLEDGEMENTS

‘I have no special talent. I am only passionately curious’. This quote exactly reflects my perspective, it could be mine. However, it is attributed to Albert Einstein. To be clear: other than with this quote, on which we both seem to share our drive, I would obviously not compare me nor my work with Einstein’s oeuvre.

Curiosity, however, seems to be a trait we do share. After many years working in the security domain, designing, advising and selling solutions for security challenges of individuals and organizations, I stayed puzzled about the arguments and reasoning of the professionals deciding on security. We could successfully discuss, debate, defend and advise solutions but neither me nor the professionals I worked with globally, could explain why exactly we do what we do to manage security risks. It was as if we deliberately ignored the core questions: is this really managing our security risk? And if it does, how do we know?

Curiosity energized me to start searching for answers to these questions. In 2013 I started the Master of Security Science & Management program at Delft TopTech, the school for executive education of Delft University of Technology. In this inspiring environment I experienced, for the first time, the vast body of scientific knowledge that is already existing. It sparked my curiosity and it made me eager to learn. On the other hand it surprised me that all this knowledge was out there but it was hardly known and applied in the professional domain. This started my small personal quest to open up this scientific security world to the professional community.

One of the first models that helped me understand risk management is the simple Hazard-Barrier-Target model (see Figure 1), presented by the inspirational Professor Ale.

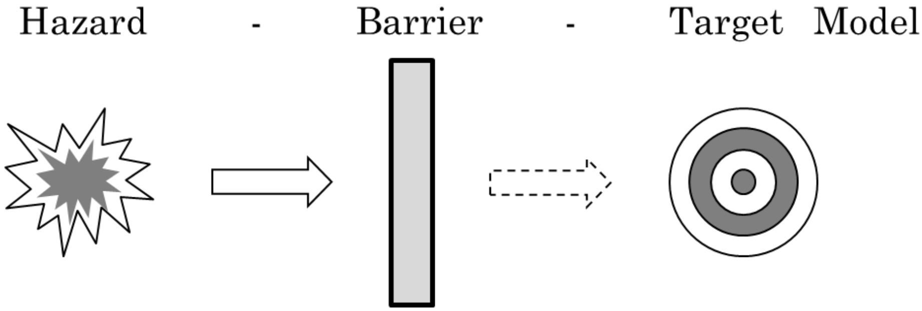


Figure 1: the hazard-barrier-target model, the barrier should stop the hazard from reaching the target (from: Risk, an Introduction, Ale, 2009)

The barrier should stop the hazard from reaching the target. As the perfect 100% secure barrier does not exist, we should implement multiple barriers: the principle of layers of defense or defense in dept. Armed with this knowledge I set out to really understand how security professionals, the people who I was dealing with for years, assess these barriers: which to implement, how much to implement, their perceived effectiveness etc. I was truly expecting that they knew things I didn't.

My master thesis was a disappointment, at least at this point. It turned out that the assumptions that are the theoretical foundation to properly apply the above mentioned models were absent. The security professionals did not 'know' the dimensions of the security risk to start with. They did not 'know' the effects of the barriers they implement and they did not 'know' if in the end the combination of implemented barriers fulfilled their expectations as they also did not 'know' what the dimensions of their accepted remaining risk should be. 'Know' is put in parentheses, the security professionals questioned had a hunch, a feeling, an idea, but could not express what that was based on. In the end my research did not answer my questions and certainly did not satisfy my curiosity.

All this is a bit long run-up to my dissertation in front of you (sorry). My curiosity continued to drive me into new research. In 2016 this cumulated in the start of my PhD aspiration. My initial question was about the barriers: how do the security professionals know or assess the effectiveness. Very soon, however, I ended up in assessments, expert judgment, decision making and psychology. Understanding decisions of security professionals proved to be less about facts and figures and more about perception, biases and heuristics. Along the way I noticed that not only I was curious, surprised, and astonished about the results, so was the professional community. The enthusiasm I encountered presenting my findings inspired me to continue.

The result is in front of you. This dissertation reflects my PhD journey of the last 7 years. I hope you are curious enough and can find the time to read it.

This is a journey I did not travel alone, there are numerous people who fortunately joined me. To start I would like to thank my family. Without their tremendous support and patience I could not ever have ended this journey of discovery. Next to thank are my managers and colleagues at Siemens. They made it possible for me to spend time and energy on my research. I would also like to thank my many scientific fellow travelers and especially my dear peer group members Anca Mutu and Daan Sutmueller with whom I spend many Fridays at our office in Delft discussing life in general and statistics in particular. Special thanks need to be addressed to Ben Ale and Coen van Gulijk who believed in me and encouraged me to start my journey. Pieter van Gelder and Wolter Pieters, who helped me to stay on course along the way, made this dissertation possible. They encouraged me when I was down, helped me when I was stuck and made sure I continued when I wanted to stop. Although at points during the journey I detested their comments, certainly when I thought I had finished a text, without them I would never had succeeded. To be honest: you were right most of the time.

Finally I would like to thank the doctoral committee. They approved the final manuscript and challenged me to improve it to the version that is in front of you.

With this dissertation my journey ends (at least for now). I hope you are as curious as me, enjoy the read!

PART 1

INTRODUCTION

INTRODUCTION

Risk, Risk Management, Uncertainty, and Decision Making: introducing Theory and Security Praxis

Studying risk assessments in the security domain turned out to be a journey through various scientific domains and crossing many scientific boundaries. The overall research questions driving this study are about how security professionals assess, reason, and decide on security risks, and where their justification is founded on. Along this journey it became clear that dealing with security risks in fact is about the psychology of decision making. In this section this journey through domains is introduced. It covers several, intensely related, topics an consists, therefore, of many short sections each covering such a topic. In between the connection with the security praxis and the specific characteristics of security risks are presented. All these topics combined result in an attempt to compose a comprehensive model of decision making. This model inspired the research presented in the following chapters. These will be introduced at the end of this section.

The practice of security risk management

This PhD study originated in curiosity: how do professionals form a judgement on security risks? These professionals are expected to manage security risks in a way that the organization they work for can reach its goals and fulfill their commitments. As these risks may or may not materialize in the future, this judgment is in fact a predictive judgement. So how can these professionals predict the future? A task that is known to be hardly possible by nature. Still organizations and society expect them to do just that and often they are even held accountable for this judgement (primarily when it turned out to be wrong).

Exploring real-life praxis of security risk assessments turned out to become studying human decision making. During the years this study lasted the subject shifted and expanded as in many others. This introduction reflects this journey. It starts with risk and one of the main components of risk: uncertainty. Exploring the concept of uncertainty lead to the emerging of a qualitative *scale of uncertainty*. To be able to deal with risks and uncertainty, over time risk management processes are developed. However different, they all follow some basic subsequent steps. The scope of each of these steps is to be defined by the professionals dealing with risks. Defining in this case actually means making choices and decisions. In short: risk management can be considered risk decision making. Reaching this inference opened up pandora's box of many decades of research. In this introduction three main areas of research in decision making are briefly introduced. As these are developed in different, independent, scientific domains they seem to be related but are, to the best of our knowledge never combined. In this introduction an attempt is made to combine these in an comprehensive decision model. This journey, the scale of uncertainty and the proposed comprehensive decision model are related to the security domain. This section ends with an introduction of the remaining chapters and sections of this dissertation.

The research questions driving this study are about how security professionals assess, reason, and decide about security risks, and where their justification is founded on. This work will not answer all the questions, it is, however, a valuable start to understand the difficult task the professionals in this domain are facing: preparing for, and thus predicting possible future security risks.

Risk

The concept of risk is puzzling human kind for centuries. Ever since people started to shift their thoughts from perceiving events as an act of god (or several gods) to a phenomenon they might be able to influence, they have tried to understand the dynamics of risks. Nowadays risks are regarded possible effects on future goals (ISO, 2018). As risks may or may not materialize in the future there is a level of uncertainty involved in risks. This uncertainty and especially trying to weigh, measure, calculate, predict, or estimate this uncertainty has occupied the thoughts of many great philosophers and scientists over the centuries.

Over time a lot of practical and experimental knowledge is collected and analyzed on risks. Many risks materialize regularly and allow for learning and extrapolation. In this way a huge body of knowledge is available in various risk domains. As long as the context of these risks is stable and not overly complex, they can be modeled and predicted to a certain extent. Early game and probability theory are examples of this. The context is known, there are a limited number of variables and possible outcomes. Over time both our understanding of the natural, and socio-economic context of various risks grew, as well as our possibilities to model more complex systems. This generated a general belief in society that the phenomenon of risk cannot only be influenced but that risks can be controlled and managed. This being the case resulted in a connecting risk to responsibility. This led to a notion in contemporary society that if risks materialize, some actor can be held accountable. This actor clearly did not manage/mitigate these risks.

Over the course of several centuries risks turned from random acts of god(s) to a phenomenon that can, and therefore should, be managed by human actors. If the root cause of some risks cannot be controlled or mitigated, like for example natural events like hurricanes, and an event is inevitable, the responsible actors are expected to be prepared and at least mitigate the effects.

Risk, Uncertainty and the Emerging Scale

The definition of risk presents the two core component of risk: uncertainty, often expressed as likelihood, and effect often referred to as impact. Risks vary in the level of the uncertainty associated with a possible effect. In trying to grasp various levels of uncertainty the need to classify them emerged. Studying literature on risk and uncertainty, discussing it during conversations, seminars, colloquia and conferences in both the academic as professional security domain, resulted in thoughts and observations on uncertainty. These thoughts and observations are merged and resulted in a graphical model of the *'scale of uncertainty'*.

As noted earlier, depending on the understanding of the context, the number of variables and the variety of possible effects, risk can be more or less modeled and predicted. In other words: the more we understand the risk, the better we can manage it. This has led to the first valuable observation in this study: there seems to be a correlation between understanding, translated in available information, and the uncertainty in risks.

On the two far ends of the scale we either know everything there is to know (known knowns) or we do not know anything (unknown unknowns). In the situation where everything is known and understood, there is no uncertainty, as we exactly know what is going to happen. This situation might be considered hypothetical as in the real world always some effects might influence our certainty.

The other end of the scale might be considered hypothetical too, as humans are able to imagine everything and based on that, nothing has to be unexpected. In reality we live our lives somewhere between these two far ends.

After extensively studying risk in literature as part of this study a *'scale of uncertainty'* emerged. Although this can be considered a by-product of this study, it will play a prominent role in the remainder of this thesis, it is considered valuable to bring some order in the arena of real life. In Figure 1 the proposed scale of uncertainty is presented.

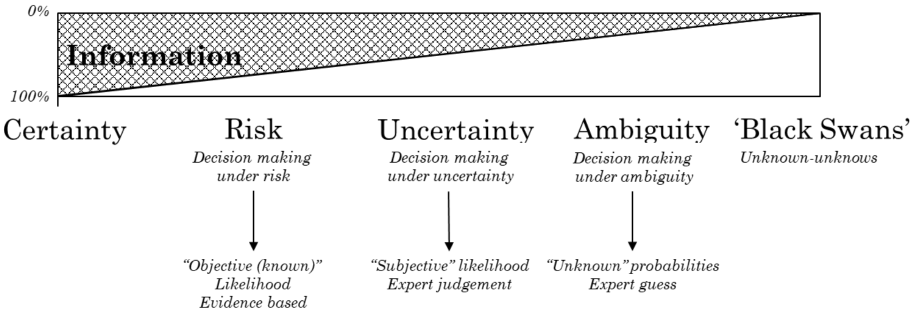

0%
100%
Information
Certainty
Risk
Decision making under risk
Uncertainty
Decision making under uncertainty
Ambiguity
Decision making under ambiguity
'Black Swans'
Unknown-unknows
"Objective (known)" Likelihood Evidence based
"Subjective" likelihood Expert judgement
"Unknown" probabilities Expert guess

Figure 1 : proposed 'scale of uncertainty' related to information

In this proposed scale, besides the two far ends, three areas of uncertainty are identified.

First area is coined the 'risk area' (note that this deviates from the general notion of risk that would encompass all levels of uncertainty). To follow the notion of risk in society this is the area where we have information on context, variables and possible effects. We 'understand' the risk, can possibly mitigate it but at least can be prepared for it. Our understanding in this area is based on information of the past, experiments and research, thus: objective and evidence based knowledge. We 'know' the possible effects and can construct a kind of cost-benefit calculation. This might be the area where actors (individuals or originations) can be held accountable, 'they could, and therefore should, know'. In this area uncertainty is often expressed in probabilities, the more narrow and mathematical interpretation of likelihood.

The next area is the area of uncertainty. In this area information is lacking, not certain, not known beyond doubt, indefinite or indeterminate. There is information available but this does not allow any firm conclusions as it is 'in the eye of the beholder' and can be interpreted differently. In this area expert judgement plays a prominent role. Experts can express uncertainty on intractable and imperfect information based on their expertise, so called expert judgement.

Finally, if information is obscure, vague, indistinct, dubious, not readily understood, not clearly expressed, is ambiguous in meaning and can be understood in multiple ways, the uncertainty grows. Even experts cannot give deeper meaning, form an opinion on little or no evidence, their opinion is more of a guess than a judgement. As in this area information is ambiguous, experts can interpret it in very different ways

and reach (very) different judgements. We dubbed this area the area of ambiguity.
The interpretations of the areas on the *scale of uncertainty* are subjective, arbitrary and overlapping. They are not meant to be exact in their application. They, together, form a frame of reference that might be useful to classify risks. In this PhD study on security risk assessments by security professionals, the main topic of this thesis, this *scale of uncertainty* was useful to distinguish different security risks and the corresponding assessments of the security professionals.

Although the *scale of uncertainty* in this context is novel, a comparable observation is Plato's divided line. Plato divided human knowledge, almost 2400 years ago, in four categories that together form a comparable scale. It runs from *noesis* (observations, observable evidence), *dianoia* (reasoning), *pistis* (belief) to *eikasia* (imagining). He positioned the first two categories as episteme (knowledge) and the last two as *Doxa* (opinion, perception). In this respect the proposed *scale of uncertainty* builds on this divided line and extends it to contemporary risk.

Different Information, Different Risk

The *scale of uncertainty* implies that collecting more information would reduce the level of uncertainty. In the majority of the professional environments uncertainty about achieving goals is to be reduced to be able to meet commitments for the future. These two premises suggest that professional actors would collect as much information as possible to reach a point at the scale as close to certainty as possible.

Information can be both intractable, information that cannot possibly be known, and imperfect, information that can be known to an actor but isn't. The first category of information makes it impossible to reach absolute certainty. The latter is depending on the effort put in collecting information. Collecting and analyzing information is time and resource consuming so professional actors can be expected to find an optimal equilibrium between uncertainty and collecting information.

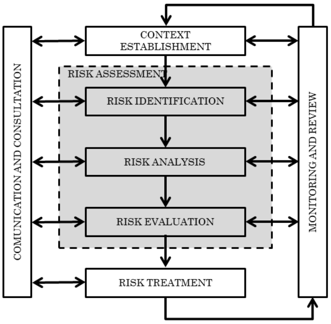
Based on the observation that the level of information represents actually the level of uncertainty, a different information position between different actors would indicate that they run a different risk.

Well informed actors might be acting in the risk area while others might be in the ambiguity area. This difference might lead actors to different risk perceptions and risk tolerance. Actors can use and misuse this difference to willingly (For example insurance) or unwillingly transfer risks to less informed actors.

The similar principle is applied for risk adoption in organizations. A situation might be to ambiguous for an organization and its departments to deal with. By setting the scope and dividing the risk over several specialized departments and/or processes, the uncertainty for each department/individual is reduced to a level where enough information is available to deal with the (part of) the risk. In this way risks in organizations are absorbed.

Risk Management

As stated in the previous paragraphs organisations need to address risk to be able to reach their goals and commitments. To be able to do this in a structured and documented way risk management processes are developed. Over time many domains implemented standardized risk management methods that all follow comparable steps: define the context, identify risks, weigh and analyse these risks, evaluate and compare them, and finally control, manage or treat them.



Examples of decisions per stage:

Decide what is in scope

Decide which risks to take into account

Decide about value of probability & impact

Decide what is acceptable/unacceptable

Decide what measures to take

Figure 2: Risk assessments as part of risk management (ANSI/ASIS/RIMS, 2015) and example decisions

A risk assessment is the ‘overall and systematic process of evaluating the effects of uncertainty on achieving objectives’ (ANSI/ASIS/RIMS, 2015, p. 5). It includes the following subsequent activities: risk identification, risk analysis and risk evaluation. It is part of a risk management process as shown on the left side of Figure 2.

Following this process organisations need to define the scope for each step. This forces them to make choices and decisions in each step. Studying risk assessment as part of risk management, in fact turned out to be studying subsequent decision making.

Decision making

Over time a huge body of knowledge on decision making is established within various fields of science and practice. This section will start with an overview of previous work and will consider three main areas of study: rational decision making focussing on optimizing/maximizing the outcome, heuristics and biases focussing on the process of human decision making and naturalistic decision making exploring real-life decision making by practitioners. Based on this work an attempt is made to combine (components of) these different scientific theories.

Decision making is an important and even vital part of human behaviour. Decision making, as part of human behaviour, already intrigued the old Greece philosophers (Zanakis et al., 2003). Humans usually have multiple options for action or inaction and make decisions numerous times a day. ‘In fact everything we do consciously or unconsciously is the result of some decision’ (Saaty, 2008, p. 83). Decisions can be almost automatic, intuitive and even without being conscious of any mental process.

On the other hand decisions can be deliberate, based on reasoning and compensatory. Both these processes are studied intensively over the last decades. The latter has been studied primarily based on optimizing or maximizing the outcome (Beach, 1993), especially in economics (Svenson, 2003). This vast research field has generated multiple theories and models like rational behaviour, Rational Choice Theory and maximization theories like Expected Utility Theory. These theories have a normative character and try to define optimal decision making.

In the second half of the last century, a growing interest emerged in observed deviations from these optimizing/maximization theories. Human decision making seemed less “rational” than rational theories predicted. Instead of trying to reach an *optimal* situation, human decision making often seems to settle for a *satisfying* state of affairs. Decision making as studied in psychology resulted in a number of well-known theories like Prospect Theory, Subjective Expected Utility theory and Bounded Rationality (Allais, 1979; Fischhoff, 1982; Gigerenzer, 1991; Gigerenzer et al., 1999; Kahneman et al., 1982; Kahneman & Tversky, 1979; Loomes & Sugden, 1983; Navarro-Martinez et al., 2018; Tversky & Kahneman, 1975, 1992). These theories explored the process of decision making (reaching commitment) rather than optimizing the actual outcome. Overall they concluded that humans often optimize their decision making process, in the sense of minimizing time and (cognitive) effort, instead of optimizing the outcome. The majority of these studies are based on experiments in laboratory settings, they presented a growing number of biases (systematic deviations from logic reasoning) and heuristics (mental shortcuts) explaining human decision making.

At the end of last century, more practical research was conducted. These studies focussed on real situations and real decision agents. It resulted in another set of theories like DiffCon theory (Svenson, 1979, 1992) and Naturalistic Decision Making (Gore & Ward, 2018; Klein, 1997, 2008; Lipshitz & Strauss, 1997; Pliske & Klein, 2003). The different scientific fields over the years, thus, produced various theories and models, all of which explain different aspects of the decision making process.

Individually, all these existing theories are valuable pieces of the puzzle of human decision making. So far there have been very few attempts to create an extended decision making framework (Morcol, 2007). It is a theoretical challenge to fit different motivations, representations and logic of human behaviour in decision making into a single framework (Olsen & March, 2004). Besides this challenge, in for example psychology, scientists tend to specialize and develop different theories and vocabularies (Roberts, 2004; Svenson, 2003). An example of such coexistence is the relation between the naturalistic decision making (NDM) approach and classical decision research. “Both communities still mostly ignore, neglect or attenuate the theoretical advances of the other” (Betsch & Haberstroh, 2005, p. 374) they even claim, “The aim of theoretical integration is incompatible with leniency on the theoretical level” (2005, p. 374). Because of this different scientific fields covering the same or strongly related subjects coexist (Stenning & Monaghan, 2005). Much to their surprise different scholars exploring different perspectives can even conclude that their respective, separate, theories actually reach similar conclusions and can be aligned (Kahneman & Klein, 2009).

Combining theoretical conceptions and practical empirical research can lead to a more comprehensive understanding (Stenning & Monaghan, 2005). Although the different research fields related to decision making are separated in era, approach or theoretical representation, they all provide valuable components to an overall framework.

So, how do the different decision theories relate to each other? Do they support each other or do they contradict? Can they be combined, and if so how? Could they together provide a comprehensive model on decision making?

To answer these questions an extensive literature review is committed. The core elements of various theories, concepts, models and research on decision making are analysed to identify similar and supplementary aspects. This chapter attempts to combine components of these well-known theories in a comprehensive decision framework. To explore and better understand real life decision making, a combination of existing theoretical concepts might enhance our overall notion of decision making.

First, decision making and a general decision making process are defined. Second, the notion of *decision making under risk* is introduced. Decision making is often, if not always, affected by uncertainty. A lack of knowledge of the decision agent about different alternatives, their probability of occurring or the consequences or effects of a decision causes uncertainty. Third, further variables influencing decision making on the decision agent are analysed. Examples of these variables are regret, responsibility, accountability and visibility. Finally, a comprehensive model is proposed, containing four levels of decision making, derived from different theoretical concepts.

What is decision making?

"A decision is a commitment to a course of action that is intended to produce a satisfying state of affairs" (Yates et al., 2003, p. 15). Decision making is considered a cognitive process. It involves an actor or group of actors, further referred to as agent. Prerequisite to a decision is the need to select one of the available alternatives. The agent needs to experience a kind of decision pressure, otherwise the agent would simply ignore the situation and end up doing nothing, or in other words, inertia or selection of the status quo alternative (Samuelson & Zeckhauser, 1988; Thaler & Sunstein, 2009).

Second, a decision involves a range of options for possible action or inaction . If there is only one option available to the decision agent, there is no need to choose and take a decision. Decision options are further referred to as alternatives.

Third, the agent is supposed to be equipped with a consideration set (Markman, 2017) or set of preferences based on objectives or goals (Aouni et al., 2005; Beisbart, 2012; Costanza et al., 1991; Saaty, 2008). This set of alternatives is the basis for decision or choice and is composed out of experience and/or extensive search.

The agent is expected to select the alternative leading to consequences that serve these preferences best, so called rational behaviour (Von Neumann & Morgenstern, 1947). The set of preferences guide the agent to a final judgement or attitude (Ajzen, 2011; Fischbein & Ajzen, 1975; Jensen, 2012).

Decision making involves a set of alternatives. Alternatives can be represented as a separate "holistic" entity if they are well known, recognizable and/or easy to classify. If decision problems or alternatives are to large or complex to handle as a whole the decision alternatives are decomposed. Usually alternatives are decomposed and represented by a set of dimensions, aspects or criteria further referred to as attributes (Aouni et al., 2005; Goodwin et al., 2004). Defining meaningful attributes is part of the pre-decision phase and related to the problem definition (Beach, 1993). An attribute is a certain aspect of an alternative. It is used to measure performance in relation to an objective. (Ajzen, 1991; Aouni et al., 2005; Goodwin et al., 2004; Madden et al., 1992; Payne et al., 1990; Saaty, 2008).

During the differentiation process, comparing, weighing and exploring the differences between the various alternatives, the attributes or the representation of the attributes can change. Alternatives can be assessed and evaluated in comparison. Decision agents often refer alternatives to a "best case" or "worst case" reference alternative (Svenson, 2003). This might even be a hypothetical alternative used as benchmark alternative. The reference alternative can also reflect the current situation or status. If no action is taken this is the “status quo” reference. Possible alternatives can be compared to the status quo alternative and can be accepted or rejected in this comparison. Especially in situation where alternatives “come one at a time” possible alternatives can be quickly and easy assessed (Kahneman et al., 1999; Samuelson & Zeckhauser, 1988; Svenson, 1992).

The theory of subsequent differentiating of alternatives and consolidation to a final superior alternative, DiffConn, suggests that a “preliminary preferred alternative” is nominated by the decision agent. This alternative is often selected via quick cognitive processes and used as reference alternative to reduce cognitive effort by comparing possible alternatives to this reference by the decision agent (Svenson, 2003). Instead of comparing a number of alternatives at the same time, using a preliminary preferred alternative reduces the comparison to multiple pair-wise comparisons.

The attributes can be evaluated objective (factual, measurable, definable, cognitive, independent of decision agent), affective (perception, perspective, dependent of decision agent) or evaluative (attractive, affective, desirable, preferable) (Svenson, 2003; Svenson & Slovic, 2002).

According to Goodwin, Wright, and Phillips (2004) the attributes can be more affect driven (subjective, perception, intuition) or value driven (objective, cognitive, rational). Van der Pligt and Vliek, working in a different scientific domain, reach a similar conclusion: the preferences of an individual decision maker are based on both cognitive and affective response to stimuli, see Figure 3. (Van Der Pligt & Vliek, 2016).

These two different approaches of evaluation relate to the so called dual process models coined as system 1 and system 2 thinking by Daniel Kahneman (Kahneman, 2011). System 1 thinking is based on automatic, instantaneous, intuitive, unconscious thinking processes driven by experiences. System 2 thinking, on the other hand, is effortful, deliberate, conscious, controlled and analytical.

Which of the previous evaluation strategies is applied by the decision maker depends on the context and available resources (Olsen & March, 2004).

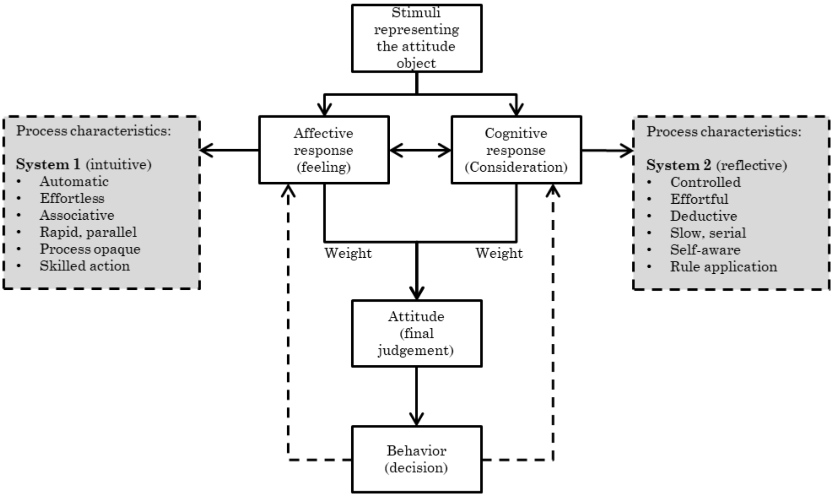


Figure 3: attitudes, cognition, affect and behavior (Van Der Pligt & Vliek, 2016) and system 1 and 2 (Kahneman & Frederick, 2002)

In order to reach a final judgement (attitude) and be able to select a possible decision alternative, the agent needs to analyse and differentiate the available alternatives (Svenson, 1992). This analysis results in a "sufficiently superior alternative" (Svenson, 2003). In other words: both the alternatives and the preferences are both defined by attributes. In this sense decision making in fact is aligning 'alternative attributes' with 'preference attributes'.

As the consequences of any alternative usually materialize in the future, a level of uncertainty is associated to decision making. The attributes, associated to an alternative, have a probability of occurring (Aouni et al., 2005).

Decision making: focus on the optimal outcome

The quality of the decision is determined by: the product of the decision and the process of the decision (Yates et al., 2003). An agent selects a sufficiently superior alternative (Svenson, 1992), the product of the decision, by applying a decision process. This process is a sequence of subsequent steps or phases as shown in Figure 4 (Parkin, 2000).

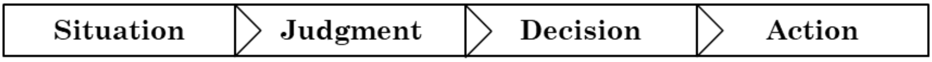


Figure 4: decision making (Parkin, 2000)

A notion of rational decision making dominated the discourse for many years during the last century. It is mainly derived from classical economics or the “homo economicus” (Schwartz, 2000). Rational Choice Theory (RTC) defines decision making as a process which optimizes/maximizes the possible outcome (Von Neumann & Morgenstern, 1947). This theoretical notion of decision making, assumes a state of “perfect rationality” (Kämper, 2000). The agent is informed about all alternatives, their attributes, consequences and associated probabilities. A state of perfect rationality is, however, in real life hard or even impossible to reach. Due to a lack of information, a lack of resources and time to gather more information, and limits to cognitive capacity, decision agents face restraints during the decision making process. The theoretical notion of classical economics is, therefore, challenged during the second half of last century. Empirical research, mainly in the field of psychology, clearly showed deviations from RTC in human decision making (Schwartz, 2000).

Decision making: exploring the process

Epochal research of Kahneman and Tversky resulted in Prospect Theory (Kahneman & Tversky, 1979). This initial theory inspired many other studies (Fischhoff, 1982; Kahneman, 2012; Kahneman et al., 1999; Kahneman et al., 1982; Slovic, 2000; Tversky & Kahneman, 1992). During this era a new notion of rationality was developed. It was proved that the human mind uses heuristics to accommodate “fast” decision making (Simon, 1956, 1982). Heuristics simplify human decision making processes to reduce resources (cognition, time, effort, etc.). They can lead to systematic deviations (also called biases) from RCT which can be interpreted as errors or non-rational behaviour. The use of these heuristics, however, turned out to maintain a reasonably high level of accuracy. The use of heuristics is generally seen as intelligent if not optimal decision making (Kämper, 2000; J. W. Payne et al., 1990;

Tversky & Kahneman, 1975). In this case *optimal decision making* is not defined in terms of reaching the optimal outcome but, as performing the optimal decision process, balancing restraints in knowledge, information, resources and time (Fischhoff, 1982; Gigerenzer et al., 1999; Gilovich et al., 2002; Kahneman, 2012; Kahneman & Frederick, 2002; Schwartz, 2004).

Another extensive and iconic field of related studies developed in parallel; Bounded Rationality (BR) (Egidi et al., 1992; Gigerenzer, 2003, 2015; Gigerenzer & Selten, 2002; Gigerenzer et al., 1999; Martignon & Krauss, 2003; Olsen & March, 2004; J. Payne & Bettman, 2001; Simon, 1956, 1982). This field mainly focused on the "judgement phase" of the decision making process (see Figure 4). Empirical research in this field showed different strategies agents apply in searching for, or creating of, alternatives. As the agents cannot reach perfect rationality (have *all* information about *all* alternatives), they stop the search for, or creation of, alternatives at some point. This point is reached when the agent has identified an alternative that fits his preferences or an alternative that is sufficiently superior to the other identified alternatives.

According to BR, the judgement phase can be detailed in two steps: Searching/creating alternatives, and stop searching/creating (see Figure 5). The extended decision making model as shown in Figure 5. is the base for this introductory chapter. The subsequent phases of decision making will be further described in following paragraphs.

The various decision strategies agents apply can be defined by different searching and stopping rules (Gigerenzer & Selten, 2002; Schwartz, 2004). As these rules are derived from empirical research they are more descriptive by nature. The term 'rules' caries a notion of normative, prescribed behaviour but in this chapter the term rules is interpreted as logic as coined by Pouliot (Pouliot, 2008).

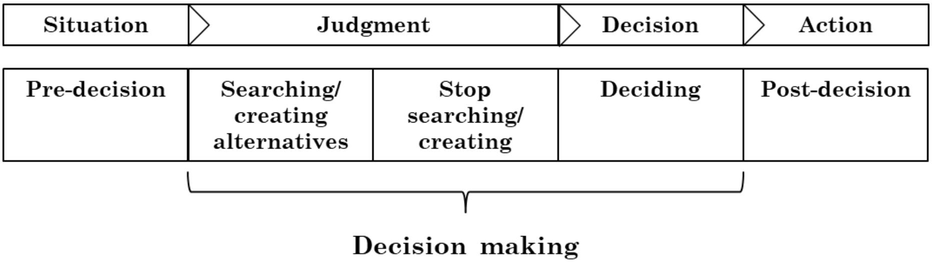


Figure 5: decision making process including Bounded Rationality

During the Pre-decision phase, situation (Parkin, 2000), or problem space (Payne et al., 1990) a decision agent becomes aware of the need to decide. This need will be further explored as far as the problem and the resources of the decision agent permit. If the outcome of this phase lead to the conclusion that a decision is inevitable, the agent will start the next phase.

Decision making: studying real life decision making

Previous scholars predominantly developed theoretical concepts and committed hypothetical experiments in laboratory settings. These settings provide valuable insights into choice behaviour, they however, leave out context and expertise. They contain all information and thus reduce uncertainties and neglect prior experiences and expertise (Evans & Feeney, 2004). To understand real-life decision making by practitioners a new domain of research emerged: NDM, Naturalistic Decision Making (Gore & Ward, 2018; Hoffman & Klein, 2017; Klein, 1997, 2008; Lipshitz et al., 2001; Lipshitz & Strauss, 1997; Markman, 2017; Pliske & Klein, 2003; Roberts & Cole, 2018).

Decision agents judge situations or problems in their context and try to *recognize* comparable situations from the past. Practitioners analyse the situation in an iterative process gathering information until they recognize past situations (Markman, 2017). This process is also coined as *recognition primed decision making* (Klein, 1993, 1997; 1993;

Ross et al., 2004; Ross et al., 2005). After studying decision making behaviour of practitioners these scholars composed the process as presented in Figure 6. When confronted with a situation the agent tries to analyse it by trying to recognize some form of familiarity based on individual expertise.

Recognition of the situation is based on four aspects: goal; what needs to be accomplished, expectancies; how the situation might evolve, cues; supporting the recognition, and possible actions. If the situation is not recognized by the agent, or in other words: is new to the agent, more information needs to be gathered, or the agent tries to 'fit' other comparable situations that might represent the situation at hand. This is a similar process as identified by Tversky & Kahneman coined as representativeness heuristic (Tversky & Kahneman, 1992). If the situation is recognized but, based on cues, expectations of development of the situation are violated, it is considered a new, not recognized situation and more information needs to be gathered. If the situation is familiar and recognized the agent will perform a mental simulation of possible actions that are known to have been used in comparable situations. If these are expected to work in the situation at hand they are executed. If there is any doubt they either will be modified until they might fit, or the situation is re-assessed.

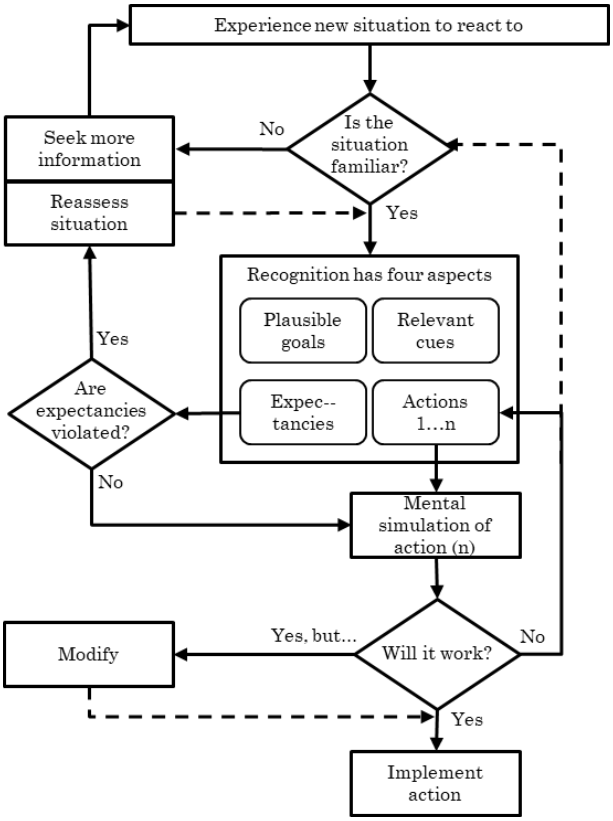


Figure 6: recognition-primed decision making model (Klein, 1993)

Decision making: attempt to combine various models

The various theories and different scientific domains try to contribute to understanding human decision making. In this chapter we tried to combine all the valuable components of those and construct a comprehensive model of individual human decision making. We also implemented the three areas derived from the novel 'scale of uncertainty' as presented in the pre-introduction chapter of this dissertation. The result is presented in Figure 7.

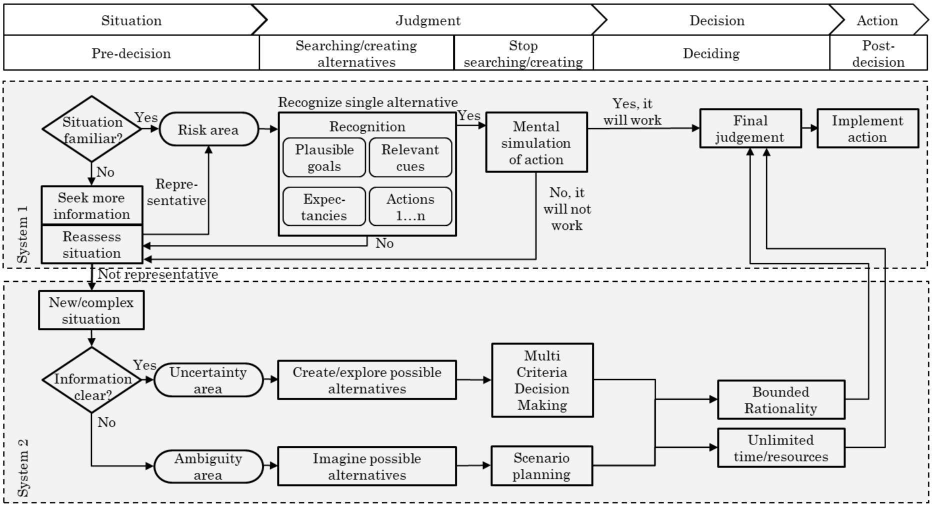


Figure 7: proposed attempt to build a comprehensive model of decision making

The main element and starting point of the new comprehensive model is familiarity or recognition by the decision maker. This part is derived from the theory of recognition primed decision making and observed in the domain of naturalistic decision making (NDM). If the situation is familiar to a decision agent a mental process can guide the agent to a course of action without much cognitive effort. This process of decision making is intuitive, often performed unconscious, effortless and automatic. It is often referred to as the fast and frugal process and system 1 decision making. With the latter the vast amount of documented heuristics and biases are applicable to this process which includes the epochal work of Kahneman, Tversky and Slovic in this new comprehensive model.

In this process often only one preliminary preferred alternative is analysed in the mental simulation, an element of the DiffConn theory. No compensatory reasoning or choice is performed.

Recognition is initiated by cues available to the decision agent. Whether or not these are recognized is depending on the expertise of the individual agent. Expertise is in this dissertation defined as: the combination of experience and knowledge. Individual decision makers, thus, might follow a different process depending on their experience, training and education. Following this model, more experience leads to more recognition, leads to more effortless and even automatic decision making. As observed in the domain of NDM, experience is adding value to decision agents.

The two feedback loops of NDM are also included: if there is doubt about the expected development of the situation and/or about the effectiveness of the assumed course of action during the mental simulation, the situations needs to be reassessed and/or more information needs to be collected. The outcome of the reassessment may lead the decision agent to either recognition or the recognition of a representative, comparable situation, or to the conclusion that this is unknown territory.

In the pre-introduction of this dissertation the *'scale of uncertainty'* is introduced. Every decision about the future, by definition, contains uncertainty. In the case of recognition this uncertainty is 'known' from training, education or science, experienced before, or dealt with before. On the proposed novel scale this is referred to as the risk area. At this part of the scale decisions are uncertain but can be based on evidence or in other words: based on information containing a known level of uncertainty. Evidence based in this case means there is undisputable proof. Based on this the decision agent can predict the outcomes of possible actions.

If the situation is not recognized the agent faces a new situation or a situation that contains cues pointing to new unfamiliar, elements or characteristics. The decision agent needs to perform a deeper analysis of both the situation and possible alternatives. In the novel introduced *'scale of uncertainty'* on top of the risk area two more areas are defined: the area of uncertainty and the area of ambiguity. They differ in the available information both in quantity and quality. As explained in the pre-introduction of this dissertation in the area of uncertainty, information is available but might be imperfect, parts of it might be even intractable, information is disputable, and conclusions are subjective.

In the area of ambiguity available information is vague, doubtful, indistinct, and allows for different interpretations. Although even these two areas are not clearly defined in itself and there is a thin line between them, we feel it is important to make a distinction. The area of uncertainty allows for expert judgement. Based on available information, experts can offer an analysis based on their expertise. Expert judgement is a scientific domain studied extensively, for example by Cooke, in which techniques are developed to evaluate expert judgement. This allows to express and evaluate expectations in this domain.

During this study in security risk assessments we felt, however, we needed to introduce the area of ambiguity. This is an area where the information is opaque so even experts and expert judgment do not or should not allow to express expectations. This is the area where expert judgment shifts to expert guess. We feel that in our contemporary society, where information is available in abundance, and it is hard to differentiate evidence from judgment from opinion, decision makers should be allowed to express their uncertainty in an area where they can be clear that even experts are guessing.

The decision process in the uncertainty area continues with searching for and creating alternatives. As the uncertainty is at a level that no undisputable conclusions can be drawn from them, techniques for Multi Criteria Decision Making (MCDM) for compensatory decision making can be applied. This is the area where cognitive effort, deliberation, and reasoning is needed (System 2).

Reasoning in MCDM can be fast and frugal as shown by the renown scholars Simon and Gigerenzer presenting the theories of bounded rationality and bounded reasoning. Their work identified several different cognitive strategies humans apply for compensatory decision making like: Satisficing (SAT), Weighed Adding Strategy (WADD), Equal Weight Strategy (EQW), Random Choice (RC), Lexicographic Strategy (LEX) and Elimination By Aspects (EBA). They are all part of the ‘adaptive toolbox’ of decision making as coined by Gigerenzer.

If the decision agent experiences no restrictions in time and/or resources, or if the impact of the decision requires it (like for example being held accountable for it), the process will be more documented and deliberate. In other words, the process of analysis of alternatives and stop searching/creating of alternatives, is depending the consequences of the decision for the decision agent and/or the available resources.

So the decision agent in this area of uncertainty is either bounded in time and (cognitive) resources or can allow more time and resources for evaluation of alternatives. Both decision strategies finally lead the decision agent to the stopping point and final judgment (the first strategy probably sooner than the second).

The proposed process in the area of ambiguity is almost similar to that of the process in the area of uncertainty. However, in this area, as information is vague, more imagination is needed and a MCDM process might result in scenario planning/analysis. Based on assumptions or expert guess this kind of analysis usually the final judgement does not result in a single alternative but rather is a range of possible future scenarios each with often a number of possible actions.

Security Risks and Daily Praxis

This PhD study focusses on security risk assessments, thus, security risk decision making by individual security professionals. The security domain is dealing with security risks. As will be presented throughout this dissertation security risks are a special class of risks. These risks originate from human malicious action. The treat actors in this domain would like to accomplish their goals which usually means damage, pain or suffer to others. Doing harm can be the sole purpose of the treat actor, like for example terror attacks, or can be inflicted as a kind of collateral damage, like for example physical or psychological impact on victims as a result of a hold up or intrusion. As these risks originate from human intent, they are dealing with the dynamics, creativity and imagination of the human mind. The threat actors in this domain try to understand and evade risk control measures. Often they conceal their preparations and actions and be as unpredictable as possible. This places security risks in the blue area of the scale of uncertainty (Figure 8).

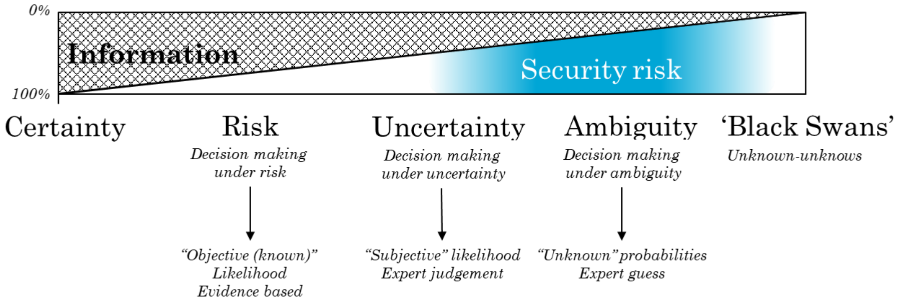

0%
100%
Information
Security risk
Certainty
Risk
Decision making under risk
Uncertainty
Decision making under uncertainty
Ambiguity
Decision making under ambiguity
'Black Swans'
Unknown-unknows
"Objective (known)" Likelihood Evidence based
"Subjective" likelihood Expert judgement
"Unknown" probabilities Expert guess

Figure 8: position of security risk on the proposed 'scale of uncertainty'

In our work we investigated how real life security practitioners, referred to as security professionals, perform a security risk assessment. Based on the characteristics of security risks we positioned them primarily in the areas of uncertainty and ambiguity, the area's where expert opinion (judgement/guess) prevails. The proposed comprehensive decision model provides the structure to explore expert judgment/guess in different stages of a decision process and via system 1 or 2 reasoning.

We studied professional security risk decision making and found that professionals are prone to apply heuristics and are vulnerable to biases in their choices. We studied the preferences of these professionals and noticed that they are not consequent in their preferences between system 1 and 2 reasoning. We studied their level of information and corresponding level of confidence and observed that they have an tendency to be overconfident, even if they are aware they base their assessment on intractable and/or imperfect information. We studied the need for information in relation to experience and learned that more experience reduces the perceived need for additional information. We studied the level of information in relation to likelihood assessments and concluded that the vast majority assigns a higher likelihood to events when more information is offered (conjunction fallacy). We studied the perception of trustworthiness of information sources and found indications for the influence on source intention on trust and trustworthiness.

In other words: we studied real life behavior of professionals safeguarding our security. The *scale of uncertainty* and the comprehensive decision model helped us to understand this behavior and pointed us towards the critical role of information in individual security risk assessments. We hope our work motivates other scholars to commit more research in this domain. We also hope to inspire the professional domain to critically reflect on their behavior and learn from our observations to improve their risk assessments.

Reading Guide

We started exploring the decision phase. Given a set of alternatives would the security professionals select the alternative with the optimized outcome. We expected that security professionals dealing with risks, and thus uncertainty, on a daily basis and educated and trained for this role, would be able to avoid heuristics and biases affecting their security risk decision making. We hypothesised that they would be able to be ‘rational’ in their decisions, meaning they would select the alternative that allows the most optimal management of security risks. Our first study presented in our paper: *Biases in Security Risk Management: Do Security Professionals follow Prospect Theory in their*

Decisions?, learned that security professionals are as vulnerable for biases as lay people in replications of the famous experiments of Kahneman & Tversky. Even in new designed experiments, representing security decisions, the majority of the security professionals followed biases leading to less optimal security outcomes. This study also pointed us to probability ignorance, coined by famous scholar Sunstein, influencing security decisions. These and more interesting findings are presented in our paper as published in the *Journal of Integrated Safety and Security Science.* This paper is presented in Part 2 Chapter 1.

The preferences of decision agents are driving their decisions as detailed in this introduction. Our second study explored the preferences of the security professionals. A survey is set up to first collect the preferences that are 'on top-of-mind' and represent the preferences directly available to the decision agents. Second a predefined list of 28 criteria are offered to the professionals. Finally the respondents are asked to rank their top 10 of most important criteria for their security risk decision making. With the latter the respondents are forced to perform a compensatory comparison of the criteria. The collected answers to the first question are regarded as quickly available and retrieved in a system 1 mental process. The last question, however, is compensatory and a system 2 process.

Comparing these results allows some conclusions about the difference between system 1 preferences and system 2 preferences. The most remarkable observed difference is human safety. Of the respondents only 24% mentioned it at the first question, while, 88% ranked it in their top 10 and it even ended overall as most important criterium in their security risk assessments. Presenting an information cue clearly influenced the preferences of the security professionals.

These results are presented during the WIT SAFE conference 2021 and published in the book WIT Transactions on THE BUILT ENVIRONMENT, volume 206, 2021. The paper: *Individual Preferences in Security Risk Decision Making: an Exploratory Study under Security Professionals*, as published is presented in Part 2 Chapter 2 of this dissertation.

The precondition that more information can reduce the uncertainty in risk assessments, leading to the composition of 'scale of uncertainty', made us study the influence of the level of security risk information professionals have available in their assessments in practice. These levels are compared to both the individual confidence level and assessment of likelihood. In the paper: *Bias and Noise in Security Risk Assessments, an Empirical Study on the Information Position and Confidence of Security Professionals*, the risk assessments of professionals are explored in relation to available information. They indicate to have exact information on security risks about half of the time (which might be an overstated perception given the fact that information about future events is intractable by nature). They, however, indicate they can estimate the impact and likelihood, even if exact information is missing, most of the time. Overall the professionals denote they are confident about their risk assessments even if they are aware their information is imperfect. This study concluded that the security professionals seem to show signs of overconfidence in their ability to assess risk and that imperfection an intractability of information seem to be ignored.

Another part of this study investigated likelihood assessments of professionals of realistic security cases. The results show an, unexpected, large range of assessments. Even respondents with similar expertise reach very different assessments. These results show so called noise. The results also show the influence of presenting more or less detailed information on the assessment of a security case.

Adding more detailed information, in general raises the estimated likelihood assessment of the professionals. These results confirm the violation of logic reasoning and confirm the vulnerability to the renowned conjunction fallacy. This paper is published in the *Security Journal* and presented in Part 2 Chapter 3.

The last study explores the different sources of security risk information and their perceived trustworthiness. As information determines the level of uncertainty, as stated in the pre-introduction of this dissertation, it is of vital importance to explore where the professional security community put their trust. What sources of information do they consider important for their security risk assessments? A brainstorm with a group of high level security professionals resulted in a list of 17 possible sources. For evaluating the credibility of information several practical and proven methods are available. In the security domain the NATO system or Admiralty code is widely used. Based on an extensive literature review on trust and trustworthiness a novel criterium of thrust is proposed to be added to the NATO system: Source Intent. This criterium seems to be missing or underestimated in the existing system and proved valuable for the evaluation of the results of this study.

The trustworthiness of the 17 sources is evaluated by a panel of security practitioners. In a survey a large group of security professionals assessed the list of sources and answered the question: 'on what information source do you base your security risk assessment?'. Both assessments resulted in a source ranking and comparing these showed some remarkable results. The paper: *Sources of Security Risk Information: What do Professionals Rely on for their Risk Assessment?* is currently under review and presented in Part 2 Chapter 4 of this dissertation.

As stated before the professional domain has shown considerable attention to this research. This resulted not only in several presentations at renown conferences but also in two professional publications. These two summarize the results of the scientific papers for a specific audience: one for the professional security community and one for the military domain. These two are presented in Chapter 5 and 6 of Part 3.

To Conclude…

This dissertation is the result of an interesting and inspiring journey that started with the original concept research question: how effective are security controls? This question directed this work to perception, assessment and decision making. It turned out to be ending in a journey through various different scientific domains, discovering godfathers and Nobel prize winners in each of them, and picking up valuable gems along the way. This dissertation is an example that for understanding and explaining reality the scientific boundaries need to be crossed and traditional silo's need to be broken. This work is a scientific contribution to the body of knowledge on professional security. It hopes to inspire other to continue this journey and inspire the professional community to learn from it. In perfect compliance with the adagio that 100% secure can never be reached, this journey will never end.

Literature

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Ajzen, I. (2011). The theory of planned behaviour: reactions and reflections. In: Taylor & Francis.

Allais, M. (1979). The so-called Allais paradox and rational decisions underuncertainty. In *Expected utility hypotheses and the Allais paradox* (pp. 437-681): Springer.

ANSI/ASIS/RIMS. (2015). Risk Assessment RA1.2015. In. Alexandria: ASIS International.

Aouni, B. d., Abdelaziz, F. B., & Martel, J.-M. (2005). Decision-maker's preferences modeling in the stochastic goal programming. *European journal of operational research, 162*(3), 610-618.

Beach, L. R. (1993). Broadening the definition of decision making: The role of prechoice screening of options. *Psychological Science, 4*(4), 215-220.

Beisbart, C. (2012). A rational approach to risk? Bayesian decision theory. In *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk* (pp. 375-404): Springer.

Betsch, & Haberstroh. (2005). *The routines of decision making* (T. Betsch & S. Haberstroh Eds.). london: Lawrence Erlbaum Associates.

Costanza, R., Daly, H. E., & Bartholomew, J. A. (1991). Goals, agenda and policy recommendations for ecological economics. *Ecological economics: The science and management of sustainability*(s 525).

Egidi, M., Marris, R. L., & Viale, R. (1992). *Economics, bounded rationality and the cognitive revolution*: Edward Elgar Publishing.

Evans, J., & Feeney, A. (2004). The role of prior belief in reasoning. *The nature of reasoning*, 78-102.

Fischbein, M., & Ajzen, I. (1975). Attitude intention and behaviour: An introduction to theory and research. *Reading Mass: Ahdison-Wesley*.

Fischhoff, B. (1982). Debiasing'in Judgment under uncertainty: heuristics and biases. Daniel Kahneman, Paul A. Slovic, and Amos Tversky (eds.), 422-444. In: New York: Cambridge University Press.

Gigerenzer, G. (1991). How to make cognitive illusions disappear: Beyond "heuristics and biases". *European review of social psychology, 2*(1), 83-115.

Gigerenzer, G. (2003). *Reckoning with risk: learning to live with uncertainty*: Penguin UK.

Gigerenzer, G. (2015). *Risk savvy: How to make good decisions*: Penguin.

Gigerenzer, G., & Selten, R. (2002). *Bounded rationality: The adaptive toolbox*: MIT press.

Gigerenzer, G., Todd, P. M., & ABC Research Group, t. (1999). *Simple heuristics that make us smart*: Oxford University Press.

Gilovich, T., Griffin, D., & Kahneman, D. (2002). *Heuristics and biases: The psychology of intuitive judgment*: Cambridge university press.

Goodwin, P., Wright, G., & Phillips, L. D. (2004). *Decision analysis for management judgment*: Wiley Chichester.

Gore, J., & Ward, P. (2018). Naturalistic Decision Making Under Uncertainty: Theoretical and Methodological Developments–An Introduction to the Special Section. *Journal of Applied Research in Memory and Cognition*.

Hoffman, R. R., & Klein, G. L. (2017). Challenges and Prospects for the Paradigm of Naturalistic Decision Making. *Journal of Cognitive Engineering and Decision Making, 11*(1), 97-104.

ISO. (2018). ISO 31000 Risk management - guidelines. In. Geneva: International Organization for Standardization.

Jensen, K. K. (2012). 16 A Philosophical Assessment of Decision Theory. *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk, 1*.

Kahneman, D. (2011). *Thinking, fast and slow*. New York.

Kahneman, D. (2012). *Ons feilbare denken: thinking, fast and slow*: Business Contact.

Kahneman, D., Diener, E., & Schwarz, N. (1999). *Well-being: Foundations of hedonic psychology*: Russell Sage Foundation.

Kahneman, D., & Frederick, S. (2002). Representativeness revisited: Attribute substitution in intuitive judgment. *Heuristics and biases: The psychology of intuitive judgment, 49*, 81.

Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise: a failure to disagree. *American psychologist, 64*(6), 515.

Kahneman, D., Slovic, P., Tversky, A., & al, e. (1982). *Judgment under uncertainty: Heuristics and biases*. Cambridge: Cambride University Press.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the econometric society*, 263-291.

Kämper, E. (2000). *Decision Making Under Risk in Organisations: The Case of German Waste Management*: Ashgate Pub Ltd.

Klein, G. (1997). The recognition-primed decision (RPD) model: Looking back, looking forward. *Naturalistic decision making*, 285-292.

Klein, G. (2008). Naturalistic decision making. *Human factors, 50*(3), 456-460.

Klein, G. A. (1993). *A recognition-primed decision (RPD) model of rapid* *decision making*: Ablex Publishing Corporation New York.

Lipshitz, R., Klein, G., Orasanu, J., & Salas, E. (2001). Taking stock of naturalistic decision making. *Journal of Behavioral Decision Making, 14*(5), 331-352.

Lipshitz, R., & Strauss, O. (1997). Coping with uncertainty: A naturalistic decision-making analysis. *Organizational behavior and human decision processes, 69*(2), 149-163.

Loomes, G., & Sugden, R. (1983). Regret theory and measurable utility. *Economics Letters, 12*(1), 19-21. doi:http://dx.doi.org/10.1016/0165-1765(83)90106-4

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and social psychology Bulletin, 18*(1), 3-9.

Markman, A. B. (2017). Combining the Strengths of Naturalistic and Laboratory Decision-Making Research to Create Integrative Theories of Choice. *Journal of Applied Research in Memory and Cognition*.

Martignon, L., & Krauss, S. (2003). Can l'homme eclaire be fast and frugal? Reconciling Bayesianism and bounded rationality. *Emerging perspectives on judgment and decision research*, 108-122.

Morcol, G. (2007). Decision making: an overview of theories, contexts, and methods. *PUBLIC ADMINISTRATION AND PUBLIC POLICY-NEW YORK-, 123*, 3.

Navarro-Martinez, D., Loomes, G., Isoni, A., Butler, D., & Alaoui, L. (2018). Boundedly rational expected utility theory. *Journal of Risk and Uncertainty, 57*(3), 199-223.

Olsen, J. P., & March, J. G. (2004). *The logic of appropriateness*. Retrieved from Parkin, J. (2000). *Engineering judgement and risk*. London: Thomas Telford Publishing.

Payne, J., & Bettman, J. (2001). Preferential choice and adaptive strategy use. In 'Bounded Rationality: the Adaptive Toolbox'.(Eds G Gigerenzer, R Selten) pp. 123–145. In: Oxford University Press: New York.

Payne, J. W., Bettman, J. R., & Johnson, E. J. (1990). The adaptive decision maker. effort and accuracy. *Insights in decision making: A tribute to Hillel J. Einhorn, 129*.

Pliske, R., & Klein, G. (2003). *The naturalistic decision-making perspective*. Cambridge: Cambridge University Press.

Pouliot, V. (2008). The logic of practicality: A theory of practice of security communities. *International organization, 62*(2), 257-288.

Roberts, A. P., & Cole, J. C. (2018). Naturalistic Decision Making:

Taking a (Cognitive) Step Back to Take Two Steps Forward in Understanding Experience-Based Decisions. *Journal of Applied Research in Memory and Cognition*.

Roberts, M. J. (2004). Heuristics and reasoning I: Making deduction simple. *The nature of reasoning*, 234-272.

Ross, K. G., Klein, G. A., Thunholm, P., Schmitt, J. F., & Baxter, H. C. (2004). *The recognition-primed decision model*. Retrieved from

Ross, K. G., Lussier, J. W., & Klein, G. (2005). From the recognition primed decision model to training. *The routines of decision making*, 327-332.

Saaty, T. L. (2008). Decision making with the analytic hierarchy process. *International journal of services sciences, 1*(1), 83-98.

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty, 1*(1), 7-59.

Schwartz, B. (2000). Self-determination: The tyranny of freedom. *American psychologist, 55*(1), 79.

Schwartz, B. (2004). The paradox of choice: Why more is less. *New York*.

Simon, H. A. (1956). Rational choice and the structure of the environment. *Psychological review, 63*(2), 129.

Simon, H. A. (1982). *Models of bounded rationality: Empirically grounded economic reason* (Vol. 3): MIT press.

Slovic, P. E. (2000). *The perception of risk*: Earthscan publications.

Stenning, K., & Monaghan, P. (2005). Strategies and knowledge representation. *The nature of reasoning*, 129-168.

Svenson, O. (1979). Process descriptions of decision making. *Organizational behavior and human performance, 23*(1), 86-112.

Svenson, O. (1992). Differentiation and consolidation theory of human decision making: A frame of reference for the study of pre-and post-decision processes. *Acta Psychologica, 80*(1-3), 143-168.

Svenson, O. (2003). Values, affect and processes in human decision making: A differentiation and consolidation theory perspective. *Emerging perspectives on judgment and decision research, 287326*.

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness*: Penguin.

Tversky, A., & Kahneman, D. (1975). Judgment under uncertainty: Heuristics and biases. In *Utility, probability, and human decision making* (pp. 141-162): Springer.

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty, 5*(4), 297-323.

Van Der Pligt, J., & Vliek, M. (2016). *The Psychology of Influence: Theory, research and practice*: Taylor & Francis.

Von Neumann, J., & Morgenstern, O. (1947). Theory of games and economic behavior, 2nd rev.

Yates, J. F., Veinott, E. S., & Patalano, A. L. (2003). Hard decisions, bad decisions: On decision quality and decision aiding. *Emerging perspectives on judgment and decision research*, 13-63.

Zanakis, S. H., Theofanides, S., Kontaratos, A. N., & Tassios, T. P. (2003). Ancient Greeks' practices and contributions in public and entrepreneurship decision making. *Interfaces, 33*(6), 72-88.

PART 2

SCIENTIFIC PUBLICATIONS

CHAPTER 1

Biases in Security Risk Management: Do Security Professionals follow Prospect Theory in their Decisions?

Johan de Wit, Wolter Pieters,

Sylvia Jansen, Pieter van Gelder

This chapter contains the paper in which the decision phase is explored. Security practitioners are confronted with a number of experiments reflecting security risk decision making with given alternatives. The vulnerability of the practitioners to various decision biases is tested and possible consequences for security risk assessments are discussed.

This paper is published in the *Journal of Integrated Security and Safety Science, Vol 1, No 1, 2021.*

Abstract

Security professionals play a decisive role in security risk decision making, with important implications for security in organisations and society. Because of this subjective input in security understanding possible biases in this process is paramount. In this paper, well known biases as observed and described in prospect theory are studied in individual security risk decision making by security professionals. To this end, we distributed a questionnaire among security professionals including both original dilemmas from prospect theory and dilemmas adapted to the context of incident prevention. It was hypothesised that security professionals dealing with risks and decision making under risk on an almost daily basis would or should be less vulnerable to decision biases involving risks, in particular when framed in terms of incident prevention. The results show that security professionals are vulnerable to decision biases at the same scale as lay people, but some biases are weaker when decision problems are framed in terms of security as opposed to monetary gains and losses. Of the individual characteristics defining experience, only the general education level observably affects vulnerability for biases in security decision making in this study. A higher general education level leads to a significantly higher vulnerability to decision biases. By highlighting the vulnerability of security professionals to decision biases, this study contributes essential awareness and knowledge for improved decision making, for example by different representation of probabilities and uncertainty.

1. Introduction

Security professionals are confronted with the complex task of making decisions in security risk management processes . They are supposed to do this on a day to day basis with little specific (scientific) knowledge about the risks they are facing. They are expected to keep track of security risks threatening their domain of responsibility, act according to the risk appetite of the organisation, and balance security risk treatment (Wolf 2018; Butler 2002; Kayworth and Whitten 2010). The measures imposed to manage, or even mitigate, security risks need to be balanced between efficiency and effectiveness on one side and acceptance and invasiveness on the other. Due to the specific characteristics of security risks, their uncertainties, and the lack of (statistical) knowledge (Farahmand et al. 2003), this seems an impossible task. Still, in practice, tens of thousands security professionals globally take security decisions between different options day by day.

The main role of security professionals is to manage security risks. They need to identify, assess, evaluate and finally mitigate security risks. They are, or would expected to be, trained and educated to do this and build expertise over the years. Risks are generally seen as consisting of a kind of likelihood or probability that an associated impact occurs. Thus, dealing with risks in fact is dealing with uncertainties and probabilities, and balance them to potential benefits (Gordon and Loeb 2006; Kayworth and Whitten 2010; Butler 2002).

To fulfil this task, security professionals, at least in theory, are supposed to base their security risk decisions on risk management processes (Talbot and Jakeman 2011; Butler 2002; ISO/IEC 2016; NEN-ISO 2009; Button 2016; Forum 2018; NIST 2018). These risk management processes, by their nature, are a sequence of risk decisions as will be detailed in later sections. They urge the security professional to consider uncertainties and translate these in likelihood, in this paper further referred to as probabilities. As risk management is supposed to be an important and even guiding part of their work, security professionals can be expected to be familiar with decision making based on uncertainties and probabilities.

Previous well known studies into human decision making, like Prospect Theory (PT) (Kahneman et al. 1982; Kahneman and Tversky

1979) and Bounded Rationality (Gigerenzer, Todd, and ABC Research Group 1999; Simon 1982), have shown however, that humans are prone to ‘misjudge’ probabilities. They apply heuristics and show biases which make decision outcomes deviate from maximization theories like expected utility theory. This body of work unequivocally shows the use of heuristics and vulnerability for biases in decision making of humans. The experiments, however, are mainly performed in groups of lay people, often students. This might lead professionals, like security professionals, to believe these phenomena are less or not at all applicable to their judgement and decision making. Decision makers in general show a prevalence of overconfidence and often mistake their subjective sense of confidence for an indication of predictive validity (Kahneman 2021). It is therefore important to identify the use of heuristics and sensibility to biases in the actual professional community. If security professionals are vulnerable to these heuristics and biases, this could lead to less effective risk treatment or less efficient use of available resources. Or in other words they might decide to choose an less optimal risk mitigation alternative. Based on the presumed use of risk management processes, experience built over years, and trainings containing risk management, security professionals are hypothesised to be prepared for dealing with probabilities. At the same time, however, it can be expected that heuristics and biases play an important role. If this study makes these phenomena apparent in this community, as it does, security professionals cannot easily deny their influence in their day to day work.

This paper addresses the main research question: Are security professionals vulnerable to decision making biases as presented in prospect theory? Security risks and measures can be very diverse and are subject to individual subjective judgement. To be able to study and compare decision making of individuals, the decision alternatives and their probability and impact are predefined. The original PT study focusses on decisions with two predefined options and thus is a suitable theory to investigate choice behaviour of security professionals. The decisions in PT are, however, defined in financial loss and gain. This might not be representing security decisions. Therefore, in the second part of this study, the decision alternatives are redefined in security risk mitigation or reduction. The expectation is that security professionals, by the nature of their work and expertise, and confronted with limited, predefined, and given probabilities, could be less biased than lay people.

To answer the research question a survey amongst a convenience sample of security professionals is committed. The survey results will answer three sub questions:

1. To what extent are security professionals vulnerable to decision making biases as presented in the prospect theory using the original monetary gain and loss decisions?
2. To what extent are security professionals vulnerable to decision making biases as presented in the prospect theory using security decisions adapted from the original monetary ones?
3. To what extent do individual characteristics and security expertise, including age, experience, education and special security training, influence the vulnerability to decision making biases?

In section 2 of this paper risks are briefly described, and the specific characteristics of security risks are discussed. Section 3 contains a short introduction of a security management process and explains the role of decision making. The decision biases studied in this research are also clarified in this section. The methodology, survey methods and research boundaries are outlined in section 4. The results are presented and analysed in section 5. Finally, the paper ends with conclusions (section 6) and discussion and recommendations (section 7).

2. The subjectivity of security risk assessments

Decisions by security professionals are inherently based on subjective risk assessments. Risk is usually, and specifically in the context of (physical) security risk, considered as an unwanted event or an event with unwanted consequences which may or may not occur (Möller 2012; Hansson 2012; Rosa 1998). Risks in general, by their nature, contain a level of uncertainty. The uncertainty in the case of risks is originating from a lack of knowledge about the risk, the context, and/or the elements of risk itself: uncertainty about probabilities, vulnerabilities or consequences (Hansson 2012; Möller 2012; Vries 2017). Decision makers confronted with this uncertainty can decide to collect more information. A precondition for this is that the decision makers have time and resources to collect additional information. One could imagine many real-life situations where time and resources are (too) limited or the situation is (too) complex to collect sufficient risk information. About some risks there is simply no or no sufficient information available (Taleb 2007).

Security and security risks are risks and incidents resulting from malicious intent (Möller 2012; Talbot and Jakeman 2011). This study is limited to these risks. In security risks, the intent and persuasion of activities performed by malicious actors combined with the need to circumvent security measures leads to the need for unpredictable and often concealed behaviour (Hansson 2012). The virtually unlimited number of possible modus operandi and situational characteristics lead to a complex risk landscape, making prediction of probabilities and impact at least very difficult but most likely impossible (Möller 2012). Epistemic limitations like the rarity of some security incidents lead to a lack of historical data. Some security incidents are common (like for example intrusions) and historical data is available, but translating this data to probabilities for specific objects is given the situational, social-cultural and individual context of specific situations not reliable. This makes general historical data often not suitable for security risk analysis for a specific case. In addition, security risk treatment takes many different shapes and forms. This large variety of possible treatment and actions offers security professionals a large basket of possible measures to choose from, ranging from physical fences to insurance policies.

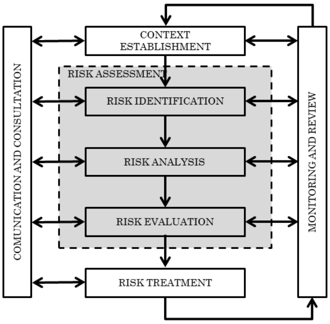
The limited body of knowledge on security risk and security risk treatment leaves the security professionals with their own judgment and perception to guide their decisions. This judgment is based on the expertise of security professionals. Individual decision making is determined by personal/subjective characteristics and environmental/context/objective characteristics (Bandura 1986; Kämper 2000; Simon 1982; Smith, Shanteau, and Johnson 2004). Expertise is understood to be specialist knowledge acquired by education and experience (Bromme, Rambow, and Nückles 2001; Dingwall and Lewis 1983). In more detail expertise of an individual is defined by: experience, accreditation, peer-identification, reliability (between and within expert), factual knowledge and the availability of subject matter experts (Shanteau and Johnson 2004; Shanteau et al. 2003; Bueno de Mesquita 2010; Cooke 1991; Bontis 2001; Smith, Shanteau, and Johnson 2004). 'Risk assessment is inherently subjective and represents a blending of science and judgment with important psychological, social, cultural and political factors' (Slovic 1999). It is clear that (individual) perception of the decision maker about risks plays a crucial role in the assessment of risk, especially when there is a lack of information like in the case of security risk.

3. Risk management and decision making

To help professionals in their quest to identify, assess and treat risks in a systematic and transparent way risk management processes are designed (Koller 1999; Talbot and Jakeman 2011; NEN-ISO 2009; Purdy 2010; ISO/IEC 2016; Parkin 2000). Each stage of the process consists of a series of decisions (see Figure 1). Risk management can be considered as a process of successive decision making (Vries 2017). This paper will follow this view.

In this paper a decision is defined as a choice leading to an outcome (Smith, Shanteau, and Johnson 2004; Jacob, Gaultney, and Salvendy 1986; Schick 1997). A decision situation is an actor facing a situation with a range of different decision alternatives. There are several assumptions about a decision making process (Doherty 2003; Collins and Ruefli 2012). First a decision process is expected to result in action or choice. Second a decision process requires the generation of a set of alternatives. Third these alternatives require a prediction of possible world states (or consequences).

The consequences of a certain alternative have a degree of certainty of materializing. This degree of certainty is depending on the level of knowledge about the alternative and the consequences given a set of variables defined by specific circumstances and context (see Figure 2: first two stages of the decision making process). In the first stage, searching, alternatives are explored and defined according to search rules. In the following stage the search for alternatives is stopped according to stopping rules. At the stopping point the actor assumes there are enough alternatives available or the time, resources and cognitive capacity are too limited to search for or create more alternatives (Gigerenzer and Selten 2002; Golub 1997; Kämper 2000). Finally, a decision process requires the assessment of the stakeholders whether a world state (or set of consequences) is desired or not. The actor is supposed to be equipped with a set of preferences. These preferences will guide the actor's decisions. The consequences of the various alternatives will be evaluated against the actor's preferences.



Examples of decisions per stage:

Decide what is in scope

Decide which risks to take into account

Decide about value of probability & impact

Decide what is acceptable/unacceptable

Decide what measures to take

Figure 1. Risk management process according to ISO 31000 (NEN-ISO 2009) with examples of decisions per stage

In this stage the decision is made which alternative to choose according to decision rules (Kämper 2000). The actor is expected to choose the alternative that serves his/her preferences best.

In the past substantial research is committed on the field of decision making under risk, starting with more normative theories like the Rational Choice Theory (RTC) the Expected Utility Theory (EUT) and the Subjective Expected Utility (SEU). These traditional decision concepts of maximization expect the actor to have knowledge of all the alternatives, all the possible consequences given specific circumstances, and context. This is also known as the Homo economicus model (Bazerman and Moore 1994).

	Decision making process			
Pre-decision	**Searching/ creating alternatives**	**Stop searching/ creating alternatives**	**Deciding**	**Post-decision**
- Awareness of problem/desire	- According to search rules	- According to stopping rules	- According to decision rules	-Consolidation (accountability, justification, dealing with dissonance etc.)

Figure 2. Decision making process, inspired by Kämper (2000); Golub (1997); Gigerenzer and Selten (2002)

In practice the preconditions of these maximizing theories are practically impossible to meet. These theories are challenged in the previous century (Tversky and Kahneman 1975; Kahneman and Tversky 1979; Kahneman et al. 1982; Simon 1956; Simon 1982; Gigerenzer 2015; Gigerenzer and Selten 2002; Gigerenzer, Todd, and ABC Research Group 1999; Fischhoff 1982; Slovic 1999; Slovic 2000). The gap between the prescriptive decision models and outcomes of descriptive experiments were described and analysed (Keren and Teigen 2004; Markman 2017). The reasons for deviations of optimization decisions theories were summarized in one of the main theories: prospect theory, PT (Kahneman and Tversky 1979; Kahneman 2012; Baron 2004). The PT, developed in the seventies of last century, is based on the results of various experiments in which the assessment of loss and gain, and the perception of probabilities by individuals is studied. These experiments showed various deviations from maximizing decision theories and inconsistencies in individual decision making. As these deviations and inconsistencies showed systematic tendencies over groups of respondents these are referred to as biases. The difference between the various decision theories like rational choice theory (RCT), expected utility theory (EUT), Prospect theory (PT) and Bounded rationality (BR), are not in the decision making process itself but can be found in the different searching, stopping and decision rules. As PT is based on experiments with pre-defined decision alternatives (usually alternative 'A' and 'B') applying searching and stopping rules is not a part of these experiments. PT and the experiments described in this paper are positioned in the 'deciding stage'.

PT presents decision heuristics and biases (Doherty 2003). The decision making heuristics and psychological biases explaining the behaviour of decision makers in PT are based on descriptive experiments. The known biases and heuristics from PT (Kahneman and Tversky 1979) are briefly described in this section. A bias is considered to show a systematic deviation from a norm. A heuristic on the other hand is considered a simplified method intended to cope with situations/problems within limited (human) processing capacity or 'rule of thumb' (Keren and Teigen 2004). Both biases and heuristics often are perceived as 'non rational' and error prone. Later research showed that the classification of some of the phenomena to be 'non-rational' can be rejected (van Erp 2017). In the experiments used in the original research the respondents are confronted with decisions with two predefined alternatives, 'A' and 'B', to choose from. In one of the experiments, for example, the respondents are asked to choose between alternative A: receive €4000 with a probability of 80%, or alternative B: receive €3000 with certainty (see decision 3, Table 1). An alternative (called prospect in PT) consists of outcome xi with probability pi. If the outcome of an alternative is certain (pi=1) the outcome is denoted by (x). Loss is denoted by –xi, a certain loss by (-x). The following phenomena from PT are part of this survey:

- The certainty effect. Actors generally tend to have a preference for certain outcomes (x) over risky outcomes even if the probability pi is high and even if the weighed outcome of the risky outcome (pi,xi) exceeds the certain outcome (x), so even when (pi,xi) > (x) actors generally prefer (x). This effect is particularly relevant as it shows a deviation from optimizing the outcome. A smaller certain effect is preferred over a larger likely effect. When allocating resources this effect may lead to lower efficiency.
- The reflection effect. Actors generally prefer a risky negative outcome (pi,-xi) over a certain negative outcome (-x) even if the probability pi is high and even if the weighed outcome of the risky outcome (pi,-xi) exceeds the certain outcome (-x), so even when (pi,-xi) < (-x), i.e. the weighed loss is higher, actors generally prefer (pi,-xi). Interestingly enough this effect shows completely reverse behaviour compared to the certainty effect when agents are confronted with loss. A lower but certain loss is avoided and a

likely larger loss is accepted. As the negative impact of security risks usually is a kind of damage, disruption, or a decline in health, well-being or prosperity, it might be comparable with loss. In the security domain security risk management and reduction of a possible negative impact is considered the main goal of a security professional (Gill 2014). So, in this domain a level of professional risk aversion might be expected. The reflection effect, however, may lead to an opposite behaviour and increase risk taking.

- The isolation effect. In a decision containing several stages, actors generally tend to ignore stages that different alternatives have in common. In such a case actors usually focus their decision on the last stage/decision only, which might lead to a suboptimal outcome. In a process of sequential decisions, like a risk management process, this effect shows a level of ignorance for a comprehensive view on a combination of decisions. The last decision of the sequence is dealt with in isolation ignoring previous ones. One of the leading elements in security risk management: layers of defence, is based on the implementation of multiple, independent, risk reduction measures. These subsequent risk reduction measures, in combination, should reduce the risk to an acceptable level. The isolation effect indicates that individuals are tempted to only take the last decision into account and ignoring the previous stages. This effect, when identified in behaviour of security professionals, could indicate that they take only the last decision or layer into account.
- Non-linear preferences (value function or probability distortion). In dealing with probabilities expectations are that the perception of percentages is linear. ‘One percent is one percent’. Experiments show however that the perception of one percent when changing from 100% to 99% is different than the perception of one percent in changing from 21% to 20%. In the same way is the perception of changing from 100% to 25% (divide by 4) different from 80% to 20%. This leads to the observation that percentages, although objective and quantitative, can have a different perception of their ‘value’ and thus can be perceived in a more subjective and qualitative way. A specially interesting phenomenon in relation

to security risks is the observation that small probabilities tend to be overrated as a result of non-linear preferences. As security risks often have a low probability of occurring this phenomenon might make decision makers overrate them.

- Insurance/lottery effect. Actors weigh alternatives not solely on the perceived probability pi but take desirability of the outcome of an alternative into account. If an outcome is 'very desirable' but has a small probability, this alternative might be preferred over an alternative with the same weighed value but with an outcome that is less desired. In combination with the reflection effect the weighing function directs decisions in the opposite direction if an alternative has a 'strong not desired outcome'. Both the desire to gamble, as a gain is at stake, and the willingness to buy insurance in the case of a possible loss are a result of this observed effect. Testing the vulnerability of security professionals for this effect might indicate their risk and insurance appetite.

As risks in general are usually weighed in terms of probability and impact these studied phenomena might have consequences for assessing risk and more specific security risks. The participants of the original experiments were mainly convenience samples of lay people and undergraduate students. The results, thus, might not reflect decision behaviour of experienced security professionals. Second, the original experiments consist of decisions with monetary gains and losses. This might not represent security risk decision making. In this paper, for the first time, to the best of our knowledge, the experiments are repeated specially targeted at security professionals and reformulated to better reflect security risk decision making. The latter is one of the main contributions of our study.

4. Methodology

In this study the experiments originating from PT are used to analyse decision making by individual security professionals. Security professionals are in this paper defined as individuals who are (partly) responsible for security risk management for a specific area of responsibility. In general this specific area of responsibility can take various forms like assets, locations, infrastructure, information, people, processes etc. The security professionals can be solely responsible or be part of decision making units. They can have a decisive or more advisory role. They can have a functional role in organisations like security officers, information security officers, risk managers or alike. They can also be consultants or part of supplier organisations. What they have in common is that they play a decisive or influencing role in security risk management.

The survey is conducted among a broad selection of participants. The online survey is made available to participants of two security conferences in The Netherlands. The participants of the ASIS Security Management Conference are mainly physical security managers. The participants of the Information and IT Security Conference, on the other hand, are mainly IT and information security managers. Further survey sessions are done in the academic Safety and Security Science group of an University. This group is involved in research and evaluations of risk management processes, risk mitigation measures and risk prevention activities. A second survey group consisted of employees of a large security systems integrator. These individuals are involved in advising, planning, and implementing security systems and services in various markets. The sample and participants can be qualified as a convenience sample (N=69). The participants cover both the IT and physical security domain, have both advisory and responsible roles and finally cover all security processes from consultancy to implementation and services. Physical and IT security are to date separated domains with different threats, measures, and even different language and culture. The risk management processes, however, are similar (ISO/IEC 2016; ISO 2018; ASIS International 2015). Thus, although the content differs, the expected risk decision behaviour of security professionals in both domains is similar.

The basis for the survey are the decisions as used by Kahneman and Tversky in their original work (Kahneman and Tversky 1979). These are used to answer the first sub question: *To what extent are security professionals vulnerable to decision making biases as presented in the prospect theory using the original monetary gain and loss decisions?* The decisions in this part of the study are used in the exact same form and format as the original decisions. The amount of monetary gain and loss is kept the same as in the original decisions; the currency is set to Euros. The results of the security professionals are compared to the original results of lay people. This comparison, using identical decisions with a discrete outcome, is done using the Chi-square test of independence, for each decision separately. This part of the study compares the vulnerability of security professionals to lay people.

In the security domain, decisions take a form different from the original monetary decisions. To address this concern the experiments are reframed in risk mitigation characteristics, one of the main contributions of this study. For the second part of the survey the decisions are thus reformulated to better reflect security risk decision making and enable comparison with the results of the original experiments. Monetary gain and loss are replaced by 'a probability of achieving risk/incident mitigation' to answer the second sub question: *To what extent are security professionals vulnerable to decision making biases when the decisions mentioned above are adapted from monetary to security decisions?* These experiments are intended to reflect real life security decisions like: which control do I implement: control measure A with these specific characteristics or control measure B with another set of specific characteristics.

The participants are asked to respond to these reformulated decisions from the perspective that they are responsible for security. The respondents are informed in advance about the, for this study considered, leading security principle: minimization security risk is their main goal. As reduction of risk for 100% is not possible, 95% is considered as the maximum achievable result. As the effectiveness of security measures is not certain in itself the prospect is defined as an expected chance of achieving an expected percentage of reduction of incidents. The probability of a monetary gain in the original decisions is thus redefined as a probability of achieving a percentage of reduction of security incidents. A monetary loss is replaced by a number of security incidents as experiencing a security incident is considered to be felt like a loss. The probability of experiencing a monetary loss in the original decisions is redefined as a probability on experiencing a number of security incidents. The ratio of the weighed expected outcome of the alternatives is kept similar and/or concordant between the two sets of decisions. For example: the respondents are asked to choose between alternative A; implement security measures with 80% probability of reducing the number of security incidents by 95%, or alternative B;

implement security measures with 100% probability of reducing the number of security incidents by 70%.

The responses to this second part of the study are compared within the same group of security professionals applying the McNemar Change test for two related samples. This test examines whether or not the responses within the same sample group differ between the two occasions for similar decision problems. Two decisions, differing from the original ones are added in this second part of the survey. These decisions offer a third decision alternative 'C': the security measures will not be implemented. These decisions also contain a cost component (see decision 18 and 19 in Table 2). Adding those criteria and alternative might lead to different decision behaviour. It might indicate a role of cost criteria in security decision making. Further details are discussed in section 5.2.

In the third section of this study the influence of personal characteristics and several aspects of individual expertise are evaluated. The third sub question: *To what extent do individual characteristics and security expertise, which includes age, experience, education and special security training, influence the vulnerability to decision making biases?* is answered based on a third set of questions. For each respondent the number of decisions in which they follow the expected bias is calculated. Grouping the respondents based on the individual characteristics age, number of years professional experience, number of years in current position, education level, and security training, a group average of number of followed biases is calculated. These group averages are compared using statistical tests (Anova). Based on these results the influence of the different studied individual characteristics on vulnerability to decision biases under study can be identified.

In addition to the individual characteristics, two general organisational classifications are collected to get a grasp of the organisational context of the respondents. First the organisational sector of the respondents is asked: public sector or private sector. The other organisational question relates to the organisational size defined in the number of employees. These two questions are included to see if there is any indication of influence of the professional environment that would justify further research. These characteristics are analysed similar to the individual characteristics.

Participants are informed about the goal of the survey, understanding decision making in the security domain and testing decision making theory of Kahneman and Tversky. The participants are asked to respond to these reformulated decisions from the perspective that they are responsible for security. Their input is processed anonymously. The survey consists of 13 decisions in the original form, see Table 1, 11 decisions with reformulated security utility (see Table 2) and 8 general/personal questions on age, experience, education, trainings and organisational classification (see Table 3).

There are drawbacks on using hypothetical survey decisions. The validity and generalizability of the results remains questionable as in every laboratory setting. In the security domain with its human dynamics and malicious intent both the threats and the measures can be perceived differently by individual security decision makers. Setting up pre-defined alternatives with a given and specified probability and consequence, however, filters out individual perception and makes results comparable. Using monetary values representing consequences also introduces some constraint. A monetary value solely might not do justice to the various perceptions and values of consequences and thus make a decision less realistic (Schneider and Barnes 2003). The upside of using this simplification of reality is the univalent perception and comparability. The assumption is that the participants have no special reason to disguise their true preferences.

5. Analysis and findings

The results are presented in the next three sections. In section 5.1 the results of the original research and lay respondents are compared to the results from the security professionals. Section 5.2 contains the results of the reformulated security decisions. The responses of the sample of security professionals on the original decisions are compared to the responses to the reformulated security decisions. Finally in section 5.3 the results of the security decisions are analysed based on individual and organisational characteristics of the respondents (age, experience, education, trainings, organisational classification, organisational size).

5.1 Analysis and findings part 1 comparing responses to original decisions

The decision problems in this part are presented to the respondents as shown in the left column of Table 1 and are labelled from 1 to 13. For example, for the first decision problem the respondent is presented with a choice between receiving €2400 for certain (alternative B) or a gamble with 33% chance to receive €2500, 66% chance to receive €2400 and 1% chance receiving €0 (alternative A). In the original study by Tversky and Kahneman 82% (n=59) of respondents chose the certain alternative. In our study, 80% of respondents (n=51) chose the certain alternative. The Chi2 test for this decision was non-significant, indicating that the security professionals did not differ in their response to this question from the respondents in the study by Tversky and Kahneman. The column ‘expected bias’ indicates the alternative that in the original study was preferred by the majority of the respondents. This behaviour is explained as bias in the original paper. The biases and the consequences of these biases are discussed in more detail in this section.

The calculations for decisions 1 to 13 are shown in Table 1. H0 cannot be rejected for all decisions except for the decisions 2, 10 and 12. For these decisions H0 can be rejected ($p<0.05$), meaning that the responses from the group security professionals differ from those of the respondents in the original study (Kahneman and Tversky 1979). The responses of these exceptions are, however, concordant between the two groups (in both samples: decision 2: $xA>xB$, decision 10: $xA<xB$, decision 12: $xA<xB$). In other words: the tendency to follow the biases is present in both sample groups. After inspection of Table 1 it is clear that the security professionals have a tendency to follow the bias. However, for dilemmas 2, 10 and 12 they seem to do so to a smaller degree than the original respondents in the original study. For the other dilemmas no difference between the two respondent groups is observed, meaning that the security professionals follow the bias to about the same degree as the original respondents. The results of the individual decisions will be discussed in more detail and related to the biases in the remaining part of this section.

Certainty effect

The responses to decisions 1 and 3 clearly show a tendency to choose certainty over risk when there is a monetary gain at stake. Although in both cases the weighed outcome (pi.xi) is higher than the certain outcome the respondents choose certainty. They are willing to 'pay' to avoid uncertainty. In decision 1 the chance of receiving less than €2400 is only 1%, the chance of receiving €100 more is 33%. The 1% probability seems to be overrated by the majority of respondents. In decision 3 the chance of receiving less than €3000 is 20% while the chance of receiving €1000 more is even 80%. The lack of statistically significant differences in the responses to these dilemmas between the two respondent groups justifies the conclusion that the sample of security professionals seems to be as vulnerable to the 'certainty effect' as lay people.

Decision 2 is comparable to decision 1 (note that in decision 2 in both alternatives A and B, 66% of receiving €2400 is removed). Whereas these decisions are similar but formulated in a different way, similar choices would be expected on both decisions. Nevertheless, Kahneman and Tversky noticed in their research that 61% of their respondents changed from alternative B for decision 1 to alternative A for decision 2. In the case of the security professionals this percentage is 44%. So, although this percentage is somewhat less than the percentage reported by Tversky and Kahneman, it shows that almost half of the security professionals make a different decision when a sure gain is changed in a probable one. The majority of the security professionals violate the EUT for both decision 1 and 2.

The responses to decision 3 clearly show the certainty effect. The alternatives described at decision 4 are exactly ¼ of the alternatives at decision 3. However, respondents in both samples provide opposite responses to dilemmas 3 and 4. The analysis of the responses from the security professionals shows that 46.4% of the respondents changes from B at decision 3 to A at decision 4 . It seems that lowering the probabilities of a gain changes decision behaviour considerably. For this result, the security professionals do also not seem to behave differently from the original respondents.

Non-linear preferences (value function or probability distortion)

The influence of the reduction of probabilities by a factor four between decisions 3 and 4 show a stronger effect on the responses to alternative B (from 100% to 25%) compared to the responses to alternative A (from 80% to 20%). 29% of the respondents stick to their choice for alternative B at both decision 3 and 4. A significant number of 46% of them changes from B to A. Only 16% chooses A at both decisions and 9% shift from alternative A at decision 3 to alternative B at decision 4. The influence of probabilities is further tested with decisions 5 and 6. The given alternatives have exactly the same weighed outcome in both decisions.

In both decisions the probabilities differ by a factor two. In decision 5 the probabilities are relatively high (45% and 90%). The respondents focus in this case on the probabilities and choose the alternative the highest probability. In decision 6 the probabilities are relatively low (1% and 2%). In this case the respondents seem to base their decision on the highest gain. 58% of the respondents from the group security professionals change from alternative B at decision 5 to alternative A at decision 6. Besides this, the security professionals and the lay people do not differ in their response to dilemmas 5 and 6. Thus, security professionals seem to be as vulnerable to the bias with regard to non-linear preference as lay people are.

Combining the results of decisions 3, 4, 5 and 6 lead to the observation that when the probabilities are relatively high and the consequence is a gain the security professionals (like lay people) base their choice on the probability (decision 3: 100% and, decision 5: 90%). When the probabilities are relatively low and the consequence is a gain the respondents seem to base their choice less on probability and more on the (desired) consequence. This is particularly interesting in the security domain where probabilities of an event occurring are relatively low. Based on these results decision behaviour of security professionals seems to shift between probabilities of 45% and 20% (probability > 45%: the majority chooses the highest probability, see decisions 3 and 5, probability < 20%: the majority chooses the preferred consequence, see decisions 4 and 6). The original results of lay people are almost identical and show similar behaviour.

Table 1. Chi-square calculation decisions 1-13

		Alternatives	Answers					Chi-square calculation		
			Security Profes-sionals			Original results Kahneman & Tversky				
			%	N	Exp. bias	%	N	X2	p-value	N
Decision 1	A	33% probability of receiving €2.500,= 66% probability of receiving €2.400,= 1% probability of receiving €0,=	20	13		18	13	0.11	0.74	136
	B	Receive €2.400,= with certainty	80	51	B	82	59			
Decision 2	A	33% probability of receiving €2.500,= 67% probability of receiving €0,=	53	34	A	83	60	14.49	**<0.05**	136
	B	34% probability of receiving €2.400,= 66% probability of receiving €0,=	47	30		17	12			
Dec. 3	A	80% probability of receiving €4.000,=	25	17		20	19	0.50	0.48	164
	B	Receive €3.000,= with certainty	75	52	B	80	76			
Dec. 4	A	20% probability of receiving €4.000,=	62	43	A	65	62	0.15	0.70	164
	B	25% probability of receiving €3.000,=	38	26		35	33			
Dec. 5	A	45% probability of receiving €6.000,=	19	13		14	9	0.67	0.41	135
	B	90% probability of receiving €3.000,=	81	56	B	86	57			
Dec. 6	A	1% probability of receiving €6.000,=	73	50	A	73	48	0.00	0.97	135
	B	2% probability of receiving €3.000,=	27	19		27	18			
Dec. 7	A	0.1% probability of receiving €5.000,=	63	40	A	72	52	1.46	0.23	136
	B	Receive €5,= with certainty	37	24		28	20			
Dec. 8	A	80% probability of losing €4.000,=	84	56	A	92	87	2.43	0.12	162
	B	Lose €3.000,= with certainty	16	11		8	8			
Dec. 9	A	20% probability of losing €4.000,=	54	36		42	40	2.13	0.14	162
	B	25% probability of losing €3.000,=	46	31	B	58	55			
Dec. 10	A	45% probability of losing €6.000,=	63	42	A	92	61	16.83	**<0.05**	133
	B	90% probability of losing €3.000,=	37	25		8	5			
Dec. 11	A	1% probability of losing €6.000,=	27	18		30	20	0.19	0.66	133
	B	2% probability of losing €3.000,=	73	49	B	70	46			
Dec. 12	A	0.1% probability of losing €5.000,=	32	20		17	12	4.22	**<0.05**	135
	B	Lose €5,= with certainty	68	43	B	83	60			
Decision 13		**First stage:**								
		75% losing, out of the game								
		25% winning, go to the second stage and choose option A or B								
		Second stage:								
	A	80% probability of receiving €4.000,=	17	11		22	31	0.55	0.46	204
	B	Receive €3.000,= with certainty	83	52	B	78	110			

Reflection effect

In their theory Kahneman and Tversky noticed opposite choices when instead of possible gains, possible losses were at stake. They labelled this the 'reflection effect'. Decision 8 is the opposite of decision 3, decision 9 the opposite of decision 4, decision 10 the opposite of decision 5 and decision 11 the opposite of decision 6. As shown in Table 1 it is highly likely that the group security professionals is responding similar to lay people at decisions 8, 9 and 11. The responses to decision 10 are concordant between the two groups. The statistically significant difference between the respondents in the study by Kahneman and Tversky and the current study for decision problem 10 shows that the security professionals are somewhat less likely to make an entirely different decision for decision problem 10 compared to decision problem 5. This can also be seen for the coupled decision problems 3-8 and 4-9, although for these decision problems the difference between the two groups do not reach statistical significance. Nevertheless, it is safe to conclude that the security professionals in this sample are also vulnerable for the reflection effect. The responses of the security professionals to the decisions 8 and 9 also violate the EUT.

The decisions 5 and 10 consist of choices with the exact same weighed outcome. Respondents are asked to choose between probabilities of 45% vs. 90%. In case of a gain (decision 5) 82% of the respondents chooses the alternative with the 90% probability. The respondents show a preference for more certainty when there is a possible gain at stake. When the possible gain is changed in a possible loss at decision 10, 63% of the respondents choose the alternative with the 45% probability. In the case of a possible loss the reflection effect seems to guide the decisions of the majority of the security professionals.

In the decisions 6 and 11 the probabilities are relatively low: 1% and 2%. Both alternatives have the exact same weighed value. At decision 6 (gain) 73.1% of the respondents chooses for the lower probability (they seem to focus on the more desirable consequence). At decision 11, where a loss is at stake, exactly the same percentage of people choose the opposite alternative with the higher probability but with also the more desirable consequence (a lower loss).

Decision 11 can be considered as coming close to security risk decisions. Usually security risks have a ‘low’ perceived probability and when materializing introduce a consequence that can be considered a loss. The responses to decision 11 seem to indicate that the perceived negative consequence drives the decision rather than the (small) difference in probability.

Lottery and Insurance effect

When gains are at stake and probabilities are relatively low, choices focus on the weight of the gain, as already shown in the section on non-linear preferences (see decisions 4 and 6 in Table 1). When this heuristic is combined with the certainty effect the lottery effect can be clearly observed. In decision 7 a small probability with high gain is offered together with a certain gain. Note that the weighed outcome of both alternatives is equal. Two thirds of the security professionals choose to gamble instead of an equally weighed certain gain. In other words they are willing to give up a certain small monetary gain (premium) for the (very small) chance on a bigger gain. The percentage of security professionals that is willing to gamble is 9% lower than in the sample of lay persons, this is , however, not significant.

The opposite effect can be observed if the gains are replaced with loses (see decision 12 in Table 1). In this case a certain loss is clearly preferred over a small possibility of a bigger loss (again with the same weighed outcome). This pattern is labelled the ‘insurance effect’. It is the willingness to accept the loss of a certain small amount to avoid a possible bigger loss. The difference between the two sample groups is in this case statistically significant. While in the original sample of lay persons 83% rather pays the certain premium to avoid a loss, in the sample of security professionals this percentage is 68%. These results seem to show that security professionals are less risk averse than lay persons at this decision. Although the majority of security professionals seem to be willing to pay the premium, almost 1 in three is willing to take the risk and would not choose ‘insurance’.

Isolation effect

When people are confronted with situations consisting of a series of subsequent decisions they tend not to consider the overall expected outcome. Instead they focus on the final decision. This phenomenon is labelled the isolation effect by Kahneman and Tversky. Based on the results of this survey it is safe to conclude that the group of security professionals is vulnerable to this effect.

Decision 13 is set up as a two stage decision. The first stage offers a 75% chance of receiving nothing and a 25% chance of entering the second stage. Respondents have no influence on this stage. In the second stage alternative A offers an 80% chance on receiving €4000 and alternative B of receiving €3000 with certainty. Notice that stage 2 is identical to decision 3. Calculating alternative A over the two stages leads to: xA = 25% * 80% * €4000 ; this equals 20% * €4000. Calculating alternative B leads to xB = 25% * 100% * €3000. Alternative B equals 25% * €3000. Notice the combined outcome of the alternative A and B over the two stages is identical to decision 4. Respondents who consider both stages are, therefore, expected to choose identically to their choice at decision 4. If the respondents only consider the second stage of decision 13 they would choose identically to decision 3. The response of the sample of security professionals to decision 13 clearly shows a strong preference for the latter. 83% of the respondents chooses alternative B at decision 13 compared to 75% at decision 3. The certainty effect is even stronger at the two-stage decision. Only 9.5% of the security professionals choose A at both decisions 13 and 4 which would show a consideration of both stages and would be the preferred outcome based on EUT. The responses of the sample of security professionals do not differ significantly from the responses of the original sample.

5.2 Analysis and findings part 2: comparing original decisions to security utility decisions

The decision problems in this part are presented to the respondents as shown in the left column of Table 2 and are labelled from 14 to 24. The alternatives at the decisions 14 to 24 are formulated with a security expected utility or prospect. For example, decision 16 is similar to decision 3 but the respondent is presented with a choice between B:

reducing security incidents with 70% for certain (this replaced the original 'receiving €3000 for certain') or A: reducing security incidents with 95% (the maximum achievable outcome) with a probability of 80% (this replaced the original '80% probability of receiving €4000'). The majority of security professionals (75%) chose for certainty at decision 3 compared to 54% at decision 16. The responses of the security professionals to the original decisions and to the reformulated decisions are compared using the McNemar Change test for two related samples. The results of the different comparisons are shown in the fourth column of Table 2. For all but decisions 16, 22 and 23 no statistically significant change in response is observed. This implies that for the majority of the decisions changing the monetary gain and loss into security gain and loss has no significant effect on the decisions made by the respondents. The perception of the security professionals of a monetary gain seems to be comparable to a reduction of security incidents (at least both lead to the same decision behaviour).

Comparing the monetary decisions to the security decisions shows concordant responses except for the decisions 22 vs. 8 and 23 vs. 9. In these two exceptions the majority of the respondents choose the alternative with the best weighed outcome when the expected utility is expressed in number of incidents (decisions 22 and 23). At decisions 8 and 9, where the utility is expressed in a monetary loss, the majority of the respondents choose the alternative with the lowest certainty due to the reflection effect (aversion to certainty of loss). These alternatives have a lower weighed outcome. As described in more detail in the methodology section a monetary loss of the original experiments is replaced by experiencing security incidents. This is based on the assumption that a security incident would be perceived as a loss. The results as detailed above, however, show different decision behaviour leading to the observation that security professionals do not seem to perceive security incidents similar as (monetary) losses. Further research into this topic is needed to verify this observation.

The decisions 18 and 19 are added to the survey to test if adding costs would change decision behaviour. In these decisions also a third choice alternative is added: the security measures will not be implemented. The monetary price of the security measures, €100.000 is an arbitrary amount. It is defined based on practical operational experience in corporate and government environments and common order of magnitude of security investments. It is high enough to need serious consideration by a security professional. On the other hand it is not as high that it would not be considered at all. Decision 18 is identical to decision 16 and decision 17 is identical to decision 19 except for the third choice alternative. The comparison of decision 16 vs. 18 shows that the majority of the respondents choose the same alternative and stick to their choice (67%), only 11 % chooses alternative C and decides not to implement the security measures.

The comparison of decision 17 vs. 19 shows a very different behaviour. 33% of the respondents stick to their choice while 59% chooses alternative C. It is clear that investing €100.000 is perceived justified by the vast majority (90%) of the respondents when security risks are reduced by 76% or 70% (the weighed outcome of decisions 16 and 18). When the risks are reduced by 18% or 19% (the weighed outcome of decisions 17 and 19) only 41% of the respondents is willing to invest this amount. These results show that security professionals weigh their investments against the perceived value they bring (in this case a probable reduction of security incidents). In search for the criteria which form the basis for security risk decisions it seems clear that the level of investments and risk reduction are related and are part of these criteria. Further research should be committed to define probable further criteria and their relationship.

5.3 Analysis and findings part 3: Influence of expertise, experience and age on security decision making

Security professionals are supposed to have expertise in their field to guide their decisions. In this survey the individual expertise is defined on some easily classifiable individual characteristics of the respondents. Accreditation and (supposed) factual knowledge are in this survey specified by education (general level and special security trainings). Experience is defined by professional position, number of years in this position, number of years professional experience and age. Table 3 shows the overall averages of the response to the reformulated security decisions 14-24 classified by the individual characteristics.

The results of the security professionals are also analysed against two general organisational classifications. First is the classification of the sectors ‘public’ or ‘private’ where the organisation of the security professionals is positioned in. The second organisational question relates to the organisational size defined in the number of employees (see Table 3).

To examine whether groups of respondents differ in their vulnerability to biases, based on the personal characteristics reported in Table 3, for each individual respondent number of decisions in which they follow the expected bias is calculated. Decision 18 and 19 are excluded from this average as they offer three options. Over the remaining nine decisions the respondents, on average, follow the expected bias at 5.98 out of 9 decisions (N=59). Based on the individual criteria relations between the individual averages and the variables age, total years professional experience, years in current position, educational level, and security trainings are investigated.

There is no statistically significant difference between the group means of the different age groups presented in Table 3, as determined by one-way Anova (F(3,55) = 1.057, p = 0.375). Also no statistically significant difference is determined between the different groups as categorized in the total years professional experience (F(4,54) = 1.292, p = 0.285) and the numbers of years in the current profession (F(4,54) = 0.594, p = 0.669). Respondents that indicate to have followed specific security training do not show a significantly different decision behaviour compared to those without this training (F(1,57) = 1.169, p = 0.284). These four individual criteria do not seem to significantly influence vulnerability to decision biases.

Table 2. Comparing security decisions vs. monetary decisions, responses of sample group security professionals

			Answers									
		Alternatives	Security decisions			Monetary decisions			McNemar		Combined	
			%	N	Exp bias	Decision	%	N	p-value	N	Exp. combined bias	Following bias %
Decision 14	A	33% probability of reducing security incidents with 95% 66% probability of reducing security incidents with 90% 1% probability of not reducing security incidents	37	22		1	20	13	0.08	59	B-B	49
	B	Certainly reduce security incidents with 90%	63	37	B		80	51				
Decision 15	A	33% probability of reducing security incidents with 95% 67% probability of not reducing security incidents	64	38	A	2	53	34	0.12	59	A-A	34
	B	34% probability of reducing security incidents with 90% 66% probability of not reducing security incidents	36	21			47	30				
Decision 16	A	80% probability of reducing security incidents with 95%	46	29		3	25	17	<0.05	63	B-B	44
	B	100% probability of reducing security incidents with 70%	54	34	B		75	52				
Decision 17	A	20% probability of reducing security incidents with 95%	78	49	A	4	62	43	0.05	63	A-A	57
	B	25% probability of reducing security incidents with 70%	22	14			38	26				
Decision 18		Implement security measures costing €100.000,= with:										
	A	80% probability of reducing security incidents with 95%	41	26								
	B	100% probability of reducing security incidents with 70%	48	30	B							
	C	These security measures will not be implemented	11	7								
Decision 19		Implement security measures costing €100.000,= with:										
	A	20% probability of reducing security incidents with 95%	25	16	A							
	B	25% probability of reducing security incidents with 70%	16	10								
	C	These security measures will not be implemented	59	37								
Decision 20	A	45% probability of reducing security incidents with 95%	29	18		5	19	13	0.25	63	B-B	56
	B	90% probability of reducing security incidents with 45%	71	45	B		81	56				
Decision 21	A	1% probability of reducing security incidents with 95%	73	46	A	6	73	50	1.00	63	A-A	56
	B	2% probability of reducing security incidents with 45%	27	17			28	19				
Decision 22		A situation in which there is:							<0.05	63	A-A	40
	A	80% probability of having 100 security incidents/year	43	27	A	8	84	56				
	B	75 security incidents/year with certainty	57	36			16	11				
Decision 23		A situation in which there is:							<0.05	63	B-B	35
	A	20% probability of having 100 security incidents/year	25	16		9	54	36				
	B	25% probability of having 75 security incidents/year	75	47	B		46	31				
Decision 24		A situation in which there is:							1.00	63	B-B	57
	A	1% probability of having 100 security incidents/year	25	16		11	27	18				
	B	2% probability of having 50 security incidents/year	75	47	B		73	49				

Table 3. Overall averages following expected bias differentiated over individual characteristics

Average following expected bias differentiated over individual characteristics (calculated over 9 dilemmas: 14, 15, 16, 17, 20, 21, 22, 23 and 24)	**Total sample:**	**Age**				**General education level**		
		<30	31-40	41-50	50>	Ass. Degr.	Bach. Degr.	Mast. degr. & PhD
N	59	9	15	21	14	8	27	24
Overall average of respondents following the expected bias	**66.5%**	64%	70%	67%	62%	51%	69%	69%
Overall average in number of dilemmas in which the expected bias is followed by individual respondents	**5.98**	5.8	6.5	6.0	5.6	4.6	6.2	6.2

	Total years professional experience					**Years in current profession**		
	<5	6-10	11-15	16-20	20>	<5	6-10	10>
N	8	8	6	11	26	29	18	12
Overall average of respondents following the expected bias	67%	66%	78%	70%	63%	68%	68%	62%
Overall average in number of dilemmas in which the expected bias is followed by individual respondents	6.0	5.9	7.0	6.3	5.7	6.1	6.1	5.6

	Specific security training		**Number of employees in organisation**				**Sectors**	
	Yes	No	0-250	250-1000	1000-5000	>5000	Public	Private
N	17	42	10	7	19	23	16	43
Overall average of respondents following the expected bias	70%	66%	71%	73%	66%	63%	70%	66%
Overall average in number of dilemmas in which the expected bias is followed	6.3	5.9	6.4	6.6	5.9	5.7	6.3	5.9

The analysis of the categories of education level, however, does show statistically significant differences. The higher the education level of the respondents, as categorized in Table 3 (for the analysis the group academic/Master and PhD are combined), the more the respondents follow the expected biases (F(2,56) = 4.883, p = 0.011). Especially the difference between respondents with an associate degree (following bias at 4.6 out of 9 dilemmas) and the other two categories (both following bias at 6.2 out of 9 dilemmas) is remarkable. Based on these results there can be concluded that higher general education seems to increase the vulnerability to follow the investigated decision biases. The limited sample size in this survey, however, makes the results less conclusive.

The organisational context as based on the size of the organisation in number of employees does not show a significant influence (F(3,55) = 1.047, p = 0.379). The organisational sector, differentiated in government or non-government also shows no significant effect (F(1,57) = 0.786, p = 0.379).

At the level of the individual respondents significant differences can be observed, however, these generate no significant pattern except for general education level.

6. Conclusions

The results of this study indicate that the expectation: 'security professionals are due to their position and experience less vulnerable to decision biases as described in Prospect Theory' needs to be rejected. Based on the analysed results in section 5.1 the vulnerability of security professionals to decision making biases using monetary gain and loss decisions can be observed. Based on the decisions 1-13 (see Table 1) it is highly likely that the group of security professionals is responding similarly to lay people. For 10 out of the 13 decisions the decisions of the two samples, the security professionals and the original sample of lay people, do not differ significantly. The responses are concordant in 12 out of the 13 decisions. The influence of *the certainty effect, the non-linear preferences, the reflection effect, the lottery and insurance effect and the isolation effect* on decision making by the majority of the sample of security professionals is clearly observed. This vulnerability to decision biases revealed on average in 70% of the sample of security professionals.

The vast majority of security professionals seems to experience the same vulnerability to biases in judging probabilities as lay people. As their work consists of dealing with security risks, which contain a level of uncertainty often expressed in a kind of probability, it is questionable if they reach an optimal decision. Although the decisions 1-13 do not reflect security decisions, the general biases in judging probabilities are found to be applicable on decision making by security professionals. Their role in the security domain and their experience does not seem to provide a better judgment of probabilities and thus risks.

The results of the reformulated decisions 14-24 show that on average two out of three respondents (66%) follow the expected biases even if the decision options are reformulated into more security-related outcomes. The results of section 5.2 (see Table 2) show that the vulnerability to decision biases is also significant when the decisions concern security utility as defined in this study.

Seventeen decisions of the total survey contained options with a different weighed outcome (the product of probability and outcome). Two different decision patterns can be observed. Ten of these decisions consist of options with a probability difference of 1% or 5% between option A and B. At eight of these ten decisions, the respondents choose the option with the best outcome, not the lowest probability. They also ignore the best weighed outcome in six decisions. The two exceptions can be explained by the certainty effect which is a strong behaviour driver as also identified in PT (Kahneman and Tversky 1979).

At all of the 7 decisions with a different weighed outcome and a probability difference of 20% or 45%, the respondents choose the option with best probability (which led to the worst weighed outcome at six of the decisions and violates maximizing theories). This leads to the following observation: if the probability difference is relatively small (in this survey 1% or 5%) respondents choose the option with the best outcome and they seem to ignore the difference in probability. If the probability difference is relatively large (in this survey 20% or 45%) they seem to base their decision solely on this and ignore the (weighed) outcome. This observation further expands the known non-linear preference effect or probability distortion.

Decisions between options with low probabilities

As security risks normally have a rather low probability of occurring it is interesting to pay special attention to the decisions 6, 11, 21 and 24 (see Table 4).

At all these decisions the options have a relatively low probability and the weighed outcome is equal (decision 21 almost equal). At all of the four decisions the majority of the respondents seem to base their choice on the desired outcome rather than the desired probability. They make identical choices in both the monetary as the security decisions. As the absolute difference is only 1% the previous observation seems to affect these decisions. The probabilities in these decisions however differ substantially when compared by each other (by a factor two). Risk is defined as a combination of probability (chance of materializing of the risk) and outcome (the expected consequences when a risk is materializing). So even if the respondents could decide to reduce the probability by a factor two (1% vs 2%) the majority choose not to.

Table 4. Responses of security professionals on decisions 6, 11, 21 and 24

	Alternatives		Answers		
			Security Professionals		Expected bias
			%	N	
Decision 6	A	1% probability of receiving €6.000,=	73	50	A
	B	2% probability of receiving €3.000,=	27	19	
Decision 11	A	1% probability of losing €6.000,=	27	18	
	B	2% probability of losing €3.000,=	73	49	B
Decision 21	A	1% probability of reducing security incidents with 95%	73	46	A
	B	2% probability of reducing security incidents with 45%	27	17	
Decision 24		A situation in which there is:			
	A	1% probability of having 100 security incidents/year	25	16	
	B	2% probability of having 50 security incidents/year	75	47	B

Based on this observation it can be stated that in dealing with low probability risks the probability is ignored by decision makers. Decision options are solely judged on their perceived outcome. For the security practice this could mean that less effort could be put in investigating the probability of security risks (as they usually have a low probability of occurring). Further, lowering the probability of a risk is considered to be a preventive measure (it is less likely that the risk will materialize). The observation that for low probability risks the probability is ignored by security professionals could, therefore, be interpreted as no or less focus on prevention. Their focus might be on reducing the impact or consequence solely. Theoretically these results indicate that the majority of the security professionals taking part in this survey seem to be less focussed on preventive measures (leading to lower probability).

Influence of costs on security decision making

Decision 18 and 19 (see Table 2) offer a third choice option C: the security measures will not be implemented. There is also an arbitrary cost component added reflecting the costs associated with implementing the security measures. The options A and B at decision 18 are identical to these options at decision 16. Comparing the response shows that 67 % of the respondents choose alike on both decisions. Only 11% decides not to implement the security measures. The reaction to decision 19 shows a different behaviour. The options A and B at decision 19 are identical to these options at decision 17. Comparing these responses shows that in this case 33% chooses alike and 59% chooses option C. Based on these results it is safe to conclude that costs play a role in decision making of the respondents. In decision 18 89% of the respondents is willing to pay the premium of €100.000 to reduce risks with a probability of 80% or 100%. In decision 19 only 41% of the respondents is willing to pay the same premium for reducing risks with a probability of 20% or 25%. This difference indicates that the willingness to invest in security measures is related to the expected benefits. Based on the data resulting from just these two decisions no detailed conclusions can be drawn about this balance between costs and benefits. It is however safe to conclude that this relation exists. Further research might be committed to further specify this relation.

Important to note is that in decisions 18 and 19 no limitations on investments are imposed. It is therefore remarkable that a part of the respondents seems to be reluctant to invest in risk reduction even without budget restrictions.

Insurance effect

Decision 12 tests the insurance effect (see Table 1). Choosing between a small premium and a small probability on a relatively substantial loss is offered to the respondents. In the original research of Kahneman and Tversky 83% of the respondents chooses the premium over the risk. The security professionals show a significant different behaviour, 68% is willing to pay the premium. As security professionals are supposed to mitigate security risk they might be expected to be risk-averse. The results however show a significantly higher percentage of them willing to take the risk compared to the original group of lay people.

The influence of expertise

Overall the respondents follow the expected bias in 6 of the 9 security decisions (decisions 14-24 except 18 and 19). Comparing the group means of the differentiated groups in age, number of years professional experience, number of years in current position, and conducted security trainings, show no significant difference. These variables do not influence the vulnerability for decision biases under study. For the security practice this seems to indicate that more experience and security knowledge as defined by these four variables does not lead to more optimized decisions.

A significant difference however is identified comparing the group means when the respondents are differentiated to education level. The results show a significant increase of vulnerability with a higher level of education. As no further detailed individual information is collected in this study no clear cause for this can be formulated. It is, however, an interesting finding which might inspire further research.

7. Discussion and recommendations

Because of the set-up of the present research, it cannot account for the full complexity of the tasks of security professionals. Because of the focus on prospect theory and associated biases, the present study highlights only one particular aspect of security decision-making. After participating in the survey several respondents reacted 'this is not the way decisions are made'. They indicated that, due to time pressures, incomplete information, and limited resource capacity, they follow different decision routines. Some of them seem to rely more on prior experience to guide their decision in a faster, more intuitive fashion. The results as presented in this paper, however, do not reveal influence of experience on the vulnerability for decision biases. This contradiction can be explained by the assumed decision process the decision maker follows. In this study the respondents are confronted with two predefined alternatives which might not comply to their real life decision making.

As already mentioned in the methodology section there are drawbacks on using hypothetical survey decisions. The validity and generalizability of the results remains questionable as a laboratory setting reflects only a selected part of reality. Due to the complexity of the security risk landscape, the virtually unlimited number of possible modus operandi, and the variation in situational, social-cultural and individual context, experiments need to simplify reality. The experiments in this study do not reflect an entire security risk assessment, they merely limit their scope to a choice between two mitigation options which in a real-life situation represents only a limited part of a risk assessment. However, we believe that PT can be made more realistic in a professional context by varying the types of questions asked. A key methodological innovation thus lies in de adaptation of generic PT dilemmas to a profession-specific context, in this case security incidents and associated probabilities.

Recommendations

Despite its importance in decision-making, the professionals in the security risk domain are largely unaware of psychological phenomena. It seems this knowledge is not included in the curricula of security professionals which in itself is an interesting observation of this study. As many decision makers, in general, show prevalence of over-confidence they might perceive their own judgement superior and believe they are not susceptible to biases. By replicating PT experiments in the actual professional domain, and adapting them to a security-specific context, the professionals acting in this domain cannot easily ignore the results and perceive their decision making superior to other humans. This awareness might be even the biggest contribution of this study to the security risk domain.

With respect to the overall research question, it is highly likely that security professionals are, in majority, vulnerable to decision making biases as presented in prospect theory. The results show that they are as vulnerable to the investigated biases as lay people, which was not expected. This will influence security risk decision making and thus a security management process. Biases might lead professionals to less optimized security risk decisions which, in turn, might influence security in organisations and society. The results of this study can raise awareness for the identified biases. The logical subsequent step would be to take these biases into account and, if considered needed, take anti-biasing countermeasures. Other fields of research already identified these ranging from a different representation of probabilities and uncertainty (Gigerenzer 2015; Kurz, Gigerenzer, and Hoffrage 1998; Payne and Bettman 2001) to changing decision making processes (Stafford, Holroyd, and Scaife 2018; Trönnberg and Hemlin 2019; Simutis 2003; Daftary-Kapur, Dumas, and Penrod 2010). Many of these countermeasures are context related and thus the applicability for security risk decision making should be evaluated on a case by case basis. These tools can improve human security risk decision making and in turn improve our security.

Literature

ASIS International. 2015. "Risk Assessment, ANSI/ASIS/RIMS RA.1-2015." In. Alexandria: ASIS International.

Bandura, Albert. 1986. Social foundations of thought and action: A social cognitive theory: Englewood Cliffs, NJ, US: Prentice-Hall, Inc.

Baron, Jonathan. 2004. Normative models of judgment and decision making, Blackwell handbook of judgment and decision making: Wiley Online Library.

Bazerman, Max H, and Don A Moore. 1994. Judgment in managerial decision making: Wiley New York.

Bontis, Nick. 2001. "Assessing knowledge assets: a review of the models used to measure intellectual capital." International journal of management reviews 3 (1):41-60.

Bromme, Rainer, Riklef Rambow, and Matthias Nückles. 2001. "Expertise and estimating what other people know: The influence of professional experience and type of knowledge." Journal of Experimental Psychology: Applied 7 (4):317.

Bueno de Mesquita, Bruce. 2010. "JUDGING JUDGMENT." Critical Review 22 (4):355-88. doi: 10.1080/08913811.2010.541686.

Butler, Shawn A. 2002. Security attribute evaluation method: a cost-benefit approach. Paper presented at the Proceedings of the 24th international conference on Software engineering.

Button, Mark. 2016. Security officers and policing: powers, culture and control in the governance of private space: Routledge.

Collins, James M, and Timothy W Ruefli. 2012. Strategic risk: a state-defined approach: Springer Science & Business Media.

Cooke, R.M. 1991. Experts in uncertainty. New York: Oxford University Press.

Daftary-Kapur, Tarika, Rafaele Dumas, and Steven D Penrod. 2010. "Jury decision-making biases and methods to counter them." Legal and Criminological Psychology 15 (1):133-54.

de Vries, Jennie. 2017. "What drives cybersecurity investment?" (Master thesis), TU Delft.

Dingwall, Robert, and Philip Simon Coleman Lewis. 1983. The sociology of the professions: Lawyers, doctors and others: Macmillan; St Martin's Press.

Doherty, Michael E. 2003. Optimists, pessimists, and realists, Emerging Perspectives on Judgement and Decision Research. Cambridge: Cambridge University Press.

Farahmand, Fariborz, Shamkant B Navathe, Philip H Enslow, and Gunter P Sharp. 2003. Managing vulnerabilities of information systems to security incidents. Paper presented at the Proceedings of the 5th international conference on Electronic commerce.

Fischhoff, Baruch. 1982. "Debiasing'in Judgment under uncertainty: heuristics And biases. Daniel Kahneman, Paul A. Slovic, and Amos Tversky (eds.), 422-444." In.: New York: Cambridge University Press.

Forum, Information Security. 2018. "Standard of Good Practice." In. Surrey: Information Security Forum.

Gigerenzer, Gerd. 2015. Risk savvy: How to make good decisions: Penguin.

Gigerenzer, Gerd, and Reinhard Selten. 2002. Bounded rationality: The adaptive toolbox: MIT press.

Gigerenzer, Gerd, Peter M Todd, and the ABC Research Group. 1999. Simple heuristics that make us smart: Oxford University Press.

Gill, Martin L. 2014. The handbook of security: Springer.

Golub, Andrew Lang. 1997. Decision analysis: an integrated approach: Wiley.

Gordon, Lawrence A, and Martin P Loeb. 2006. "INFORMATION SECURITY EXPENDITURES." Communications of the ACM 49 (1):121.

Hansson, Sven Ove. 2012. "A Panorama of the Philosophy of Risk." In Handbook Of risk theory, 27-54. Springer.

ISO. 2018. "ISO 31000 Risk management - guidelines." In. Geneva: International Organization for Standardization.

ISO/IEC. 2016. "ISO/IEC 27000 International standard Information Technology Security techniques." In. Geneva: ISO.

Jacob, Varghese S, Larry D Gaultney, and Gavriel Salvendy. 1986. "Strategies and biases in human decision-making and their implications for expert systems." Behaviour & Information Technology 5 (2):119-40.

Kahneman, Daniel, Sibony, Olivier., Sunstein, Cass R, 2021. Noise, a Flaw in Human Judgment. London: William Collins.

Kahneman, Daniel. 2012. Ons feilbare denken: thinking, fast and slow:

Business Contact.

Kahneman, Daniel, Paul Slovic, Amos Tversky, and et al. 1982. Judgment under uncertainty: Heuristics and biases. Edited by Daniel Kahneman. Cambridge: Cambride University Press.

Kahneman, Daniel, and Amos Tversky. 1979. "Prospect theory: An analysis of decision under risk." Econometrica: Journal of the econometric society:263-91.

Kämper, Eckard. 2000. Decision Making Under Risk in Organisations: The Case Of German Waste Management: Ashgate Pub Ltd.

Kayworth, Tim, and Dwayne Whitten. 2010. "Effective information security requires a balance of social and technology factors." MIS Quarterly executive 9 (3):2012-52.

Keren, Gideon, and Karl H Teigen. 2004. "Yet another look at the heuristics and biases approach." Blackwell handbook of judgment and decision making: 89-109.

Koller, Glenn Robert. 1999. The Practical Guide to Risk Assessment and Decision Making: CRC Press.

Kurz, Elke, Gerd Gigerenzer, and Ulrich Hoffrage. 1998. "Representations of uncertainty and change: Three case studies with experts." In.: Sonderforschungsbereich 504, Universität Mannheim & Sonderforschungsbereich 504, University of Mannheim.

Markman, Arthur B. 2017. "Combining the Strengths of Naturalistic and Laboratory Decision-Making Research to Create Integrative Theories of Choice." Journal of Applied Research in Memory and Cognition.

Möller, Niklas. 2012. "The concepts of risk and safety." In Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk, 55-85. Springer.

NEN-ISO. 2009. "NEN/ISO 31000 (nl) Risicomanagement-Principes en richtlijnen." In. Delft: NEN.

NIST, National Institute of Standards and Technology. 2018. "Framework for Improving Critical Infrastructure Cybersecurity." In. Gaithersburg.

Parkin, James. 2000. Engineering judgement and risk. London: Thomas Telford Publishing.

Payne, JW, and JR Bettman. 2001. "Preferential choice and adaptive strategy use. In ‘Bounded Rationality: the Adaptive Toolbox’.(Eds G Gigerenzer, R Selten) pp. 123–145." In.: Oxford University Press: New York.

Purdy, Grant. 2010. "ISO 31000: 2009—setting a new standard for risk management." Risk Analysis 30 (6):881-6.

Rosa, Eugene A. 1998. "Metatheoretical foundations for post-normal risk." Journal of Risk Research 1 (1):15-44.

Schick, Frederic. 1997. Making choices: A recasting of decision theory. Cambridge: Cambridge University Press.

Shanteau, James, and Paul Johnson. 2004. Psychological investigations of competence in decision making: Cambridge University Press.

Shanteau, James, David J Weiss, Rickey P Thomas, Julia Pounds, and Bluemont Hall. 2003. "How can you tell if someone is an expert? Empirical assessment of expertise." Emerging perspectives on judgment and decision research:620-41.

Simon, Herbert A. 1956. "Rational choice and the structure of the environment." Psychological review 63 (2):129.

Simon, Herbert Alexander. 1982. Models of bounded rationality: Empirically grounded economic reason. Vol. 3: MIT press.Simutis, Z.M. 2003. "Program in Basic Research 2002-2003." In. Fort Belvoir: US Army Research Institute.

Slovic, Paul. 1999. "Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield." Risk Analysis 19 (4):689-701.

Slovic, Paul Ed. 2000. The perception of risk: Earthscan publications.

Smith, Kip, James Shanteau, and Paul Johnson. 2004. Psychological investigations of competence in decision making: Cambridge University Press.

Stafford, Tom, Jules Holroyd, and Robin Scaife. 2018. "Confronting bias in judging: A framework for addressing psychological biases in decision making."

Talbot, Julian, and Miles Jakeman. 2011. Security risk management body of knowledge. Vol. 69: John Wiley & Sons.

Taleb, Nassim Nicholas. 2007. The black swan: the impact of the highly improbable. New York: Random House.

Trönnberg, Carl-Christian, and Sven Hemlin. 2019. "Challenging investment decision-making in pension funds." Qualitative Research in Financial Markets.

Tversky, Amos, and Daniel Kahneman. 1975. "Judgment under uncertainty: Heuristics and biases." In Utility, probability, and human decision making, 141-62. Springer.

van Erp, Noel. 2017. "A Bayesian framework for risk perception." (Doctoral dissertation) Delft University of Technology.

Wolf. 2018. "An empirical study examining the perceptions and behaviours of security-conscious users of mobile authentication." Behaviour and Information Technology 37 (4):320-34.

CHAPTER 2

Individual Preferences in Security Risk Decision Making: an Exploratory Study under Security Professionals

Johan de Wit, Wolter Pieters, Pieter van Gelder

What are the main attributes of risks that are considered by security practitioners during their risk assessments? These preferences are studied during a ‘fast and frugal’ system 1 assessment and during a system 2 compensatory ranking. Interesting differences are observed between these two assessments. Professional preferences of security professionals seem to be not consistent.

This paper is published in the book: *WIT Transactions on THE BUILT ENVIRONMENT*, *volume 206, 2021* and presented at the *WIT SAFE conference 2021*.

Abstract

Risk assessments in the (cyber) security domain are often, if not always, based on subjective expert judgement. For the first time, to the best of our knowledge, the individual preferences of professionals from the security domain are studied. In on online survey they are asked to mention, rate and rank their preferences when assessing a security risk. The survey setup allows to differentiate between easy accessible or 'on top of mind' attributes and guided or stimulated attributes. The security professionals are also challenged to both non-compensatory and compensatory decision making on the relevance of the attributes. The results of this explorative study indicate a clear difference and shift in the individual perceived relevance of attributes in these different settings. Another remarkable finding of this study is the predominant focus on impact attributes by the respondents and the less significant position of likelihood or probability. The majority of professionals seem to ignore likelihood in their security risk assessment. This might be due to so called probability neglect as introduced by other scholars. the security in organisations and society is depending on the assessment and judgement of these professionals, understanding their preferences and the influence of cognitive biases is paramount. This study contributes to this body of knowledge and might raise attention to this important topic in both the academic and professional security domain.

1. Introduction

The security risk field is dealing with malicious, and therefore man-made, risks. Risks in general contain a level of uncertainty by nature as they involve a future state of affairs. The aspect of malicious intent of security risks add an extra dimension to this uncertainty. Malicious actions, like for example an intrusion, usually are meant to be unpredictable, concealed and evade existing risk controls.

The dynamic context of security risks, with ever changing modus operandi, in combination with the large variety of situations, both in location and time, add to the uncertainty. Because of this information about past security risks and events, if available, is often not sufficient to estimate or predict future security risk. The assessment of the uncertainty of security risks, therefore, is for a large part based on expert judgement rather than based on evidence or objective data.

The individuals assessing security risks, in this study referred to as security professionals, often, if not always, apply a risk management process of some sort to structure their assessment. The various risk management processes contain obvious process stages like: establishing the context, risk identification, risk analysis, risk evaluation and risk treatment.

So far little scientific studies are conducted exploring individual preferences and priorities guiding security professionals in their daily praxis of security risk decision making during these risk management processes. These professionals play a decisive or advisory role in security risk treatment, hence, they are determining or at least influencing the security in organisations and society. Understanding their individual preferences and priorities is of vital importance to understand their security risk judgement. The purpose of this exploratory study is to examine the criteria, further referred to as attributes, and their priority, security professionals consider when assessing a security risk.

An online survey is conducted under security professionals of both the physical and cybersecurity domain. The survey set up is explained in more detail in the Method and materials section.

This study is, for the first time, exploring security risk assessments by security professionals. What are the individual preferences and priorities of security professionals? Do they change after a ‘second thought’? Is individual expertise influencing these preferences? The purpose of this exploratory study is to enhance our understanding of individual decision making influencing the security in our society.

Section 2 presents a brief overview of the theoretical background of security risks, risk assessments and decision making. In section 3 the research method is explained followed by the results and analysis section. This paper ends with conclusions and discussion in section 5.

2. Security Risk Assessments and Decision Making

In this section first the characteristics of security, security risks and risk management processes are described followed by a theoretical background of decision making, cognitive biases, especially the availability heuristic.

2.1 Security, security risks and risk management

Keeping objects and organisations secure is the prime task of security professionals [1]. They have a decisive or advisory role in dealing with security risks. According to the ISO 31000, Risk management – Principles and guidelines, risk is “the effect of uncertainty on objectives. According to Hansson [2] ‘knowledge about a risk is knowledge about the unknown’. This knowledge is in many cases incomplete and, therefore, will have to be supplemented or even replaced by expert judgment [3]. The latter is certainly the case in security related events.

Expert judgement is considered a degree of belief, based on tacit knowledge and expertise [4]. These subjective interpretations and assessments are not only based on ‘hard-to-measure’ expertise but are also prone to numerous cognitive biases and heuristics. This has led many scholars to question the viability of such uncertainty assessments. Still in many domains, like security, there are no alternatives or objective procedures available. Therefore, intuitive judgements of uncertainty play an essential role in decisions [5].

2.2 Decision making

“A decision is a commitment to a course of action that is intended to produce a satisfying state of affairs” [6]. A decision involves a range of options for possible action or inaction. Decision options are further referred to as alternatives in this study. The decision agent is supposed to be equipped with a set of preferences based on objectives or goals.

In order to reach a final judgement and be able to select a possible decision alternative, the agent needs to analyse and differentiate the available alternatives [7]. Each alternative is, therefore, defined by a set of attributes associated with consequences when materializing. An attribute is defined as a certain aspect of an alternative. It is used to measure performance in relation to an objective.

Besides this more functional explanation of decision making, focussed on maximizing subjective expected utility, other functionalist metaphors, like accountability, influence human decision making. ‘Accountability refers to the implicit or explicit expectation that one may be called on to justify one’s beliefs, feelings and actions to others’ [8]. Due to the responsibility for managing something as important as security risks, the security professionals in this study can be expected to, consciously or unconsciously, consider accountability in their decisions.

The individual response to attributes consists of two main components: an affective response and a cognitive response. These relate to the so-called dual-process models. The most renown of these models is the system 1 and 2 model by Daniel Kahneman [9]. The affective response is related to system 1 which is considered to be more intuitive, automatic, fast, experience based and requires little cognitive effort. System 2, on the other hand, is considered deliberate, slow, concentrated, compensatory, and demands considerable cognitive effort. In the huge body of work on decision making that has evolved since the 1970s multiple heuristics and biases are identified and analysed. These heuristics and biases influence or even direct individual decision making.

This study focusses on availability (heuristic) which is considered one of the prominent general-purpose heuristics. A large body of research demonstrated that judgements in general are based on the information that is most accessible to the decision agent at the time of the judgement. Both ease of recall and content of recall (the number of associations) influences the estimation of likelihood and thus perceived risk.

Van der Pligt and Vliek [10] added a valuable observation to the availability heuristic. Combining the ease of recall and content of recall to decision attributes not only influences the estimation of possible frequencies, but also influences the judgement of prevalence or commonness of a situation. A prevalent situation or attribute is widely accepted or favoured and this leads these scholars to the observation that prevalence adds to the weight of an attribute. In other words: availability of information of an attribute leads to a higher priority of this attribute.

3. Method and Materials

This survey is committed to explore the attributes of security risks security professionals consider and prioritize when assessing security risks. The attributes of security risks which are considered by security professionals during their security risk assessment are, therefore, collected and analysed. The explorative results are retrieved via an online survey conducted between June 13, 2019 and August 28, 2019. Participation in the survey was promoted in both the IT and physical security professional community. It was promoted via LinkedIn and Twitter, both in general and in special interest groups like Security management, ASIS Europe and ASIS International, Dutch cybersecurity platform. Second, a direct email campaign was launched targeting the existing professional network of the researchers. Third, the survey was published via the website of The Hague Security Delta, a Dutch security cluster of businesses, governments and knowledge institutions. Finally, the survey was promoted on several conferences and meetings via flyers. The sample of respondents (N= 248) is regarded to be a convenience sample.

To challenge the respondents the survey starts with an open ended question. This question ask them to come up with the attributes (in the survey referred to as criteria) they consider when assessing security risks. These answers express what is ‘on top of mind’ and quickly available for the respondents in a blind recall without prompting from external stimuli. This open ended question allows the respondents to answer based on their complete knowledge, perception and experience without restrictions. The question offers a maximum of 10 answer options (first field forced response). This question evokes the respondents to show their attitude based on the attributes they take into account when judging security risks and measures. The answers to these questions serve as an index of quickly or most available attributes. This availability of attributes is related to the well-known availability heuristic. The answers to these open ended questions reflect the priority of, in this case, attributes related to security risk assessment. They can be considered as most prominent by the security professionals at the point of time of answering the survey.

Table 1: Predefined security risk attributes

Predefined Security risk criteria:	
Context impact criteria: 1 Perceived Impact (general) 2 Impact on health and safety of employees 3 Impact on health and safety of customers, or visitors 4 Impact on surroundings/community 5 Impact on business process (including IT downtime) 6 Impact on supply chain 7 Financial impact 8 Legal impact/liability 9 Environmental impact 10 Damage to the reputation of the organization 11 Impact on public opinion 12 Physical damage to assets 13 Data loss 14 Data disclosure (including privacy sensitive data) 15 Loss of data integrity 16 Disclosure or loss of intellectual property	**Individual/personal impact criteria:** 17 Personal responsibility/accountability 18 Damage to personal reputation 19 Management attention 20 Personal liability 21 Personal financial loss 22 Personal conscience 23 Regret of no or inadequate action **Likelihood/Probability:** 24 Probability/likelihood of risk (general) **Other/Risk perception:** 25 Fear of a security risk 26 Involuntariness of risk taking 27 Uncontrollability of risk 28 Lack of knowledge about a risk

To be able to determine the priority of attributes in multiple attribute decision making in a fuzzy environment two subsequent processes are involved: rating and ranking of attributes [11]. In the second part of the survey the respondents are asked to assign a priority to a predefined list of 28 security risk attributes (see Table 1). Each of the presented attributes can be rated using a five point Likert scale: extremely important, very important, moderately important, slightly important, not at all important. As the rating is done per individual attribute the rating is non-compensatory. The predefined list of attributes is derived from risk assessment tools like the ISO 27005, Information security risk management and the ASIS International Risk assessment and the SCM model. Four attributes influencing risk perception are also added to the list dread (fear), knowledge of the risk, whether or not the exposure to a risk can be influenced and finally if the risk can be managed or controlled.

In the third part of the survey the respondents are forced to set priorities over the 28 predefined attributes. They are asked to rank their top 10 (1 is the most important attribute etc.). To avoid order biases, or response order bias the list of predefined attributes is automatically randomized for each participant. At this point in the survey the respondents are asked to rethink their position on risk attributes for the third time and this time they even need to apply compensatory mental models. This is considered to be system 2 thinking. Comparing the answers to the open ended questions of the first part and the ranking answers to this third part is considered to show the difference in the judgement of security risk attributes between system 1 and system 2.

The survey ends with nine questions on individual characteristics: functional description, number of years in current position, number of years security expertise, number of years professional expertise, age, education level, specific security trainings, job sector, size of organization in number of employees.

Open ended questions usually lower the completion rate of a survey due to the required cognitive effort of the respondents. Taking survey fatigue into account the order of the survey questions is organized to start with the most demanding open-ended questions and lower the cognitive effort with each question. After agreeing the consent statement (N=248) 60% of the respondents stopped the survey at the start of the open ended questions. Of the remaining 99 participants 81 completed the entire survey.

4. Results and Analysis

In this section the results of the survey are discussed in three parts: the result and analysis of the open ended questions, the results and analysis ot the rating questions, the results and analysis of the ranking questions. Finally these results are combined and compared.

4.1 Part one: open ended questions

The two open ended questions are answered in plain text by 99 respondents. Four of these did not answer seriously, their answers are excluded from the analysis. To answer the first question: 'When you assess a security risk, which criteria do you consider or take into account during your assessment?', in total 463 free text fields are filled, containing 516 identifiable and interpretable answers. These answers are considered to be 'on top of mind', easy available and primarily originating from system 1 thinking.

For a first interpretation of the answers the method of manual inductive or grounded coding is applied, the coding process thus allowed the main attributes and their structure to emerge. The coding frame that emerged from the manual inductive coding process revealed common risk components beyond the two expected general risk components following the narrow definition of risk: probability/likelihood and consequence/impact. The respondents seem to have included components of the risk management process leading to the final assessment of security risks. In the narrow scope as intended by the researchers risk assessment is forming a judgment of a security risk based on the two general attributes likelihood and consequence.

The observed categories are in line with the risk management process as detailed in security risk standards like the American National Standard: Risk Assessment, issued by ANSI, ASIS and RIMS [12], see Figure1.

As impact and consequence are not specifically defined in the survey the vast majority of the respondents used 'impact', only four used the word 'consequence'. In the analysis of the answers in this study the categories impact an consequence are combined. This study focusses on the narrow definition of risk assessment (see Figure 1).

The categories emerging from the inductive coding process fit the predefined risk attributes as presented in section 3. The list of predefined risk attributes, however, contains attributes that seem to be 'not on top of mind' and they are not mentioned by the respondents. These attributes mainly concern individual/personal impact attributes and risk perception attributes. There are also three impact categories that some of the respondents pointed out that were not included in the predefined criteria list: Impact on trust, impact on/for customers, and

political/national impact. The results of the open ended answers limited to the intended narrow definition of risk assessment are presented in Table 2.

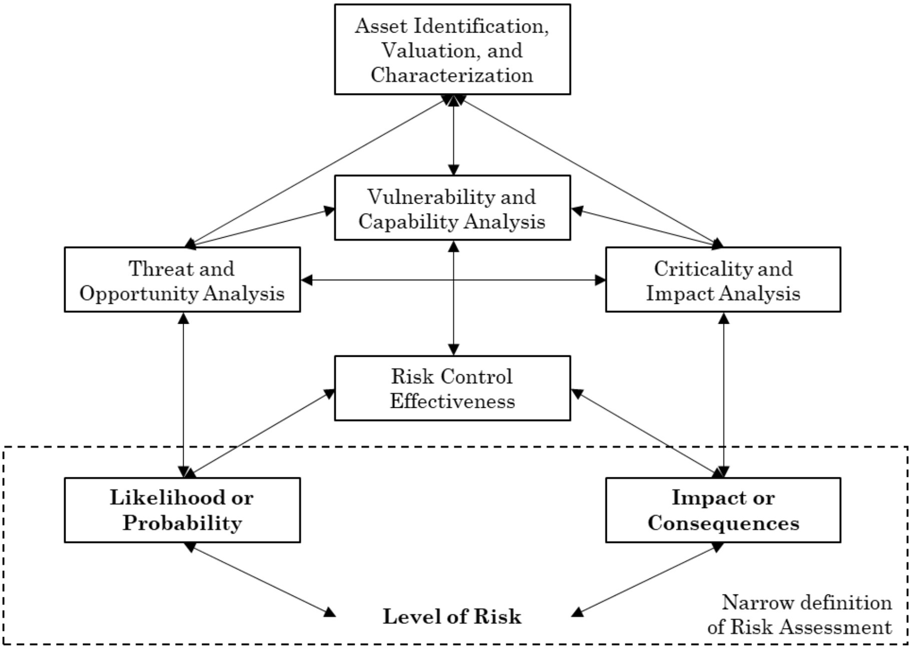

Asset Identification, Valuation, and Characterization
Vulnerability and Capability Analysis
Threat and Opportunity Analysis
Criticality and Impact Analysis
Risk Control Effectiveness
Likelihood or Probability
Impact or Consequences
Level of Risk
Narrow definition of Risk Assessment

Figure 1: 'Determining the level of risk', risk management process according to American National Standards Institute

The categories emerging from the inductive coding process fit the predefined risk attributes as presented in section 3. The list of predefined risk attributes, however, contains attributes that seem to be 'not on top of mind' and they are not mentioned by the respondents. These attributes mainly concern individual/personal impact attributes and risk perception attributes. There are also three impact categories that some of the respondents pointed out that were not included in the predefined criteria list: Impact on trust, impact on/for customers, and political/national impact. The results of the open ended answers limited to the intended narrow definition of risk assessment are presented in Table 2.

A reliability analysis was carried out on the answers to the open ended questions. Cronbach's alpha showed the answers to reach low internal reliability, α = 0.469.

Further correlation analysis showed various significant but low correlations between the individual attributes (r values between 0.21 and 0.492). The correlation between attribute 14 and 15 reached a moderate level (r= 0.688, p<0.05). The inductive coding process shows clearly that the largest answer category relates to impact (192 answers). The vast majority of respondents, 87%, mentions one or more impact attributes.

Table 2: Descriptive analysis, inductive coding, sub categories of answers within the categories impact/consequence and likelihood/probability

Question 1: When you **assess a security risk**, which criteria do you consider or take into account during your assessment?			
Free text entries, manually, inductive or grounded coding		Number of answers:	Percentage of respondents:
1	Perceived impact of the security risk	50	53%
2	Impact on health and safety of employees	23	24%
3	Impact on health and safety of customers, visitors	-	-
4	Impact on surroundings/community	10	10%
5	Impact on business process (including IT process/downtime)	27	28%
6	Impact on supply chain	7	7%
7	Financial impact	13	14%
8	Legal impact/liability	3	3%
9	Environmental impact	4	4%
10	Damage to the reputation of the organisation	14	15%
11	Impact on public opinion	-	-
12	Physical damage to assets	8	8%
13	Data loss	11	11%
14	Data disclosure (including privacy sensitive data)	9	9%
15	Loss of data integrity	4	4%
16	Disclosure or loss of intellectual property	2	2%
17	Personal responsibility/accountability	2	2%
18	Damage to personal reputation	-	-
19	Management attention	2	2%
20	Personal liability	-	-
21	Personal financial loss (e.g. dismissal, loss of incentives)	-	-
22	Personal conscience	-	-
23	Regret of no or inadequate action	-	-
24	Probability/likelihood of risk	42	43%
25	Fear of a security risk	-	-
26	Involuntariness of risk taking	-	-
27	Uncontrollability of risk	-	-
28	Lack of knowledge about a risk	-	-
	Impact on trust	2	2%
	Impact on/for customers	5	5%
	Political/national impact	3	3%

It is remarkable to observe that only 43% of the respondents mentions the other main component of risk expressing uncertainty. Likelihood, probability, frequency or chance is mentioned only by 42 respondents. As almost all respondents mention impact criteria and less than half of them mentions likelihood there seems to be a predominant focus on impact/consequences.

Using the chi-squared tests there are no significant influences of individual characteristics observed. Education level, specific security trainings, age, and professional an security experience do not seem to influence the answers to the open ended questions.

4.2 Part two: rating criteria

In the second part of this study the predefined list of risk attributes is presented to the respondents. Each of the presented attributes can be independently rated using a five point Likert scale: extremely important, very important, moderately important, slightly important, not at all important. This list of attributes is considered an external stimulus to the respondents. It is analysed how this stimulus influences the priorities of the respondents.

The results show the influence of a stimulus: the respondents rate the majority of the attributes important even if they did not have them on top of mind at the first question. On average (the red graph in Fig.2) the rating concentrates in the vicinity of ‘very important’. The reliability analysis (Cronbach’s alpha) showed the rating to reach high internal reliability, $\alpha = 0.88$.

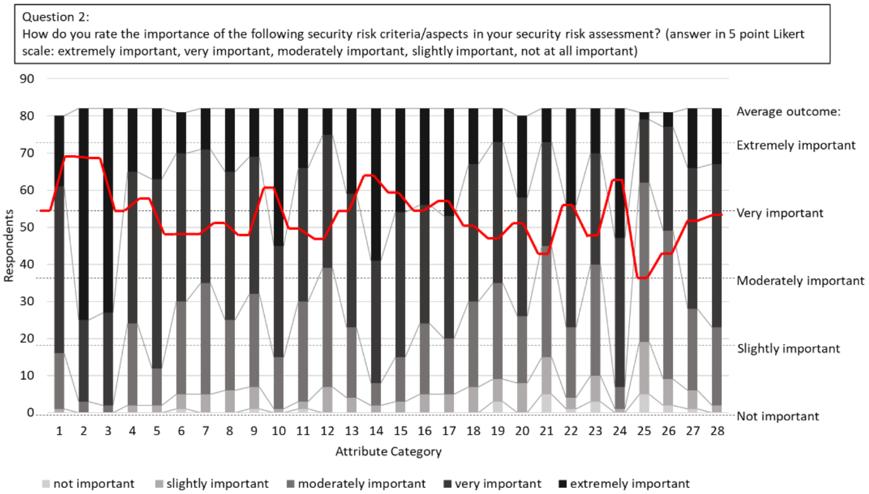
The absolute results of these answers are not considered of much value because the rating is assigned non-compensatory. The relative differences between the answers are considered of more value to be able to identify individual preferences.

The average answer is calculated by assigning a value to the Likert scale (extremely important is 5 points etc.). The Likert scale is thus considered a continuous variable.

Correlation analysis showed various significant but low to medium correlations between the individual attributes (r values between 0.212 and 0.640). The only strong and significant correlation is identified between attribute 2 and 3 ($r= 0.900$, $p<0.05$).

4.3 Part three: ranking the attributes

When rating the attributes as analysed in the previous section respondents do not have to compare the attributes and can express their preferences without the need to make trade-offs. In the third part of the survey, however, the respondents are asked to rank the attributes and compose their individual top 10 of most important attributes. This is a form of compensatory decision making in which the aspects of and preferences to an attribute need to be weighed. This kind of decision making takes considerable cognitive effort and is considered a system 2 process. Each respondent can freely assign a rank (1 is most important etc.) to the 28 predefined attributes. To avoid order bias the attributes are presented in a random order to each respondent. 70 respondents completed this ranking task correctly. For overall comparison each top 10 listing is assigned a value (a number 1 listing 10 points etc.).



Question 2:
How do you rate the importance of the following security risk criteria/aspects in your security risk assessment? (answer in 5 point Likert scale: extremely important, very important, moderately important, slightly important, not at all important)

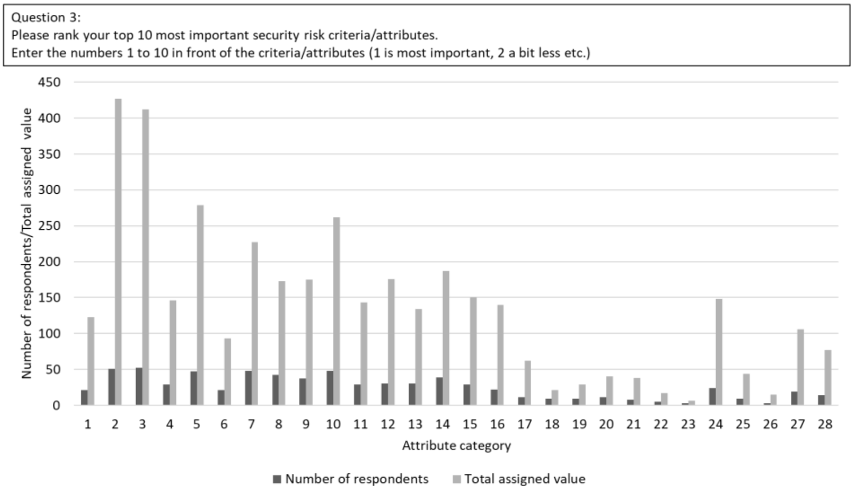
Figure 2: Descriptive analysis, rating of predefined risk attributes

The total value assigned to each attribute as well as the number of respondents listing an attribute in their top 10 is shown in Figure 3.

It is clear that the impact on health and safety of employees (attribute 2) and of customers, clients and visitors (attribute 3) are overall considered the most prominent attributes in security risk assessments. This is in line with the results of the attribute rating (see previous section). Attribute 2 is listed by 73% of the respondents, attribute 3 by 74%. At the answers to the open ended questions only 24% mentioned health and safety.

The predefined list, in this experiment considered a stimulus, seem to have changed preferences of a large group of respondents.

The other main component of risk assessments: likelihood or probability shows a very different pattern. At the open ended questions 43% of the respondents state they take this attribute into account. At the rating question this attribute is rated on average between very important and extremely important. At the ranking question, however, only 34% of the respondents rank it in their top 10. This attribute received in total 148 points and rank at the 11 place of important attributes. As stated above the attribute likelihood is often listed at the open questions in combination with impact in general.



Question 3:
Please rank your top 10 most important security risk criteria/attributes.
Enter the numbers 1 to 10 in front of the criteria/attributes (1 is most important, 2 a bit less etc.)

Figure 3: Descriptive analysis, ranking of predefined risk attributes

These respondents (29%) seem to follow the, easy accessible, general definition of risk in their answers (risk = likelihood x impact). As they ranked the more detailed impact attributes in the third question they clearly choose impact over likelihood and might even ignore likelihood completely. These results comply to previous work, probabilities of events are not easy to define and people often disregard probability entirely [13], [14].

Table 3: Comparing the 10 most prominent attributes over three assessment processes

	Question 1: When you **assess a security risk**, which criteria/attributes do you consider or take into account during your assessment? Please name the criterion and describe it briefly.		Question 2: How do you **rate the importance** of the following security risk criteria/attributes in your security risk assessment? (answer in 5 point Likert scale: extremely important, very important, moderately important, slightly important, not at all important)		Question 3: Please **rank your top 10** most important security risk criteria/attributes. Enter the numbers 1 to 10 in front of the criteria/attributes (1 is most important, 2 a bit less etc.)		
Top 10 rank	Top 10 is based on the proportion of the respondents listing attributes	% of resp.	Top 10 is based on the value the respondents assign to attributes (max. is 5: extremely important)	Av. rating	Top 10 is based on the combination of the proportion of the respondents listing attributes **and** the value they assign to them (a top 1 listing is 10 points, a top 9 is 9 points etc.)	Total pts	% of resp.
1	1 Perceived impact of the security risk	53%	2 Impact on health and safety of employees	4.78	2 Impact on health and safety of employees	427	73%
2	24 Probability/likelihood of risk	43%	3 Impact on health and safety of customers, clients or visitors	4.76	3 Impact on health and safety of customers, clients or visitors	412	74%
3	5 Impact on business process (including IT downtime)	28%	14 Data disclosure (including privacy sensitive data)	4.49	5 Impact on business process (including IT downtime)	279	67%
4	2 Impact on health and safety of employees	24%	24 Probability/likelihood of risk	4.44	10 Damage to the reputation of the organisation	262	69%
5	10 Damage to the reputation of the organisation	15%	10 Damage to the reputation of the organisation	4.36	7 Financial impact	227	69%
6	7 Financial impact	14%	15 Loss of data integrity	4.23	14 Data disclosure (including privacy sensitive data)	187	56%
7	13 Data loss	11%	5 Impact on business process (including IT downtime)	4.16	12 Physical damage to assets	176	43%
8	14 Data disclosure (including privacy sensitive data)	9%	17 Personal responsibility/accountability	4.15	9 Environmental impact	175	53%
9	12 Physical damage to assets	8%	22 Personal conscience	4.08	8 Legal impact/liability	173	60%
10	6 Impact on supply chain	7%	16 Disclosure or loss of intellectual property	4.06	15 Loss of data integrity	150	41%

Table 3 finally presents an overview of the top 10 most prominent attributes over the three survey parts. The results show differences in priorities. The reaction of the respondents is clearly influenced by the list of predefined attributes that is inserted in the survey as a stimulus. A large group of respondents changes their priorities.

5. Conclusions and Discussion

The survey set up provided interesting information about the priorities of attributes in a security risk assessment. This section starts with a summary of the main results, followed by conclusions and discussion.

The survey started with the open ended question: 'When you assess a security risk, which criteria/attributes do you consider or take into account during your assessment? Please name the criterion and describe it briefly.' This question allowed the respondents to answer based on their complete knowledge, perception and experience without restrictions and without any primer or influence from the researchers. The answers to these questions serve as an index of quickly or most available attributes. These are considered as most prominent by the security professionals at the point of time of answering the survey. The results show a predominant focus on impact attributes. Both in number of answers (192) as in the proportion of respondents mentioning one or more impact attributes (87%) this attribute category seems to be considered most relevant for security risk assessments. As a risk is often defined as a combination of uncertainty or likelihood and impact it is remarkable that less than half of the respondents (43%) mentions this second risk component. This might indicate that the likelihood of a security risk is not 'on top of mind' and might be considered less important.

The survey continued with a set of rating questions. The respondents are confronted with a list of 16 context impact attributes, 7 individual/personal impact attributes, a likelihood/probability attribute and four risk perception attributes. They are asked to rate the importance of each attribute using a five point Likert scale. The answers show a strong internal consistency and are, on average, centred around very important. The attributes rated highest are attribute 2: Impact on health and safety of employees (average 4.78 on a scale of 5) and

attribute 3: Impact on health and safety of customers, clients or visitors (average 4.76 on a scale of 5). These two attributes have reach strong correlation ($r= 0.90$, $p < 0.05$). The majority of the respondents rate these attributes extremely important (attribute 2: 69.5% of the respondents, attribute 3: 67.1% of the respondents) and very important (attribute 2: 26.8%, attribute 3: 30.4%).
The third part of the survey consisted of a ranking question: 'Please rank your top 10 most important security risk criteria/attributes'. In this part of the survey the respondents are forced to make trade-offs between their favourite attributes. This is considered to be compensatory decision making (system 2). As in the previous rating question the health and safety attributes (attribute 2 and 3) are considered most important by the respondents. Overall the ten most highly ranked attributes are all context impact attributes. It is remarkable that the likelihood/probability attribute is ranked in their top 10 by only 34% of the respondents and ended overall at the 11th place. These results clearly indicate a predominant focus on impact attributes in accessing security risks by security professionals. Both the personal/individual impact attributes and the risk perception attributes (based on the SCM model) are not considered of much relevance by the respondents when confronted with the compensatory ranking.

This explorative study clearly shows the influence of stimuli on decision making by security professionals. Attributes that are not 'on top of mind' and might even be, consciously or unconsciously, ignored in first instance, are considered very relevant after pointing to them. The most prevalent example are the two health and safety related attributes (attribute 2 and 3). They are only mentioned by 24% of the respondents in the first part of the survey. In the second part almost all respondents rate them extremely and very important while in the third part these attributes ended at the first and second place of the overall ranking. For real life daily praxis this could mean that without guidance the respondents take different attributes into account compared to if they are helped with tooling (in this case a predefined list). The consequence of this observed behaviour is that decisions made with or without tooling could be made on different grounds and define the outcome of the decision making process. A simple checklist could already help. Based on these results it can be concluded that attributes of security decisions that are considered extremely and very important by the majority of the respondents (see the rating question) are simply forgotten or ignored without help.

The second major finding is the lack of importance the security professionals in this study seem to appoint to likelihood/probability. At the open ended question less than half of the respondents (43%) mention likelihood or probability (87% of them mentions one or more impact attributes). At the rating, however, the majority rates it extremely important (43%) and very important (49%). When they are forced to compare the attributes in the third part of the survey only 34% of the respondents ranks likelihood/probability in their individual top 10. The assessment of likelihood or probability by people is based on their knowledge and beliefs and the assessments will thus vary over individuals. A subjective assessment of likelihood is hard for most people and they disregard likelihood entirely when confronted with risky choices [13].

Probability neglect is coined by Cass Sunstein [14]. According to him this cognitive bias explains disregarding probability when assessing low-probability but high-impact threats. People tend to focus on the impact and ignore likelihood when strong emotions are involved. He also relates these emotions to the availability heuristic. Affect-rich decisions increase probability neglect [15]. This cognitive bias does not state that people neglect the likelihood, in situations where they can envision the impact (availability heuristic) and experience strong emotions the likelihood of occurring becomes less relevant or even irrelevant to them. Sieron [16] added to this observation that, however the statistical likelihood of a high impact threat might be very small, people still want to avoid experiencing it. A small statistical likelihood does not mean this threat cannot affect the decisionmaker.

The respondents in this study might react according to these theories. The security risk domain is familiar to them so they can be expected to be able to envision the impact of security risks and threats. As it is there field of responsibility to decide upon or advice on managing these risks they can also be expected to feel affected by the possible impacts of these risks and threats. Finally, however small the statistical likelihood might be, the security risk or threat might materialize tomorrow and can affect their field of responsibility.

The important findings of this study might inspire other scholars to replicate them in other risk domains. They will raise awareness in both the academic as the professional security risk domain to the influence of cognitive biases on security risk decision making. This might lead to the development of de-biasing methods which can be added to existing security risk management processes enhancing security risk decision making. Managing security risks in organizations and society is of vital importance, understanding the decisions by individuals responsible for it is paramount.

Literature

[1] Talbot, J., & Jakeman, M., Security Risk Management Body of Knowledge (Vol. 69), John Wiley & Sons, 2011.

[2] Hansson, S. O., A Panorama of the Philosophy of Risk. Handbook of Risk Theory (pp. 27-54), Springer: New York, 2012.

[3] Möller, N., The concepts of risk and safety. Handbook of Risk Theory (pp. 55-85), Springer: New York, 2012.

[4] Cooke, R. M., Experts in Uncertainty, Oxford University Press: New York, 1991.

[5] Tversky, A., Koehler, D. J., Support Theory: A Nonextensional Representation of Subjective Probability. Psychological review, 101(4), 547, APA: Washington DC, 1994.

[6] Yates, J. F., Veinott, E. S., Patalano, A. L., Hard Decisions, Bad Decisions: On Decision Quality and Decision Aiding. Emerging Perspectives on Judgment and Decision Research (pp. 13-63), Cambridge University Press, 2003.

[7] Svenson, O., Differentiation and Consolidation Theory of Human Decision Making: A Frame of Reference for the Study of pre-and post-Decision Processes. Acta Psychologica, 80(1-3), 143-168, Elsevier: Amsterdam, 1992.

[8] Tetlock, P. E., The Impact of Accountability on Judgment and Choice: Towards a Social Contingency Model. Advances in experimental social psychology, 25(3), 331-376, Elsevier: Amsterdam, 1992.

[9] Kahneman, D., Thinking, Fast and Slow, Business Contact: Amsterdam, 2012.

[10] Pligt, J. van der, Vliek, M., The Psychology of Influence: Theory, Research and Practice, Taylor & Francis: Abingdon-on-Thames, 2016.Gilovich, T., Griffin, D., Kahneman, D., Heuristics and Biases: The Psychology of Intuitive Judgment, Cambridge university press, 2002.

[11] Ribeiro, R. A., Fuzzy Multiple Attribute Decision Making: a Review and New Preference Elicitation Techniques. Fuzzy sets and systems, 78(2), 155-181, Elsevier: Amsterdam, 1996.

[12] ANSI/ASIS/RIMS, Risk Assessment RA1, ASIS International: Alexandria, 2015.

[13] Evans, D., Risk Intelligence: How to Live with Uncertainty, Simon and Schuster: New York, 2015.

[14] Sunstein, C. R., Probability Neglect: Emotions, Worst Cases, and Law, The Yale Law Journal, 112(1), 61-107, New Haven, 2002.

[15] Suter, R. S., Pachur, T., & Hertwig, R., How Affect shapes Risky Choice: Distorted Probability Weighting versus Probability Neglect. Journal of Behavioral Decision Making, 29(4), 437-449, John Wiley & Sons, 2016.

[16] Sieroń, A.,Does the COVID-19 Pandemic refute Probability Neglect? Journal of Risk Research, 23 (7-8), 855-861, Routeledge, 2020.

CHAPTER 3

Bias and Noise in Security Risk Assessments, an Empirical Study on the Information Position and Confidence of Security Professionals

Johan de Wit, Wolter Pieters, Pieter van Gelder

As the level of information is equivalent to the level of uncertainty in risk assessments, it is paramount to explore the level of information the security professionals have available in their daily practice. In this chapter this level is identified and the consequences for confidence and risk assessments is explored.

This paper is published in *Security journal* at 06 July 2023 (Springer Nature).

Abstract

Professionals working in both the physical and cybersecurity domain need to assess and evaluate security risks. As information on risks in general and security risks in particular is often imperfect and intractable, these professionals are facing a challenge in judging both likelihood and consequences, but how much do their existing psychological biases play a role in these judgments? In this paper we present new empirical evidence on the perception of the information position and confidence levels of security professionals, the influence of detailed information and the conjunction fallacy, and the level of noise in security assessments. This paper adds to the literature by examining, for the first time, risk assessments by professionals in realistic, real life, security cases. The results show clear indications for overconfidence, comparative ignorance, influence of the conjunction fallacy, and influence of individual experience on security decision making in the professional security domain. The observed phenomena might have far reaching effects on security risk management in organizations and society.

1. Introduction

The security risk field is dealing with malicious, and therefore, man-made, risks. These risks vary from physical security risks like intrusions, theft, holdup's all the way to cyber security risks like hacking attempts, ransomware attacks, and IP theft. Nowadays these two domains converge as physical and cyber attacks and threats collide into hybrid threats. To manage these risks, both governments and organizations have introduced security management processes and security staff to assess, evaluate, and manage security risks (ANSI/ASIS, 2012; ASIS_International, 2015). Security staff, further referred to as security professionals, are educated and trained to perform these tasks. They need to decide, on a daily basis, which risks to take into account, decide how to evaluate them and which security controls to implement.

These decisions are not easy though. In the case of future events originating from complex interactions between multiple independent human agents, occurrence frequency or probability data are often lacking. The assessment of the uncertainty of security risks, therefore, is often based on expert judgment rather than based on evidence or objective data (Möller, 2012; Talbot & Jakeman, 2011).

As part of their role security professionals are expected to address this uncertainty and form a predictive judgment. Their judgment is often the primary input for risk decisions and allocation of resources (Alruwaii & Brooks, 2008). At the same time, human decision making has proven to be not only based on reasoning but is prone to mental short cuts or heuristics, and biases which are defined as systematic deviations from reasoning (Gigerenzer & Selten, 2002; Kahneman, 2012; Simon, 1982; Slovic, 2000; Tversky & Kahneman, 1975). As the security of society and organizations is thus heavily depending on the individual, subjective judgment of security professionals, understanding their decisions based on their assessments, is paramount to understand security risk management.

In this paper, we present the results of a study in which we ask security professionals to indicate their information position (the level of availability of precise information and/or evidence) when assessing security risks, and to estimate the likelihood of realistic security events for which we vary the descriptions to explore the influence of more or less information. These experiments are based on the conjunction fallacy, predicting that likelihood estimates increase when case descriptions have more specific information, whereas they should actually decrease. Beside the corresponding bias in security risk judgments, the predictive judgments of the individual security professionals might show noise, i.e., a between-subject variance in likelihood estimates within a single condition, where one would hope that different experts give similar judgments instead.

This empirical study will answer the following questions:

- do security professionals usually have exact information on security risks,
- are they usually confident about their predictive judgments,
- would more information grow their confidence,
- is their judgment of likelihood depending on more or less information
- do security likelihood judgments vary under influence of the conjunction fallacy.

The influence of individual expertise of these questions is analyzed. As the future cannot be certain by nature, professionals might be expected to ‘know that they cannot possibly know’ (known unknowns). Based on this the confidence of security professionals in their predictive judgments can be expected to be limited.

In the next section the theory on security risks, predictive judgments, expert judgment, bias, and noise are briefly discussed. In the section research method the experiments and survey setup are detailed followed by a section in which the results are analyzed. The paper ends with a discussion section and conclusions.

2. Theory and Background

Security teams are tasked to manage security risks to keep them at an acceptable level. The individuals responsible for managing and accessing security risks, in this study referred to as security professionals, often, if not always, apply a risk management process of some sort to structure their assessment.

Risks are defined as the effect of uncertainty on objectives (ISO, 2018). In this definition an effect is understood as a deviation, positive or negative, from the expected, often referred to as consequences. The uncertainty of risks is usually referred in terms of their likelihood. "Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood" (ISO, 2019, p. 6). The understanding and judgment of a risk are, thus, related to the availability of information about it. As Hansson states: 'Knowledge about a risk is knowledge about the unknown' (Hansson, 2012, p. 34).

Various risk management processes consist of subsequent process stages: establishing the context, risk identification, risk analysis, risk evaluation and risk treatment (ANSI/ASIS/RIMS, 2015; Information_Security_Forum, 2018; ISO, 2018; ISO/IEC, 2011). They also stipulate feed-back loops to establish an on-going, recurring process. As explained in the introduction, this is inherently a decision-making activity, involving decisions on how to evaluate and treat the risks.

Entering the domain of decision making opens up centuries of research, debate, and established theories and practices. Individual decision making is studied ever since the ancient Greek philosophers. As Aristotle stated: the origin of action is choice, and that of choice is desire and reasoning … good action and its opposite cannot exist without a combination of intellect and character' (Allingham, 2002). During the last half century renown scholars have unraveled human decision making and especially the cognitive processes guiding them (Baron, 2004; Carbone et al., 2017; Slovic, 2010).

So far, however, little scientific studies are conducted exploring individual decision making by security professionals in their daily praxis of security risk decision making. These professionals play a decisive or advisory role in security risk treatment; hence, they are determining or at least influencing the security in organizations and society. Understanding their individual preferences and priorities, and the role of information and uncertainty, is of vital importance to understand their security risk judgment.

Judgment of the uncertainty component of risks is related to the deficiency, or in other words availability, of information of an event. Intractable uncertainty is the result of a lack of information than cannot possibly be known (Kahneman, 2021). Even with unlimited resources and/or time this information cannot possibly be learned. On the other hand there is imperfect information, information that could be known but is not. Risk decision makers can decide to retrieve more information and enhance their imperfect information position. Often decision makers should or could know that the information they need to decide on is imperfect or even intractable. Many decision makers, however, seem to ignore their lack of information. This attitude is referred to as objective ignorance (Kahneman, 2021). The obvious fact that the future is hard or even impossible to predict is often ignored by decision makers (Jain et al., 2013). This attitude of ignorance allows decision makers to have confidence in their decision making, and they mistake their confidence for predictive validity (Kahneman et al., 2021).

In the security domain, both intractability and imperfect information contribute to a lack of risk information and a situation of ambiguity, a situation in which likelihoods either do not exist or are not known (Carbone et al., 2017). It is, therefore, often supplemented or even replaced by subjective expert judgment (Möller, 2012).

Expert judgment is considered a degree of belief, based on tacit knowledge and expertise (Cooke, 1991). Subjective interpretation, further referred to as judgment, forms the primary input for security risk assessments and risk management processes. Individual judgment is based on the available information, tacit knowledge and 'hard-to-measure' expertise. As this judgment is meant to assess risks, which are possible future events, it is referred to as predictive judgment. The outcome of some of these predictive judgments might become clear in the (near) future and in this cases these judgments can be verified. Examples of these are weather forecasts or predictions on elections. If the predictive judgments involve probabilistic predictions they are often, if not always, non-verifiable (Kahneman et al., 2021). If for example the predictive probabilistic judgment of a risk materializing is 15%, whether or not this particular risk materializes does not allow to verify the judgment. The probability judgment of 15% means this risk materializes 15% of the times in similar circumstances. This prediction of 15% will be valid whether or not this risk materializes. Only after a substantial amount of time and 'similar circumstances,' it might become clear if 15% of the time in similar circumstances is a valid predictive judgment. Due to characteristics of security risks and their large variety of modus operandi, the similarity of circumstances is questionable and thus predictions for security risks can be regarded as non-verifiable by nature.

The huge body of knowledge on judgment and decision making under risk has identified numerous flaws in individual assessments and judgment. Beside biases, which are defined as systematic deviation, human judgment is susceptible to noise (see Figure 1). Previous work by the authors concluded that security professionals are vulnerable to decision biases to the same extent as lay people (de Wit et al., 2021). Noise, or precision, is the unwanted variability in professional individual judgments. When confronted with the exact same context and information individuals, even trained professionals, can reach different conclusions, often even very different based on personal characteristics (Andersson et al., 2020). Noise or system noise can be differentiated in between subjects noise: level noise, and within subjects noise: pattern noise and occasional noise (Kahneman, 2021). Level noise is a categorial, systematic, difference between individuals. Based on personal beliefs, convictions or opinion the judgment of one individual can systematically differentiate from the judgment of another individual (Andersson et al., 2020). A security professional can for example be more risk averse in general than another and based on that reach other judgments. Pattern noise is an individual, case by case, variation of an individual. Some specific aspects of security risks can evoke a stronger response by a security professional for example because of previous experiences (Dumm et al., 2020). So the judgment of an individual professional on average might show high risk tolerance except for, for example, holdups where this individual can be very risk averse due to a personal experience. Finally there is substantial evidence that noise is influenced by the occasion. The time of day, the weather, mood etc. influences judgment of individuals.

The influence of the phenomena bias and noise on human judgment has led many scholars to question the viability of such uncertainty assessments. Still in many domains, like security, there are no alternatives or objective procedures available (Hansson, 2012; Möller, 2012; Tversky & Kahneman, 2004). Therefore, predictive, intuitive judgments of uncertainty play an essential role in these decisions (Charness et al., 2020; Kuhn & Sniezek, 1996; Tversky & Koehler, 1994).

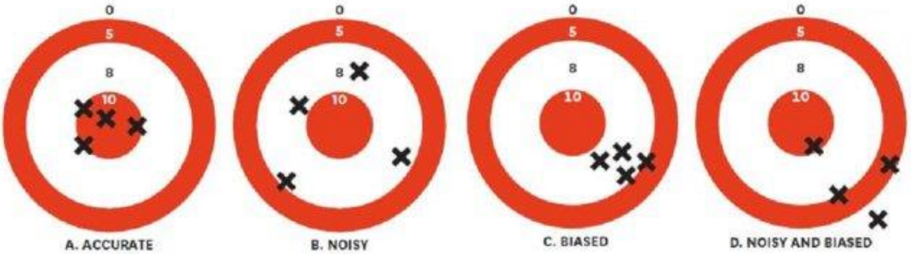


Figure 1: Target shooting as metaphor explaining bias (accuracy) and noise (precision), reprinted with permission from "Noise: How to Overcome the High, Hidden Cost of Inconsistent Decision Making" by Daniel Kahneman, Andrew M. Rosenfield, Linnea Gandhi, Tom Blaser. Harvard Business Review, October 2016. Copyright 2026 by Harvard Business Publishing; all rights reserved.

In this study for the first time, to the best of our knowledge, security risk assessments by security professionals are analyzed to explore the influence of information on bias and noise. The respondents in this study are confronted with case descriptions of realistic security risk assessments and are asked to assess the level of likelihood of each case. By randomly varying the presented information between groups of subjects variations of the likelihood assessments can be observed. These variations might be caused by both biases (accuracy) and noise (precision). Comparing the average group assessments shows possible biases (between group comparison) while the within group analysis shows possible noise.

A convenience sample of practitioners form both the security and cybersecurity domain are confronted with realistic security cases with a varying level of information to explore the influence of more or less detailed information on individual likelihood assessments. These experiments relate to the renowned conjunction fallacy. This fallacy identifies a phenomenon that shows that more detailed information of a situation leads humans to perceive an event as more likely. Logic reasoning, however, would lead to the exact opposite conclusion. Various other scholars have identified very consistent behavior influenced by the conjunction fallacy (Bonini et al., 2004; Fantino et al., 1997; Fiedler, 1988; Gigerenzer, 1991; Hertwig & Gigerenzer, 1999; Ludwin-Peery et al., 2020; Stolarz-Fantino et al., 2003; Tentori et al., 2004; Tentori & Crupi, 2012; Tversky & Kahneman, 1983).

Many of these studies, however, are based on hypothetical situations in laboratory settings which do not seem to explain real-life behavior (Charness et al., 2020). These studies often involve lay people as respondents who might not be representative for real-life decision makers as risk taking is domain specific (Charness et al., 2020). Our study, on the other hand, investigates judgments of security practitioners on realistic, real-life, cases. The experiments in this study compare between subjects judgments based on different sets of information. The conjunction fallacy is very suitable to explore the systematic deviation caused by more or less detailed information.

In this study several phenomena regarding information, judgment and confidence are explored in the professional security domain. First professionals working in the security domain are questioned about their information position when assessing likelihood and consequences of security risks in real life. As risks are uncertain by nature and especially on risks in the security domain information is often limited or lacking, it is expected that security professionals will acknowledge this. Second: based on this expected meager information position it is hypothesized that security professionals might show modest confidence in their assessments. Third: more experience, training, and education, thus building individual expertise, on the other hand, is expected to raise and individuals confidence level. Fourth: the possible differences in individual likelihood assessments (noise) are inquired. It is hypothesized that professionals with comparable expertise will reach comparable likelihood assessments in identical case studies. Finally it is expected that varying detailed security case information, by applying the conjunction fallacy, will influence likelihood assessments of security professionals.

3. Research Method

For this study an online survey is set up with Qualtrics survey software. We will investigate both the physical security as well as the cyber security domains. However, related, the physical and cybersecurity domain differ in risk and threat context. The surveys for the two domains are kept identical except for the case descriptions of the two cases as will be detailed below.

The survey starts with questions on the information position of the security professionals in real life on both likelihood and consequence, the two main components of a risk assessment. They are asked how often they:

- know the likelihood exactly,
- do not know the likelihood exactly but have quantified information,
- do not know the likelihood exactly but can estimate the likelihood,
- do not know the likelihood exactly and cannot estimate it.

The respondents can answer these questions using a five point Likert scale: always, most of the time, about half of the time, sometimes, never. These four questions are repeated for the consequences. The results of these questions indicate the real-life information position of the security professionals in this study and might confirm the position of many scholars that in (security) risk assessments often accurate information is lacking.

These questions are followed by questions about the confidence the respondents feel about their assessments for both likelihood and consequence. A third question asks if the respondents would feel more confident if they would have more information about security risks. The respondents can answer these questions using a similar five point Likert scale: always, most of the time, about half of the time, sometimes, never.

Note that the order of these questions forces the respondents to evaluate their information level and get aware of their (lack of) information first. The questions on their confidence level are answered, thus, in full awareness of their available information. Combined the information and confidence questions indicate the level of objective ignorance (knowing/being aware information is lacking and still have confidence in your judgment).

The core of the survey consists of three cases testing the conjunction fallacy. Two of these cases consist of a case description followed by a question asking for a likelihood judgment (Cases 1 and 2). The third case is a replication of the original problem statement as used by Kahneman and Tversky. The context is reformulated to fit the security domain. As this reformulated problem shows the conjunction fallacy in plain sight, logic reasoning or recognition of the fallacy might influence the assessment of the respondents in the other two cases. Therefore, the reformulated problem is presented to the respondents as the third and final case study.

The reformulated problem consists of a short case description followed by a choice between two options. The respondents are asked to indicate which option they consider more likely. The first option has a general and short formulation. The second one is identical to the first option but is extended with more detailed information. Showing the two answers at the same time, in other words showing the conjunction rule, should or could guide the respondents to choose the shorter, more general, option. The second, more detailed, option, obviously is a sub-set of the first and should, therefore, be considered less likely.

The reformulated problem is kept identical for both the physical and cybersecurity community:

Case introduction:

Your organization is a large, international, pharmaceutical corporation based in the EU. Your R&D department has focused the last months on research in developing a COVID-19 vaccine. This department made considerable progress and is considered to be one of the global front runners and ahead of other research institutes. Last week you discovered a serious attempt to steal information.

What is more likely:

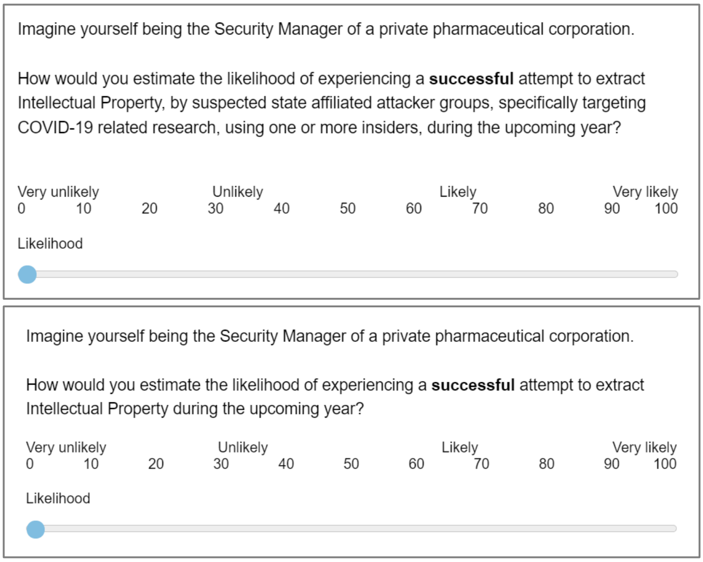
o *This attack is launched by an organized crime organization*

o *This attack is launched by an organized crime organization targeting IP (Intellectual Property) related to COVID-19 research*

Note: this case is developed and presented to the respondents before in the real world COVID-19 vaccines were available. At the time the surveys were conducted in both the physical and cybersecurity domain several pharmaceutical corporations around the world were in the race of developing vaccines and there were indications (in the press) of attempts of IP theft at these kind of corporations. This case description can, therefore, be considered realistic.

Cases 1 and 2 are based on the same approach as the reformulated problem; however, in these two cases, the respondents are asked to estimate the likelihood of the case. Of each case there are two versions, a short and an extended version where three additional information elements are added. The respondents are automatically and randomly assigned to either the short or the extended version in a way that each respondent is offered one short version of an case and an extended version of the other. About half of the respondents first assessed the short version of Case 1 followed by the extended version of case 2 (group A). The other part of the respondents first assessed the extended version of case 1 followed by the short version of case 2 (group B). The likelihood estimation can be answered via a slider on a scale which offers the respondents both a probability scale (0-100%) and a qualitative likelihood scale (very unlikely, unlikely, likely, very likely). In Figure 2 the short and extended version of the same case are shown including the slider scale. After each case the respondents are asked to rate the importance of each information element for their likelihood assessment using a three point Likert scale (very important, important, not important). These two cases do not show or refer to the conjunction fallacy in any way. The respondents have no indication that they are offered a short or extended version.

To fit the two cases to the two domains, physical and cybersecurity, the description is adjusted to reflect domain specific realistic and recognizable cases. Case 1 is almost identical to the already discussed reformulated Problem (Case 3). The description of case 2 is made more specific for each domain. All case descriptions are based on real-life incidents or threats that were available in public sources (often in the press) at the time of conducting the surveys. Thus, they can be considered realistic. The structure of the cases and the number of additional detailed information aspects is identical for both domains. Table 1 shows all the case descriptions.



Imagine yourself being the Security Manager of a private pharmaceutical corporation.

How would you estimate the likelihood of experiencing a **successful** attempt to extract Intellectual Property, by suspected state affiliated attacker groups, specifically targeting COVID-19 related research, using one or more insiders, during the upcoming year?

Imagine yourself being the Security Manager of a private pharmaceutical corporation.

How would you estimate the likelihood of experiencing a **successful** attempt to extract Intellectual Property during the upcoming year?

Figure 2: examples of the extended (top) and short (bottom) version of the security case experiment for the physical security domain showing the slider with the double scale

Finally the respondents are asked to express their expertise in a number of questions about individual characteristics. They are asked to indicate their age, number of years professional experience and number of years security experience. The current function of the respondents is asked including the number of years in this position. Finally they are asked to indicate their general education level (associate degree, bachelor degree or Master degree/PhD) and if any specific security trainings are completed. These individual characteristics may influence the individual assessments of the respondents.

The explorative results are retrieved via this online survey conducted between September 2020 and February 2021. Participation in the survey is promoted in both the IT and physical security professional community. It is promoted via LinkedIn and Twitter, both in general and in special interest groups like Security management, ASIS Europe and ASIS International, Dutch cybersecurity platform. Second, a direct email campaign is launched targeting the existing professional network of the researchers. Third, the survey is promoted via the Information Security Forum world conference: Digital 2020 (cybersecurity domain) and ASIS Europe 2021 conference (physical security domain). The sample of respondents (N = 166) is regarded a convenience sample.

Table 1: case descriptions differentiated for the physical and cybersecurity domain, divided in group A and B (italic text indicates the three additional detailed information aspects in the extended case description)

Cybersecurity domain		**Physical security domain**	
Group A:	**Group B:**	**Group A:**	**Group B:**
Case 1 short:	**Case 1 extended:**	**Case 1 short:**	**Case 1 extended:**
Imagine yourself being the CISO of a private pharmaceutical corporation. How would you estimate the likelihood of experiencing a successful attempt to extract Intellectual Property during the upcoming year?	Imagine yourself being the CISO of a private pharmaceutical corporation. How would you estimate the likelihood of experiencing a successful attempt to extract Intellectual Property, *by suspected Chinese attacker groups, specifically targeting COVID-19 related research, using spear phishing techniques,* during the upcoming year?	Imagine yourself being the Security Manager of a private pharmaceutical corporation. How would you estimate the likelihood of experiencing a successful attempt to extract Intellectual Property during the upcoming year?	Imagine yourself being the Security Manager of a private pharmaceutical corporation. How would you estimate the likelihood of experiencing a successful attempt to extract Intellectual Property, *by suspected state affiliated attacker groups, specifically targeting COVID-19 related research, using one or more insiders,* during the upcoming year?
Case 2 extended:	**Case 2 short:**	**Case 2 extended:**	**Case 2 short:**
Imagine yourself being the CISO of a Fortune 500 corporation. How would you estimate the likelihood of experiencing a successful attempt to execute a ransomware attack, *by criminal Russian hacker groups, using new targeted ransomware like WastedLocker, targeting the main ERP system (Enterprise Resource Planning),* during the upcoming year?	Imagine yourself being the CISO of a Fortune 500 corporation. How would you estimate the likelihood of experiencing a successful attempt to execute a ransomware attack during the upcoming year?	Imagine yourself being the Security Director of a fortune 500 logistics corporation. How would you estimate the likelihood of experiencing a successful attempt *of bribery of employees of subcontractors, by organized crime organizations,* to facilitate international drug trafficking, *using maritime transport,* during the upcoming year?	Imagine yourself being the Security Director of a fortune 500 logistics corporation. How would you estimate the likelihood of experiencing a successful attempt to facilitate international drug trafficking, during the upcoming year?

4. Results and Analysis

The results on the information position of the professionals are presented in Table 2. The security professionals indicate that, on average, about half the time they know the likelihood and consequences exactly. The respondents also indicate that they, on average, only sometimes, cannot estimate likelihood and consequences. One in four even indicates that they can always estimate likelihood and consequences, based on their experience and knowledge, even when they indicate they know they do not have accurate information.

Table 2: The information position of security professionals in security risk assessments.

When evaluating security risks in general:	Always (1)	Most of the time (2)	About half the time (3)	Some-times (4)	Never (5)	Median answer	Mean answer*
I know the **likelihood** of security events **exactly**	2.0%	33.0%	19.3%	24.9%	20.8%	About half the time	3.29
I do not know the **likelihood** exactly but I have **quantified** information (evidence based probability)	4.6%	38.1%	23.4%	29.9%	4.1%	About half the time	2.91
I do not know the **likelihood** exactly but I **can estimate** the likelihood based on my experience and knowledge	9.6%	51.3%	23.9%	14.7%	0.5%	Most of the time	2.45
I do not know the **likelihood** exactly and I **cannot estimate** the likelihood based on my experience and knowledge	0.5%	13.7%	8.1%	54.3%	23.4%	Sometimes	3.86
I know the **consequences** of security events **exactly**	3.3%	42.4%	21.2%	19.6%	13.6%	About half the time	2.98
I do not know the **consequences** exactly but I have **quantified** information (evidence based probability)	3.3%	39.7%	20.7%	31.5%	4.9%	About half the time	2.95
I do not know the **consequences** exactly but I **can estimate** the likelihood based on my experience and knowledge	7.1%	49.5%	21.7%	19.6%	2.2%	Most of the time	2.60
I do not know the **consequences** exactly and I **cannot estimate** the likelihood based on my experience and knowledge	0.5%	12.0%	8.7%	50.5%	28.3%	Sometimes	3.94
** considering the Likert scale a continues variable from always = 1 to never = 5*							

Overall they claim to be confident about their judgment of likelihood and consequences most of the time (see Table 3).

Table 3: Confidence levels of security professionals.

When evaluating security risks in general:	Always (1)	Most of the time (2)	About half the time (3)	Sometimes (4)	Never (5)	Median answer	Mean answer*
I feel confident about my assessments of the **likelihood** of security risks	8.3%	59.4%	20.0%	10.6%	1.7%	Most of the time	2.38
I feel confident about my assessments of the **consequences** of security risks	9.4%	64.4%	15.6%	9.4%	1.1%	Most of the time	2.28
I would feel **more confident** if I had more information on security risks	28.9%	33.3%	8.9%	27.8%	1.1%	Most of the time	2.39
** considering the Likert scale a continues variable from always = 1 to never = 5*							

Individual characteristics might influence confidence. The respondents are asked to indicate their age, number of years professional experience, number of years security experience, the number of years in their current position, their general education level (associate degree, bachelor degree or Master degree/PhD) and if any specific security trainings are completed. To reduce this number of characteristics and explore their structure and influence all six items were subjected to an exploratory factor analysis with oblique rotation. The Kaiser-Meyer-Olkin measure verified the sampling adequacy for the analysis, KMO = 0.741, Bartlett's test of sphericity v2 (15) = 302.18, $p < 0.005$, indicating that correlation structure is adequate for factor analyses.

Factor 1, reflecting experience, is comprised of four characteristics (age, number of years professional experience, number of years security experience, the number of years in their current position) that explain 44.4% of the common variance from all variables with factor loadings of 0.647 to 0.894. Factor 2 reflects specific security trainings and is comprised of one characteristic explaining 17.2% of the variance with a factor loading of 0.840. The final factor, reflecting education level, explains 16.6% of the variance with a factor loading of 0.840. All three factors have Kaiser's criterion of eigenvalues equal or greater than 1 and are sufficiently orthogonal to each other.

To assess the relationship between these factors and the confidence level of the respondents a Spearman's rank correlation is computed between the three factors and the three questions of Table 3.

Factor 1, experience, shows a negative correlation with the likelihood confidence level, r(164) = -0.158, p = 0.043. This factor also shows a negative correlation with the consequence confidence level, r ((164) = -185, p = 0.017. Finally this factor shows a positive correlation with the confidence vs need for information level, r(164) = 0.229, p = 0.003. These results show that more experience significantly raises the number of occasions in which the respondents have confidence in their own assessments of likelihood and consequences. More experience, on the other hand, significantly reduces the number of occasions in which the respondents would require more information to be more confident.

No significant correlations are discovered between security specific trainings, factor 2, and confidence levels. These results indicate that completing security specific trainings do not influence the level of confidence of the respondents in their own assessments.

The third and final factor, education level shows a significant positive correlation with the likelihood confidence level, r(164) = 0.179, p = 0.021, and the consequence confidence level, r(164) = 0.239, p = 0.002. No significant correlation is noted between factor 3 and the confidence vs need for information level. A higher education level, thus, leads the respondents to less occasions in which they are confident about their assessments of likelihood and consequences.

Table 4 shows the combined results of the first knowledge question as it asked for the most exact information (Table 2) and the confidence questions. A normative assumption might be that respondents that indicate to have exact information can be expected to be confident about their assessments and the opposite. Following this assumption the diagonal from the upper left corner (always exact knowledge and always confident) to the lower right corner (never exact knowledge and never confident) show the respondents which seem to align their knowledge and confidence. As stated in the introduction exact knowledge on future events is considered intractable knowledge. The respondents in the dotted oval, more than half of the respondents (likelihood: 54.4%, consequences: 67.2%), thus, seem to overestimate their knowledge. The lower left area (gray) contains respondents confirming to lack exact information most often but are often confident about their assessments. These respondents (likelihood: 33.3%, consequences: 22.8%) seem to show objective ignorance being more confident than their information position would permit.

Table 4: Information vs confidence levels of security professionals (in number of respondents).

When evaluating security risks in general:	I feel confident about my assessments of the **likelihood** of security risks					
Note: in number of respondents	Always	Most of the time	About half the time	Some-times	Never	**Total:**
I know the **likelihood** of security events exactly:						
Always	2	1	-	-	-	3
Most of the time	11	45	7	1	-	64
About half the time	2	22	8	1	0	33
Sometimes	-	25	13	2	1	41
Never	-	14	8	15	2	39
Total:	15	107	36	19	3	180
When evaluating security risks in general:	I feel confident about my assessments of the **consequences** of security risks					
Note: number of respondents	Always	Most of the time	About half the time	Some-times	Never	**Total:**
I know the **consequences** of security events exactly:						
Always	2	4	-	-	-	6
Most of the time	14	56	6	1	-	77
About half the time	1	26	11	1	-	39
Sometimes	-	22	6	4	1	33
Never	-	8	5	11	1	25
Total:	17	116	28	17	2	180

Case 1

Figure 3 shows the results of case 1 (the results of both the physical and cybersecurity domains are combined). Professionals working in the same domain with comparable general knowledge reach, based on identical information, likelihood assessments ranging from 0%-100% for the short version of case 1 (n = 90) and 10% to 100% for the extended version of case 1 (n = 87).

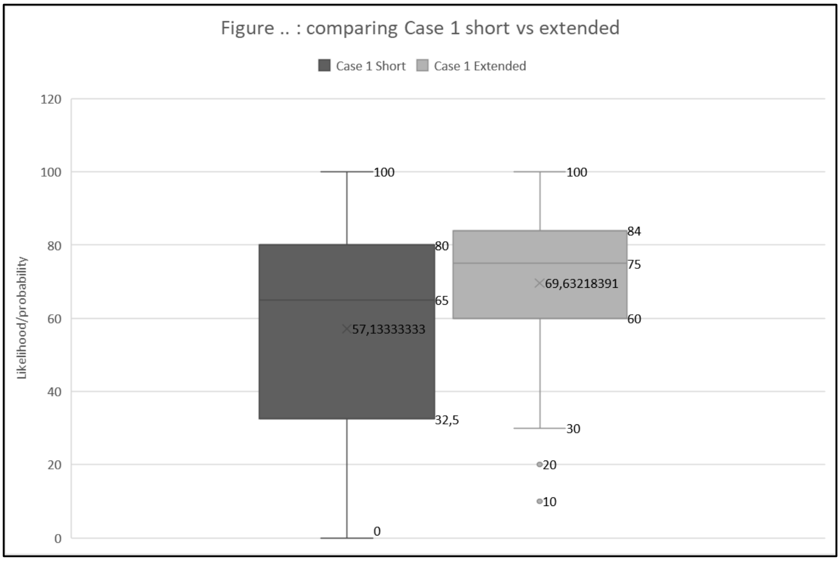


Figure 3: results of likelihood assessments of case 1

The median answer for case 1 short is 65%, the average answer is 57.1% (M = 57.1, SD = 26.33, Q1 = 32.5%, Q3 = 80%). The median answer for case 1 extended is 75%, the average answer is 69.6% (M = 69.6, SD = 21.56, Q1 = 60%, Q3 = 84%). An independent sample T-test is conducted to compare these assessments: the identified average difference of 12.5% is significant, t(175) = -3.449, p = 0.001.

The group of respondents assessing the extended case, including specific conditions, estimated the likelihood on average at 69.6% while the group assessing the short version of the same case, thus, without specific conditions, estimated the likelihood 57.1%. This significant mean difference seems to express the effect of the conjunction fallacy (the assumption that more specific conditions are more probable).

Case 2

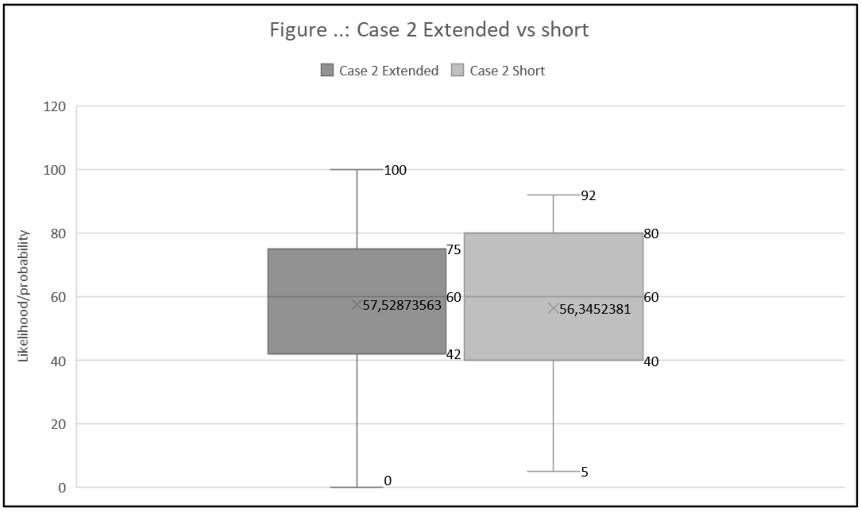


Figure 4: results of likelihood assessments of case 2

Figure 4 shows the results of case 2. The results of this case show almost no influence of the conjunction fallacy. The average likelihood assessment of the case 2 extended option is only slightly higher (M = 57.5%, SD = 24.43, n = 87) than the average likelihood assessment of the case 2 short option (M = 56.3%, SD = 23.83, n = 84). This difference is not significant.

The results of case 1 seem to show the effects of the conjunction fallacy while the results of case 2 do not. This different average reaction to these two cases can be caused by either the difference between the content of the cases (the structure and number of specific conditions of the two cases is identical) and/or a possible difference between the two randomly assigned groups. The difference in content of the two cases will be analyzed in the discussion section. As the structure of the two cases is identical for this section we assume they would evoke comparable reactions.

Table 5 shows the composition of the two groups in which the group of respondents confronted with the short version of case 1 first followed by the extended version of case 2 is denoted as group A. Group B assessed the extended version of case 1 first followed by the short version of case 2.

Both groups reacted similar to the conjunction fallacy as presented in the reformulated problem (case 3). Three out of four respondents of both groups selected the answer with more specific conditions and thus show vulnerability for the conjunction fallacy.

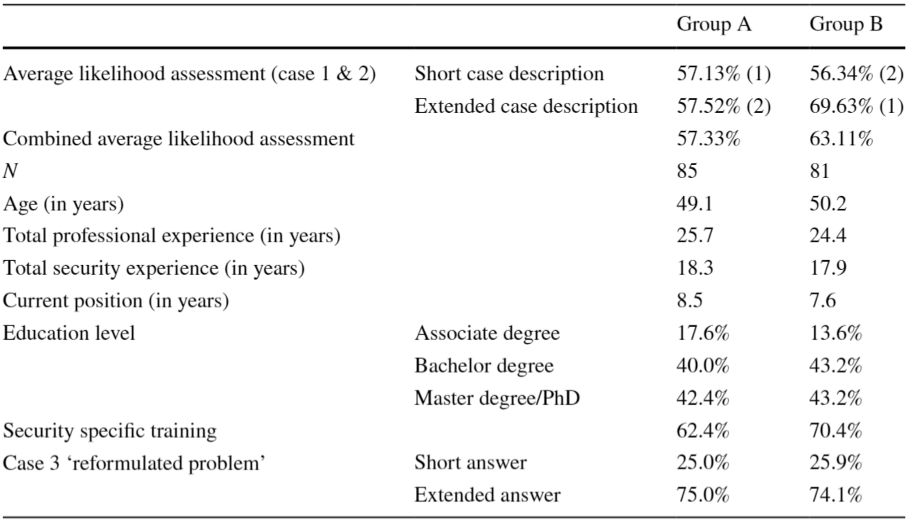
There are also no significant differences between average individual characteristics of the two groups. As there seems to be no indication for a difference between the groups and they are equally vulnerable to the conjunction fallacy, we might expect comparable risk assessments.

Combining the average likelihood assessments of the two cases for each individual respondent shows an average for the respondents in group A of 57.33% while the respondents in group B on average assess the likelihood 63.11%. On average group B estimates the likelihood of the combined two cases 5.8% higher (absolute difference) which is a relative difference of 9.2%.

Case 3 Security Conjunction: the reformulated problem

A total of 165 respondents answered the reformulated problem. 42 (25.5%) considered the first (short) option more likely, 123 (74.5%) the second (extended) one. In the physical security domain 58.8% of the respondents followed the fallacy and choose the extended option. Of the respondents active in the cybersecurity domain even 81.6% selected the extended option.

Table 5: Comparing characteristics of randomly composed groups A and B.



		Group A	Group B
Average likelihood assessment (case 1 & 2)	Short case description	57.13% (1)	56.34% (2)
	Extended case description	57.52% (2)	69.63% (1)
Combined average likelihood assessment		57.33%	63.11%
N		85	81
Age (in years)		49.1	50.2
Total professional experience (in years)		25.7	24.4
Total security experience (in years)		18.3	17.9
Current position (in years)		8.5	7.6
Education level	Associate degree	17.6%	13.6%
	Bachelor degree	40.0%	43.2%
	Master degree/PhD	42.4%	43.2%
Security specific training		62.4%	70.4%
Case 3 'reformulated problem'	Short answer	25.0%	25.9%
	Extended answer	75.0%	74.1%

5. Conclusions and Discussion

On average the respondents indicate that they have exact or quantified information about likelihood and consequences about half the time. This finding deviates from the expectation that security professionals would recognize their information position about security risks as both imperfect and intractable. However, they also indicate that they can estimate the likelihood and consequences most of the time (and only sometimes cannot estimate at all). Assuming that the respondents are right about their knowledge position they assess risk half of the time based on information (evidence based). On the other hand they assess security risks without proper information also half of the time and still come up with an estimation of likelihood and consequences. As these assessments have a serious impact on security risk decision making and the allocation of resources to manage, mitigate and/or accept these risks, it is worth noting that these decisions do not seem to be based on evidence about half of the time.

The perception of the respondents on their information position can be questioned. As risk assessments are in fact predictive judgments and the information about the future can be considered intractable by nature, this perception of the security professionals can be considered audacious.

Overall the majority of the security professionals in this study indicate that they are always or most of the time confident about their assessments (for likelihood assessments 67.7%, for consequence assessments 73.8%). This level of confidence can be considered in agreement with the information position considering the perceived information position of the professionals as indicated above. It was hypothesized that the security professionals would show modest confidence based on the assumption that exact and/or evidence based information on security risks is often lacking. They, however, seem to ignore the latter and thus show a higher level of confidence than expected. As the respondents on average indicate to hold exact or quantified information only half of the time, they, thus, might be considered overconfident about their risk assessments. Combining the perceived information position of the professionals with their confidence reveals objective ignorance. A portion of respondents indicate they have exact information only sometimes or even never but are confident most or half of the time (for likelihood assessments 33.3%, for consequence assessments 23.3%). These respondents are aware of their lack of exact information but are confident nevertheless. This lack of information does not seem to affect their ability to form a predictive judgment and be confident about it.

Individual characteristics influence confidence levels. As hypothesized more professional and security experience significantly raises the confidence level of the security professionals. More experienced security professionals are more often confident about their assessments of both likelihood and consequences. More experienced security professionals also indicate that more information would raise their confidence level to a lesser extent than less experienced professionals indicate. In short these results seem to indicate that more experience leads to higher levels of (over)confidence and less need for additional information. These findings confirm results previous work (Desender et al., 2018; Sieck & Yates, 1997). A higher education level on the other hand significantly reduces the confidence in likelihood and consequences assessments. These results might prove the adage ‘the more you know, the more you realize you don't know’ as other scholars also found (Wright & Ayton, 1986). Security specific trainings do not significantly influence confidence level or the need for additional information.

The third case (reformulated problem) in this study clearly proved the significant influence of more detailed information on likelihood assessments as expected. Three in four of the security professionals assess the likelihood of a more detailed case higher. This case offered the two answer options in one single view, showing the conjunction fallacy in plain sight. This, however, did not lead the majority of the professionals to apply logical reasoning and select the option with the shorter description. These results replicate numerous previous studies in other domains showing the power of details, stories, and assumptions. This study, for the first time, shows this effect on a realistic real-life security risk case.

The significant effects of the conjunction fallacy on security risk likelihood assessments are visible in the results of case 1. The likelihood of the short case is on average estimated at 57.1% while the likelihood of the extended version is estimated at 69.6%. In contrast to the expectation it is worth to note that the assessments of the security professionals, with similar backgrounds, professions, and experience, show a substantial variance or so called system noise (short case description: M = 57.1%, SD = 26.33%, extended case description: M = 69.6%, SD = 21.56%). Even with the presented limited case descriptions their assessments of the likelihood vary from unlikely to very likely. As these security professionals each decide or influence security risk decision making in their own organization, these results denote the possible variation in response to similar risks between different organizations.

The likelihood assessments of the two groups at case 2 show different results compared to case 1. There is hardly any difference in the likelihood assessment of the short case description (M = 56.3%, SD = 23.83%) and the assessment of the extended case description (M = 57.5%, SD = 24.43%). The level of system noise is similar to case 1.

As the two randomly assigned groups do not significantly differ in characteristics (see Table 5), the difference between the likelihood assessments of cases 1 and 2 can only be caused by either the experiment setup and/or the different subject/content of the cases. In the following several possible explanations for the difference in overall response form group A and B are discussed.

The characteristics of the respondents in the two groups do not differ significantly; however, their average assessment of the two cases combined shows a significant difference. The average assessment of the two cases is 5.8% point higher in group B compared to group A. One of the possible explanations for this difference could be so called level noise, variability of judgment between individuals (fe. some security professionals might be more risk averse than others). Correcting the average assessments of the two cases for this possible level noise would lead to an average difference between the short and extended versions at case 1 of 6.7% point and for case 2 of 7% point. In both cases the extended version is assessed a comparable higher likelihood. Assuming this reasoning valid the conjunction fallacy raises the likelihood assessment with 6.7-7% point.

The setup of the experiment led the respondents to first assess case one followed by case two. As a consequence group A was first presented a short description of case 1 followed by an extended description of case 2. Group B, on the other hand, was confronted with first an extended description (case 1) followed by a short case description (case 2). The assessments of the first case might influence the respondents at their assessment of the second case, for example by the anchoring effect. This cognitive bias points at a human tendency to focus on a first piece of information to make subsequent judgments. Even if this piece of information is not related to the following judgment, this 'anchor' is proven to be influential. In this case the first assessment might become an anchor for the second assessment. We observe almost no difference in the average likelihood assessments over all group A respondents for the short and extended case study descriptions (57.1% vs 57.5% resp), which might suspect an anchoring effect, although no definitive proof can be given for such effect based on the current data. The average likelihood assessments over all group B respondents for the short and extended case study descriptions does show a large difference (69.6% vs. 56.3% resp), but also here no definitive proof can be given that there is absence of the anchoring effect. There might be other factors which influence the difference in the average likelihood assessments over the group respondents for the short and extended case study descriptions.

The two cases each describe a realistic, actual, real-life security risk. The first case describes a situation which, at the time of the experiments, was very relevant and discussed publicly. The second case is as relevant and actual as the first but was less prominent. The difference between the results of the two domains might be explained by the theory of hints (Kohlas & Monney, 2013). Previous work by Brachinger and Monney explains the fallacious behavior of individuals as indicated by the conjunction fallacy (Brachinger & Monney, 2003). In their study they show that individuals confronted with a choice, in which only vacuous mindless hints and no precise hints are available, are forced to refer to their general knowledge to retrieve a subjective probability. In such situations the subjective interpretation of simple hints guides the decision maker. In this study both case introductions contain only vacuous hints. None of these hints indicates any precise information about the likelihood of interest by an organized crime organization, the target Intellectual Property (IP) or even more specific IP related to COVID-19 research. The simple (supporting) hints in the introduction about the position on the development of a COVID-19 vaccine at the hypothetical pharmaceutical corporation, might imply a large value at stake leading to interest of various malicious actors like organized crime. These simple hints can also lead to the interpretation that the most obvious information to extract is IP related to COVID-19 research. Other possible, and equally realistic, options like an attempt to extract commercial information by a foreign competitor or state affiliated actor might be discarded by the respondents. The same arguments apply on the second case of which the structure is similar.

Forcing the respondents to refer to their individual frame of reference, prior experience or expertise, as this theory stresses, can explain the difference between the results in between the two cases. The first case related to very prominent and available information and discussion while for the subject of the second case was less attention at that point in time.

This theory might also explain the difference in response between the physical en cybersecurity domain at case 3. In the physical security domain 58.8% of the respondents followed the fallacy and chose the extended option. Of the respondents active in the cybersecurity domain 81.6% selected the extended option. Both the domains are closely related but deal with different threats. As an indication: the top threat in the cybersecurity domain in 2020 was IP theft by various threat vectors (ISACA, 2020) while in the physical security domain the top threat in

2020 was malicious physical access (ENISA, 2020). The respondents originating from the cybersecurity domain, therefore, might relate more to option: ‘organized crime organization targeting IP related to COVID-19 research.’ It fits their frame of reference, might lead to a stronger representativeness, recognition and emotion, and thus, availability. According to the theory of hints and the study of Brachinger and Monney this explains the fall for the conjunction fallacy. An important consequence of this conclusion can be that professionals with domain expertise, and thus a deeper subjective interpretation of simple hints, and readily available information or even experience (Dumm et al., 2020), assess a higher likelihood to risks in their domain than non-domain experts.

In agreement with the hypothesis the results of this study clearly show the influence of the conjunction fallacy on the judgment of security professionals. The consequence of this fallacy in the security domain can influence security risk assessments by these practitioners considerably. Following the fallacy, retrieving more specific, detailed and recognizable information may lead the individual professional to consider a case, incident, or threat more likely which in turn might lead to distorted risk assessments in organizations and society. Security professionals, facing the difficult daily task to assess security risks, often based on little accurate information, seem to be confident about their predictive judgment. This study hopes to raise awareness for possible flaws, unknown overconfidence, and ignorance of security professionals. As a whole, these findings have important implications for the professional security community and anyone depending on it.

Literature

Allingham, M. (2002). Choice theory: A very short introduction. OUP Oxford.

Alruwaii, A., & Brooks, D. J. (2008). *Organisational security: A propositional study to map expert knowledge.* Paper presented at the Proceedings of The 1st Australian Security and Intelligence Conference.

Andersson, O., Holm, H. J., Tyran, J.-R., & Wengström, E. (2020). Robust inference in risk elicitation tasks. *Journal of Risk and Uncertainty, 61*(3), 195-209.

ANSI/ASIS. (2012). Security Management Standard: Physical Asset Protection. In. Alexandria: ASIS International.

ANSI/ASIS/RIMS. (2015). Risk Assessment RA1.2015. In. Alexandria: ASIS International.

ASIS_International. (2015). Risk Assessment, ANSI/ASIS/RIMS RA.1-2015. In. Alexandria: ASIS International.

Baron, J. (2004). *Normative models of judgment and decision making*: Wiley Online Library.

Bonini, N., Tentori, K., & Osherson, D. (2004). A different conjunction fallacy. *Mind & Language, 19*(2), 199-210.

Brachinger, H. W., and P.A. Monney. 2003. The conjunction fallacy: explanations of the linda problem by the theory of hints. International Journal of Intelligent Systems 18(1): 75-91.

Carbone, E., Dong, X., & Hey, J. (2017). Elicitation of preferences under ambiguity. *Journal of Risk and Uncertainty, 54*(2), 87-102.

Charness, G., Garcia, T., Offerman, T., & Villeval, M. C. (2020). Do measures of risk attitude in the laboratory predict behavior under risk in and outside of the laboratory? *Journal of Risk and Uncertainty, 60*(2), 99-123.

Cooke, R. M. (1991). *Experts in uncertainty*. New York: Oxford University Press.

de Wit, J., Pieters, W., Jansen, S., & van Gelder, P. (2021). Biases in security risk management: Do security professionals follow prospect theory in their decisions? *Journal of Integrated Security and Safety Science, 1*(1), 34-57.

Desender, K., Boldt, A., & Yeung, N. (2018). Subjective confidence predicts information seeking in decision making. *Psychological Science, 29*(5), 761-778.

Dumm, R. E., Eckles, D. L., Nyce, C., & Volkman-Wise, J. (2020). The representative heuristic and catastrophe-related risk behaviors. *Journal of Risk and Uncertainty, 60*(2), 157-185.

ENISA. 2020. Physical manipulation, damage, theft, loss. ENISA Threat Landscape. https://www.enisa.europa.eu/publications/physical-manipulation-damage-theft-loss

Fantino, E., Kulik, J., Stolarz-Fantino, S., & Wright, W. (1997). The conjunction fallacy: A test of averaging hypotheses. *Psychonomic Bulletin & Review, 4*(1), 96-101.

Fiedler, K. (1988). The dependence of the conjunction fallacy on subtle linguistic factors. *Psychological research, 50*(2), 123-129.

Gigerenzer, G. (1991). How to make cognitive illusions disappear: Beyond "heuristics and biases". *European review of social psychology, 2*(1), 83-115.

Gigerenzer, G., & Selten, R. (2002). *Bounded rationality: The adaptive toolbox*: MIT press.

Hansson, S. O. (2012). A Panorama of the Philosophy of Risk. In *Handbook of risk theory* (pp. 27-54): Dordrecht: Springer Science+Business Media B.V.

Hertwig, R., & Gigerenzer, G. (1999). The 'conjunction fallacy'revisited: How intelligent inferences look like reasoning errors. *Journal of Behavioral Decision Making, 12*(4), 275-305.

Information_Security_Forum. (2018). Standard of Good Practice. In. Surrey: Information Security Forum.

ISACA. 2020. Top Cyberattacks of 2020 and How to Build Cyberresiliency. https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency

ISO. (2018). ISO 31000 Risk management - guidelines. In. Geneva: International Organization for Standardization.

ISO. (2019). ISO 22301 Security and resilience - Business continuity management systems - Requirements. In. Geneva: International Organization for Standardization.

ISO/IEC. (2011). ISO/IEC 27005 Information technology_Security_techniques_Information security risk management. In. Geneva: ISO.

Jain, K., Mukherjee, K., Bearden, J. N., & Gaba, A. (2013). Unpacking the future: A nudge toward wider subjective confidence intervals. *Management Science, 59*(9), 1970-1987.

Kahneman, D. (2012). *Ons feilbare denken: thinking, fast and slow*: Business Contact.

Kahneman, D., Sibony, O., Sunstein, C.R. (2021). *Noise, a Flaw in Human Judgment*. London: William Collins.

Kohlas, J., and P.A. Monney. 2013. A mathematical theory of hints: An approach to the Dempster-Shafer theory of evidence (Vol. 425): Dordrecht: Springer Science+Business Media B.V.

Kuhn, K. M., & Sniezek, J. A. (1996). Confidence and uncertainty in judgmental forecasting: Differential effects of scenario presentation. *Journal of Behavioral Decision Making, 9*(4), 231-247.

Ludwin-Peery, E., Bramley, N. R., Davis, E., & Gureckis, T. M. (2020). Broken physics: A conjunction-fallacy effect in intuitive physical reasoning. *Psychological Science, 31*(12), 1602-1611.

Möller, N. (2012). The concepts of risk and safety. In *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk* (pp. 55-85): Dordrecht: Springer Science+Business Media B.V.

Sieck, W., & Yates, J. F. (1997). Exposition effects on decision making: Choice and confidence in choice. *Organizational behavior and human decision processes, 70*(3), 207-219.

Simon, H. A. (1982). *Models of bounded rationality: Empirically grounded economic reason* (Vol. 3): MIT press.

Slovic, P. (2010). The feeling of risk. In New perspectives on risk perception. New York: Routledge

Slovic, P. E. (2000). *The perception of risk*: Earthscan publications.

Stolarz-Fantino, S., Fantino, E., Zizzo, D. J., & Wen, J. (2003). The conjunction effect: New evidence for robustness. *American Journal of Psychology, 116*(1), 15-34.

Sunstein, C. R. (2005). *Laws of fear: beyond the precautionary principle*: Cambridge University Press.

Talbot, J., & Jakeman, M. (2011). *Security risk management body of knowledge* (Vol. 69): John Wiley & Sons.

Tentori, K., Bonini, N., & Osherson, D. (2004). The conjunction fallacy: A misunderstanding about conjunction? *Cognitive Science, 28*(3), 467-477.

Tentori, K., & Crupi, V. (2012). On the conjunction fallacy and the meaning of and, yet again: a reply to. *Cognition, 122*(2), 123-134.

Tversky, A., & Kahneman, D. (1975). Judgment under uncertainty: Heuristics and biases. In *Utility, probability, and human decision making* (pp. 141-162): Springer.

Tversky, A., & Kahneman, D. (1983). Extensional versus intuitive reasoning: The conjunction fallacy in probability judgment. *Psychological review, 90*(4), 293.

Tversky, A., and D. Kahneman. (2008). Extensional versus intuitive reasoning: The conjunction fallacy in probability judgment. Reasoning: Studies of human inference and its foundations, 114-135.

Tversky, A., & Koehler, D. J. (1994). Support theory: A nonextensional representation of subjective probability. *Psychological review, 101*(4), 547.

Wright, G., & Ayton, P. (1986). Subjective confidence in forecasts: A response to Fischhoff and MacGregor. *Journal of Forecasting, 5*(2), 117-123.

CHAPTER 4

Sources of Security Risk Information: What do Professionals Rely on for their Risk Assessment?

Johan de Wit, Wolter Pieters, Pieter van Gelder

As became clear in the previous chapters information is the foundation of risk assessments by professionals. The logical next question emerged: where do the security professionals get their information from? This chapter addresses this question by addressing the following research questions: What sources of security risk information are considered by practitioners? How reliable are these sources as perceived by these practitioners? Which sources are applied in security risk assessment praxis? Are the most applied sources also perceived as the most credible ones? Can we observe differences between security professionals based on their expertise (experience and knowledge)?

In this study the NATO system for intelligence evaluation or Admiralty code is applied. To evaluate trust in a source to full extent a novel criterion is added to this system: source intention. This criterion proved useful in the analysis of the results.

This paper is currently under review with the journal: The Information Society *2021*. The version published in this dissertation is the resubmitted version with the requested minor revisions incorporated.

Abstract

Security risks, such as sabotage and cyberattacks, are an increasing threat to business and government processes. Security risks originate from malicious human action, of which often exact historical information is lacking. This makes them less suitable for probabilistic modelling, leaving the judgment and assessment of security professionals as the primary input for security risk management. In this study we explore the information sources professionals use for this purpose, improving understanding of their daily praxis. Sources of security risk information are collected, their quality and trustworthiness is assessed, and their application in security risk assessments is analyzed. Quality is assessed by a panel of experienced security practitioners by applying the NATO system for intelligence evaluation, with source intention as additional criterion. Actual application is analyzed in a survey among security professionals. The results consist of a comparative ranking of both assessed quality and daily application of sources. Experts are ranked first for perceived quality and are also most applied in daily praxis, and individual/personal experience comes second. The additional criterion of source intention explained the lower level of application of information from science. This study provides the basis for enhancing security risk management by a more conscious selection of sources.

1. Introduction

Stating that predicting the future is impossible by definition is stating the obvious (Kahneman, Sibony, and Sunstein 2021). However, globally thousands of risk professionals do this on a daily basis. They manage risks, which are defined as “the effect of uncertainty on objectives” (ISO 2018). Forecasting potential future effects and predicting uncertainties, in other words predicting the risk future is part of their risk management processes and is usually labelled risk assessment (see Figure 1).

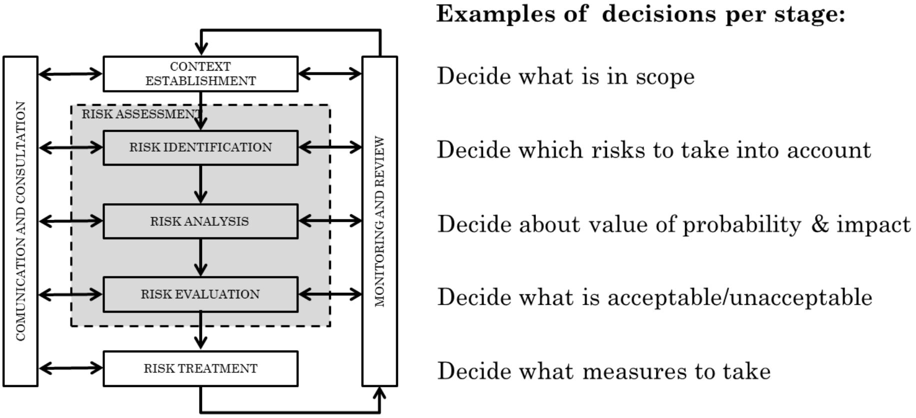

Examples of decisions per stage:
COMUNICATION AND CONSULTATION
CONTEXT ESTABLISHMENT
RISK ASSESSMENT
RISK IDENTIFICATION
RISK ANALYSIS
RISK EVALUATION
RISK TREATMENT
MONITORING AND REVIEW
Decide what is in scope
Decide which risks to take into account
Decide about value of probability & impact
Decide what is acceptable/unacceptable
Decide what measures to take

Figure 1. Risk management process according to ISO 31000 (NEN-ISO 2009) with examples of decisions per stage

Security in society and organizations is heavily depending on this assessment, or in other words judgment, of these security professionals. It is, therefore, of the utmost importance to understand how these professionals form their opinion and judgment. Their predictive judgement is based on information available to them. Security in this work is considered to be initiated by malicious intent, a definition grounded in the physical security domain. The respondents surveyed in this study both have an physical and cyber security background. Previous work of the authors showed that security professionals indicate to have detailed information on security risk, on average, in half of their security risk assessments. They also indicate they almost always can assess and decide upon a security risk, even if they have no detailed information (de Wit, Pieters, and van Gelder 2023). These findings sparked follow-up research questions about the sources of this information.

This study is explorative and descriptive, driven by the curiosity to add to a deeper understanding of human security risk assessments. The research questions answered in this study are:

- What sources of security risk information are considered by practitioners?
- How reliable are these sources as perceived by these practitioners?
- Which sources are applied in security risk assessment praxis?
- Are the most applied sources also perceived as the most credible ones?
- Can we observe differences between security professionals based on their expertise (experience and knowledge)?

This study focusses on possible sources of security risk information, their perceived quality, and their level of application in security risk assessment by security practitioners. First the possible sources of security risk information are collected in an expert consultation. This resulted in a list of 17 possible sources of security risk information. Second, the reliability, credibility and intention of these possible sources is assessed by a practitioners panel. This resulted in a source quality ranking which is considered a normative reference. Finally, by means of an online survey, a large group of security professionals is consulted on the application of these sources in their daily praxis. The individual expertise of the professionals is collected in the survey to explore if this influences their application of information sources. Previous work of the authors showed that more experienced security professionals value information to a lesser extent in their security risk assessment than less experienced practitioners (de Wit, Pieters, and van Gelder 2023).

So far, to the best of our knowledge, no comparable research is done in this security domain.

The next section will briefly detail the background of judgment, expertise, information sources and their quality. The research and analysis methods are explained in the method section followed by a section presenting the results. The paper ends with a discussion and conclusions section.

2. Background

Risks might seem hard to assess but over time a substantial body of knowledge has been gathered on risks. Historical data makes it possible to form evidence-based predictions under the precondition of similar context and circumstances. Security risks, the topic of this paper, deal with malicious human acts and actors (Möller 2012; Husák et al. 2018; Krisper, Dobaj, and Macher 2020). The main characteristics of these acts, trying to be unpredictable, be concealed, and evade existing risk controls, generates a large variety and constantly evolving number of modus operandi (Talbot and Jakeman 2011; Deb, Lerman, and Ferrara 2018). In combination with an almost unlimited variety of situations and context, in both location and time, security risks are hard to predict on solid data (de Meij 2010; Oppelaar 2006; Stanovich and West 2000). Often there is limited historical information on specific security risks and/or a different context might not allow an application of this data in specific circumstances. In the domain under study, security risk assessments, therefore, expert judgment is the predominant inception for these assessments (Möller 2012; Talbot and Jakeman 2011; Krisper, Dobaj, and Macher 2020; Powell et al. 2019).

To manage risks in a structured manner, over time risk management processes have been developed (Jerman-Blažič 2008). Various domains dealing with risks developed specific processes, which, however, all contain similar subsequent steps. The assessment of risks is a part of these processes and consists of three subsequent steps: risk identification, risk analysis and risk evaluation (ISO 2018; ISO/IEC 2016, 2011; Alhawari et al. 2012). The risk professionals dealing with this task need to inform themselves about possible current and future threats, and analyze and evaluate these (Mandel and Irwin 2021). The latter steps are usually performed on the, broadly accepted, two main components of risks: likelihood (expressing uncertainty) and impact (expressing effect). However theoretically impossible, as stated in the first line of the introduction, they do their best to be prepared for possible, unpredictable, future events.

In this sense risk management seems to be closely related to forecasting. Forecasting is defined as: intelligence work or guessing about the future (Tetlock and Gardner 2016). The term forecasting might give the impression of quantitative or scientific methods and processes, like weather forecasting, however, good predictions are based on how you think not on what your know (Tetlock and Gardner 2016). In other words: proper forecasting is about the quality of available information and, more importantly, how this information is processed.

How individuals process information to reach a judgement is extensively studied over time in the domain of expert judgment (Cooke 1991; Ryan et al. 2012; Skjong and Wentworth 2001; Einhorn 1974; Meyer and Booker 2001; Cooke and Goossens 2008). These studies primarily focus on (determining) the accuracy of experts and their judgments. Expert judgement is considered a degree of belief, based on tacit knowledge and expertise (Cooke 1991; Ajzen 2011; Fischbein and Ajzen 1975). This tacit knowledge should be an important element of knowledge management and an competitive advantage for organizations (Johannessen, Olaisen, and Olsen 2001). The related field of Naturalistic Decision Making (NDM) focusses primarily on expertise of practitioners. NDM studies the, often not conscious, process of assessment and decision making by real-life practitioners (Klein 1993; Klein 1997, 2008; Gore and Ward 2018; Hoffman and Klein 2017; Lipshitz et al. 2001; Lipshitz and Strauss 1997; Markman 2017; Pliske and Klein 2003; Roberts and Cole 2018). According to NDM, practitioners comprise their assessment based on recognition of cues. These cues trigger recollection of both memories and knowledge of the individual practitioner. These in turn allow the practitioner to perform a mental simulation and assess/compare the real-life situation with the simulation. This field of study, predominantly empirical and exploratory, focused on real-life praxis. It turned out to be very much in line with the renowned, more theoretical, laboratory research in the field of heuristics and biases, much to the surprise of the two ‘godfathers’ in these fields: Gary Klein and Daniel Kahneman (Kahneman and Klein 2009). For example: the recognition of cues (the cornerstone of NDM) seems to be closely related to the availability heuristic (the most prevalent heuristic in the domain of heuristics and biases).

A large body of research demonstrated that judgements in general are based on the information that is most accessible to the decision agent at the time of the judgement (Citroen 2011). Information in this work is defined as ‘knowledge obtained from investigation, study or instruction (Merriam-Webster, https://www.merriam-webster.com/dictionary/information). Agents rarely try to retrieve all information but process (just) enough information that comes to mind to form a judgment with subjective certainty (Schwarz and Vaughn 2002). In our current society information is omnipresent and available in abundance, agents need to select information that is both available to them, and is of use in the given context (Weber 1987). An important criterion for selecting information is based on the perceived reliability of the source of information (Viljanen 2005; Hertzum et al. 2002). Other scholars have identified the strong relation between knowledge management, or in other words information management and risk management (Alhawari et al. 2012).

This study focusses on information and especially its origin: the sources of information. Information is considered to generate so called message cues (Trumbo and McComas 2003). In other words, information is one of the possible cues triggering the process of NDM in a decision maker.

The quality of information is besides the quality of the content depending on the quality of the source of this information. Sources can be classified based on characteristics like for example: content, origin/reputation, and recognition (Dongo, Cardinale, and Aguilera 2019), or more detailed: accurate, trustworthy, accessible, ease of use, free, active/updated, comprehensive, familiar (Kim and Sin 2011). In summary these characteristics can be grouped in two overarching characteristics: the quality and the availability of the information/source (O'Reilly III 1982). In their study Kim & Sin found that the first is considered more important by their participants, but, their behavior showed otherwise (Kim and Sin 2011) as O’Reilly and Hertzum also concluded earlier (Hertzum et al. 2002; O'Reilly III 1982).

Analyzing and classifying information and information sources is of vital importance in the security domain (Powell et al. 2019; Gal-Or and Ghose 2005; Johnson 2010). Especially in the security intelligence community tools and methods are developed and applied to classify information and information sources (Powell et al. 2019; Seagle 2015; Korkisch 2010).

Table 1: Outline of the Admiralty Code or NATO System (Powell et al. 2019)

Source Reliability	Description
A - Completely reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B - Usually reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C - Fairly reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D - Not usually reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E - Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F – Reliability cannot be judged	No basis exists for evaluating the reliability of the source
Information Credibility	**Description**
1 - Completely credible	Logical, consistent with other relevant information, confirmed by independent sources
2 – Probably true	Logical, consistent with other relevant information, not confirmed
3 – Possibly true	Reasonably logical, agrees with some relevant information, not confirmed
4 - Doubtful	Not logical but possible, no other information on the subject, not confirmed
5 - Improbable	Not logical, contradicted by other relevant information
6 – Truth cannot be judged	The validity of the information cannot be determined

In this domain the quality of information is also predominantly evaluated based on both the reliability of the content and the source, applying the international and broadly accepted evaluation criteria known as the Admiralty Code or NATO System (see Table 1). The NATO system classifies the reliability of sources on: authenticity, trustworthiness and competency. These characteristics are evaluated against past experience with the sources. Note that the first five categories of the scale are ordinal and the sixth represents the inability to categorize the information. nominal These characteristics are evaluated against past experience with the sources.

The NATO system is not free of debate. Overtime several scholars have presented shortcomings and recommendations to improve this

NATO system. Applying this system and assessing information and information sources remains largely a human, and thus subjective, task with all its limitations and possible flaws (Capet and Delavallade 2014; Icard 2019, 2023). The system evaluates the information and the source of information separately. However, a source might be considered reliable for information in a certain context but might not be in another situation (as will also be discussed further down in this section). By separating the assessment of the information and the source of this information this contextual relationship might be disregarded (Capet and Delavallade 2014).

The scale of the NATO system is also subject of debate. The current scale is considered evaluative and does not allow for a more objective, descriptive perspective on information (Icard 2023). An assessor should be allowed to clearly segregate facts from interpretations. The result is an proposed 3x3 matrix where information is classified as: true, indeterminate or false. The source can be classified as honest, imprecise or dishonest (Icard 2023). Other studies conclude that assessors tend to group the NATO system's scale of six classifications in three groups, positive: upper three classifications, negative: bottom two and neutral: the one between (Mandel et al. 2023).

As the 'original' NATO system is well known and accepted in the security community it is applied in this study. However, in this paper a novel addition is proposed based on theories on trust. The characteristics of the NATO system on source reliability all relate to the notion of trustworthiness. Trust is the attitude that takes to the trustworthiness of a source (Viljanen 2005). "Trust is of central importance because quality is a perceived property and, thus, assessing the quality of an information source is essentially a matter of establishing to what extent one is willing to place trust in it" (Hertzum 2002, 1).

The trustworthiness of a source, whether a source is worthy of confidence, is context dependent (O'Hara 2012; Viljanen 2005; Bennett 2020). A source might be very competent, and thus trusted, in one domain, but might be incompetent in others. Whether a source is worthy of acceptance and original and can therefore be considered real or genuine or in other words authentic (Lehman et al. 2019; Van Leeuwen 2001), depends on reputation, recognition or credentials attributed to the source. These are characteristics for assured reliance, or trust, in a source.

Trust is usually not solely based on facts and evidence. McAllister defines two types of trust: cognitive trust, based on evidence and knowledge (trusting with the head), and affective trust, based on emotional ties with others (trusting with the heart) (McAllister 1995). The latter relates to familiarity with the source (Denize and Young 2007). Source familiarity allows for easier and more precise determinable trustworthiness (Hertzum 2002). Non-familiar sources of information are treated with more caution (Hertzum et al. 2002). The NATO system does not explicitly refer to these phenomena. They will, however, be of value to explain the perceived source reliability in the discussion and conclusions section.

In available literature about trust another property of trust is deemed important. Besides the perceived competence of the source the perceived intent or agency of the source is essential for the trustworthiness of the source (Hawley 2012; O'Hara 2012). Sources of information may have deviating goals, intentions and incentives that can alter their trustworthiness. Even though sources might be considered competent, their information might be comprehensive, consistent, accurate and up to date, they still may be suspected of following an agenda that is not in line with the receiver of information (Hawley 2012). In this paper source intention is interpreted as the sources apparent (or hidden) aspirations, goals, objectives or incentives. These might deviate from the assessors intentions.

While the competence of a source is often stable over time or might show gradual changes, intentions of sources, on the other hand, can be very volatile and might even change overnight (for example due to bribery, extorsion or other external pressure). Specifically evaluating source intention as part of classification of information can be considered of vital importance. In the original NATO code source intention might be considered a component of source reliability and assessed together with competence. Due to the specific importance of intent in the literature on trust and trustworthiness and the volatile character of source intention, a separate assessment of source intention is proposed. To enhance the quality of the NATO system, to classify information and information sources, a novel, additional, classification scale for source intention is proposed. This novel scale (see Table 2) is set up, tested, and evaluated in this study by a practitioners panel.

Table 2: proposed addition to the NATO code for classification of source intention

Source Intention	Description
I - Completely shared intentions	No doubt of source intention or aspiration, goals and objectives are in line; has a history of shared intentions
II - Usually shared intentions	Minor doubt about source intention or aspiration, goals and objectives are in line; has a history of shared intentions most of the time
III - Fairly shared intentions	Doubt of source intention or aspiration, goals and objectives might be in line; had shared intentions in the past
IV - Not usually shared intentions	Significant doubt about source intention or aspiration, goals and objectives might not be in line; had shared intentions in the past
V – No shared intentions	Lacking in transparency of source intention; goals and objectives might not be in line; had different intentions in the past
VI – Intention cannot be judged	No basis exists for evaluating the intention of the source

Other scholars identified this characteristic in perceived deviating goals and intentions in risk communication by industry and governmental risk communicators. Although these sources are considered competent their information is considered less trustworthy because of a potential deviating agenda. Industry is perceived to follow commercial incentives and governments try to accomplish policy goals. Due to these possibly expected diverging intentions, these sources are typically considered less trustworthy (Fessenden-Raden, Fitchen, and Heath 1987; McCallum, Hammond, and Covello 1991; Slovic, Flynn, and Layman 1991; Trumbo and McComas 2003).

The third novel classification criterion is added to the two existing quality criteria of the NATO system (see Figure 2). This study primarily focusses on these quality criteria as perceived by security practitioners.

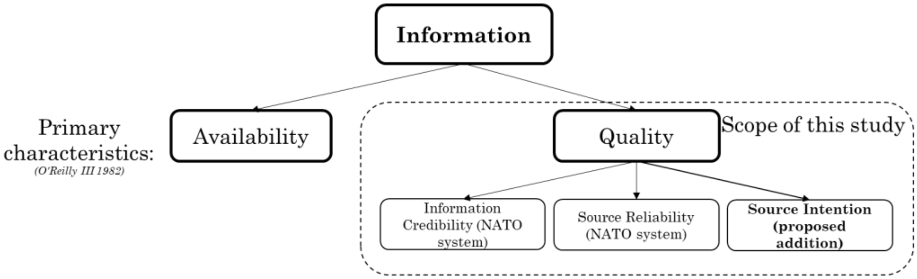

Information
Primary characteristics:
(O'Reilly III 1982)
Availability
Quality
Scope of this study
Information Credibility (NATO system)
Source Reliability (NATO system)
Source Intention (proposed addition)

Figure 2 : characteristics of information and information sources

The assessment of security risks is predominantly based on expert judgment. This judgment in turn is based on security risk information available to the agent at the time of the assessment. The quality of this information is, obviously, influencing the security risk assessment. This study seeks to evaluate this quality by focusing on the (perceived) quality of the source of information. To be able to assess the quality of information, the NATO system offers a solid and well accepted base. As the intention of the source of information is not explicitly assessed in this system for this study an additional classification is set up and applied.

3. Research Method

To explore the perceived trustworthiness and application of various information sources of security risk information, practitioners from the security domain were consulted. Different groups of practitioners participated in:

1) a small brainstorm session to collect the most prominent possible sources of information,
2) a panel consultation to rank the source quality,
3) a large scale survey amongst security professionals to explore the application of these sources of information.

The quality ranking of the panel consultation will be compared to the real life application of information sources.

First a list of possible sources of risk information is composed during a brainstorm session with the senior members (n=8) of a Security Council in 2020. This predefined list of possible sources of security risk information consists of 17 predefined sources:

- Peers (people in your network with the same role),
- Experts (knowledgeable people recognized in the field),
- Expert communities,
- Higher management,
- colleagues,
- Internal intelligence,
- External intelligence (government),
- External intelligence (commercial),
- Public sources like media,
- Social media sources,
- Government or government agencies,
- Consultants/consulting organizations,
- Science/scientific publications,
- Supplier organizations,
- Personal experience,
- Personal training/education,
- My ‘gut feeling’.

This is considered a comprehensive list, but, in the next phase of this research the practitioners panel is offered the opportunity to add possibly missing sources. In the results section these possible additional sources are presented and discussed. This comprehensive list is used as primary input for the panel consultation resulting in a quality ranking of information and the survey to explore the real-life application of security risk information sources.

For the ranking of the quality of these predefined sources a practitioners panel is formed by addressing experienced respondents that indicated, in response to a previous survey, to be willing to participate in follow-up research. This panel consists of 18 experienced security practitioners from both the physical and security domain: on average 28 years of security experience, 83% followed specific security trainings, education level: associate degree 11%, bachelor degree 22%, master/PhD degree 67%. Table 3 shows the professional position of the panelists.

Table 3: professional environment of the practitioners panel

My working environment is best described as:	N:
Government/government agency: responsible security role	3
Government/government agency: advisory security role	1
Private organization: responsible security role	3
Private organization: advisory security role	6
Private organization: security supplier	2
Research/education	2
Other:	1
‘ a variety of the above’	

In an online consultation the members of this practitioners panel are invited to rate the source reliability, information credibility and source intention of each of the predefined sources (see Table 1 and 2). The analysis of this consultation results in a quality ranking of the security risk information sources which is considered a normative reference. These results are collected in July 2022.

In order to rank the perceived source quality based on these three criteria, a method of Multiple-Criteria Decision Making (MCDM) is selected. In this study a Technique for Order Performance by Similarity to Ideal Solution (TOPSIS) analysis is applied (a variation of the Analytical Hierarchy Process technique, AHP). The purpose of AHP is to capture the experts knowledge. AHP uses exact values to express a decision maker's opinion in a comparison of alternatives (Hota, Sharma, and Pavani 2014). TOPSIS is one of the most classical, compensatory, MCDM methods originally developed by Wang and Lee (Wang and Lee 2007). The concept of this method is find the alternatives with the closest distance to the positive ideal solution (d_i^*) and the farthest distance to the negative ideal solution (d_i^-). Ranking takes place on the closeness coefficient ($CC_i = d_i^* / (d_i^- + d_i^*)$).

As the topic of this study includes various imprecise and non-numerical criteria, fuzzy logic is added to the TOPSIS method. Fuzzy technique for order preference by similarity to ideal solution (FTOPSIS) is a MCDM method specifically developed for ordering based on non-numerical criteria that can be fuzzified using fuzzy logic (Nădăban, Dzitac, and Dzitac 2016; Salih et al. 2019; Sevkli et al. 2010). 'Fuzzy logic can deal with information arising from computational perception and cognition, that is, uncertain, imprecise, vague, partially true, or without sharp boundaries. Fuzzy logic allows for the inclusion of vague human assessments in computing problems' (Singh et al. 2013, 1). The subsequent steps of this method are presented in Figure 3 .

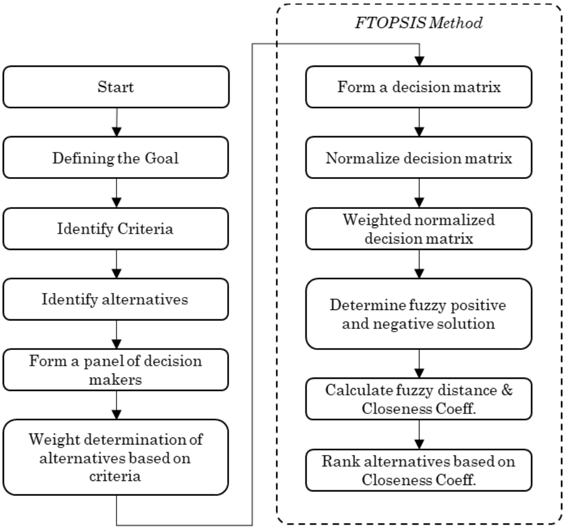

FTOPSIS Method
Start
Defining the Goal
Identify Criteria
Identify alternatives
Form a panel of decision makers
Weight determination of alternatives based on criteria
Form a decision matrix
Normalize decision matrix
Weighted normalized decision matrix
Determine fuzzy positive and negative solution
Calculate fuzzy distance & Closeness Coeff.
Rank alternatives based on Closeness Coeff.

Figure 3: Steps of the Fuzzy TOPSIS method (Sevkli et al. 2010; Hota, Sharma, and Pavani 2014).

The decision problem to be solved with Fuzzy TOPSIS is defined as follows: which possible source of security risk information is considered most trustworthy based on the criteria: Source reliability, information credibility, and source intention?

The overall perceived quality ranking resulting from the FTOPSIS method will be used, as a quality reference, to compare the results of the main survey presented in this study on the application of sources in daily praxis.

In the third part of this study the research question: ‘on what information source do you base your security risk assessment?’ is addressed. The exploratory results of the main survey are retrieved online between September 2020 and February 2021. Participation in the survey is promoted in both the IT and physical security professional community. It is promoted via LinkedIn and Twitter, both in general and in special interest groups like Security management, ASIS Europe and ASIS International, Dutch cybersecurity platform. Second, a direct email campaign is launched targeting the existing professional network of the researchers. Third, the survey is promoted via the Information Security Forum world conference: Digital 2020 (cybersecurity domain) and ASIS Europe 2021 conference (physical security domain). The sample of respondents (N = 174) is regarded a convenience sample. About one third of the respondents have a general risk/management background, two thirds followed specific security trainings/education of which physical vs IT/cybersecurity is evenly divided.

This survey is set up with Qualtrics survey software. The survey consists of a question to explore the application of possible sources of risk information. The respondents are asked, for each individual source, to indicate the level of application in their security risk assessments by rating the importance via a three point Likert scale is offered: very important, moderately important, not important.

To check whether the presented list is comprehensive the respondents are offered the opportunity to add additional information sources via an open box answer possibility. This question offers the respondents to add any possible missing source of security risk information. Based on the results of this question the comprehensiveness and, thus, validity of the predefined list of information sources can be determined.

The predefined list is offered randomized to the respondents to avoid order bias (primacy, regency, contrast and assimilation effects).

In the main survey the respondents are asked to express their expertise in a number of questions about individual characteristics. They are asked to indicate their age, number of years professional experience and number of years security experience. The current function of the respondents is asked including the number of years in this position. Finally they are asked to indicate their general education level (associate degree, bachelor degree or Master degree/PhD) and if any specific security trainings are completed. The possible influence of these characteristics on the application of information sources is explored.

Finally the quality ranking of the information sources by the panel consultation is compared to the ranking of the application of sources resulting from the large scale survey amongst security professionals.

4. Results and Analysis

First the results of the perceived source quality ranking by the practitioners panel consultation are presented. This panel of security practitioners (N=18) analyzed the predefined list of information sources by assessing each source using the two criteria of the NATO System (see Table 1) and the additional criterion, source intention (see Table 2). Two of the panelists mentioned an additional source of information:

1. ‘Books published by domain experts’
2. ‘Statistics relating to past events, frequency/ impact’

The first is considered a part of the already defined source: experts. The second is interpreted as a kind of information that can have its origin in multiple sources. Historical information can be supplied by experts, intelligence communities, suppliers, expert communities etc. and even can be regarded as part of personal experience. Both additions are considered already represented in the list and are, therefore, not interpreted as an additional source of information. As shown in Table 4 six times the answer: ‘N/A I do not consult this source’ is selected. These are all selected by one single panelist. All the other panelists indicate they apply all the predefined sources.

Table 4: classification results security practitioners panel from completely reliable (A) to completely unreliable (F), completely credible (1) to completely not credible (6) and completely shared intention (I) to completely unshared intention (VI), (numbers indicate the number of panelists assigning a certain rating).

Predefined information sources:	Source reliability							Information credibility							Source intention						
	A	B	C	D	E	F	n/a	1	2	3	4	5	6	n/a	I	II	III	IV	V	VI	n/a
Peers	1	14	3	-	-	-	-	1	12	5	-	-	-	-	2	15	1	-	-	-	-
Experts	5	11	2	-	-	-	-	5	11	2	-	-	-	-	5	10	3	-	-	-	-
Expert communities	3	9	6	-	-	-	-	4	10	4	-	-	-	-	5	8	5	-	-	-	-
Higher management	-	5	9	4	-	-	-	1	7	6	3	1	-	-	1	11	3	3	-	-	-
Colleagues	-	7	10	1	-	-	-	-	6	12	-	-	-	-	3	11	4	-	-	-	-
Internal intelligence	4	10	4	-	-	-	-	5	9	4	-	-	-	-	5	9	4	-	-	-	-
External intelligence (government)	2	14	2	-	-	-	-	4	11	3	-	-	-	-	3	10	5	-	-	-	-
External intelligence (commercial)	1	11	5	1	-	-	-	2	9	6	1	-	-	-	-	7	9	2	-	-	-
Public sources like media	-	2	11	4	1	-	-	-	3	11	2	1	1	-	-	5	5	4	4	-	-
Social media sources	-	1	2	9	3	3	-	-	-	5	8	3	1	1	-	1	5	4	5	2	1
Government or government agencies	2	10	6	-	-	-	-	2	9	7	-	-	-	-	3	9	5	1	-	-	-
Consultants/consulting organizations	-	7	10	1	-	-	-	1	7	9	1	-	-	-	2	5	10	1	-	-	-
Science/scientific publications	3	12	3	-	-	-	-	5	11	2	-	-	-	-	3	11	4	-	-	-	-
Supplier organizations	-	4	11	2	1	-	-	-	9	7	1	-	-	1	-	8	7	2	-	-	1
Personal experience	2	9	7	-	-	-	-	3	13	2	-	-	-	-	10	7	1	-	-	-	-
Personal training/education	-	13	5	-	-	-	-	2	12	4	-	-	-	-	6	9	3	-	-	-	-
My ‘Gut feeling’	-	6	12	-	-	-	-	-	8	9	-	-	-	1	6	7	3	-	-	1	1

The results as presented in Table 4 corroborate with previous studies (Baker, McKendry, and Mace 1968; Samet 1975). The results of the security practitioners panel, as shown in Table 5, are analyzed using the FTOPSIS method. The final outcome of the Fuzzy TOPSIS analysis is presented in Table 5. In this table, the values are obtained by applying the FTOPSIS method as detailed in the method section.

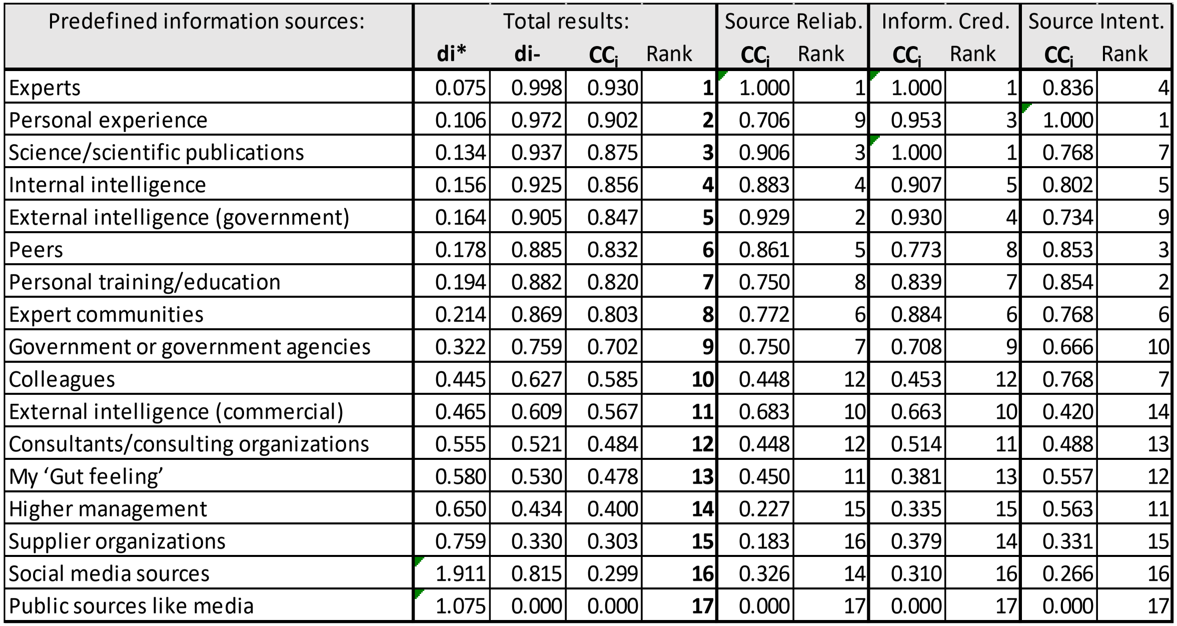
The results of Table 4 with the 17 alternatives and the three criteria are transferred to a decision matrix. This matrix is normalized and weighted resulting in a best and worst alternative (maximum vs minimum value) per criterion. For the criteria source reliability and information reliability the best (highest valued) alternative is Experts. For the criterion source intention the best alternative is personal experience. The worst alternative for all three criteria is Public sources like media. The last three columns in Table 5 reflect the ranking of the alternatives per criterion (1.000 is best, 0.000 is worst).

Based on these best and worst alternatives the Euclidian distance of each of the outcomes to the best and worst alternative is calculated (di* and di-). Combing these leads to the closeness coefficient (CCi) which can then be ordered into a final ranking.

Overall the source: experts, defined as knowledgeable people recognized in the field, are indicated to be the most trustworthy source of security risk information. They are considered to be the most reliable source, share completely credible information, but do not always share the same intentions (as they are ranked 4 on this criterion). Science/scientific publications, for example, are as a source considered reliable (rank 3) and this source shares equally credible information as the experts (rank 1), but on the other hand this source of information is perceived to not completely share the same intentions (rank 7).

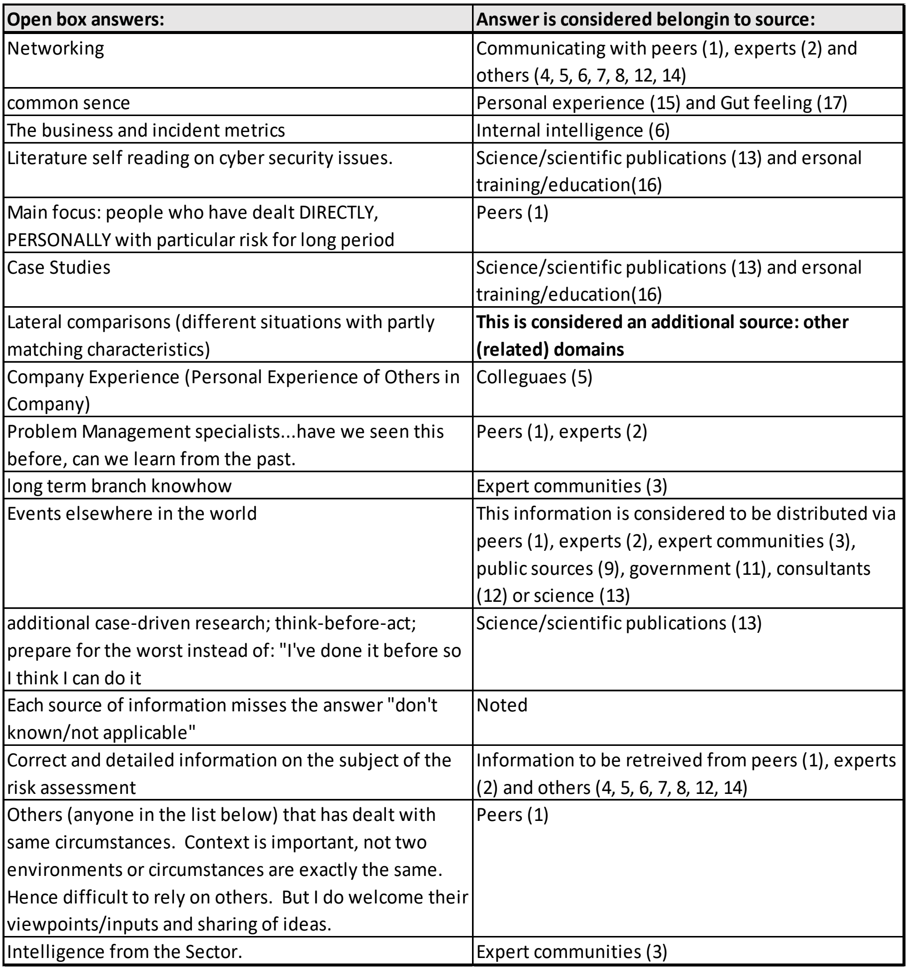
The results show high perceived reliability of personal experience as a source of security risk information.

Table 5: results of the FTOPSIS analysis, total results over the three criteria combined, in rank order based on the closeness coefficient CCi, followed by the results of each of the individual criteria: source reliability, information credibility, and source intention



Predefined information sources:	Total results:				Source Reliab.		Inform. Cred.		Source Intent.	
	di*	**di-**	**CC_i**	Rank	**CC_i**	Rank	**CC_i**	Rank	**CC_i**	Rank
Experts	0.075	0.998	0.930	**1**	1.000	1	1.000	1	0.836	4
Personal experience	0.106	0.972	0.902	**2**	0.706	9	0.953	3	1.000	1
Science/scientific publications	0.134	0.937	0.875	**3**	0.906	3	1.000	1	0.768	7
Internal intelligence	0.156	0.925	0.856	**4**	0.883	4	0.907	5	0.802	5
External intelligence (government)	0.164	0.905	0.847	**5**	0.929	2	0.930	4	0.734	9
Peers	0.178	0.885	0.832	**6**	0.861	5	0.773	8	0.853	3
Personal training/education	0.194	0.882	0.820	**7**	0.750	8	0.839	7	0.854	2
Expert communities	0.214	0.869	0.803	**8**	0.772	6	0.884	6	0.768	6
Government or government agencies	0.322	0.759	0.702	**9**	0.750	7	0.708	9	0.666	10
Colleagues	0.445	0.627	0.585	**10**	0.448	12	0.453	12	0.768	7
External intelligence (commercial)	0.465	0.609	0.567	**11**	0.683	10	0.663	10	0.420	14
Consultants/consulting organizations	0.555	0.521	0.484	**12**	0.448	12	0.514	11	0.488	13
My ‘Gut feeling’	0.580	0.530	0.478	**13**	0.450	11	0.381	13	0.557	12
Higher management	0.650	0.434	0.400	**14**	0.227	15	0.335	15	0.563	11
Supplier organizations	0.759	0.330	0.303	**15**	0.183	16	0.379	14	0.331	15
Social media sources	1.911	0.815	0.299	**16**	0.326	14	0.310	16	0.266	16
Public sources like media	1.075	0.000	0.000	**17**	0.000	17	0.000	17	0.000	17

Table 6 : additional sources of security risk information as answered to the open box question



Open box answers:	Answer is considered belongin to source:
Networking	Communicating with peers (1), experts (2) and others (4, 5, 6, 7, 8, 12, 14)
common sence	Personal experience (15) and Gut feeling (17)
The business and incident metrics	Internal intelligence (6)
Literature self reading on cyber security issues.	Science/scientific publications (13) and ersonal training/education(16)
Main focus: people who have dealt DIRECTLY, PERSONALLY with particular risk for long period	Peers (1)
Case Studies	Science/scientific publications (13) and ersonal training/education(16)
Lateral comparisons (different situations with partly matching characteristics)	**This is considered an additional source: other (related) domains**
Company Experience (Personal Experience of Others in Company)	Colleguaes (5)
Problem Management specialists...have we seen this before, can we learn from the past.	Peers (1), experts (2)
long term branch knowhow	Expert communities (3)
Events elsewhere in the world	This information is considered to be distributed via peers (1), experts (2), expert communities (3), public sources (9), government (11), consultants (12) or science (13)
additional case-driven research; think-before-act; prepare for the worst instead of: "I've done it before so I think I can do it	Science/scientific publications (13)
Each source of information misses the answer "don't known/not applicable"	Noted
Correct and detailed information on the subject of the risk assessment	Information to be retreived from peers (1), experts (2) and others (4, 5, 6, 7, 8, 12, 14)
Others (anyone in the list below) that has dealt with same circumstances. Context is important, not two environments or circumstances are exactly the same. Hence difficult to rely on others. But I do welcome their viewpoints/inputs and sharing of ideas.	Peers (1)
Intelligence from the Sector.	Expert communities (3)

In the main online survey a larger group of security practitioners participated. They indicated on which sources they base their security risk assessments. This question is answered by 174 respondents (the answer options were not mandatory so some respondents did not assess each source). The respondents are offered the opportunity to add information sources to the 17 on the predefined list. Sixteen additional sources are mentioned in the open box answer possibility. In the left column of Table 6 these answers are presented (including occasional misspelling). In the right column the answers are interpreted. Except for one they all are considered to be already represented in the predefined list. The answer containing 'lateral comparisons' is considered a valuable addition. It is interpreted as: *'Risk information from other domains like safety, business continuity etc.'*. As this additional source emerged as a result of the last survey it could not be included in further analysis. It is, however, a valuable additional source to be included in future research.

Table 7: On what information source do you base your security risk assessment? total results of the main survey, results of the FTOPSIS analysis, followed by the results of the practitioners panel (see also Table 5)

Predefined information sources:	Very imp.	Mod. Imp.	Not imp.	N	Total results main survey:				Results panel:	
	% of resp.	% of resp.	% of resp.		**di***	**di-**	**CC_i**	Rank	**CC_i**	Rank
Experts	76.4	22.4	1.1	174	0.000	0.935	1.000	**1**	0.930	1
Personal experience	61.8	35.5	2.9	173	0.151	0.792	0.840	**2**	0.902	2
Internal intelligence	56.1	41.6	2.3	173	0.194	0.744	0.793	**3**	0.856	4
Peers	56.1	39.9	4.0	173	0.210	0.734	0.777	**4**	0.832	6
Personal training/education	54.0	42.5	3.4	174	0.213	0.725	0.773	**5**	0.820	7
Expert communities	53.4	43.1	3.4	174	0.218	0.720	0.768	**6**	0.803	8
External intelligence (government)	50.0	45.3	4.7	172	0.273	0.670	0.710	**7**	0.847	5
Government or government agencies	44.2	51.7	4.1	172	0.313	0.621	0.665	**8**	0.702	9
Science/scientific publications	48.6	41.6	9.8	173	0.328	0.631	0.658	**9**	0.875	3
Colleagues	43.7	50.0	6.3	174	0.324	0.614	0.655	**10**	0.585	10
External intelligence (commercial)	35.5	54.1	10.5	172	0.444	0.498	0.528	**11**	0.567	11
My 'Gut feeling'	29.9	56.3	13.8	174	0.507	0.430	0.459	**12**	0.478	13
Consultants/consulting organizations	22.4	62.6	14.9	174	0.574	0.348	0.377	**13**	0.484	12
Public sources like media	19.5	60.9	19.5	174	0.646	0.280	0.302	**14**	0.000	17
Higher management	15.5	69.9	23.6	174	0.721	0.201	0.218	**15**	0.400	14
Supplier organizations	16.4	60.8	22.8	171	0.727	0.202	0.218	**16**	0.303	15
Social media sources	11.0	51.4	37.6	173	0.935	0.000	0.000	**17**	0.299	16

The results of the survey are presented in Table 7. The ranking of the application of the sources is based on a similar FTOPSIS analysis to allow a comparison with the perceived source quality ranking of the practitioners panel.

The ranking of the quality of the information sources seems in line with the ranking of the application of sources. There are, however, a few differences. Information from peers seems to be applied a little more (rank 4) than their quality (rank 6) might indicate. Information resulting from personal training/education is also applied more (rank 5) while the quality is ranked 7 by the practitioners panel. Intelligence information from government shows the opposite result. The most remarkable difference between quality and application is the information source science and scientific publications. The panel ranked the quality of this source of information high (rank 3) but the application of this information source is stalling at rank 9.

In this survey the individual experience of the respondents is collected: their number of years professional experience and security experience, age, education level and completed specific security trainings. A brief analysis of the influence of these characteristics on the application of information sources is performed.

Individual differences in age, education level and completed security trainings did not show any significant influence on the application of the information sources. Professional and security experience did show significant effects on the application of some of the sources. More individual experience, based on number of years' experience, seems to reduce the application of commercial external intelligence following from the chi-square statistic alongside its degrees of freedom, sample size and -value, (x2 (10, N=172)=18.3, p=.047), public sources like media (x2 (10, N=174)=22.5, p=.013), and information offered by government/government agencies (x2 (10, N=172)=21.6, p=.017). On the other hand increasing experience, in number of years, seems to increase the application of personal experience (x2 (10, N=173)=18.6, p=.045) and gut feeling (x2 (10, N=174)=22.8, p=.011).

5. Discussion and Conclusions

The first research question of this study: What sources of security risk information are considered by practitioners? yielded a predefined list of 17 possible sources as compiled during a brainstorm session with senior experts (n=8). This list is supported and not further supplemented during the panel consultation (n=18). In the main survey (n=174) one possible additional source is proposed: *Risk information from other domains like safety, business continuity etc.* Future research might include this additional source of security risk information.

In the second part of this study a security practitioners panel (N=18) assessed and classified the predefined list of security risk information sources. To answer the second research question: How reliable are these sources as perceived by these practitioners, they assessed the sources by applying three criteria, as presented in Figure 1. The results, analyzed applying the MCDM FTOPSIS methodology, allowed a quality ranking of the predefined list of information sources. The results are presented in Table 5. This table shows the source quality ranking. The overall ranking in this table compared to the ranking of the individual criteria allows some interesting observations.

Experts are perceived to be the highest quality sources of information unless the fact that their intention (rank 4) seems not always to be in line with the intention of the panelists. More remarkable is the second highest ranking of ‘personal experience’. The intention of the individuals is, as might be expected, completely in line. The credibility of information originating from personal experience is ranked third, the reliability of this source, on the other hand, is only ranked 9th. This overall second highest ranking of ‘personal experience’ is in line with findings in previous work of the authors on confidence of security professionals in respect to their security risk assessments. Even if they are aware of incomplete security risk information they still have confidence in their assessments (de Wit, Pieters, and van Gelder 2023). The practitioners panel in this study, on the other hand, assign little credibility to their own gut feeling. Gut feeling is, however, knowing without knowing why (Kahneman, Sibony, and Sunstein 2021) and thus, can be considered a kind of experience (Klein, 2008). The panelists seem to perceive gut feeling and experience as different sources of which the first is less trusted.

Science/scientific publications are ranked third, the information credibility of this source is regarded top ranked (equal to experts). The intention of science is ranked 7th. These results might indicate the perceived high quality of science but a limited alignment of intention which might be interpreted as a limited practical use. The ranking of the intention of the source ‘external intelligence (government)’ is even lower at rank 9. This source is considered one of the most reliable, rank 2, their information credibility is ranked 4th.

Overall the proposed additional criterion ‘source intention’ seems to add interesting additional information on information sources that would not have been noticed with the original NATO system. This additional criterion seems to add value to a deeper assessment of sources and might be added in future evaluations.

This study does seem to confirm previous work in other domains that risk communication by government and industry is considered less trustworthy (Fessenden-Raden, Fitchen, and Heath 1987; McCallum, Hammond, and Covello 1991; Slovic, Flynn, and Layman 1991; Trumbo and McComas 2003). Government sources rank relatively low on the perceived source quality list (rank 5 and 9) and industry even lower (rank 11, 12 and 15).

Table 7 shows the results of the main survey answering the third research question of this study: Which sources are applied in security risk assessment praxis? These results, combined with the results of the quality ranking, allow answering the research question: are the most applied sources also perceived as the most credible ones?

The two rankings are, besides a few minor differences, similar. This indicates that the perceived high quality information sources, as assessed by the practitioners panel, are applied and perceived as important for risk assessments in praxis, as indicated by the group of respondents. The most remarkable difference between the rankings is the source: science/scientific publications. It is perceived a high quality source (rank 3 by the panel) but seems to be less applied in daily praxis (rank 9 by the respondents). This might be explained by the additional proposed information quality criterion: source intention. The panelists assign a high source reliability to science/scientific publications (rank 3), the highest information credibility (rank 1 ex aequo with experts) but on source intention it is ranked at position 7. This means that there is at least some doubt on source intention or aspiration, goals and objectives might be in line (but this is not certain). The results of the main survey seem to support this. The respondents indicate that they do not think this source is important for their daily practice. Without the proposed additional criterion on information quality: source intention, this could not properly be explained.

Familiarity, which is found important by other scholars as referred to in the background section (Redmiles, Kross, and Mazurek 2016; Denize and Young 2007; Hertzum et al. 2002; McAllister 1995) seems to be reflected in the results of this study. Information from peers who can be considered familiar, seems to be applied a little more (rank 4) than their quality (rank 6) might indicate. This could also be a result of the influence of source availability (Kim & Sin, 2011; O'Reilly III, 1982) as information from peers can be expected to be easy available and accessible. Previous work by other scholars indicated that, although, the quality of information/information sources is indicated to be most important, in praxis the availability of information/information sources is driving behavior and the application of information (Kim and Sin 2011; Hertzum 2002; O'Reilly III 1982). Sources from within the own organization can also be considered familiar (Hertzum, 2002). The source internal intelligence (4) ranks high, however, the other internal sources are ranked relatively low: colleagues (10), and higher management (14).

Interpersonal communication is found driving concern over risk more than mediated communication (Trumbo 1996; Kasperson et al. 2012). The top 5 ranking of the application of information sources (Table 7) show sources that can be interpreted as primarily interpersonal. These sources are found to amplify risk signals and, thus, can be expected to raise the risk perception of the security professionals.

Another factor influencing trust is a source is found to be credibility within a community (Kasperson et al. 2012). In this study and survey experts are defined as: knowledgeable people recognized in the field. In this study experts are ranked first in both the quality ranking and the ranking of application in daily praxis. These results seem to confirm the findings of Kasperson. Whom we trust is further based on a similarity in basic values rather than competence (Earle and Cvetkovich 1995). If we would translate ‘similarity in basic values’ to ‘shared intentions’, the proposed additional criterion ‘source intention’ would, according to Earle & Cvetkovich, guide us to the top trusted sources. The last column of Table 5 shows the ranking of sources based on the source intention criterion. Top ranked are personal experience (1) and personal training/education (2) which would indicate that the professionals foremost trust themselves. Previous research by the authors already showed a high level of confidence of the professionals even if they lack adequate information (de Wit, Pieters, and van Gelder 2023). Very close behind these personal sources are peers (3) and experts (4). Both might be considered to have a 'similarity in basis values' supporting the findings of other scholars.

The trustworthiness of risk communication by commercial organizations and government is found to be limited in other studies (Fessenden-Raden et al., 1987; McCallum et al., 1991; Slovic et al., 1991; Trumbo & McComas, 2003). This study seems to confirm this. Commercial sources like external commercial intelligence (11), consultants (12), and supplier organizations (15) are at the lower end of this ranking. They might contain too much marketing and are, therefore, considered less trustworthy (Redmiles, Kross, and Mazurek 2016). Government sources rank somewhat higher: external government intelligence (5), government/government agencies (9). As other scholars concluded this lower perceived trustworthiness is primarily caused by deviating goals of both commercial and government risk information sources. The commercial and government sources indeed rank even lower on the source intention scale (last column of Table 5): commercial intelligence (14), consultants (13), supplier organizations (15), external government intelligence (9), government/government agencies (10).

Finally the research question: can we observe differences between security professionals based on their expertise (experience and knowledge), is answered. The individual characteristics of the respondents seem to influence the application of a few of the information sources during their security risk assessments. A significant negative association is identified between experience, both professional and security, on applying the sources:

- commercial external intelligence (p=.047),
- public sources like media (p=.013),
- and government/government agencies (p=.017)

More experienced professionals seem to value these sources less than unexperienced professionals. On the other hand significant positive associations are identified between experience and the sources:

- personal experience (p=.045),
- gut feeling (p=.011)

Note the difference in p-values that indicate a stronger significance.

It seems that more experienced practitioners have more confidence in their own perception and judgement. Previous work of the authors of this study also identified the influence of experience on confidence and the need for additional information in security risk assessments. More experienced security professionals express higher levels of confidence, even if risk information is known to be incomplete. This indicates confidence in their own expertise. More experienced security professionals also indicated they have a lesser need for additional information in general than less experienced professionals when assessing security risks, even if the information is known to be incomplete (de Wit, Pieters, and van Gelder 2023). The results in this survey seem to confirm these findings, at least for some of the information sources.

This study is exploratory and studying phenomena in the security domain that, to the best of our knowledge, have not been studied before. The exploratory nature of this research results in interesting findings that: a, identify topics for future research in the academic domain and b, help the professional domain understanding their daily praxis and offers valuable insights for reflection. The findings of our study can improve professional security risk assessments by assigning weights to the sources delivering information with the highest perceived quality. Therefore this study offers a quality ranking of possible sources of information to the professional domain. The in this study applied enhanced NATO system additionally presents the professional community a tool for the assessment of their sources. Organizations and individuals providing risk information, on the other hand, can find valuable cues in this study to improve their quality. As the English philosopher and physician John Locke remarked over 300 years ago: *'The improvement of understanding is for two ends: first, our own increase of* *knowledge; secondly, to enable us to deliver that knowledge to others.'* This paper seeks to do both and hopes to encourage the academic as well as the professional security domain to translate the offered knowledge into improvement of selection and assessment of sources of security risk information.

Literature

Ajzen, Icek. 2011. "The theory of planned behaviour: reactions and reflections." In.: Taylor & Francis.

Alhawari, Samer, Louay Karadsheh, Amine Nehari Talet, and Ebrahim Mansour. 2012. "Knowledge-based risk management framework for information technology project." *International Journal of Information Management* 32 (1):50-65.

Baker, James D, James M McKendry, and Douglas J Mace. 1968. *Certitude judgments in an operational environment*. Vol. 200: US Army Behavioral Science Research Laboratory.

Bennett, Matthew. 2020. "Should I do as I'm told? Trust, Experts, and COVID-19." *Kennedy Institute of Ethics Journal* 30 (3):243-63.

Capet, Philippe, and Thomas Delavallade. 2014. *Information evaluation*: Wiley Online Library.

Citroen, Charles L. 2011. "The role of information in strategic decision-making." *International Journal of Information Management* 31 (6):493-501.

Cooke, Roger M. 1991. *Experts in uncertainty*. New York: Oxford University Press.

Cooke, Roger M, and Louis LHJ Goossens. 2008. "TU Delft expert judgment data base." *Reliability Engineering & System Safety* 93 (5):657-74.

de Meij, Cachet. 2010. *Subjectieve en objectieve veiligheid: een overbrugbare kloof?* : Erasmus University.

de Wit, J., Pieters, W., & van Gelder, P. (2023). Bias and noise in security risk assessments, an empirical study on the information position and confidence of security professionals. Security Journal, 1-22.

Deb, Ashok, Kristina Lerman, and Emilio Ferrara. 2018. "Predicting cyber-events by leveraging hacker sentiment." *Information* 9 (11):280.

Denize, Sara, and Louise Young. 2007. "Concerning trust and information." *Industrial Marketing Management* 36 (7):968-82.

Dongo, Irvin, Yudith Cardinale, and Ana Aguilera. 2019. Credibility analysis for available information sources on the web: a review and a contribution. Paper presented at the 2019 4th International Conference on System Reliability and Safety (ICSRS).

Earle, Timothy C, and George Cvetkovich. 1995. *Social trust: Toward a cosmopolitan society*: Greenwood Publishing Group.

Einhorn, Hillel J. 1974. "Expert judgment: Some necessary conditions and an example." *Journal of applied psychology* 59 (5):562.

Fessenden-Raden, June, Janet M Fitchen, and Jenifer S Heath. 1987. "Providing risk information in communities: Factors influencing what is heard and accepted." *Science, Technology, & Human Values* 12 (3/4):94-101.

Fischbein, M, and I Ajzen. 1975. "Attitude intention and behaviour: An introduction to theory and research." *Reading Mass: Ahdison-Wesley*.

Gal-Or, Esther, and Anindya Ghose. 2005. "The economic incentives for sharing security information." *Information Systems Research* 16 (2):186-208.

Gore, Julie, and Paul Ward. 2018. "Naturalistic Decision Making Under Uncertainty: Theoretical and Methodological Developments–An Introduction to the Special Section." *Journal of Applied Research in Memory and Cognition*.

Hawley, Katherine. 2012. *Trust: A very short introduction*: OUP Oxford.

Hertzum, Morten. 2002. "The importance of trust in software engineers' assessment and choice of information sources." *Information and Organization* 12 (1):1-18.

Hertzum, Morten, Hans HK Andersen, Verner Andersen, and Camilla B Hansen. 2002. "Trust in information sources: seeking information from people, documents, and virtual agents." *Interacting with computers* 14 (5):575-99.

Hoffman, Robert R, and Gary L Klein. 2017. "Challenges and Prospects for the Paradigm of Naturalistic Decision Making." *Journal of Cognitive Engineering and Decision Making* 11 (1):97-104.

Hota, HS, LK Sharma, and S Pavani. 2014. "Fuzzy TOPSIS method applied for ranking of teacher in higher education." In *Intelligent Computing, Networking, and Informatics*, 1225-32. Springer.

Husák, Martin, Jana Komárková, Elias Bou-Harb, and Pavel Čeleda. 2018. "Survey of attack projection, prediction, and forecasting in cyber security." *IEEE Communications Surveys & Tutorials* 21 (1):640-60.

Icard, Benjamin. 2019. "Lying, deception and strategic omission: definition and evaluation." Université Paris sciences et lettres.

Icard, Benjamin. 2023. "Facts versus Interpretations in Intelligence: A Descriptive Taxonomy for Information Evaluation."

ISO. 2018. "ISO 31000 Risk management - guidelines." In. Geneva: International Organization for Standardization.

ISO/IEC. 2011. "ISO/IEC 27005 Information technology_Security_techniques_Information security risk management." In. Geneva: ISO.

ISO/IEC. 2016. "ISO/IEC 27000 International standard Information Technology Security techniques." In. Geneva: ISO.

Jerman-Blažič, Borka. 2008. "An economic modelling approach to information security risk management." *International Journal of Information Management* 28 (5):413-22.

Johannessen, Jon-Arild, Johan Olaisen, and Bjørn Olsen. 2001. "Mismanagement of tacit knowledge: the importance of tacit knowledge, the danger of information technology, and what to do about it." *International Journal of Information Management* 21 (1):3-20.

Johnson, Loch K. 2010. *The Oxford handbook of national security intelligence*: Oxford University Press.

Kahneman, Daniel, and Gary Klein. 2009. "Conditions for intuitive expertise: a failure to disagree." *American psychologist* 64 (6):515.

Kahneman, Daniel, Olivier Sibony, and Cass R. Sunstein. 2021. *Noise, a Flaw in Human Judgment*. London: William Collins.

Kasperson, Jeanne X, Roger E Kasperson, Nick Pidgeon, and Paul Slovic. 2012. "The social amplification of risk: Assessing 15 years of research and theory." *Social contours of risk*:217-45.

Kim, Kyung-Sun, and Sei-Ching Joanna Sin. 2011. "Selecting quality sources: Bridging the gap between the perception and use of information sources." *Journal of Information Science* 37 (2):178-88.

Klein, Gary. 1997. "The recognition-primed decision (RPD) model: Looking back, looking forward." *Naturalistic decision making*:285-92.

Klein, Gary. 2008. "Naturalistic decision making." *Human factors* 50 (3):456-60.

Klein, Gary A. 1993. *A recognition-primed decision (RPD) model of rapid decision making*: Ablex Publishing Corporation New York.

Korkisch, F. 2010. "NATO gets better intelligence." *IAS Reader, Strategy Paper*:1-2010.

Krisper, Michael, Jürgen Dobaj, and Georg Macher. 2020. Assessing Risk Estimations for Cyber-Security Using Expert Judgment. Paper presented at the European Conference on Software Process Improvement.

Lehman, David W, Kieran O'Connor, Balázs Kovács, and George E Newman. 2019. "Authenticity." *Academy of Management Annals* 13 (1):1-42.

Lipshitz, Raanan, Gary Klein, Judith Orasanu, and Eduardo Salas. 2001. "Taking stock of naturalistic decision making." *Journal of Behavioral Decision Making* 14 (5):331-52.

Lipshitz, Raanan, and Orna Strauss. 1997. "Coping with uncertainty: A naturalistic decision-making analysis." *Organizational behavior and human decision processes* 69 (2):149-63.

Mandel, David R, and Daniel Irwin. 2021. "Uncertainty, intelligence, and national security decisionmaking." *International Journal of Intelligence and CounterIntelligence* 34 (3):558-82.

Mandel, David R, Daniel Irwin, Mandeep K Dhami, and David V Budescu. 2023. "Meta-informational cue inconsistency and judgment of information accuracy: Spotlight on intelligence analysis." *Journal of Behavioral Decision Making* 36 (3):e2307.

Markman, Arthur B. 2017. "Combining the Strengths of Naturalistic and Laboratory Decision-Making Research to Create Integrative Theories of Choice." *Journal of Applied Research in Memory and Cognition*.

McAllister, Daniel J. 1995. "Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations." *Academy of management journal* 38 (1):24-59.

McCallum, David B, Sharon Lee Hammond, and Vincent T Covello. 1991. "Communicating about environmental risks: How the public uses and perceives information sources." *Health Education Quarterly* 18 (3):349-61.

Meyer, Mary A, and Jane M Booker. 2001. *Eliciting and analyzing expert judgment: a practical guide*: SIAM.

Möller, Niklas. 2012. "The concepts of risk and safety." *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk* 1:55-85.

Nădăban, Sorin, Simona Dzitac, and Ioan Dzitac. 2016. "Fuzzy TOPSIS: A general view." *Procedia computer science* 91:823-31.

O'Hara, Kieron. 2012. "A general definition of trust."

O'Reilly III, Charles A. 1982. "Variations in decision makers' use of information sources: The impact of quality and accessibility of information." *Academy of management journal* 25 (4):756-71.

Oppelaar, Wittebrood. 2006. "Angstige burgers: de determinanten van gevoelens van onveiligheid onderzocht."

Pliske, Rebecca, and Gary Klein. 2003. *The naturalistic decision-making perspective*, *Emerging Perspectives on Judgement and Decision Research*. Cambridge: Cambridge University Press.

Powell, Thomas, Serena Oggero, Joris Schook, and Emma Westerveld. 2019. "Dealing with Uncertainty in Hybrid Conflict: A Novel Approach and Model for Uncertainty Quantification in Intelligence Analysis."

Redmiles, Elissa M, Sean Kross, and Michelle L Mazurek. 2016. How i learned to be secure: a census-representative survey of security advice sources and behavior. Paper presented at the Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.

Roberts, Aaron PJ, and Jon C Cole. 2018. "Naturalistic Decision Making: Taking a (Cognitive) Step Back to Take Two Steps Forward in Understanding Experience-Based Decisions." *Journal of Applied Research in Memory and Cognition*.

Ryan, Julie JCH, Thomas A Mazzuchi, Daniel J Ryan, Juliana Lopez De la Cruz, and Roger Cooke. 2012. "Quantifying information security risks using expert judgment elicitation." *Computers & Operations Research* 39 (4):774-84.

Salih, Mahmood M, BB Zaidan, AA Zaidan, and Mohamed A Ahmed. 2019. "Survey on fuzzy TOPSIS state-of-the-art between 2007 and 2017." *Computers & Operations Research* 104:207-27.

Samet, Michael G. 1975. "Quantitative interpretation of two qualitative scales used to rate military intelligence." *Human Factors* 17 (2):192-202.

Schwarz, Norbert, and Leigh Ann Vaughn. 2002. "The availability heuristic revisited: Ease of recall and content of recall as distinct sources of information."

Seagle, Adriana N. 2015. "Intelligence sharing practices within NATO: An english school perspective." *International Journal of Intelligence and CounterIntelligence* 28 (3):557-77.

Sevkli, Mehmet, Selim Zaim, Ali Turkyilmaz, and Metin Satir. 2010. An application of fuzzy Topsis method for supplier selection. Paper presented at the International Conference on Fuzzy Systems.

Singh, Harpreet, Madan M Gupta, Thomas Meitzler, Zeng-Guang Hou, Kum Kum Garg, Ashu MG Solo, and Lotfi A Zadeh. 2013. "Real-life applications of fuzzy logic." In.: Hindawi.

Skjong, Rolf, and Benedikte H Wentworth. 2001. Expert judgment and risk perception. Paper presented at the the eleventh international offshore and polar engineering conference.

Slovic, Paul, James H Flynn, and Mark Layman. 1991. "Perceived risk, trust, and the politics of nuclear waste." *Science* 254 (5038):1603-7.

Stanovich, Keith E, and Richard F West. 2000. "Individual differences in reasoning: Implications for the rationality debate?" *Behavioral and brain sciences* 23 (5):645-65.

Talbot, Julian, and Miles Jakeman. 2011. *Security risk management body of knowledge*. Vol. 69: John Wiley & Sons.

Trumbo, Craig W. 1996. "Examining psychometrics and polarization in a single-risk case study." *Risk Analysis* 16 (3):429-38.

Trumbo, Craig W, and Katherine A McComas. 2003. "The function of credibility in information processing for risk perception." *Risk Analysis: An International Journal* 23 (2):343-53.

Van Leeuwen, Theo. 2001. "What is authenticity?" *Discourse studies* 3 (4):392-7.

Viljanen, Lea. 2005. Towards an ontology of trust. Paper presented at the International conference on trust, privacy and security in digital business.

Wang, Yu-Jie, and Hsuan-Shih Lee. 2007. "Generalizing TOPSIS for fuzzy multiple-criteria group decision-making." *Computers & Mathematics with Applications* 53 (11):1762-72.

Weber, Martin. 1987. "Decision making with incomplete information." *European journal of operational research* 28 (1):44-57.

PART 3

PROFESSIONAL PUBLICATIONS

CHAPTER 5

Unwrapping Bias in Security Decisisons: Illogical Decision Making?

Johan de Wit, Claire Meyer

This chapter is a reprint from an original cover story in Security Management, the award-winning publication of ASIS International, the preeminent international organization for security professionals. It covers a summary of the results of the papers presented in the chapters 1 and 3. It is the version for the professional domain in which some brief actions for enhancing decision making are added.

This article is published in the *Security Management, May/June 2022* and ended on the fifth place of most viewed articles of 2022 of this journal.

SECURITY
MANAGEMENT
Unwrapping
Bias in
Security
Decisions
Cognitive biases color our judgment. For security professionals, this can have serious ramifications for risk assessments.
By Johan de Wit and Claire Meyer

Cover Story

Even when we try to limit outside influence and make purely rational, logical decisions, humans are still incredibly susceptive to cognitive peculiarities that color our judgment. For security professionals, this can have serious ramifications for reasonable risk assessments.

Do you consider yourself an above-average decision maker? Does logic drive most, if not all, of your security risk mitigation decisions? Think again.

Most security professionals believe that they are better decision makers than the average person, but recent research has proven this is not the case. In fact, security leaders often fall prey to the same biases as the majority of the population, and they may find themselves relying on gut feelings and prior experience over facts and probability. Unlike for most people, however, security professionals' biases could have significant ramifications on risk management and safety decisions.
Awareness is the first step to correct this issue, and recent research into security professionals' decision-making tools has unveiled myriad pitfalls.

Risk Management Processes

Risk management processes—including the guidance published in the Risk Assessment Standard from ANSI, ASIS, and RIMS—appear organized and can be interpreted as precise, accurate, and objective. External context, likelihoods, vulnerabilities, existing controls, risk tolerance, and options are communicated and considered fairly, driving additional risk identification, analysis, evaluation, and treatment as required.

Closer inspection, however, reveals subjective human decision making plays a major role. Each step in the process is a decision: What do we consider to be part of the context? What threats do we take into account, against what assets, and within what timeframe? Which controls do we compare, and what is their effectiveness? Do we evaluate that effectiveness? If so, how and how often?

Subjective decisions like these structure the content of a security management process, and the output reflects the personal judgment of the security decision maker.

This should not be particularly surprising, given the nature of risk. The Risk Assessment Standard defines risk as the "effect of uncertainty on the achievement of strategic, tactical, and operational objectives," and the definition clearly indicates the two main components of risk and risk assessments: effects (often referred to as consequences) and uncertainty (often expressed as likelihood or probability). Because any risk refers to a future state of affairs, it is by definition impossible to predict exactly. After all, as Sven Ove Hansson wrote in the Handbook of Risk Theory, "Knowledge about risk is knowledge about the unknown."

The security risk field is dealing with malicious—and therefore manmade—risks. This aspect of security management adds an extra dimension to the uncertainty. People performing malicious actions, such as intrusions or thefts, try to be unpredictable or concealed to evade existing risk controls. This dynamic context—with bad actors' ever-changing modus operandi and the large variety of situations, including locations and times—adds to the uncertainty.

While past security risks and events help inform the risk assessment process, they do not provide certainty about future risks. Therefore, risk assessments are a combination of experience, expert judgment, and objective facts and evidence. And that judgment—however well informed by past experience—is susceptible to assumptions and biases.

Bias vs. Logic

Over the centuries, philosophers worldwide have explored the concepts of human judgment and decision-making processes. Eventually, they settled on maximization theories—humans are supposed to apply a form of rational decision making with the goal of achieving the best possible outcome. For example, a purely rational human would search the supermarket shelves until he or she uncovered the perfect jar of pasta sauce—weighing variables of volume, price, nutritional value, and taste.

In reality, however, few people apply that depth of rationality to everyday decisions. Instead, they grab a sauce that is good enough for what they need and move on—a concept psychologists dub "satisficing." There are many reasons that cause a consumer to settle on one item over another or, from a security lens, to make one risk mitigation choice over another. Often, those reasons hinge on personal preferences and cognitive biases.

In 1979, scholars Amos Tversky and Daniel Kahneman introduced the prospect theory, which clearly identified systematic ways in which humans make decisions that are not optimized for the best possible outcome. Decisions turn out to be less logic-based and more prone to heuristics, mental shortcuts, and biases.

Kahneman, who received the Nobel Prize in Economics in 2003 for his work, espouses that there are two systems of thinking: fast and slow. Fast decisions rely on intuition and prior experience, and they are almost automatic. A firefighter arriving at the scene of a blaze may make split-second decisions based on his or her experience with similar past events. But if the firefighter confronts bright green flames or some other abnormality, decision making is likely to slow down, becoming more deliberate as the firefighter weighs information and debates possibilities. This takes significantly more brainpower, so humans tend to revert to fast decision making whenever possible.

However, where security decisions are concerned, it can be invaluable to exert the extra effort to slow down, debate different possibilities, and bring in different points of view to make more informed, rational decisions that acknowledge biases but don't fall prey to them.

Information and Confidence

Humans are notoriously overconfident. An infamous 1981 study by Swedish researcher Ola Swenson found that 93 percent of Americans considered themselves above average drivers. Statistically, this is impossible. But security professionals seem to fall into the same trap when it comes to making informed decisions, believing that the rules of informed and rational decision making can be circumvented with enough professional experience.

One of the authors of this article (de Wit) has studied security risk decision making within both physical security and cybersecurity domains in recent years as part of a doctoral research program. Over a span of three surveys so far—including approximately 170 security decision makers—researchers explored security professionals' relationship with information and how it affects decisions and the influence of biases on decision making.

According to the author's research, 56.6 percent of security professionals indicated that even if they lack exact information on the consequences of security risk, they can still estimate it; 60.9 percent said they could accurately estimate a risk's likelihood, even without exact information. Three-quarters said that situations where they can estimate neither the consequences nor the likelihood rarely occur.

This lack of exact information—which the security professionals were cognizant of—did not influence the confidence they expressed in this own judgment. When asked how confident they were in their security judgments concerning the consequences of risks, no fewer than 73.8 percent indicated they were always confident or confident most of the time. Likewise, 67.7 percent said the same of their security judgment when it came to the likelihood of risks.

Security professionals had preferences for some information sources over others, as well. Experts (76.3 percent) and peers (56.4 percent) were the most trusted, and 62.2 percent said their own experience is very important for their judgment. Only 15 percent said information from higher management is very important for risk management decisions.

The more experience security professionals have, the more confident—and potentially overconfident—they are in their decisions, the research found.

Researchers also asked whether the security professionals would like more information to make their decisions, and the more experienced professionals refused, choosing to rely on their gut feelings instead.

Biases to Watch

A huge number of cognitive biases have been identified in recent years, and those biases can wreak havoc on risk management decisions. The author's research analyzed a set of biases against security decision making practices and found several that are likely to influence risk management.

Certainty effect. It's time for a gamble: If you had to make a choice between a 100 percent chance of receiving $150 or an 80 percent chance of receiving $200, which would you choose? When the outcome is a gain, decision makers under the influence of the certainty effect will tend to prefer certainty over a 20 percent chance of receiving nothing, even though the choice of an 80 percent chance at $200 is optimal.

Security professionals show a similar level of vulnerability as laypeople for this bias. Three-quarters of security professionals selected the certain but less optimal outcome, indicating that in real-life situations they may not maximize security risk reduction or may spend resources less efficiently. Even when researchers exchanged the monetary gains and losses with security risk reduction to reflect a more realistic situation, this effect guided the decision of the security professionals.

Reflection effect. This is similar to the certainty effect, but the reflection effect looks at losses instead of gains. If you have a certainty of losing $150 or an 80 percent chance of losing $200 (and therefore a 20 percent chance of losing no money at all), people will regularly take the gamble.

Security professionals gamble here at a similar rate to laypersons. When a possible loss is at stake, 84 percent of security professionals take the gamble for a possible higher loss than accepting a certain but lower loss. As one might expect risk-avoidance behavior from security risk professionals, this finding is surprising.

Isolation effect. Very few decisions happen in isolation, and when a decision contains several stages, decision makers tend to ignore the first stages and focus on the last one only. This bias demonstrates a level of ignorance about the comprehensive view on a combination of decisions—how one factor will influence another—and it can lead to suboptimal outcomes.

Fortunately, an antidote to this bias is one of the fundamental principles in security. A layered defense strategy is the implementation of multiple, independent risk reduction measures. These layers, when taken in combination, should reduce risk to an acceptable level.

Unfortunately, you can test susceptibility to the isolation effect, and 83 percent of security professionals in the research chose suboptimal outcomes. What might this look like in concentric layers of security? Most likely the isolation effect would come into play when one of the layers receives an outsized amount of attention and the rest of the layers are neglected.

Nonlinear preferences. One percent is one percent, no matter which percent it is, right? Wrong—at least where human decision making is concerned. This bias (also known as value function or probability distortion) demonstrates that the perception of one percent when changing from 100 percent to 99 percent is very different than when changing from 21 percent to 20 percent. This also works in larger percentage jumps—100 to 25 versus 80 to 20, for example. Both were divided by four, but the change in perceived value from 100 percent to a quarter feels significantly more drastic. (Research has determined that the single percentage change between 100 and 99 percent is weighted to hold the value of 5.5 percent, oddly enough.)

Small probabilities tend to be overrated as a result of nonlinear preferences, which can strongly effect security decisions. For example, the probability of a terrorist attack is usually quite low, but security professionals are likely to devote outsized resources to mitigating that risk, both because of its potential high impact and the bias for nonlinear preferences, adding additional weight to the low probability.

Conjunction fallacy. Consider two scenarios in which you are the security manager of a private pharmaceutical situation:

1) *How would you estimate the likelihood of experiencing a successful attempt to extract intellectual property during the upcoming year?*

2) *How would you estimate the likelihood of experiencing a successful attempt to extract intellectual property by suspected state-affiliated attacker groups specifically targeting COVID-19 research, using one or more insiders during the upcoming year?*

Did the additional conjunctions—by suspected state-affiliated attacker groups, specifically targeting COVID-19 research, and using one or more insiders—change your risk assessment? Logic would lead to the conclusion that the short version is more likely, as the additional details make the case more specific and reduce the likelihood. The results of research on security professionals show the opposite effect.

The survey participants were divided into two groups and were presented with either the short or long version of the scenario. On average, the likelihood of the longer scenario was estimated 12.5 percent higher. Nearly three-quarters of security professionals assessed that the detailed case study was more likely than the shorter one, with no significant influence one way or the other for security training or education level.

This is an example of the conjunction fallacy—the more detailed a scenario, the more realistic and likely it feels. This has potentially serious implications for real-life security risk assessments, though. More information on a security risk almost automatically and unconsciously raises the risk assessment of individual security risk decision makers when, logically, the more specific details should reduce the likelihood. This could lead, for example, a retailer to invest time and resources in addressing the risk of a high-profile flash robbery at a flagship store—which is a specific, low-frequency incident at a specific location—instead of shoplifting as a whole.

Corrective Action

The research indicated that security professionals are as vulnerable to laypeople to studied cognitive biases. As a result, their decisions are likely to be influenced by bias and might turn out to be less optimal, efficient, or effective. Security and professional experience, security training, and level of education do not show an observable significant effect on circumventing cognitive bias.

However, all hope is not lost. Once security professionals begin to recognize biases at work in their decision-making processes, they can take action to mitigate them—at least on less time-sensitive, large-scale decisions like organizational strategy or broad risk mitigation efforts. There are many techniques available to root out the influence of bias and mitigate its risks, and while extensive research has been done on this topic elsewhere, a few simple suggestions to start with are listed below.

Gather a group. Multiple viewpoints and healthy debate can help identify cognitive missteps and uncover unorthodox solutions. If appropriate, bring in uncommon participants—such as interns, security officers, HR professionals, or facilities staff—for additional perspectives. Consider appointing a devil's advocate within the group to challenge every assumption and point out potential pitfalls. This person is meant to be somewhat exasperating, so appoint the naysayer with care and outline his or her responsibilities to the group.

Slow down. Fast thinking often relies on snap decisions and intuition, rather than reason. If the situation allows, plan to make decisions over longer periods of time and use that time to gather additional information and input.

Aim for options. Don't stop after you reach one strong contender to mitigate risk. Aim for five instead. By fixating on the first strong solution, decision makers fall into systems of fast thinking. Requiring additional options will require a decision maker to slow down, reconsider available information and possibilities, and arrive at a better-reasoned conclusion.

Undercut the optimism. Optimistic thinking is a hallmark of many decision-making missteps. Harvard Business Review recommended performing a premortem, which imagines a future failure and then explains the cause. This technique helps identify problems that the optimistic eye for success fails to spot. At the same time, it helps decision makers prepare backup plans and highlights factors that may influence success or failure.

The most important step in this process is to recognize the “flaw in human judgment,” as Kahneman calls it. And despite security professionals’ proclaimed confidence in their own judgment, they are as vulnerable as anyone else to bias and similar cognitive peculiarities. Knowing what you don’t know and acting on that awareness should make security practitioners more reasoned in their judgment.

Johan de Wit works for Siemens Smart Infrastructure as the technical officer, enterprise security, and he is involved in global Siemens portfolio development. He holds a master’s degree in security science and a PhD research position at Delft Technical University where he is exploring the characteristics of security risk assessments.

Claire Meyer is managing editor of Security Management. Connect with her on LinkedIn or contact her directly at claire.meyer@asisonline.org

Literature

Risk Assessment Standard: https://store.asisonline.org/risk-assessment-standard-e-book.html

Handbook of Risk Theory: https://link.springer.com/referencework/10.1007/978-94-007-1433-5

Maximizing vs. satisficing: https://www.psychologytoday.com/us/blog/science-choice/201506/satisficing-vs-maximizing

Thinking, Fast and Slow: https://www.amazon.com/Thinking-Fast-Slow-Daniel-Kahneman-dp-0385676514/dp/0385676514/ref=dp_ob_title_bk

Cybersecurity domain research: https://www.witpress.com/Secure/elibrary/papers/SAFE21/SAFE21016FU1.pdf

Prospect theory, security professionals: https://journals.open.tudelft.nl/jiss/article/view/5700

Overconfident drivers: https://www.sciencedirect.com/science/article/abs/pii/0001691881900056?via%3Dihub

Corrective action, HBR: https://hbr.org/2017/03/root-out-bias-from-your-decision-making-process

HBR, premortems: https://hbr.org/2015/05/outsmart-your-own-biases

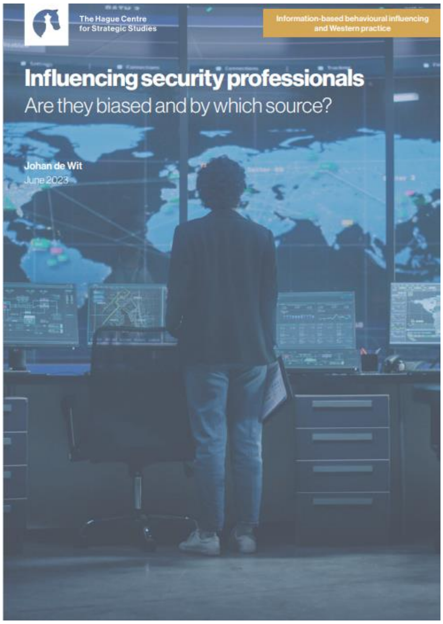
CHAPTER 6

Influencing Security Professionals, are They Biased and by Which Source?

Johan de Wit

This chapter is a reproduction of a paper published by The Hague Centre for Strategic Studies (HCSS) as part of the project: Platform Influencing Human Behaviour, commissioned by the Royal Netherlands Army. The aim of this platform is to build and share knowledge on information-based behavioural influencing in the military context. This paper, as presented in this chapter, presents brief summaries of the four studies, presented in part 2 of this dissertation, each exploring factors that drive our intuitive or reasoned perceptions of risk.

This peer reviewed article is published online via the HCSS website: https://hcss.nl/report/influencing-security-professionals-are-they-biased-and-by-which-source/ on 12 June 2023.


The Hague Centre for Strategic Studies
Information-based behavioural influencing and Western practice
Influencing security professionals
Are they biased and by which source?
Johan de Wit
June 2023

Paper series: Information-based behavioural influencing and Western practice

Paper series: Information-based behavioural influencing and Western practice.

The military application of information has a long history in influencing the outcome of war and conflict on the battlefield. Be it by deceiving the opponent, maintaining troop confidence, or shaping public opinion. These tactics are placed under the banner of influencing human behaviour. Behavioural influencing is the act of meaningfully trying to affect the behaviour of an individual by targeting people's knowledge, beliefs and emotions.

Within the Dutch armed forces these tactics fall under title of Information Manoeuvre. With the ever-larger and more evasive employment of information-based capabilities to target human cognition, the boundaries of the physical and cognitive battlefield have begun to fade.

This paper is published as part of the project Platform Influencing Human Behaviour, commissioned by the Royal Netherlands Army. The aim of this platform is to build and share knowledge on information-based behavioural influencing in the military context. We bring together international experts and practitioners from both military and academic backgrounds to explore the military-strategic, ethical, legal, and societal issues and boundaries involved. Responsibility for the content rests solely with the authors and does not constitute, nor should it be construed as, an endorsement by the Royal Netherlands Army.

For this paper series scholars, experts and policymakers submitted their papers on the employment of information-related capabilities to influence human behaviour in the military context. From the perspective of an individual European or NATO country's perspective. The Information-based behavioural influencing and Western practice paper series is edited by Arthur Laudrain, Laura Jasper and Michel Rademaker.

Seven papers will be published in this series. These are the following:

- Deception as the Way of Warfare. Armed Forces, Influence Operations and the Cyberspace paradox. By Colonel dr. Peter B.M.J. Pijpers, Netherlands Defence Academy and University if Amsterdam, and Brigadier General prof. dr. Paul A.L. Ducheine, Netherlands Defence Academy and University of Amsterdam
- Influencing security professionals: are they biased and by which source? By Johan de Wit, TU Delft & Siemens Smart Infrastructure
- A discursive analytical approach to understanding target audiences. How NATO can improve its actor-centric analysis. By Yannick Smits, Research Master Middle Eastern studies Leiden University
- The concept of Information Manoeuvre: Winning the Battle of Perceptions. By Judith T. van de Kuijt (TNO), N. Keja (TNO), J.C. Slaager (TNO)
- Smart Tactics or Risky Behaviour? The Lawfulness of Encouraging Civilians to Participate in Targeting in an Age of Digital Warfare. By Pontus Winther, LL.D. Swedish Armed Forces, and Per-Erik Nilsson, Ph.D. Swedish Defence Research Agency and Associate Professor at Uppsala University

- Cognitive Warfare as Part of Society: Never-Ending Battle for Minds. By Robin Burda, Ph.D. candidate Security and Strategic Studies Masaryk University
- Behavioural Influence Interventions in the Information Environment: Underlying Mechanisms and Technologies. By dr. Hans Korteling (TNO), Beatrice Cadet (TNO), Tineke Hof (TNO)

While risk is often portrayed mathematically, our response is more often instinctive. Understanding the factors that drive how we think about and act upon risk is critical.

General Stanley McChrystal,
US Army, retired[1]

Abstract

This paper presents brief summaries of four studies that explore the factors that drive our intuitive or reasoned perceptions of risk. The first part presents two studies on information and the sources of information that are the foundations for this risk perception. The second part of this paper presents the summaries of two studies that explore the biases and heuristics that affect the decision maker in the interpretation of information. These studies are all conducted in the professional security domain to investigate real-life security risk decision making. The summaries in this paper do not include extensive methods and analysis sections, we kindly refer to the published full papers. The results in this paper identify some fundamental human traits that can be exploited to influence human decision behaviour. On the other hand, any responsible decision maker should be aware of them and take them into account in their own daily praxis, as the results clearly and undoubtedly show the effects of these phenomena on judgements of, especially, experienced professionals

[1] Stanley A. McChrystal, Risk, a user's guide (New York: Penguin business, 2021).

Introduction

In the domain of security risks, which is dealing with risks originating from malicious human action, risk assessments are predominantly based on expert judgment.[2] Although information on threats and risks might be available, it is often incomplete and imperfect so expert interpretation is usually influencing and/or decisive for a security risk assessment.

Human decision making is prone to heuristics and biases as decades of scientific work demonstrated.[3] [4] [5]

Our work, as part of a PhD research project, studies the influence of heuristics and biases on individual risk decision making and risk assessments. The influence of information, triggering heuristics and biases, is the cornerstone of our studies. Several of them, both published and to be published, presented evidence of the influence of biases and heuristics on risk decision making and assessments by security practitioners. Our research has shown that:

- biases lead to less effective security decisions by professionals,
- risk attribute preferences can be influenced,
- more detailed information raises the likelihood perception,
- the widespread existence of probability ignorance in security risk decision making,
- security decision makers show objective ignorance,
- security decision makers are notorious overconfident even if they are aware their information is incomplete and imperfect

Our work may not directly answer the research questions and issues as posed for the Platform Influencing Human Behaviour, and is not specifically addressing decision making in a military context. Our studies might, however, contribute some valuable insights in individual risk decision making and risk assessments.

[2] Niklas Möller, “The concepts of risk and safety,” in Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk (Springer, 2012).
[3] Daniel Kahneman and Amos Tversky, “Prospect theory: An analysis of decision under risk,” Econometrica: Journal of the econometric society (1979).
[4] Herbert Alexander. Simon, Models of bounded rationality: Empirically grounded economic reason, vol. 3 (MIT press, 1982).
[5] Gerd Gigerenzer, Risk savvy: How to make good decisions (Penguin, 2015)

This perspective can help forming the needed policies for influencing individual security assessments of military decision makers. This paper presents brief summaries of four different studies of security risk assessments in the security domain by individual risk professionals.

They address two main topics:

1. the information on which assessments are based (identify sources, how much security risk information is available, how does this influence confidence)
2. biases and heuristics influencing the interpretation and perception of this information (study of vulnerability for known biases, conjunction fallacy, availability/on top-of-mind study, system 1 and 2 thinking)

In the next section the results of two studies are presented that explore security risk information. Both studies are briefly introduced and the relevant results are presented. The following section contains two studies into the vulnerability for, and influence of, biases on security risk decision making. This paper ends with some overall conclusions. In the summaries of the studies a research method section is deliberately left out to make this paper fit the maximum size. We kindly refer to the full papers for an extensive overview of the methods and analysis.

Topic 1: Information, the Foundation of Risk Assessments

In this section we present a summary of the results of two studies. In the first study we explore the information position of security professionals (the level of availability of precise information and/or evidence). We investigate how this position influences the confidence in their own judgment. The influence of individual expertise, on both the need for information and confidence levels, is examined. This study is published in a full paper: *“Bias and Noise in Security Risk Assessments, an Empirical Study on the Information Position and Confidence of Security Professionals”*, published in: Security Journal. The second study collects the possible sources of security risk information. It explores both the perceived quality and trustworthiness, and the application in real life of information sources. This study is published in a full paper: *“Sources of*

Security Risk Information: What do Professionals Rely on for their Risk Assessment?", currently under review.

The first empirical study addresses the following research questions:

- Do security professionals have exact information on security risks during their risk assessments?
- How confident are they about their security risk assessment?
- Would more information grow their confidence?

The results of a survey on the information position of security professionals are presented in Table 1. The professionals are asked to indicate, based on their real life praxis, the level of detail of security risk information available to them. The study focusses on the two main components of risk: impact and uncertainty expressed as likelihood. The security professionals indicate that, on average, about half the time they know the likelihood and consequences of the security risks they are assessing exactly. The respondents also indicate that they, on average, only sometimes, cannot estimate likelihood and consequences. One in four even indicates that they can always estimate likelihood and consequences, based on their experience and knowledge, even when they indicate they know they do not have accurate information.

This finding deviates from the expectation that security professionals would recognize their information position about security risks as both imperfect and intractable. As the future cannot be certain by nature, professionals might be expected to 'know that they cannot possibly know' (known unknowns). [6] They, however, indicate that they can estimate the likelihood and consequences most of the time. Assuming that the respondents are right about their knowledge position, they assess risks half of the time based on information (evidence based). On the other hand they assess security risks without proper information also half of the time and still come up with an estimation of likelihood and consequences. As these assessments have a serious impact on security risk decision making and the allocation of resources to manage, mitigate and/or accept these risks, it is worth noting that these decisions don't seem to be based on evidence about half of the time.

[6] Daniel Kahneman, Olivier Sibony, and Cass R. Sunstein, Noise, a Flaw in Human Judgment (London: William Collins, 2021).

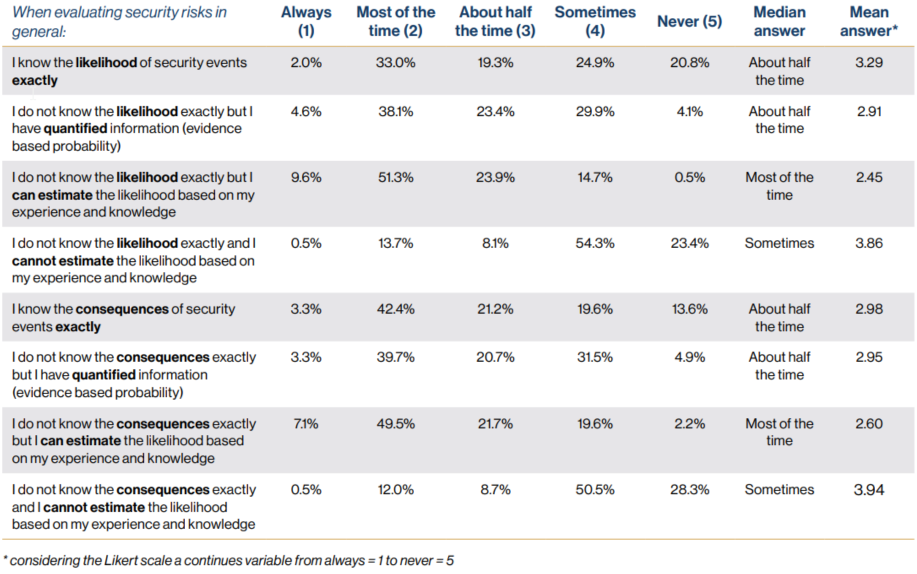
The perception of the respondents on their information position can be questioned. As risk assessments are in fact predictive judgements and the information about the future can be considered intractable by nature, this perception of the security professionals can be considered audacious.

Overall, the respondents claim to be confident about their judgement of likelihood and consequences most of the time (see Table 2).

Again: as the future cannot be certain by nature, the confidence of security professionals in their predictive judgements is expected to be limited. Overall the majority of the security professionals, however, indicate that they are always or most of the time confident about their assessments.

It is hypothesized that the security professionals would show modest confidence based on the assumption that exact and/or evidence based information on security risks is often lacking. They, however, seem to ignore the latter and thus show a higher level of confidence than might be expected. As the respondents, on average, indicate to hold exact or quantified information only half of the time, they, thus, might be considered overconfident about their risk assessments.

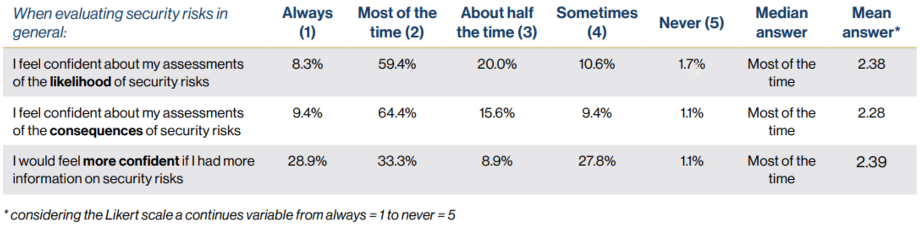
Table 1: The information position of security professionals in security risk assessments.



When evaluating security risks in general:	Always (1)	Most of the time (2)	About half the time (3)	Sometimes (4)	Never (5)	Median answer	Mean answer*
I know the **likelihood** of security events **exactly**	2.0%	33.0%	19.3%	24.9%	20.8%	About half the time	3.29
I do not know the **likelihood** exactly but I have **quantified** information (evidence based probability)	4.6%	38.1%	23.4%	29.9%	4.1%	About half the time	2.91
I do not know the **likelihood** exactly but I **can estimate** the likelihood based on my experience and knowledge	9.6%	51.3%	23.9%	14.7%	0.5%	Most of the time	2.45
I do not know the **likelihood** exactly and I **cannot estimate** the likelihood based on my experience and knowledge	0.5%	13.7%	8.1%	54.3%	23.4%	Sometimes	3.86
I know the **consequences** of security events **exactly**	3.3%	42.4%	21.2%	19.6%	13.6%	About half the time	2.98
I do not know the **consequences** exactly but I have **quantified** information (evidence based probability)	3.3%	39.7%	20.7%	31.5%	4.9%	About half the time	2.95
I do not know the **consequences** exactly but I **can estimate** the likelihood based on my experience and knowledge	7.1%	49.5%	21.7%	19.6%	2.2%	Most of the time	2.60
I do not know the **consequences** exactly and I **cannot estimate** the likelihood based on my experience and knowledge	0.5%	12.0%	8.7%	50.5%	28.3%	Sometimes	3.94

** considering the Likert scale a continues variable from always = 1 to never = 5*

Table 2: Confidence levels of security professionals.



When evaluating security risks in general:	Always (1)	Most of the time (2)	About half the time (3)	Sometimes (4)	Never (5)	Median answer	Mean answer*
I feel confident about my assessments of the **likelihood** of security risks	8.3%	59.4%	20.0%	10.6%	1.7%	Most of the time	2.38
I feel confident about my assessments of the **consequences** of security risks	9.4%	64.4%	15.6%	9.4%	1.1%	Most of the time	2.28
I would feel **more confident** if I had more information on security risks	28.9%	33.3%	8.9%	27.8%	1.1%	Most of the time	2.39

** considering the Likert scale a continues variable from always = 1 to never = 5*

Combining the perceived information position of the professionals with their level of confidence reveals objective ignorance.[7] A portion of respondents indicate they have exact information only sometimes or even never but are confident most or half of the time. These respondents are aware of their lack of exact information but are confident nevertheless. This lack of information doesn't seem to aect their ability to form a predictive judgement and be confident about it.

In this study the respondents are asked to indicate their age, number of years professional and security experience, their general education level (associate degree, bachelor degree or master degree/PhD) and if any specific security trainings are completed.

More professional and security experience significantly raises the confidence level of the security professionals. More experienced security professionals are more often confident about their assessments of both likelihood and consequences. More experienced security professionals also indicate that more information would raise their confidence level to a lesser extent than less experienced professionals indicate. In short these results seem to indicate that more experience leads to higher levels of (over)confidence and less need for additional information.

A higher education level on the other hand significantly reduces the confidence in likelihood and consequences assessments. These results might prove the adage 'the more you know, the more you realise you don't know' as other scholars also found. 8 Security specific trainings do not significantly influence confidence level or the need for additional information.

[7] Cass R Sunstein, Laws of fear: beyond the precautionary principle (Cambridge University Press, 2005).

In the second study the origin of security risk information, the sources of information, are explored and studied. Possible sources of security risk information are collected, their quality and trustworthiness are assessed, and the level of their application in real life security risk assessments is analysed. The research questions answered in this study are:

- What sources of security risk information are considered by practitioners?
- How reliable are these sources as perceived by these practitioners?
- Which sources are applied in security risk assessment praxis?
- Are the most applied sources also perceived as the most credible ones?
- Can we observe dierences between security professionals based on their expertise (experience and knowledge)?

Analysing and classifying information and information sources is of vital importance in the security domain. [9] [10] [11] Especially in the security intelligence community tools and methods are developed and applied to classify information and information sources. [12] [13] In this domain the quality of information is also predominantly evaluated based on both the reliability of the content and the source, applying the international and broadly accepted evaluation criteria known as the Admiralty Code or NATO System (see Table 3).

[8] George Wright and Peter Ayton, “Subjective confidence in forecasts: A response to Fischhoff and MacGregor,” Journal of Forecasting 5, no. 2 (1986).

[9] Thomas Powell et al., “Dealing with Uncertainty in Hybrid Conflict: A Novel Approach and Model for Uncertainty Quantification in Intelligence Analysis,” (2019).

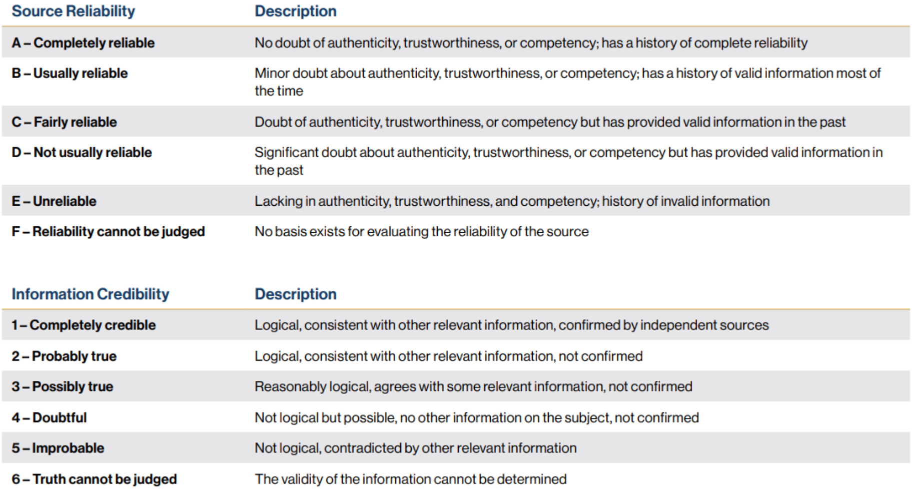
[10] Esther Gal-Or and Anindya Ghose, “The economic incentives for sharing security information,” Information
Systems Research 16, no. 2 (2005).

[11] Loch K Johnson, The Oxford handbook of national security intelligence (Oxford University Press, 2010).

[12] Adriana N Seagle, “Intelligence sharing practices within NATO: An english school perspective,” International
Journal of Intelligence and CounterIntelligence 28, no. 3 (2015).

[13] F Korkisch, “NATO gets better intelligence,” IAS Reader, Strategy Paper (2010).

Table 3: Outline of the Admiralty Code or NATO System.



Source Reliability	Description
A – Completely reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability
B – Usually reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time
C – Fairly reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D – Not usually reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E – Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F – Reliability cannot be judged	No basis exists for evaluating the reliability of the source

Information Credibility	Description
1 – Completely credible	Logical, consistent with other relevant information, confirmed by independent sources
2 – Probably true	Logical, consistent with other relevant information, not confirmed
3 – Possibly true	Reasonably logical, agrees with some relevant information, not confirmed
4 – Doubtful	Not logical but possible, no other information on the subject, not confirmed
5 – Improbable	Not logical, contradicted by other relevant information
6 – Truth cannot be judged	The validity of the information cannot be determined

The NATO system classifies the reliability of sources on: authenticity, trustworthiness and competency. These characteristics are evaluated against past experience with the sources.

These characteristics of the NATO system on source credibility all relate to the notion of trust/trustworthiness. Trust is the attitude that takes to the trustworthiness of a source.[14] ‘Trust is of central importance because quality is a perceived property and, thus, assessing the quality of an information source is essentially a matter of establishing to what extent one is willing to place trust in it’. [15]

In available literature about trust another property of trust is deemed important, besides the perceived competence of the source the perceived intent or agency of the source is essential for the trustworthiness of the source. [16] [17] Sources of information may have deviating goals, intentions and incentives that can alter their trustworthiness.

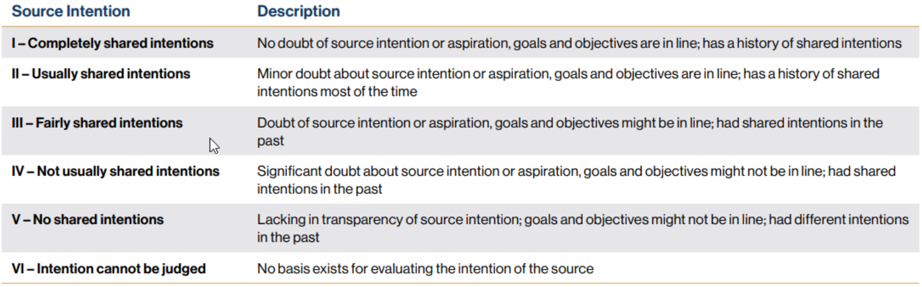
[14] Lea Viljanen, “Towards an ontology of trust” (paper presented at the International conference on trust, privacy and security in digital business, 2005).
[15] Morten Hertzum et al., “Trust in information sources: seeking information from people, documents, and virtual agents,” Interacting with computers 14, no. 5 (2002).
[16] Katherine Hawley, Trust: A very short introduction (OUP Oxford, 2012).
[17] Kieron O’Hara, “A general definition of trust,” (2012).

Even though sources might be considered competent, their information might be comprehensive, consistent, accurate and up to date, they still may be suspected of following an agenda that is not in line with the receiver of information.

While the competence of a source is often stable over time or might show gradual changes, intentions of sources, on the other hand, can be very volatile and might even change overnight (for example due to bribery, extorsion or other external pressure). Evaluating source intention as part of classification of information can be considered of vital importance. In the original NATO code, source intention might be considered a component of source reliability and assessed together with competence.

Due to the specific importance of intent in the literature on trust and trustworthiness and the volatile character of source intention, in this study a separate assessments of source intention is proposed. In addition to the NATO code, a new classification scale is set up and tested in a practitioners panel (see Table 4).

Table 4: Proposal addition to the NATO system for classification of source intention.



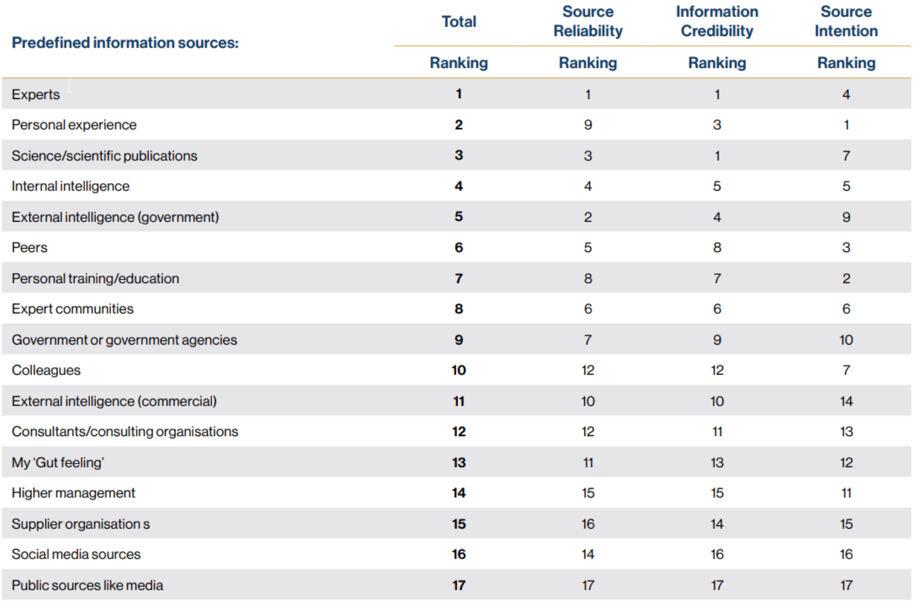
Source Intention	Description
I – Completely shared intentions	No doubt of source intention or aspiration, goals and objectives are in line; has a history of shared intentions
II – Usually shared intentions	Minor doubt about source intention or aspiration, goals and objectives are in line; has a history of shared intentions most of the time
III – Fairly shared intentions	Doubt of source intention or aspiration, goals and objectives might be in line; had shared intentions in the past
IV – Not usually shared intentions	Significant doubt about source intention or aspiration, goals and objectives might not be in line; had shared intentions in the past
V – No shared intentions	Lacking in transparency of source intention; goals and objectives might not be in line; had different intentions in the past
VI – Intention cannot be judged	No basis exists for evaluating the intention of the source

To explore the perceived trustworthiness and application of various information sources of security risk information, practitioners from the security domain are consulted. Different groups of practitioners participated in 1) a small brainstorming session to collect the most prominent possible sources of information, 2) a panel consultation to rank the source quality, and 3) a large-scale survey amongst security professionals to explore the application of these sources of information.

First a list of possible sources of risk information is composed during a brainstorming session with senior security professionals. This predefined list of possible sources of security risk information consists of 17 predefined sources as presented in the first column of Table 5.

For the ranking of the quality of these sources a practitioners panel is consulted. This panel consisted of 18 experienced security practitioners: on average 28 years of security experience, 83% followed specific security trainings, education level: associate degree 11%, bachelor degree 22%, master/PhD degree 67%. In an online consultation, the members of this panel are asked to rate the source reliability, information credibility and source intention of each of the predefined sources. The results of this consultation are analysed using a method for analysing Multiple-Criteria Decision Making: Fuzzy Technique for Order Performance by Similarity to Ideal Solution (FTOPSIS). The ranking is presented in table 5.

Table 5: Results of the FTOPSIS analysis, total results over the three criteria combined, in rank order followed by the results of each of the individual criteria: source reliability, information credibility, and source intention.



Predefined information sources:	Total	Source Reliability	Information Credibility	Source Intention
	Ranking	Ranking	Ranking	Ranking
Experts	**1**	1	1	4
Personal experience	**2**	9	3	1
Science/scientific publications	**3**	3	1	7
Internal intelligence	**4**	4	5	5
External intelligence (government)	**5**	2	4	9
Peers	**6**	5	8	3
Personal training/education	**7**	8	7	2
Expert communities	**8**	6	6	6
Government or government agencies	**9**	7	9	10
Colleagues	**10**	12	12	7
External intelligence (commercial)	**11**	10	10	14
Consultants/consulting organisations	**12**	12	11	13
My 'Gut feeling'	**13**	11	13	12
Higher management	**14**	15	15	11
Supplier organisation s	**15**	16	14	15
Social media sources	**16**	14	16	16
Public sources like media	**17**	17	17	17

These results seem to confirm previous work in other domains that risk communication by government and industry is considered less trustworthy. [18] [19] [20] [21] Commercial sources like external commercial intelligence (11), consultants (12), and supplier organisations (15) are at the lower end of this ranking. They might contain too much marketing and are, therefore, considered less trustworthy.

Government sources rank somewhat higher: external government intelligence (5), government/government agencies (9). As other scholars concluded this lower perceived trustworthiness is primarily caused by deviating goals of both commercial and government risk information sources. The commercial and government sources indeed rank even lower on the source intention scale (last column of Table 5): commercial intelligence (14), consultants (13), supplier organisations (15), external government intelligence (9), government/government agencies (10).

In the main survey of this study 174 security professionals answered the research question: ‘on what information source do you base your security risk assessment?’ (see Table 6).

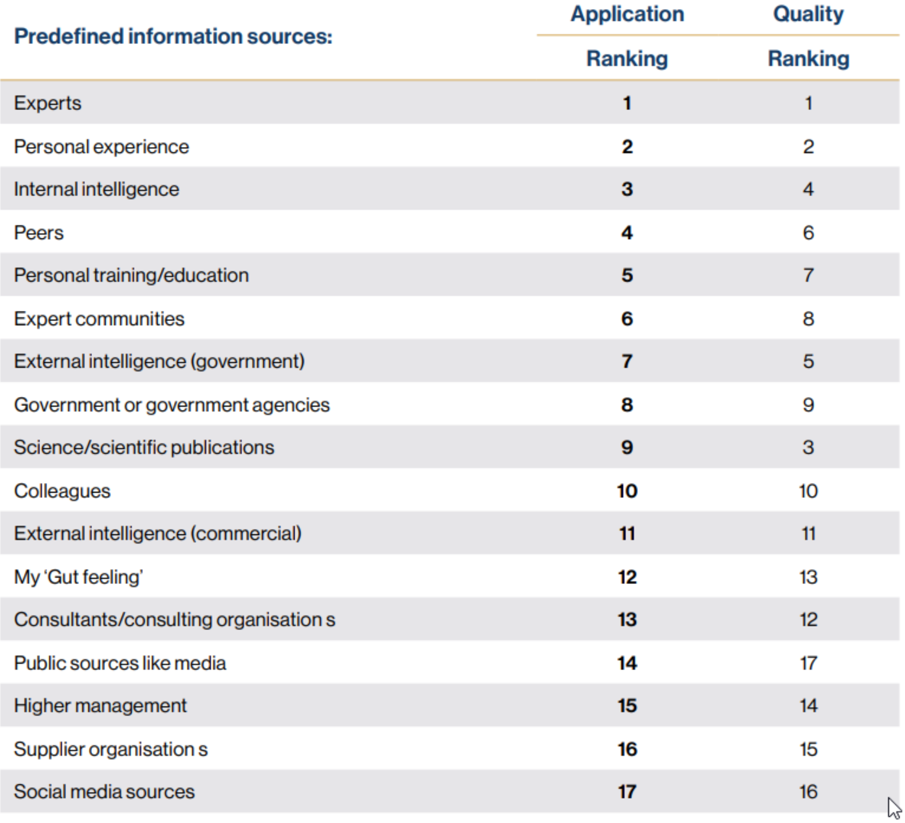
[18] June Fessenden-Raden, Janet M Fitchen, and Jenifer S Heath, “Providing risk information in communities:
Factors influencing what is heard and accepted,” Science, Technology, & Human Values 12, no. 3/4 (1987).

[19] David B McCallum, Sharon Lee Hammond, and Vincent T Covello, “Communicating about environmental risks: How the public uses and perceives information sources,” Health Education Quarterly 18, no. 3 (1991).

[20] Paul Slovic, James H Flynn, and Mark Layman, “Perceived risk, trust, and the politics of nuclear waste,” Science 254, no. 5038 (1991).

[21] Craig W Trumbo and Katherine A McComas, “The function of credibility in information processing for risk
perception,” Risk Analysis: An International Journal 23, no. 2 (2003).

Table 6: On what information source do you base your secuirty risk assessment? Total results of the main survey, followed by the results of the practitioners panel (identical to Table 5).



Predefined information sources:	Application	Quality
	Ranking	Ranking
Experts	**1**	1
Personal experience	**2**	2
Internal intelligence	**3**	4
Peers	**4**	6
Personal training/education	**5**	7
Expert communities	**6**	8
External intelligence (government)	**7**	5
Government or government agencies	**8**	9
Science/scientific publications	**9**	3
Colleagues	**10**	10
External intelligence (commercial)	**11**	11
My 'Gut feeling'	**12**	13
Consultants/consulting organisation s	**13**	12
Public sources like media	**14**	17
Higher management	**15**	14
Supplier organisation s	**16**	15
Social media sources	**17**	16

The two rankings are, besides a few minor differences, similar. This indicates that the perceived high quality information sources, as assessed by the practitioners panel, are applied and perceived as important for risk assessments in praxis, as indicated by the group of respondents. The most remarkable difference between the rankings is the source: science/scientific publications. It is perceived a high-quality source (rank 3 by the panel) but seems to be less applied in daily praxis (rank 9 by the respondents). This might be explained by the additional proposed information quality criterion: source intention.

The panellists assign a high source reliability to science/scientific publications (rank 3), the highest information credibility (rank 1 ex aequo with experts) but on source intention it is ranked at position 7.

This means that there is at least some doubt on source intention or aspiration, goals and objectives might be in line (but this is not certain). Without the proposed additional criterion on information quality: source intention, this could not properly be explained. It seems this new criterion as proposed in this paper, as an addition to the two criteria of the renowned NATO system, is of added value when evaluating the quality of sources of information.

Individual characteristics of the respondents do not seem to be of much influence on the application of information sources during their security risk assessments. It seems that more experienced practitioners have more confidence in their own perception and less in government, commercial and social media sources.

Topic 2: Perception, Human Processing of Information

This section also presents brief summaries of two studies. In the first study the vulnerability of trained security professionals to known psychological and behaviour biases is examined. Does professional experience and training reduce the vulnerability to known and systematic distortion of judgment? This study is published in a full paper: “Biases in Security Risk Management: Do Security Professionals follow Prospect Theory in their Decisions?” in the Journal of Integrated Security and Safety Science.

The second study shows the results of several realistic security risk assessments. In these scenarios the descriptions are varied to explore the influence of more or less information. These experiments are based on the conjunction fallacy, predicting that likelihood estimates increase when case descriptions have more specific information, whereas they should actually decrease. This study is to be published in a full paper: “Bias and Noise in Security Risk Assessments, an Empirical Study on the Information Position and Confidence of Security Professionals,” in : Security Journal.

The first study addresses the main research question: Are security professionals vulnerable to decision making biases as presented in Prospect Theory (PT)? PT has evolved in the 1970s and was driven by

Amos Tversky and Daniel Kahneman, [22] who later received a Nobel prize for this work. After multiple experiments they concluded that the majority of people do not follow maximising theories in their decision making.

The normative phenomenon of 'Homo Economicus', humans always choose the option with the highest perceived utility, was denied. Instead, humans were found to follow decision behaviour that might be qualified as non-rational in the traditional economic sense. These renown scholars identified multiple biases, which are systematic deviations from a norm or rational judgment.

The original PT study focusses on decisions with two predefined options. The original experiments are, however, defined in financial loss and gain. This might not be representing security decisions. Therefore, in the second part of this study, the decision alternatives are redefined in security risk mitigation or reduction. The expectation is that security professionals, by the nature of their work and expertise, and confronted with limited, predefined, and given probabilities, could be less biased than lay people.

The results of this study clearly indicate that this expectation needs to be rejected. Based on the analysed results the vulnerability of security professionals to decision making biases using the original monetary gain and loss decisions showed an equal vulnerability to biases as lay people. Reformulating these experiments to reflect real life security decisions hardly changed the outcomes. The influence of the certainty effect, the non-linear preferences, the reflection effect, the lottery and insurance effect and the isolation effect on decision making by the majority of the sample of security professionals is clearly observed. This vulnerability to decision biases is revealed, on average, in decision behaviour of 70% of the sample of security professionals. In this short summary we will not further explain these biases, but the bottom line is that they all influence decision making in a way that the outcome is not maximised. The work of security professionals can be considered to be managing/mitigating risks, this study shows decision making that does maximise the outcome. It is safe to conclude that the studied biases can negatively affect optimal risk reduction.

[22] Kahneman and Tversky, "Prospect theory: An analysis of decision under risk."

The core of the second study consists of cases testing the conjunction fallacy. The conjunction fallacy is a bias which identifies a flaw in logic reasoning. In theory the more specific a situation is, the less likely it would be compared to a less specific situation. The specific situation represents a subset of the generic situation. In practice, however, more details enhance the likelihood perception of humans (see Figure 1). In this study this phenomenon is explored to identify if it would influence the likelihood perception of professionals in real life risk assessments.

The case presented in this summary is a replication of the original problem statement as used by Kahneman and Tversky. [23] The context is reformulated to fit the security domain. As this reformulated problem shows the conjunction fallacy in plain sight, logic reasoning or recognition of the fallacy might influence the assessment of the respondents.

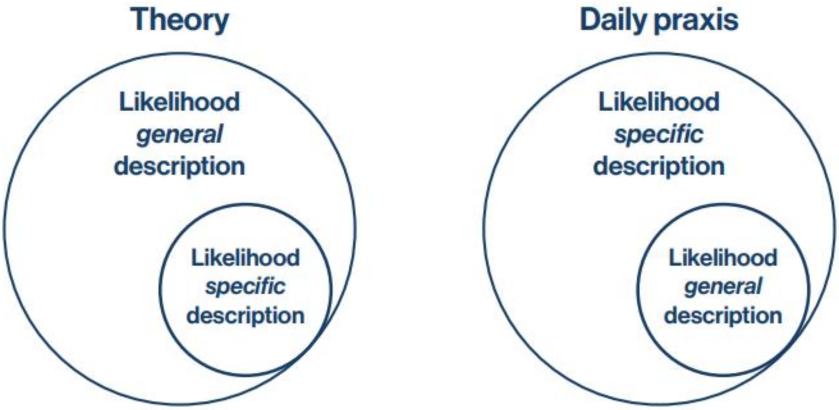

Theory
Likelihood *general* description
Likelihood *specific* description
Daily praxis
Likelihood *specific* description
Likelihood *general* description

Figure 1: The conjunction fallacy explained.

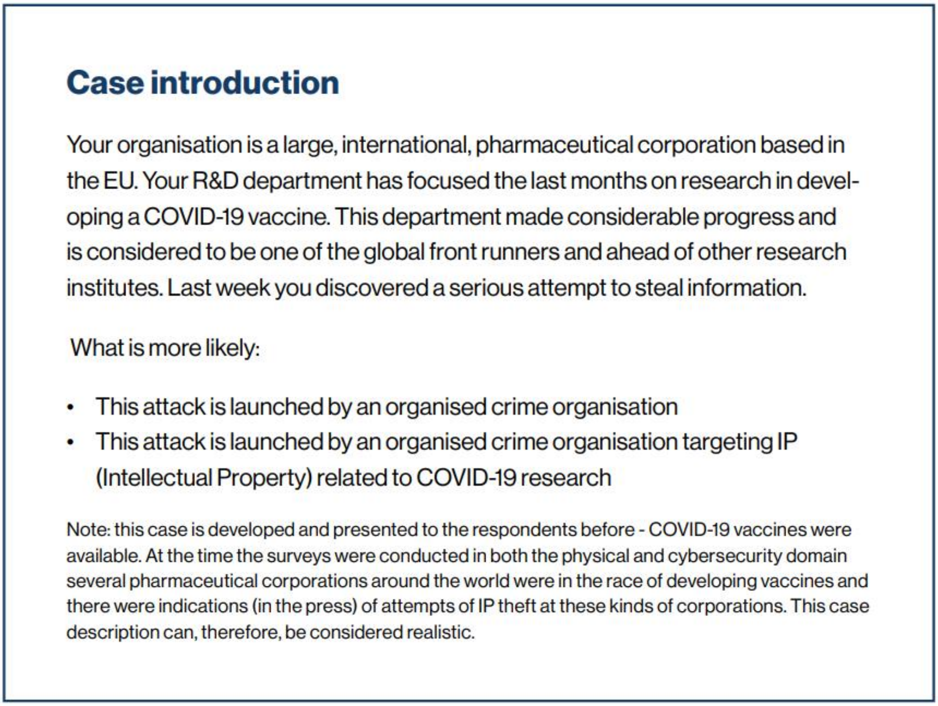
The reformulated problem consists of a short case description followed by a choice between two options. The respondents are asked to indicate which option they consider more likely. The first option has a general and short formulation.

[23] Amos Tversky and Daniel Kahneman, "Extensional versus intuitive reasoning: The conjunction fallacy in probability judgment," Preference, belief, and similarity: Selected writings by Amos Tversky (2004).

The second one is identical to the first, but is extended with more detailed information.

Showing the two answers at the same time, in other words showing the conjunction rule, should or could guide the respondents to choose the shorter, more general, option. The second, more detailed, option, obviously is a sub-set of the first and should therefore be considered less likely.

This reformulated problem is presented to professionals of both the physical and cybersecurity domain:



Case introduction

Your organisation is a large, international, pharmaceutical corporation based in the EU. Your R&D department has focused the last months on research in developing a COVID-19 vaccine. This department made considerable progress and is considered to be one of the global front runners and ahead of other research institutes. Last week you discovered a serious attempt to steal information.

What is more likely:

- This attack is launched by an organised crime organisation
- This attack is launched by an organised crime organisation targeting IP (Intellectual Property) related to COVID-19 research

Note: this case is developed and presented to the respondents before - COVID-19 vaccines were available. At the time the surveys were conducted in both the physical and cybersecurity domain several pharmaceutical corporations around the world were in the race of developing vaccines and there were indications (in the press) of attempts of IP theft at these kinds of corporations. This case description can, therefore, be considered realistic.

A total of 165 respondents answered the reformulated problem. 25.5% considered the first (short) option more likely, 74.5% the second (extended) one. In the physical security domain 58.8% of the respondents followed the fallacy and chose the extended option. Of the respondents active in the cybersecurity domain even 81.6% selected the extended option.

The top threat in the cybersecurity domain in 2020 was IP theft by various threat vectors [24], while in the physical security domain the top threat in 2020 was malicious physical access. [25] The respondents originating from the cybersecurity domain, therefore, might relate more to the extended option. It fits their frame of reference, might lead to a stronger representation, recognition, emotion and thus availability. According to the theory of hints and the study of Brachinger and Monney [26] this explains the fall for the conjunction fallacy.

An important consequence of this conclusion can be that professionals with domain expertise, and thus, a deeper subjective interpretation of so-called simple hints, and readily available information or even experience, [27] assess a higher likelihood to risks in their domain than non-domain experts.

In agreement with the hypothesis the results of this study clearly show the influence of the conjunction fallacy on the judgement of security professionals. As a consequence, security risk assessments by practitioners are probably influenced considerably by more detailed information. Following the fallacy, retrieving more specific, detailed and recognisable information may lead the individual professional to consider a case, incident or threat more likely which in turn might lead to distorted risk assessments in organisations and society. These findings have important implications for the professional security community and anyone depending on it.

[24] "Top Cyberattacks of 2020 and How to Build Cyberresiliency," ISACA, 2020.

[25] "Physical manipulation, damage, theft, loss, ENISA Threat Landscape," ENISA, 2020.

[26] Hans Wolfgang Brachinger and Paul–André Monney, "The conjunction fallacy: explanations of the linda problem by the theory of hints," International journal of intelligent systems 18, no. 1 (2003).

[27] Randy E Dumm et al., "The representative heuristic and catastrophe-related risk behaviors," Journal of Risk and Uncertainty 60, no. 2 (2020).

Overall Conclusions

Our results make clear that professional security risk decision makers are as vulnerable to biases as lay people. This may lead to misconception of real-world risks. In roughly half of the real-life assessments detailed security risk information is lacking. This might even be considered overestimated (professionals perceive they have more detailed information than can be expected given the fact that the future is unpredictable by nature). Even if they are right, in half of the situations they seem to base their judgement on security risks without adequate information. The professionals indicate they can estimate a risk most of the time and even one in four assures they can always assess a security risk (even without information).

Overall, the security professionals show (over)confidence in their judgements, again even if they are aware there is no detailed evidence for their judgement. Our studies show that more experience leads to more (over)confidence and less need for more information. In other words: more experienced practitioners will base their judgment on less information. Even if they know information is lacking, they will decide without trying to retrieve more information.

The sources of information with the highest perceived quality seem to be applied most in real-life praxis. The top 5 sources of information for security risks assessments, as applied by professionals, contain two individual sources: personal experience and training/education. These are considered very important and are in line with the previous conclusion that experienced practitioners are prone to use their expertise for their judgment.

The other 3 in the top 5: experts, internal intelligence and peers, can be considered a part of the direct network of professionals. To influence them means these sources need to be influenced. There is also the danger of the resonation of information in a so called ‘echo chamber’ or bubble.

As our studies proved the vulnerability of professionals for well-known biases and heuristics, these might be leveraged to influence decisions and behaviour. Especially interesting is the conjunction fallacy: more detailed information raises the assessment of likelihood. If detailed information is communicated in the individual network of professionals, and resonated in echo chambers, it will most likely raise the likelihood perception.

The cornerstone of influence seems to be storytelling with details that trigger recognition of the individual risk assessor. More experience leads to more recognition which in turn might lead to a raised perception of likelihood.

Even the most experienced and best educated professional is human, and thus biased. The professional that is aware of this can reduce his/her own biased perception, but can also use it to influence others.

As we started this paper with a quote of McChrystal [28] we will also end with him:

> ‘At the end of the day, we can’t choose to have or have not biases – we have them. So we must identify and carefully consider them.’

[28] Stanley A. McChrystal, Risk, a user’s guide (New York: Penguin business, 2021).

Literature

Brachinger, Hans Wolfgang, and Paul–André Monney. “The Conjunction Fallacy: Explanations of the Linda Problem by the Theory of Hints.” International journal of intelligent systems 18, no. 1 (2003): 75-91.

Dumm, Randy E, David L Eckles, Charles Nyce, and Jacqueline VolkmanWise. “The Representative Heuristic and Catastrophe-Related Risk Behaviors.” Journal of Risk and Uncertainty 60, no. 2 (2020): 157-85.

“Physical Manipulation, Damage, Theft, Loss, Enisa Threat Landscape.” ENISA, 2020.

Fessenden-Raden, June, Janet M Fitchen, and Jenifer S Heath. “Providing Risk Information in Communities: Factors Influencing What Is Heard and Accepted.” Science, Technology, & Human Values 12, no. 3/4 (1987): 94-101.

Gal-Or, Esther, and Anindya Ghose. “The Economic Incentives for Sharing Security Information.” Information Systems Research 16, no. 2 (2005): 186-208.

Gigerenzer, Gerd. Risk Savvy: How to Make Good Decisions. Penguin, 2015.

Hawley, Katherine. Trust: A Very Short Introduction. OUP Oxford, 2012.

Hertzum, Morten, Hans HK Andersen, Verner Andersen, and Camilla B Hansen. “Trust in Information Sources: Seeking Information from People, Documents, and Virtual Agents.” Interacting with computers 14, no. 5 (2002): 575-99.

“Top Cyberattacks of 2020 and How to Build Cyberresiliency.” ISACA, 2020.

Johnson, Loch K. The Oxford Handbook of National Security Intelligence. Oxford University Press, 2010.

Kahneman, Daniel, Olivier Sibony, and Cass R. Sunstein. Noise, a Flaw in Human Judgment. London: William Collins, 2021.

Kahneman, Daniel, and Amos Tversky. “Prospect Theory: An Analysis of Decision under Risk.” Econometrica: Journal of the econometric society (1979): 263-91.

Korkisch, F. “Nato Gets Better Intelligence.” IAS Reader, Strategy Paper (2010): 1-2010.

McCallum, David B, Sharon Lee Hammond, and Vincent T Covello. “Communicating About Environmental Risks: How the Public Uses and Perceives Information Sources.” Health Education Quarterly 18, no. 3 (1991): 349-61.

McChrystal, Stanley A. Risk, a User's Guide. New York: Penguin business, 2021.

Möller, Niklas. "The Concepts of Risk and Safety." Chap. 3 In Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk, 55-85: Springer, 2012.

O'Hara, Kieron. "A General Definition of Trust." (2012).

Powell, Thomas, Serena Oggero, Joris Schook, and Emma Westerveld. "Dealing with Uncertainty in Hybrid Conflict: A Novel Approach and Model for Uncertainty Quantification in Intelligence Analysis." (2019).

Redmiles, Elissa M, Sean Kross, and Michelle L Mazurek. "How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior." Paper presented at the Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

Seagle, Adriana N. "Intelligence Sharing Practices within Nato: An English School Perspective." International Journal of Intelligence and CounterIntelligence 28, no. 3 (2015): 557-77.

Simon, Herbert Alexander. Models of Bounded Rationality: Empirically Grounded Economic Reason. Vol. 3: MIT press, 1982.

Slovic, Paul, James H Flynn, and Mark Layman. "Perceived Risk, Trust, and the Politics of Nuclear Waste." Science 254, no. 5038 (1991): 1603-07.

Sunstein, Cass R. Laws of Fear: Beyond the Precautionary Principle. Cambridge University Press, 2005.

Trumbo, Craig W, and Katherine A McComas. "The Function of Credibility in Information Processing for Risk Perception." Risk Analysis: An International Journal 23, no. 2 (2003): 343-53.

Tversky, Amos, and Daniel Kahneman. "Extensional Versus Intuitive Reasoning: The Conjunction Fallacy in Probability Judgment." Preference, belief, and similarity: Selected writings by Amos Tversky (2004): 221-56.

Viljanen, Lea. "Towards an Ontology of Trust." Paper presented at the International conference on trust, privacy and security in digital business, 2005.

Wright, George, and Peter Ayton. "Subjective Confidence in Forecasts: A Response to Fischho and Macgregor." Journal of Forecasting 5, no. 2 (1986): 117-23

PART 4

CLOSING

CONCLUDING CHAPTER

Facts & Belief in Security Risk Decision Making: The Impact on the Professional Domain

This final chapter concludes this dissertation. It does not repeat the conclusions as already recapitulated in the summary and describe in detail in the individual chapters. In this final chapter the results are merged leading to a discussion of three phenomena: *facts*, opposing *belief* and *probability ignorance*. Finally the consequences of these results for the professional (security) domain are presented.

The Research Questions

The initial research question at the go-no go meeting of this PhD study was defined as: *How is the effectiveness of security measures determined by security professionals?* It was already clear from the start that information on security risks available to professionals and the interpretation of it would play an important role in exploring this determination process.

The professional risk domain is determining if a risk needs to be managed by applying a risk management process. Risk management processes usually consist of a risk assessment (including the steps: risk identification, risk analysis and risk evaluation), followed by risk treatment. Each of these steps is fuelled by (risk) information. Professionals collect, interpret and are expected to analyse this information and come to a conclusion. Based on the extensive literature study committed at the start, determining, the core activity in the original research question, ended up to become a research question on decision making. Over the course of this study the overall research question evolved into *understanding how security professionals assess, reason, and decide about security risks, and where their justification is founded on.*

This study, thus, focusses on information and perception, or facts vs beliefs as it is referred to in this concluding chapter. As it is focussed on '*understanding*', this study is explorative and explanatory by nature.

In the introductory chapter the '*how*' questions are answered based on a study of available literature. A level of information is related to the level of uncertainty constructing the *scale of uncertainty*. Further a *comprehensive model of decision making*, novel in its kind, is introduced composed of elements of renown decision theories. Both models form a frame of reference for the detailed research questions in the core chapters of this dissertation:

Part 2 Chapter 1:

- Are security professionals vulnerable to decision making biases as presented in prospect theory?

- To what extent are security professionals vulnerable to decision making biases as presented in the prospect theory using the original monetary gain and loss decisions?
- To what extent are security professionals vulnerable to decision making biases as presented in the prospect theory using security decisions adapted from the original monetary ones?
- To what extent do individual characteristics and security expertise, including age, experience, education and special security training, influence the vulnerability to decision making biases?

Part 2 Chapter 2:

- What are the individual preferences and priorities of security professionals?
- Do they change after a 'second thought'?
- Is individual expertise influencing these preferences?

Part 2 Chapter 3:

- Do security professionals usually have exact information on security risks?
- Are they usually confident about their predictive judgements?
- Would more information grow their confidence?
- Is their judgement of likelihood depending on more or less information?
- Do security likelihood judgements vary under influence of the conjunction fallacy?

Part 2 Chapter 4:

- What sources of security risk information are considered by practitioners?
- How reliable are these sources as perceived by these practitioners?
- Which sources are applied in security risk assessment praxis?
- Are the most applied sources also perceived as the most credible ones?
- Can we observe differences between security professionals based on their expertise (experience and knowledge)?

The answers to this collection of research questions are not, again, repeated one by one in this chapter. For the detailed answers we kindly refer to the previous chapters. The answers to these questions are all, however, reflected in this chapter by combining them in what turned out to be the three main phenomena of this study: facts, belief and probability ignorance. This chapter starts with a brief summary of research limitations and ends with an overview of impact on the professional community and society.

Summary of Limitations

As in every study our research has limitations. The data is gathered in the professional security environment in both the physical and cyber security domain. Finding and activating respondents for surveys and experiments is challenging.

As this study seeks to explore real life security decisions and assessments, potential respondents preferably have professional position in the security domain. As detailed in the subsequent chapters these practitioners are therefore invited via professional conferences, professional communities (online and physical), and via direct mailing in the professional network of the researchers. As part of the surveys and experiments the respondents are asked for personal characteristics like age, number of years professional experience, number of years security experience, education level, specific security trainings, professional position. These characteristics allow to compare ingroup results based on these. Each scientific chapter of this dissertation (part 2) includes an analysis of the influence of expertise on the results. In this work it is assumed that the participants have no special reason to disguise their true preferences.

Parts of this study are based on experiments and case assessments. There are drawbacks on using such hypothetical questions. The validity and generalizability of the results remains questionable as in every laboratory setting. In the security domain with its human dynamics and malicious intent both the risks and controls can be perceived differently by individual security decision makers. Setting up pre-defined alternatives with a given and specified probability and consequence, however, filters out individual perception and makes results comparable (part 2, chapter 1). The cases as presented in part 2 chapter 3 serve a similar purpose. Offering the respondents a limited but identical set of information allows to compare the results. Although hypothetical these cases were intended to reflect real life situations. Therefore these were discussed with practitioners in the field (colleagues and peers of the researcher).

To avoid researcher bias as much as possible the survey questions and experiments are discussed in the PhD peer group to gain feedback from a diverse group with a different scientific background. Part of the surveys are also discussed and set up during the specific Graduate School training: 'How to make a questionnaire and conduct an interview'. Finally all surveys and experiments are discussed with the both PhD promotors to allow for scientific scrutiny.

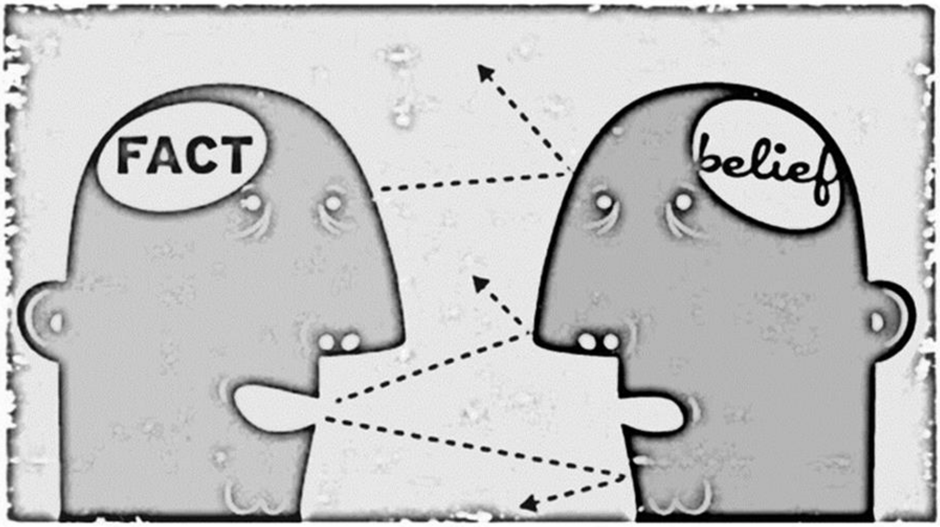
Each scientific chapter includes more detailed research limitations.

Summary of the Answers

Our studies concluded that security professionals are as vulnerable to biases as lay people and education and training hardly influences this. It is observed that the professionals deem their own experience as a source for risk information important and, based on that, perform system 1 decision making often. Combined with the fact that this system 1 decision making is intuitive and prone to biases, it is safe to conclude that security risk decision making by security professionals is biased.

Biased security decisions in itself can lead to less optimal risk management and less efficient allocation of resources. The professionals are aware of their lack of information but seem reluctant to retrieve more information, a phenomenon that grows with experience. This awareness does not encourage the professionals to be realistic and humble about their own decision making and judgment: they are in majority (over)confident. As the overall research questions indicate, this study focusses on understanding and exploring the phenomenon of security risk assessments, reasoning and decision making.

Our results unfortunately stop at this point: we pointed at this inaccuracy in risk decision making hoping this raises awareness in the professional community. By making these phenomena known, we hope the professional community is able to learn and take these findings into account. The logical next question, what can/should we do about it?, was not in scope of the underlying research, but is loosely addressed in the professional Part 3 Chapter 5 of this dissertation, in which some recommendations are suggested to reduce the inaccuracy in decision making. A publication targeting the professional audience provides some guidance for implementing these recommendations. We can only hope other scholars will continue and come up with anti-biasing techniques and decision enhancing techniques, specifically targeting the security domain, to support the professional community in their task to secure society. In the next sections the three main phenomena of this study, facts, belief, and probability ignorance, are discussed ending with an overview of the impact of this study on the professional community and society.



Facts vs Beliefs

As stated in previous chapters: the future is unknown by definition (Harris, 2020; Kahneman, Sibony, & Sunstein, 2021; McChrystal, 2021). Information about the future might be imperfect (can become available with effort/resources) but a part of the information of the future will be intractable and can never be known. Depending on the regularity, comparability and/or stability of the situation, predictions, based on past experiences, can vary from calculations to pure speculation. The knowledge position of decision actors can vary and so does the level of uncertainty and, thus, risk.

As introduced at the very start of this dissertation the 'scale of uncertainty' (see Figure 1) is a graphical display of information about the risk future. More factual on the left side, more belief on the right. In real life praxis resources or even the interest might be lacking to collect additional information. As will be stated in the next sections of this chapter, fast feedback is often lacking in the security domain and the situation is seldom stable which makes this domain less suitable for probabilistic modelling (Möller, 2012).

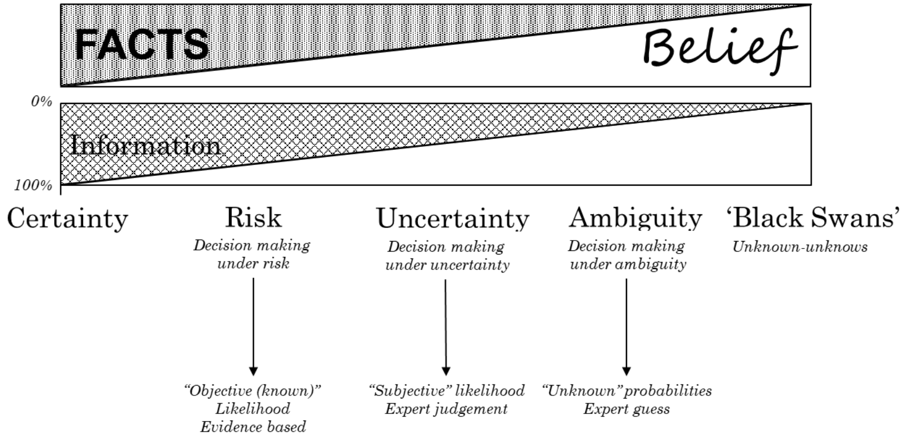

FACTS
Belief
0%
Information
100%
Certainty
Risk
Decision making under risk
Uncertainty
Decision making under uncertainty
Ambiguity
Decision making under ambiguity
'Black Swans'
Unknown-unknows
"Objective (known)" Likelihood Evidence based
"Subjective" likelihood Expert judgement
"Unknown" probabilities Expert guess

Figure 1 : proposed 'scale of uncertainty' related to information and facts & belief

It seems that facts and belief are in a delicate pax de deux, facts are the basis for belief but on the other hand belief can orchestrate facts that support it.

Belief

As stated in the preface, this scientific journey started with the initial questions about the (perceived) effectiveness of barriers. It, however, turned out to become an exploration of various, often 'T- shaped',

scientific domains like decision making, game theory, behavioural psychology, expert judgement, probability theory, and many more. Starting from maximizing/optimizing normative theories like economics, rational decision making and alike, in which we expected to find some clues about the optimal method to evaluate and select security barriers, this journey soon turned into psychology of decision making and opened pandora's box full of different theories and models.
The overall research questions driving this study became about how security professionals assess, reason, and decide about security risks, and what their justification is founded on.

In assessing risks individual actors and organisations follow a series of subsequent steps to reach a final decision: identification and analysis of risks (collect and process information), and reasoning (the evaluation of this information). Reasoning is often defined as inferring or thinking in orderly rational ways, introducing rationality into the arena of thought.

Rationality is a phenomenon that is hard to define and its meaning changes over time and seems to vary between various scientific domains. A definition that suits this work, as it contains the elements as identified in the underlying research, is posed by Steven Pinkerton: rationality is the ability to use knowledge to attain goals (p36, Pinkerton, 2021). In this book knowledge is defined as justified true belief. So rationality is the ability to apply justified true belief to attain goals. The definition of risk, as earlier referred to in Part 1 Chapter 3, also contains goals referred to as objectives: Risks are defined as the effect of uncertainty on objectives (ISO, 2018). In other words: the ability to apply justified true believe helps to attain goals and the effects of uncertainty might endanger them.

Risk management can, thus, be interpreted as applying justified true belief to manage the effects of uncertainty on objectives.

In Part 2 Chapter 4 the sources for justification of belief are explored. Interesting to note here is that personal experience (2) and personal training/education (5) ranked high in the list of both most used and most trusted sources. The justification of true belief seems to be, in this case, belief in oneself. To put it bluntly: one of the justifications for true belief is *my* belief. This comes close to gut feeling which is defined as knowing without knowing why (Kahneman et al., 2021). Other top ranked sources for justification are: experts (1), internal intelligence (3) and peers (4). My belief seems, besides belief in myself, also to be based on the beliefs of others.

As true belief is partly based on *my* belief this might support the (over)confidence in own judgement as identified in the study presented in Part 2 Chapter 3. The fact that the majority of the security professionals state they can estimate a security risk most of the time, even if they are aware information is lacking. This so called non-regressive prediction (Harris, 2020), might relate to this believe in one's own belief. Stated in the same chapter: more experience enhances this effect and reduces the need to collect more information before an assessment can be done, similar to the finding presented in Part 2 Chapter 3.

Intuition, like gut feeling defined as thinking that you know something, without knowing why, is in fact is recognition (Harris, 2020). It makes sense that experience and recognition are positively correlated. So: more experience > more recognition > more intuition based decision making.

Intuition based decision making is one of the cognitive modes of reasoning. Dual-process models of the mind or two systems thinking, as coined by Kahneman (Kahneman, 2011), reflects two modes of thinking, or ways that ideas come to mind (this dual-process model is in more detail introduced in the introductory chapter on page 46). System 1 thinking is fast, intuitive, passive, automatic, without asking for it, and performed completely unconscious of the process. System 2 thinking on the other hand is slow, deliberate, performs reasoning, is considerate and requires focus and cognitive effort. It's about effortless vs effortful thinking.

The study in Part 2 Chapter 2 shows the difference in preferences between these two systems. When asked about their preferences in security risk decision making, the topics that are on top of mind (system 1) differ from the ones that are mentioned when the professionals are forced to compensatory decision making (system 2). The most remarkable difference identified in this study is the topic of human safety. It was on top of mind by only 24% of the professionals as an attribute they apply in their risk assessments. After deliberate reasoning almost all of the respondents ranked this topic in their top 10 and 73% of the professionals even ranked it 1st (most important preference topic for their risk assessment). It is important to observe that preferences in automatic, fast security decision making differ from more reasoned security decision making. As many scholars note that the majority of human decision making is done using system 1 thinking (Harris, 2020; McChrystal, 2021) this might be reason for concern.

The results of the experiments presented in Part 2 Chapter 1 show the vulnerability of security professionals for biases. These biases, which are defined as systematic deviations and inconsistencies, predominantly come to effect in system 1 reasoning. In this chapter the possible consequences for security risk decision making are exposed.

Another giant that forms the foundation of this research is Gary Klein. His work on Naturalistic Decision Making (NDM) and studies of real life decision making revealed the significance of recognition in decision making. The professionals he studied assessed situations quickly (and often accurately) by recognition of cues (aspects) retrieved from experience. In his work experience is, thus, deemed paramount. There is scientific tension between NDM and the biases and heuristics scholars. Kahneman and Klein spent almost six years exploring the differences and commonalities of their approaches. They ended up concluding that they fail to disagree (Kahneman & Klein, 2009). The main topic where their perspectives were expected to deviate was whether intuition based decision making leads to the best decision. Intuition is explained as the recognition of patterns in reality (Klein, 1993). Klein put a lot of trust in recognition based on experience, Kahneman has spent much of his scientific career showing the biases related to intuition (system 1). Finally they came up with three prerequisites for ‘good’ decision making based on intuition.

Intuition works when:

1. The situation is regular/predictable
2. An individual has enough exposure to these situations
3. There is rapid feedback on judgements/guess/actions

In other words the individual decision maker must have the opportunity to learn from previous situations and the situation at hand needs to be comparable to these previous ones.

If these prerequisites are met, and the situation is considered familiar, system 1 decision making is performed and has a good chance to lead to a good decision (see Figure 6 in the Introduction of this dissertation). If the situation is not considered familiar system, the situation requires a second thought and system 2 decision making is performed.

In the domain under study, security risk decision making, these prerequisites seem to be absent. As stated in Part 2 Chapter 1, this domain is characterized by malicious intent that is meant to be unpredictable, often concealed, circumvents existing controls and consists of a virtually unlimited number of possible modus operandi and situational characteristics. The situation is not meant to be regular/predictable. An individual decision maker is often exposed to a limited number of comparable incidents. And finally the feedback loop for judgments/decision on controls is lacking (individual decision makers often have no possibility to tell if nothing happened because a control is implemented or nothing happened because no one tried). This domain, thus, seems to be not suitable for intuition based decision making. The results of the study in Part 2 Chapter 3 show that the security professionals are not hindered by a lack of detailed information, they indicate they can almost always form a judgment. Even if they are aware information is not available to them they still show a high level of confidence in their judgment. It is uncomfortable to conclude that in a domain of utmost importance, justification for true belief is often lacking, according to the security professionals. If justification is lacking, 'true' cannot be confirmed which leaves only belief as the sole source of security risk decision making. A disturbing finding is that more experience leads to more confidence and less perceived need for a second thought. More experience, in other words, leads to more, biased, intuitive decision making.

Facts

As presented in Part 2 Chapter 3 the professionals working in the security domain state themselves that, on average, exact knowledge of security events is lacking in half of their risk assessments (which is probably overrated). So in half of the risk assessments beliefs seem to be based on facts and evidence and in the other half beliefs are based on assumptions (take for granted or true). On the scale of uncertainty, as introduced in the preface of this dissertation, security risks are, thus, positioned primarily in the area of uncertainty as detailed information is often lacking.

The sources of security risk information are explored in the study presented in Part 2 Chapter 4. Table 7 in this chapter shows the ranking of most used sources of security risk information. Top ranked are experts, defined as knowledgeable people recognized in the field. Apart from the individual, personal, information sources, as mentioned in the previous section, the ranking continues with internal intelligence (3), peers (4), expert communities (6), external government intelligence (7), government/government agencies (8). Science/scientific publications is ranked 9, although, in the quality ranking it was ranked third. Commercial risk information is ranked relatively low: external commercial intelligence (11), consultants/consulting organizations (13), and supplier organizations (16). It seems that commercial risk information is both perceived of relatively lower quality and is therefore deemed less important. Colleagues (10) and higher management (15) are also low ranked. Finally public sources like media (14) and social media (17) are perceived less important. Our study did not investigate whether these last sources are perceived to supply facts or beliefs. More experienced professionals seem to value commercial external intelligence, public sources like media, and government/government agencies, less than unexperienced professionals. On the other hand significant positive associations are identified between experience and the sources personal experience and gut feeling. It seems that more experienced practitioners have more confidence in their own perception and judgement.

Assuming that the professionals are right in their perception of the availability of exact knowledge on security events, half of their assessments is based on detailed security risk information. The study presented in Part 2 Chapter 1 identified the vulnerability of the professionals for known biases. Overall the security risk decision making of almost seven out of ten professionals is guided/influenced by biases leading to sub-optimal outcomes (not the maximum possible outcome). In the security domain this could mean that, often scarce, resources are not allocated with maximum effect in focus, in this case a maximum reduction of security risk.

As mentioned in the previous section, the absence of detailed information in half of their assessments does not hinder the professionals from assessing security risks and even be confident about their assessments. As they are aware information is lacking, one could assume that they would rather retrieve more information (if possible) to boost their confidence in their security risk assessments. In Part 2 Chapter 3 this assumption is explored. Overall 29% of the surveyed security professionals (N=166) indicate that they would always be more confident about their risk assessments if they had more information. 33% of them would be more confident most of the time, 9% about half the time, 28% only sometimes and 1 % never. A large portion of the security professionals (71%) seem to imply that not in all situations they need more information to be more confident. They might either know all there is to know or are satisfied with the available information. The latter refers to the decision making concept of ‘satisficing’ (Gigerenzer & Selten, 2002; Gigerenzer, Todd, & ABC Research Group, 1999; Simon, 1982). More experienced security professionals demonstrate a higher level of confidence in their assessments and indicate that more information would raise their confidence to a lesser extent than less experienced professionals. A higher education level, on the other hand, leads to a significantly higher increase on confidence level if more information would be available. In other words: more experience leads to less need for more information, a higher education level raises the need for more information.

In Part 2 Chapter 3 the results of experiments with real life case studies are presented. Professionals working in the security domain are offered short case descriptions and are asked to assess the likelihood of each of them. Much to our surprise the likelihood assessments of the professionals of the individual cases showed a broad distribution. Based on the exact same information and context the assessments of the security professionals varied between very unlikely to very likely. Due to the fact that detailed information is often lacking (Part 2 Chapter 3) the judgment of these professionals is guiding security risk assessments. As the professionals state themselves in Part 2 Chapter 4, personal experience is the second most important source of security risk information. It is at least troubling that security professionals, even with comparable back grounds, reach such a variety of assessments or so called noise (explained in Part 2 Chapter3).

The experiments as mentioned above are also set up to explore the influence of the amount of (detailed) information. The professionals were randomly split into two groups. To each group we presented two case studies, one of them with a short case description, the other one with an extended, more detailed description. With these experiments we were testing the conjunction fallacy. This fallacy shows that more detailed information raises the perceived likelihood of a case while logic reasoning would lead to a lower likelihood. We could observe the effects of this fallacy in our experiments. The perceived likelihood of the detailed cases was higher. Even in a separate experiment in which the respondents were asked to select the option with the highest likelihood, and the two options are shown to the respondents at the same time, the fallacy prevailed over logic reasoning. No less than 3 out of 4 respondents (N=165) followed the fallacy and chose against the logical valid option. In the results we noticed that this even went up to 4 out of 5 for a the cybersecurity professionals. One of the cases might be more familiar or recognizable to them. As we modelled in the introduction in Part 1, recognition of a situation would lead decision makers to perform a system 1 process which is the natural habitat of heuristics and biases.

To conclude this part: more information is no guarantee for better, more reasoned or rational decisions. On the contrary: more information can lead to more bias. Even with information available, the perception of this information by the individual decision maker can trigger biases and cause noise in their decisions.

Risk: Likelihood x Impact ?

The definition of risk is described in Part 2 Chapter 3: Risks are defined as the effect of uncertainty on objectives (ISO, 2018). The two components of risk, effect and uncertainty, are often expressed as impact and likelihood. Over the course of this research it became clear that the security professionals clearly showed so called probability ignorance (Sunstein, 2002, 2005). The possible impact of a security risk seems to guide their decision making over the likelihood of it.

The study as presented in Part 2 Chapter 1, showed that the professionals, when confronted with two options with an equally weighed security outcome, prefer the one with the lowest impact. The results show, however, the existence of a ‘tipping point’. If the absolute difference in likelihood between the two options is 5% or lower the vast majority base their choice on the smallest impact. If the absolute

difference in likelihood is 20% or higher they predominantly let their decision be guided by likelihood. The results of this study do not allow a more precise identification of this tipping point. It is safe to conclude that for risks with low perceived likelihood, like many security risks, the possible effects of security decisions on small likelihoods, result in low likelihood differences. The results of this study indicate that this probably will be ignored by the vast majority of professionals.
Part 2 Chapter 2 presents the results of a study into the most prominent preferences of security professionals when assessing security risks. The first open ended question of this study allows the professionals the freedom to indicate their preferences which are on top of their mind. It is remarkable that only 43% of the professionals indicate they consider likelihood. On the other hand 86% of the professionals mention one or more impact criteria. In the remainder of this study the professionals are asked to first rate the importance of a predefined list of aspects. Likelihood is rated extremely important/very important by 92% of the professionals. Overall this made likelihood rated 4 of most important criteria. In the final part of the study the professionals are asked to rank their most important criteria. Despite the fact that the vast majority of the professionals rated likelihood extremely/very important, likelihood was selected in the top 10 by only 34% of the professionals. Overall this criterion ended at rank 11. The ten most important criteria applied in security risk assessments, as indicated by the professionals, are all criteria related to impact. These results, again, seem to identify ignorance of probability.

The experiments in Part 1 Chapter 3 include real life security cases of which the professionals are asked to assess the perceived likelihood of occurring. Confronted with the exact same information the security professionals reach very different judgements of likelihood. These results indicate that these professional assessments can vary substantially. The value of likelihood assessments can, at least based on these results, be questioned. Other scholars also identified the influence of noise on assessments (Kahneman et al., 2021).

The results of the various studies in this dissertation seem to confirm probability ignorance in security risk decisions. Assessments/decisions on security risks are mainly driven by possible perceived impact. Confronted with situations that might produce a possible negative impact, the obvious human reaction is to try to avoid this (Sunstein, 2002, 2003, 2005). Especially if the negative impact is perceived severe, a dreaded risk, this might be avoided at any cost. Is this case likelihood, however small it may be, is not considered any more. An example is the so called '1% doctrine': even if there's just a 1 percent chance of the unimaginable coming true, act as if it is a certainty. This doctrine, assigned to Dick Cheney, at the time vice - president of the United States, can be regarded as a formalized form of probability ignorance. According to the results of this PhD research, it seems that security risks, often with a perceived dreaded impact, are triggering the same response in the professional security community.

As this research also identified a substantial level of noise in likelihood assessments by experienced professionals, likelihood might be considered less important in security risk assessments. Resources to analyze likelihood might be better spent.

Implications for the Professional Domain and Society

What started out of curiosity turned out to become a very relevant topic in the physical and cyber security domain. As the studies are based on field research with large groups of professionals it was not unnoticed by the professional society. Over 500 responses were collected in various surveys, experiments and workshops. This lead inevitably to requests to share the results in both the professional cyber and physical security communities (unfortunately these two domains are still largely separated from each other).

Not only the results are presented at various prestigious professional conferences, at most of them some of the experiments are repeated with live audiences confirming the published results. Overall an estimated 1500 professionals have taken part in presentations and experiments in both live and online conferences.

(Some of) The results are presented at:

- ASIS Security Management Congres 2016
- Innovatie congres Ministerie Veiligheid en Justitie 2016

- IT & Information Security congress 2017, Heliview
- Kennislab NVVK (Nederlandse Vereniging voor Veiligheidskunde) Workshop cybersecurity 2019
- Digital 2020 ISF World Congress (Information Security Forum)
- ASIS Europe 2021
- BCI World Conference & Exhibition 2021 (Business Continuity Institute)
- Aalto University Executive Education, Workshop 2022
- Thought Leadership Summit OSPAs 2023 Outstanding Security Performance Awards)

Overall the responses to these presentations were very positive. It turned out that behavioural psychology and psychology of decision making was hardly known and not a part of the curricula of security trainings and education. The participants were usually very surprised to learn about biases and especially their own vulnerability for them. During the many conversations with the participants it also became clear that the professionals hardly seem to consult science, scientific papers and books, and scientific conferences. Science, on the other hand, appears to be hardly putting effort in reaching out to the professional community by publishing their work in professional journals and translating scientific results in practical application. In the epilogue of this thesis a perspective on science as experienced during this PhD journey is presented.

As stated in the preface, this thesis is an attempt to bridge the gap between science and praxis. This individual quest, at a small scale, resulted not only in presentations during the conferences mentioned above, it also resulted in two professional publications. The first, kindly allowed to be reprinted in this thesis by ASIS International, was published in Security Magazine (see Part 3 Chapter 5). This award-winning publication of ASIS International is written primarily for security professionals. The paper: *Illogical Decision Making? Unwrapping Bias in Security Decisions* was chosen to be the cover article of the May/June 2022 copy of this magazine. It turned out to be ranked fifth of best online read articles of 2022 of this magazine with over 2495 online reads at 20 February 2023. A read or view might be considered the professional equivalent of a citation. As this magazine is also sent to over 36000 security professionals in print (to the members of ASIS

International) it can be assumed that probably even a few thousand more have read it via their printed copy.
The second professional paper: *Influencing security professionals: Are they biased and by which source?* is published as a result of a call for papers for the project: Platform Influencing Human Behaviour, commissioned by the Royal Netherlands Army. The Hague Centre for Strategic Studies (HCSS) collected novel research on the subject Information-based behavioural influencing. This paper is peer reviewed via HCSS (see Part 3 Chapter 6). It is published online at 12 June 2023. This paper presents a brief summary of the four scientific publications of Part 2 of this dissertation. It is shared and promoted via LinkedIn (3837 impressions at 29 June 2023) and Twitter (5587 views at 29 June 2023). Until this date this paper is ranked fourth most downloaded paper from this institute with 139 downloads.

It is safe to conclude that the quest to bring science to daily praxis has, at least on this small scale, succeeded. All this attention from the professional community, as received in return, shows the serious interest in this topic and the relevance for this domain. This work, at least, raised awareness about, and knowledge on, this topic. "Acknowledging the complexity and scale of the problem is our only real chance to shift our misperceptions, individually and collectively" (Duffy, 2018, p. 19).

One of the obvious questions of this domain followed almost in every discussion: what can we do about it? This question is not been part of the scope of this study. However, in the professional publication presented in Part 3 Chapter 5 a brief overview is of possible measures is provided to enhance individual decision making and reduce the influence of possible bias.

One of the first possible countermeasures is to discuss decisions in a diverse group of people (McChrystal, 2021; Osmani, 2017). Different people might have different information, experience and expertise. As identified in the study presented in Part 2 Chapter 3 even with the exact same information different professionals reach (very) different conclusions.

As stated in the introduction decisions are primarily performed using system 1 reasoning that is prone to bias and heuristics. As presented in Part 2 Chapter 2, giving first impressions a second thought might change a final judgement. So it might make sense to put some additional effort in rethinking a decision before letting intuition run off with it (Boissin, Caparos, Voudouri, & De Neys, 2022; Croskerry, Singhal, & Mamede, 2013).

Over time various debiasing techniques are identified that are proven to enhance decision making (Bettinghaus, Goldberg, & Lindquist, 2014; Gigerenzer, 1991; Larrick, 2004; Soll, Milkman, & Payne, 2015).

Satisficing, settle for an option that is acceptable instead of optimal (Gigerenzer et al., 1999; Herbert A. Simon, 1956), might be avoided if the stopping rules are adjusted (Gigerenzer, 2015). Invest time in finding more options and comparing them leads to compensatory reasoning (system 2) and might optimize the outcome.

Finally this research confirmed the influence of (over)confidence, especially in judgment of experienced decisions makers. Stimulating the ability to question own intuition and judgement can help avoiding (over)confidence. Many studies in various domains are committed on this topic (Croskerry & Norman, 2008; Lambert, Bessière, & N'Goala, 2012; Russo & Schoemaker, 1992; Russo, Schoemaker, & Russo, 1989; Van Zant & Moore, 2013).

This brief summary of techniques to enhance decision making might be far from sufficient for practical application. We can only hope that the substantial interest of the professional security community, as displayed in this last section, inspires other scholars to continue this work.

As we started this paper with a quote of McChrystal we will also end with him:

> "At the end of the day, we can't choose to have or not have biases – we have them. So we must identify and carefully consider them. It is imperative to identify biases and do what we can to limit and correct for their impact on our decision making"

(McChrystal, 2021, p. 124).

We hope that the reader, after taking notice of the findings presented in this dissertation, is able to take this final advice and improve judgment and decision making.

At the end of the day even highly skilled security professionals are prone to flaws in their reasoning and judgement.

In the end it turned out
that we are human after all……..

Literature

Bettinghaus, B., Goldberg, S., & Lindquist, S. (2014). Avoiding auditor bias and making better decisions. *Journal of Corporate Accounting & Finance, 25*(4), 39-44.

Boissin, E., Caparos, S., Voudouri, A., & De Neys, W. (2022). Debiasing System 1: Training favours logical over stereotypical intuiting. *Judgment and Decision Making, 17*(4), 646-690.

Croskerry, P., & Norman, G. (2008). Overconfidence in clinical decision making. *The American journal of medicine, 121*(5), S24-S29.

Croskerry, P., Singhal, G., & Mamede, S. (2013). Cognitive debiasing 1: origins of bias and theory of debiasing. *BMJ quality & safety, 22*(Suppl 2), ii58-ii64.

Duffy, B. (2018). *The perils of perception: Why we're wrong about nearly everything*: Atlantic Books.

Gigerenzer, G. (1991). How to make cognitive illusions disappear: Beyond "heuristics and biases". *European review of social psychology, 2*(1), 83-115.

Gigerenzer, G. (2015). *Risk savvy: How to make good decisions*: Penguin. Gigerenzer, G., & Selten, R. (2002). *Bounded rationality: The adaptive toolbox*: MIT press.

Gigerenzer, G., Todd, P. M., & ABC Research Group, t. (1999). *Simple heuristics that make us smart*: Oxford University Press.

Harris, S. (2020). The Biology of Good and Evil. In *Making Sense.* London: Transworld Publishers.

Harris, S. (2020). The Map of Misunderstanding. In *Making Sense.* London: Transworld Publishers.

Kahneman, D. (2011). *Thinking, fast and slow*. New York.

Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise: a failure to disagree. *American psychologist, 64*(6), 515.

Kahneman, D., Sibony, O., & Sunstein, C. R. (2021). *Noise, a Flaw in Human Judgment*. London: William Collins.

Klein, G. A. (1993). *A recognition-primed decision (RPD) model of rapid decision making*: Ablex Publishing Corporation New York.

Lambert, J., Bessière, V., & N'Goala, G. (2012). Does expertise influence the impact of overconfidence on judgment, valuation and investment decision? *Journal of Economic Psychology, 33*(6), 1115-1128.

Larrick, R. P. (2004). Debiasing. *Blackwell handbook of judgment and decision making*, 316-338.

McChrystal, S. A. (2021). *Risk, a user's guide*. New York: Penguin business.

Möller, N. (2012). The concepts of risk and safety. *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk, 1*, 55-85.

Osmani, J. (2017). Heuristics and Cognitive Biases: Can the Group Decision-Making Avoid Them? *Academic Journal of Interdisciplinary Studies, 5*(3 S1), 225.

Russo, J. E., & Schoemaker, P. J. (1992). Managing overconfidence. *Sloan management review, 33*(2), 7-17.

Russo, J. E., Schoemaker, P. J., & Russo, E. J. (1989). *Decision traps: Ten barriers to brilliant decision-making and how to overcome them*: Doubleday/Currency New York.

Simon, H. A. (1956). Rational choice and the structure of the environment. *Psychological review, 63*(2), 129.

Simon, H. A. (1982). *Models of bounded rationality: Empirically grounded economic reason* (Vol. 3): MIT press.

Soll, J. B., Milkman, K. L., & Payne, J. W. (2015). A user's guide to debiasing. *The Wiley Blackwell handbook of judgment and decision making, 2*, 924-951.

Sunstein, C. R. (2002). Probability neglect: Emotions, worst cases, and law. *The Yale Law Journal, 112*(1), 61-107.

Sunstein, C. R. (2003). Terrorism and probability neglect. *Journal of Risk and Uncertainty, 26*(2), 121-136.

Sunstein, C. R. (2005). *Laws of fear: beyond the precautionary principle*: Cambridge University Press.

Van Zant, A. B., & Moore, D. A. (2013). Avoiding the pitfalls of overconfidencewhile benefiting from the advantages of confidence. *California Management Review, 55*(2), 5-23.

EPILOGUE

In this epilogue some personal observations are shared on the PhD process, the scientific community, the professional community and the gap between them. Diving into academic education and research after a professional career of about 30 years led to some remarkable experiences. Some differences between the two communities turned out to be bigger than expected but some turned out to be smaller, both communities actually try to achieve comparable goals. This epilogue is personal, readers might disagree, have different experiences or, on the other hand, might recognize parts of it. Whether these observations reflect broader trends or are just a results of individual traits, remains debatable, a debate the author is more than willing to have.

As already mentioned in this dissertation my PhD journey started out of curiosity. This curiosity is grounded in the will to understand certain phenomena in my domain of work: physical and cyber security. It is very much related to the content, the object of interest. Soon after starting my PhD process I learned that doing research seems to be more about the scientific process and that the topic sometimes seems to be secondary importance. Reading papers and attending scientific conferences, colloquia and seminars strengthened this observation. Often the main body of work and the debate during conferences and colloquia is about the method and analysis. Understandably the method and analysis need to withstand scientific scrutiny but my personal observation is that conclusions and their impact, therefore, often receive less attention. This sparks the impression that the conclusions seem to be considered less important.

In my humble quest to bring the scientific and professional worlds in contact, I have learned the hard way. I have invited scientists to present their work to a professional audience, it more than once became annoying for both sides. Professionals expect clear, actionable, conclusions and a way forward. Scientists have a tendency to focus more on their scientific method and analysis. Understandably scientific conclusions and advice usually contain a bandwidth of uncertainty and are often limited to the more or less exact defined scope of research. Professionals, however, often need to translate this into ‘binary’ action. To put it a little black and white: science is about the method, professionals need an actionable outcome. In general science is focused on the question, professionals on the answer. I came to respect both perspectives along the way and to be honest I became more of a scientist than I expected at the start.

One of the weird consequences of the scientific focus on method and analysis I observed is that a scientist does not necessarily have to be an subject matter expert (SME) on the topic under study. More than once I encountered (starting) PhD researchers completely new in their field of study. As a result there might be a disconnect between the study and the field. Some studies are of less practical relevance than they could be, some study phenomena are known in praxis already of which a SME would be aware.

The professional community, on the other hand, seems to be less interested in investing their resources in research. Scientific literature and conferences are not consulted or even ignored. Professional participation in scientific research is often limited. In the professional domain there is a growing tendency to digest information only via infographics, 'one-pagers' and executive summaries, short easy to digest information. The result is that context, background, limitations and nuance are usually left out. Scientific information does not necessarily fit such communication. Without effort the professional community is missing valuable and available scientific insights that might otherwise have improved their operation.

The scientific community is guided by their own KPI's which drives them in directions not necessary in line with the needs of professionals in society. Scientific success seems to be measured by publications in scientific journals, preferably with a high impact factor, and the citations following from it. These journals are mainly focused on, and read by, other scientists, citations are mainly citations in other scientific papers by other scientists. So this turns out to be 'science for scientists', not particularly science for application in society. On one hand this is understandable and even sensible as in-depth scientific debate between specific scientific experts is needed to bring science to a next level. This scientific scrutiny is a prerequisite for solid and reproducible knowledge. These KPI's, however, seem to keep science in the scientific domain (only) and no incentives to bring knowledge to professionals in society seem to be in place.

Another way of directing science is via research programs and grants. Nowadays these usually contain the requirement to include non-scientific organizations as partners in the research project. They also often include a mandatory reporting channel to professionals and society. This is a first step that needs to be encouraged and should, in my opinion, get a more prominent position in the research projects.

and/or organize communication outside the scientific community. This does, however, not reduce the need for scientific publications with the consequences listed above.

Small side note: winning grants is very comparable to winning commercial tenders. This could bring these communities closer if science is willing to learn from the commercial communication and experience as practiced in the professionals community.

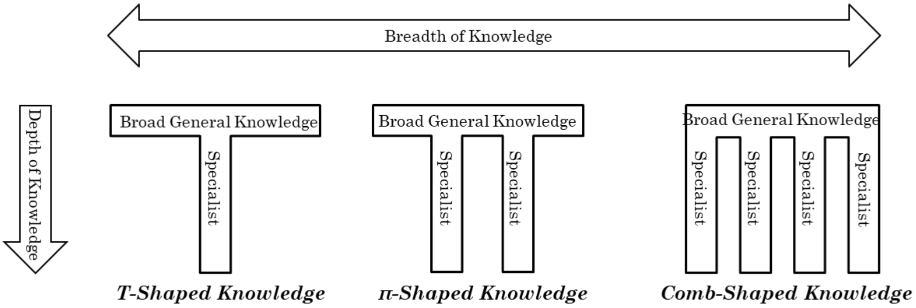


Figure 1: T, π, and comb-shaped knowledge (CertiBanks, 2021)

As this dissertation showed, real world phenomena and problems hardly fit a 'T-shaped' scientific domain (see Figure 1). Most often combinations of knowledge are needed to understand them. Problems in daily praxis most often need a holistic or multi discipline approach and preferably need team members with comb-shaped knowledge and expertise. Figure 1 shows a probably hypothetical comb-shaped specialist but even a more realistic and less perfect 'old-comb-shaped' specialist (see Figure 2) might be preferred over a T-shaped one.

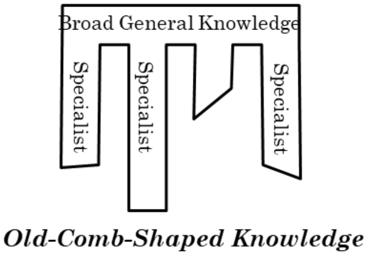


Figure 2: the 'old'-comb-shaped knowledge profile

During this PhD journey it is observed that science is, still, often working in narrowly bounded domains (see also the paragraph in the introductory chapter at page ..). Work is published in (highly) specialized, domain specific, journals and conferences. In this way knowledge keeps contained to these domains as there is hardly an incentive to work cross domain. The result is that several separated domains develop comparable or complementary theories but they are hardly exchanged. Separate domains develop their own definitions and vocabulary and often even refuse to cooperate as stated and referenced at page 43 of the introduction.

A remarkable reference, as also used in this dissertation, is the study: Conditions for intuitive expertise: a failure to disagree by Daniel Kahneman and Gary Klein (Kahneman & Klein, 2009). They worked in separated scientific domains on decision making. The title explains that they expected to have very different opinions on the topic of intuitive expertise in decision making but finally concluded that their work was complementary and supportive.

Publishing cross-domain studies during this PhD process turned out to be challenging as many journals seem to be single domain (although they might state otherwise in their journal description). A topic might not be considered as belonging to their specific domain of interest or interesting for their, again specific, readership. More progress can be made with less resources if scientist would take the effort to cross their, self-created, boundaries.

Both the scientific and the professional domain are driven by their own goals and work in their best interest. Spending time and resources on collecting, understanding and applying scientific knowledge, by the professional community, and translate scientific results into actionable and applicable knowledge and communicate them by the scientific community seems for both a bridge too far. My personal observation, leading to a bit of a disappointment, is that both sides do not seem to be willing to invest in understanding and cooperating with each other. Call it naïve but personally I believe both can benefit from mutual support. Probably I am not the first, nor the last, to address this issue. At least I hope some readers, on either side, might notice this message and take action. If only a handful of people get inspired I consider my personal quest to close the gap successful.

Literature

CertiBanks (Producer). (2021). From I-Shaped to T-Shaped – Why IT Professionals need to be Multi-Skilled.

Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise: a failure to disagree. *American psychologist, 64*(6), 515.

CURRICULUM VITAE

Johan de Wit works for Siemens Smart Infrastructure in a non-commercial role as Technical Officer Enterprise Security EMEA. He is involved in global Siemens security portfolio development and follows national and international trends and developments in the fields of safety, security and risk management, crisis management, smart buildings and business continuity.

He owns a master's degree in Security Science and Management and holds a PhD research position at TU Delft.

He is a member of various government committees, advisory boards, workgroups and communities of practice of norm institutions, government, academia and business associations in the Netherlands like: National Cyber Security Center, ASIS, Information Security Forum, Overseas Security Advisory Board (OSAC), National Network Risk Management.

He is a regular (non-commercial) speaker at conferences and universities and publishes papers and articles.

Scientific Publications:

De Wit, J., Pieters, & van Gelder, P. (2023). Sources of security risk information: What do professionals rely on for their risk assessment? Under Review: The Information Society, Taylor & Francis Online

De Wit, J. Pieters, W., & van Gelder, P. (2023). Bias and noise in security risk assessments, an empirical study on the information position and confidence of security professionals. *Security Journal*, 1-22.

De Wit, J.J., Pieters, W., & van Gelder, P. H. (2022). Individual preferences in security risk decision making: an exploratory study under security professionals. *Safety and Security Engineering IX*, 206, 187.

Rajkumar, V.S., Musunuri, S., Stefanov, A., Bruijns, S., de Wit, J., Klaar, D., Louh, A., Thoen, A., Palensky, P. (2022) A Blueprint for Cyber Security of Brownfield Substations. In *CIGRE PARIS SESSION 2022* (Paper ID – 10348)

Rajkumar, V.S., Stefanov, A., Musunuri, S., de Wit, J. (2021) Exploiting

ripple20 to compromise power grid cyber security and impact system operations. In *CIRED 2021*-The 26th International Conference and Exhibition on Electricity Distribution (Vol. 2021, pp. 3092-3096). IET.

De Wit, J., Pieters, W., Jansen, S., & van Gelder, P. (2021). Biases in Security risk management: Do security professionals follow prospect theory in their decisions? Journal of Integrated Security and Safety Science, 1(1), 34-57.

Professional Publications:

De Wit, J.J. (2023). Influencing security professionals: are they biased and by which source? HCSS. https://hcss.nl/report/influencing-security-professionals-are-they-biased-and-by-which-source/

De Wit, J.J. (2023). Convergence of Physical and IT Security in Critical Infrastructure, Great! But what about OT? In: *Cyber-Physical Security and Critical Infrastructure.* White paper CoESS & International Security Ligue

De Wit, J.J., Meyer, C. (2022). Illogical decision making. *Security Management* (published by ASIS International). Vol May/June, pp. 26-31

De Wit, J.J. (2019). Smart cities: Informatiedelen om de 'perfect place' te creëren In: *Quo vadis Smart city? De toekomst van een slimme stad.* SIVVPress

De Wit, J.J. (2017). Technologie en security: nieuwe kansen of extra risico's? In: *Na Vandaag, de toekomst van een veilige samenleving.* SIVVPress

De Wit, J.J. (2017). Business continuity belangrijker dan veiligheid, Vloeken in de kerk. *NVVK Info,* vol. 3, pp.14-17

De Wit, J.J. (2017). Business continuity onderzoek 2017: Gevolgen terrorisme onderschat. *Security Management*, vol.10, pp. 14-17

De Wit, J.J. (2017). Aandacht voor business continuity, onderzoek naar de status van business continuity in Nederland 2017. *Siemens Whitepaper*

De Wit, J.J. (2017). Continuity Planning for Climate Change. W*hitepaper Business Continuity Institute & Siemens*

De Wit, J.J. (2015). Veiligheid, risicomanagement en subjectiviteit. *Security Management*, vol. 11, pp.44-47

De Wit, J.J. (2015). Aandacht voor business continuity. *Security Management*, vol. 1/2, pp.38-40.

De Wit, J.J. de (2015). Verborgen gebreken in de 'defence in depth' theorie. *Beveiliging Totaal 2015*, pp. 89-100, B+B Vakmedianet, Alphen aan den Rijn, ISBN 978 9462152328

De Wit, J.J. (2014). Hoe fysiek is informatiebeveiliging? In: *Beveiliging Totaal 2014*, pp. 105-108, B+B Vakmedianet, Alphen aan den Rijn, ISBN 978 9462151086

De Wit, J.J. (2014). Defence in Depth theorie: Verborgen gebreken. *Security Management*, vol. 9, pp.32-35.

De Wit, J.J. (2014). Balans tussen efficiency en veiligheid door slim combineren. W*eekblad Facilitair & gebouwbeheer*, vol. 428, week 44, pp.36.

De Wit, J.J. (2014). Aandacht voor business continuity, onderzoek naar de status van business continuity in Nederland 2014. *Siemens Whitepaper*

De Wit, J.J. (2014). Toegangscontrole: van systeem naar proces. *Weekblad Facilitair & gebouwbeheer*, vol. 403, week 15, pp.29-31.

De Wit, J.J. (2013). Fysieke toegangscontrole effectief? *Security Management*, vol. 12, pp.10-13. Also published as Siemens Whitepaper

De Wit, J.J. (2013). Fysieke beveiliging van informatie. *Security Management*, vol. 11, pp.10-13. Also published as Siemens Whitepaper

De Wit, J.J. (2013). Informatiebeveiliging en fysieke dreigingen. *Security Management,* vol. 10, pp.33-35. Also published as Siemens Whitepaper

De Wit, J.J. de, Hoe fysiek is informatiebeveiliging? Onderzoek naar de Bijdrage van fysieke toegangscontrolemaatregelen aan informatiebeveiliging. Master thesis published as *Siemens Whitepaper*

De Wit, J.J. (2012). Aandacht voor business continuity, onderzoek naar de status van business continuity management. *Siemens Whitepaper*

Personalia

Name:	Johannes Jacobus de Wit
Date of birth:	27 December 1965
Place of birth:	Rotterdam
Titles:	BEc. MSSM
Institute:	Delft University of Technology Faculty of Technology, Policy and Management Safety & Security Science Group Jaffalaan 5 2628 BX Delft The Netherlands

Education

2016 - 2023	PhD Candidate, Delft University of Technology
2011 - 2013	Master of Security Science & Management, Delft TopTech
2005 - 2006	Post HBO, DHM Security Management
1991 - 1995	HEAO Bedrijfseconomie
1983 - 1986	MTS Energietechniek
1977 - 1983	HAVO

Positions

1999 – now	Siemens Nederland NV	
	2022 – now	Technology Officer Enterprise Security EMEA
	2005 – 2022	Solution Manager Enterprise Security
	2001 – 2005	Bedrijfsleider accountteam Telecommunications, Banking
	1999 – 2001	Projectmanager
1995 – 1999	Hollandsche Beton Groep, Ergon	
1985 – 1995	GTI Utrecht BV	