Dutch Citizens and Digitalization: Seeking Individual Cyber Resilience

Oostdam, Jos C.

Dutch Citizens and Digitalization: Seeking Individual Cyber Resilience

Leiden University

Faculty of Governance and Global Affairs

Executive Master Cyber Security

Author: Jos C. Oostdam

Student number: s2811855

Date: 18 January 2022

Supervisors: Dr. J. Shires, Dr. T. van Steen

Acknowledgments

Many thanks to my thesis supervisors Dr. James Shires and Dr. Tommy van Steen for their inspiring lectures and opinions, the sharing of their knowledge and experiences, the stimulation of critical thinking, and the constructive feedback.

Also, I would like to express my sincere gratitude to my partner for his relentless support, and providing the space necessary to be able to write this thesis.

I am grateful to the interviewees for their time and sincere conversations which have provided valuable input.

Finally, I would like to thank my employer for enabling the development of my competences by supporting the education.

Abstract

Dutch citizens are being challenged to cope with digitalized processes, products, and services and related cybersecurity risks. If their individual cyber resilience is inadequate, cyber related incidents may cause resistance against digitalization, thus undermining national interests. Understanding the conceptual elements attributed to individual cyber resilience may increase understanding how to improve individual cyber resilience at individual and government level. Resilience theories, the NIST framework and human behaviour theories contain conceptual elements which add up to the theory, that individual cyber resilience is defined as 'To continuously look for, recognize and classify personal valuables and temporary states of being related to information technology to evaluate associated cost-benefit calculations. To be aware of the influence of emotion, beliefs, and mental shortcuts on this process of evaluation, and to subsequently take supportive action appropriate to the personal tier.' A case study of the Dutch Digitalization Strategy and discourse analysis of interview data demonstrate that strengthening individual cyber resilience as a derivative of the digitalization objective can lead to deficiencies in improving individual cyber resilience at government level. Taking personal responsibility for applying the conceptual elements is key to improve individual cyber resilience at individual level.

(Key words: Resilience, individual cyber resilience, citizens, digitalization, strategy, behaviour)

Table of contents

Glossary

Ability	The individual outcome after dynamic interaction of physical, social, demographic, educational, cultural, financial and mental, behavioural and emotional factors that may overlap and influence each other via organizations, social communities, and within society (Lederer et al., 2014, pp. 258–259).
Attitudes	"The motivators of performance, the basis for continued competent performance. They include values, aspirations and priorities." (Vuorikari et al., 2016, p. 39)
Citizen	A person who has the legal right to belong to a country (Oxford Advanced Learner's Dictionary, 2021a).
Competences	"The proven ability to use knowledge, skills and individual, social and/or methodological abilities, in work or study situations and in professional and individual development. […] competence is described in terms of responsibility and autonomy." (European Commission, 2008, p. 13)
Cyber resilience	The quality of resilience against threats in or from cyberspace.
Cyberattack	A combination of tactics and techniques (The MITRE Corporation, 2022) used to intentionally manipulate automated processes without previous consent, with unintended exposure, undesirable changes, and/or harm as a result.
Cyberspace	Virtual and physical networks where information technology systems are connected for communication and information purposes (R. Bryant, 2001) including related activities (van den Berg, 2018) by human beings and systems.
Government	The group of people who are responsible for controlling a country or a state (Oxford Advanced Learner's Dictionary, 2021b).
Knowledge	"The outcome of the assimilation of information through learning. Knowledge is the body of facts, principles, theories and practices that is related to a field of work or study." (European Commission, 2008, p. 13)

Problem solving	"An individual's capacity to engage in cognitive processing to understand and resolve problem situations where a method of solution is not immediately obvious. It includes the willingness to engage with such situations in order to achieve one's potential as a constructive and reflective citizen." (OECD, 2014, p. 30)
Skills	The ability to apply knowledge and use know-how to complete tasks and solve problems. In the context of the European Qualifications Framework, skills are described as cognitive (involving the use of logical, intuitive and creative thinking) or practical (involving manual dexterity and the use of methods, materials, tools and instruments) (European Commission, 2008, p. 13).

1 Introduction

1.1 Motivation and subject

Dutch citizens are being challenged to cope with an increasing amount of digitalized processes via internet. Equipped with mostly basic digital skills, they google for holiday destinations, facetime with family, and save money by switching from utility and insurance companies within a couple of clicks. Besides commercial organizations, the Dutch government also encourages the use of its digitalized services. Home address changes and crime reports can be performed without leaving home.

Traditional methods are given up to embrace a new reality. Previously, citizens' information needs were facilitated by means of coupons, telephone information lines and local offices. Nowadays, these facilities may have been replaced by frequently asked questions at websites, email contact and chat functionalities. Meanwhile, citizens receive information about risks, threats and incidents related to internet. They are warned by their banks to never share credentials by phone, via text messages or by email. They receive news items about hacks, ransomware and data leaks, and may receive suspicious digital messages. Their reading and writing skills must be supplemented by the possession, use and maintenance of electronic devices to be able to cope with digitalized processes and stay secure at the same time.

Cybersecurity threats are part of Dutch citizens' daily life, whether they are online or offline, adult or child, as societal processes like finance, public transport and traffic control are digitalized. Households are faced with the integration of microchips into items like modems, meters, smartphones, televisions and solar panels. The trade-off between timely introduction of smart products to the market at an acceptable price for consumers, and security of these products on the long term, is usually to the detriment of the latter. Being interconnected in cyberspace, the Dutch government and citizens may exchange information about cybersecurity risks and recommended responses. However, they may and will have different interests and perspectives on cybersecurity (Shires, 2019). National interests to profit from economic and societal digitalization opportunities may be in contrast with personal interests of citizens to protect their identity and online activities.

Therefore, it is of imperative importance that citizens become and stay individual cyber resilient to protect personal (in)tangible valuables, those of organizations. It is argued that being resilient in real life may increase the resilience of a nation (Edwards, 2009, p. 47; Walklate et al., 2012).

When not fully aware and capable in recognizing and understanding cybersecurity risks, appropriate responses and interests, citizens' may experience anxiety, fear and even resistance regarding digitalization. Besides, mental shortcuts may even unconsciously undermine personal behaviour in cyberspace, and thus subvert individual cyber resilience.

The subject of this thesis is to improve understanding what individual cyber resilience means, and to what extent it is strengthened by the Dutch government. The benefit of this research is an increased understanding of the concept of cyber resilience and individual cyber resilience, and potential areas of improvement on individual and government level.

Theories related to resilience, cyber resilience, cybersecurity and human behaviour related to digitalization processes are scrutinized to define elements related to individual cyber resilience. As digital security may not only rely on citizens' skills and behaviour alone (Coventry et al., 2014, p. 19), a case study of the Dutch Digitalization Strategy, a multi-year and multi-disciplinary government approach to profit from perceived digitalization opportunities by strengthening supportive conditions, is presented.

Being a member state from the start of the European unification (European Union, 2021), The Netherlands has always been strongly connected to and supported the European Union and its regulations. As expected from member states, European directives and regulations are always being converted into national regulation, policies and guidelines. Therefore, this thesis refers mainly to European laws, guidelines and frameworks as basis for the strategy and policies of the Dutch government.

This research is academically relevant because it increases the understanding of elements attributed to individual cyber resilience which may be beneficial to increased cyber resilience of the Dutch society. This research is also practically relevant as the attained insights may support evaluation and improvement of related governmental interventions. This research is based on reports and data by the European Union and the Dutch government, qualitative interviews, and (peer reviewed) scientific literature.

1.2 Problem statement and research questions

Digitalization of processes, products and services may have impact on personal skills, knowledge and abilities. This has been scrutinized by scholars, for example regarding digitalization in organizations (Andriole, 2018; Spöttl & Windelband, 2021), cybersecurity exercises (Brilingaitė et al., 2020; Mäses

et al., 2018), and educational environments (Lorenz et al., 2018; Makdoun et al., 2021; SLO, 2021). However, terms like competences, skills, knowledge and abilities appear to be used interchangeably. For example, Andriole argues the need of skills and competences for digital transformation, but refers only to knowledge and experience requirements in eight out of nine areas (Andriole, 2018).

Having the knowledge what to do may not imply that this knowledge is consistently performed in practice due to inconsistent human behaviour. For example, research amongst 1.038 individual citizens with smart household devices (Thiel et al., 2019) shows that 87% confirm that smart devices should be protected. Although they have secured mostly computers and security cameras, they do not secure their other smart devices.

Ignoring the possibility of a cyberattack is not an option anymore (Wilding, 2016). As attackers and/or their facilitators will continuously innovate their techniques, tactics and procedures to circumvent cybersecurity methods (Overvest et al., 2019, p. 11), it can be argued an individual using digitalized processes will sooner or later inevitably face a cyberattack despite their digital competences. Besides, as network interconnections increase, an individual may apparently not fully understand how information technology systems may be interconnected, and how related processes have been designed. As a result, one may be unaware about what is actually happening in these systems. Also, digitalization of products and services has caused a rise in conflict between business interests and security interests (Van Niekerk & Von Solms, 2010). Low production costs, high margins and a short time-to-market compete with time required for product quality and security by code review and the provisioning of future software updates. As the amount of software code within society increases due to digitalization, the amount of bugs in software code will increase as well. Although code is written to represent the coder's functional intention, it may be misused for different purposes. Finally, even the most secured (and even air gapped) systems may be porous. A system may be perceived as safe, until a previously unknown software bug is discovered, thus be vulnerable to an attack the other day. As systems are being managed and handled by human beings, the human factor may also be the cause of (un)intentional cyber incidents.

At that point in time, it is of crucial importance to national, business and individual interests that a citizen is able to come back online at short term with at most minor individual harm, while maintaining trust in digitalization and confidence in personal skills. Becoming, being and staying resistant against cyberattacks, may be crucial to profit from the assumed opportunities and benefits.

In order to understand the individual ability to limit personal harm, cope with and recover from incidents in cyberspace, we need to analyse and integrate currently separate theories regarding resilience, cybersecurity and human behaviour.

The research objective is to develop a scientific definition of individual cyber resilience, to understand to what the extent it is strengthened by government policy, to understand what government officials aim to achieve in this area, and how it may be improved. Therefore, the definition of the main research question is:

RQ: *To what extent is individual cyber resilience strengthened by the Dutch government, and how may individual cyber resilience be improved at individual and government level?*

The answer to this question is based on the answers to the following six sub-questions:

SQ 1: *What elements may be attributed to cyber resilience?*

Scientific theories and an international cybersecurity framework are integrated to define the cyber resilience concept.

SQ 2: *How may human behaviour influence cyber resilience?*

Human behaviour theories and empirical research are applied to the cyber resilience concept to understand how human behaviour may support or subvert cyber resilience.

SQ 3: *What is individual cyber resilience?*

The cyber resilience concept and the influence of human behavioural aspects are used to build up a theoretical definition of individual cyber resilience.

SQ 4: *What is the current government strategy to strengthen individual cyber resilience?*

A case study of the Dutch Digitalization Strategy and related reports are performed and assessed against the theoretical definition of individual cyber resilience.

SQ 5: *What do government officials aim to achieve regarding individual cyber resilience?*

To answer this question, qualitative interviews are performed to improve understanding of the Dutch Digitalization Strategy, and related aims towards individual cyber resilience.

SQ 6: *What concerns and challenges do government officials experience in achieving these aims?*

During qualitative interviews, in-depth questions are asked about the extent to which the envisaged individual cyber resilience goals are being achieved to understand related concerns and challenges.

1.3 Reading guide

Chapter one includes the motivation underlying this research, the problem statement and the research questions. Chapter two is allocated to the literature review. It contains an analysis of resilience, cyber resilience, and human behaviour theories, and a case study of the Dutch Digitalization Strategy. In chapter three, the thesis methodology is being explained, including the data collection and data analysis method. In chapter four, the research results are presented. In chapter five, the answer to the main research question is discussed and recommendations are being presented.

When research objects like the government, organizations, citizens, and individuals are mentioned, they are attributed to The Netherlands. Where reference is made to ‘she/her’ in this thesis, this may also be read as 'he/his' or ‘they/their’.

2 Literature review

In this chapter, scientific resilience theories, cyber resilience theories, and a cybersecurity framework are examined and assessed to understand and define a concept of cyber resilience. Then, human behaviour theories are applied to this concept to improve understanding how human behaviour may support or subvert cyber resilience. This will result in a theoretical definition of individual cyber resilience.

2.1 The concept of cyber resilience

In the context of this thesis, cyber resilience is defined as the quality of resilience against threats in or from cyberspace. Cyberspace may be perceived as virtual and physical networks where information technology systems are connected for communication and information purposes (R. Bryant, 2001) including related activities (van den Berg, 2018) by human beings and systems.

2.1.1 Resilience

The term resilience is used in technological, biological, psychological, economic, organizational and cultural environments (Southwick et al., 2014a). Resilience is attributed to strength rather than weakness (Fergus & Zimmerman, 2005). Literature review indicates that organizations and scholars may present resilience as a concept without careful definition. For example, scholars related to the Institute of Electrical and Electronics Engineers (IEEE) have applied the term in their peer reviewed academic article without further specification (Weil & Murugesan, 2020). On the contrary, several researchers have performed extensive research to the history, variety and meaning of resilience (Dunn Cavelty et al., 2015; Walklate et al., 2012; Zebrowski, 2013).

A number of researchers have reported resilience as a process. Psychologists (American Psychological Association, 2012) perceive resilience as a process of personal adaptation and opportunity to personal growth when experiencing threats or difficulties. Health researchers (Fergus & Zimmerman, 2005) agree to this definition, and add that the presence of supportive factors are preconditional. The presence of resources is also attributed to resilience and continuation of well-being by other scholars (Southwick et al., 2014b, p. 11). Other investigators (Panter-Brick & Leckman, 2013) argue that resilience is a process that requires time to evolve as experiences are being processed in the human brain and may lead to behavioural adaptation. According to Belgium scholars

(Vandoninck, D'Haenens, et al., 2013), resilience is a process of experiencing and overcoming problems, and learning from personal mistakes.

Resilience as a process may indicate motion, fluctuating in speed and intensity, and temporary in nature, as it connects security and insecurity over time (Dunn Cavelty et al., 2015). Some scholars argue that resilience may be perceived as an outcome, due to its perceptible effect on well-being (Panter-Brick & Leckman, 2013) and as result by overcoming risk (Fergus & Zimmerman, 2005).

The relation between resilience and risk is also argued by Rutter (Rutter, 2006). He argues that exposure to risk, stress and adversity may strengthen resistance to such events in the future and enhance coping (Rutter, 2012), thus increasing individual resilience. When elaborating on his vision, one may argue that focus on prevention and protection against risks from happening alone might not be sufficient to increase individual resilience. This is substantiated by scholars in crisis management (Boin et al., 2013, p. 87) who argue that increasing resilience requires continuous involvement in practical activities such as vulnerability assessments, scenarios and exercises.

As circumstances in life are subject to permanent change, thus in cyberspace as well, it can be argued that being resilient in real life as well as cyberspace is a temporary state of being.

Scholars (Shires & Hakmeh, 2020) define cyber resilience as "the ability to withstand and rapidly recover from disruption". Researchers (Herrington & Aldrich, 2013) argue that cyber resilience is the robustness and ability to survive while maintaining performances and availability. They qualify system diversity as a "valuable source of resilience" which may be at stake by efficiency and cost reduction targets. Zhang (Zhang, 2010) relates the increase of digitalized and automated processes with a decrease in resilience. Regarding system diversity, he argues that digital uniformity to support economic goals comes at the expense of manual and analogue processes which used to provide an alternative way of working.

Cyber resilience is commonly attributed to functional abilities. The Dutch National Coordinator for Counterterrorism and Security (NCTV) has defined cyber resilience as "the ability to reduce (relevant) risks to an acceptable level through a collection of measures to prevent cyber incidents and to detect them when cyber incidents have occurred, limit damage and make recovery easier" (NCTV, 2021, p. 14).

Scholars (Vandoninck, d'Haenens, et al., 2013) have defined online resilience as the ability to apply problem-solving approaches when a negative situation is being experienced to prevent future harm. The European Commission (European Commission, 2020b) connects resilience with personal (digital)

skills to reduce dependency on external factors. They suggest the need for individual preparedness and response to the changing digital environment.

Bryant (W. D. Bryant, 2015) refers to cyber resilience by envisioning three functional characteristics of bamboo. First, bamboo has the ability to flexibly and temporarily take a different position without giving in to the original position on the ground. Second, its round and relatively small shape provides a limited attack surface. Finally, it is part of a larger field of similar plants who are jointly able to streamline their positions to be less vulnerable as a whole.

The beforementioned resilience and cyber resilience theories and definitions provide five conceptual elements which are valuable in the build-up to a concept of cyber resilience. Cyber resilience is a process, as it implies ongoing development and interrelated activities. Cyber resilience is a temporary state of being in which threats, risks, uncertainties, complicating factors and/or perceived problems related to information technology arise and disappear. Cyber resilience is relative to specific assets, which may be tangible such as a computer or smart phone, as well as intangible like passwords, recommended responses, malware protection software, and support by experts. Cyber resilience requires cost-benefit calculations, based on evaluations and trade-offs related to threats, risks, circumstances, resources and well-being to be harmful, appropriate, and/or acceptable. Finally, cyber resilience requires action. This includes noticeable performance in practice, such as verbal or physical responses to situations, update performance and participation in exercises.

Based on the beforementioned theories and definitions, it is now understood which theoretical elements should be part of the concept of cyber resilience. To explore whether an international cybersecurity framework may contain elements to be additional to the theoretical concept, the NIST framework is examined and assessed in the next section.

2.1.2 NIST framework

The framework of the National Institute of Standards and Technology (NIST) (NIST, 2018) is a commonly accepted outline for achieving improvement of cybersecurity in practice. Initially developed in 2014 to address cyber risks within critical infrastructures, the NIST framework may be nowadays applied to other organizations and individuals as well (Overvest et al., 2019, p. 26). The NIST framework consists of the components Core, Tiers, and Profile, which will be examined for additional value to the concept of cyber resilience.

Figure 1. NIST Framework Core (NIST, 2019)

The Core component contains five functions (see figure 1). Each function contains categories and subcategories, describing activities to obtain specific outcomes. The NIST function Identify concerns the identification of systems, data and services most valuable in relation to personal value, substitutability, privacy and financial independence. It also includes understanding of the environment in which cyber threats, risks and vulnerabilities take place to define potential impact. This is input for cost/benefit considerations regarding risk reduction to an acceptable level. The NIST function Protect is related to management of physical, remote and online access by authorized users to locations and devices. It includes a plan for recommended responses for different situations. An example of a recommended response is promoted by the Dutch banking branch in their cyber awareness campaign "Hang up, click away, call your bank!" (Banken.nl, 2013). Education and training might be necessary (NIST, 2018, p. 31) to perform these tasks with confidence. The NIST function Detect concerns recognition and understanding suspicious behaviour, unusual activities and deviant situations. At this point, a cyberattack may not have started yet, already be happening, or have been finished. The NIST function Respond concerns the implementation of recommended responses to limit the consequences of an alleged cyberattack. The NIST function Recover includes activities to ensure the return to one's pre-attack situation at most acceptable loss of information, devices, trust and confidence. Recover also includes an update of the prepared, individual recommended responses.

	Risk Management Process	Integrated Risk Management Program	External Participation
Partial	• Not formalized • Reactive	• Limited awareness • Irregular risk management • Private information	No external collaboration
Risk Informed	• Approved practices • Not widely use as policy	• More awareness • Risk-informed, processes & procedures • Adequate resources • Internal sharing	Not formalized to interact & share information
Repeatable	• Approved as Policy • Update regularly	• Organization approach • Risk-informed, processes & procedures defined & implemented as intended, and reviewed • Knowledge & skills	• Collaborate • Receive information
Adaptive	Continuous improvement	• Risk-informed, processes & procedures for potential events • Continuous awareness • Actively	Actively shares information

Figure 2. NIST Framework Tiers (Simanjuntak, n.d.)

The Tier component (NIST, 2018, pp. 8–11) describes four levels of cybersecurity risk management practices: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4) (see figure 2). Each Tier has its own matching level of accuracy, thoroughness and completeness in cybersecurity risk information, knowledge, and activities. It should be noted that cybersecurity involves customization, because every organization and individual has a unique combination of risks, threats, vulnerabilities, competences, interests and trade-offs (NIST, 2018, p. 2). Therefore, the corresponding tier may vary.

The Profile component enables to define the appropriateness of specific Core (sub) categories for target groups and sectors and their objectives. For example, maintaining trade secrets is an objective of manufacturers (Stouffer et al., 2019), and maintaining resilience is an objective of smart grid operators (Marron et al., 2019). However, they differ as to which data security subcategories apply to the NIST Protect feature. Definitions of a Current Profile as well as a Target Profile may support the development of a specific roadmap for cybersecurity improvement of a target group.

In the context of this thesis, the Tier component appears to have added value to the identified theoretical cyber resilience elements. As each tier has its own degree of accuracy, thoroughness and completeness of knowledge, management, and activities related to risk information, this will influence the quality of cost-benefit calculations and actions, and thus the level of cyber resilience.

The Core components has no identified added value to the concept of cyber resilience. Cyber resilience as a process corresponds with the NIST circle as a closed loop. Cyber resilience being a temporary state of cybersecurity, related to specific assets, and requiring cost-benefit calculations, are part of the Identify function. Cyber resilience requiring action is applied by using verbs for each NIST function that imply an action.

Although the Profile component has no identified value to the cyber resilience concept either, it may contribute to cyber resilience intervention planning by defining specific target groups and appropriate activities.

2.1.3 Discussion

To answer the first sub-question *What elements may be attributed to cyber resilience?*, resilience and cyber resilience theories, definitions, and the NIST framework have been examined. They have provided valuable insights and elements attributed to cyber resilience. Therefore and up to this point, the concept of cyber resilience may be defined as:

"To continuously look for, recognize and classify specific assets and temporary states of being related to information technology, to evaluate associated cost-benefit calculations, followed by supportive action appropriate to the present tier."

This relatively rational, theoretical definition may contain a number of unconscious assumptions regarding behaviour which may deviate in reality. For example, it may be postulated that an individual is not always able or willing to be continuously alert on valuables in every circumstance. Besides, it has been argued that an individual may not even possess the knowledge or ability to assess a situation to be potential harmful, for example due to inscrutable networks interconnections. Also, attacker tactics such as social engineering may initially seem unrelated to information technology, and therefore not be initially recognized as potential harmful. For example, an attacker pretending to be a supportive bank employee may influence the beliefs of an individual to help with online access to her bank account for worse. Finally, as technology and attack tactics evolves, new situations unknown to an individual may arise and trigger mental shortcuts.

As these personal competences are related to cognitive processes, it is assumed that examination of these processes by means of human behaviour theories will improve understanding how behaviour in cyberspace may support or subvert the predefined concept of cyber resilience. This examination is performed in the next section.

2.2 Behaviour in cyberspace

According to human behaviour theories, multiple cognitive processes and mental shortcuts take place before action is observable. In this section, these processes and shortcuts are examined to identify how human behaviour may influence cyber resilience.

2.2.1 Introduction

Individuals have different backgrounds and life experiences based on different social contexts. As a result, personal values, norms, risk perceptions, and considerations may differ per individual. Besides, as life is an ongoing process by nature, individuals may show different levels of cyber resilience over time. Also, they may act differently due to variation and development in competences (Southwick et al., 2014a). At the same time, technology and tactics evolute as well. Behavioural responses effectively applied in the past may not be appropriate or as effective in the future. As information systems become increasingly more secured, the human factor becomes increasingly the weakest link (Schneier, 2000).

The relationship between behaviour, personal well-being, and information technology systems has been subject to research. Research amongst 474 students indicates that proactive responses to cyberattacks caused a protective effect on emotional well-being (Brighi et al., 2019, p. 7). Scholars (Brighi et al., 2019; Vandoninck, D'Haenens, et al., 2013) support the role of coping strategies in being resilience. Two main coping strategies, emotion-focused and problem-focused, have generally been recognized and are defined in the Transactional Model of Stress and Coping (Lazarus & Folkman, 1984). Focus on coping with emotions is related to management of negative feelings, and coping with problems is attributed to problem solving (Brighi et al., 2019, p. 2).

To improve understanding of emotions and cognitive processes that precede observable action, three theories are examined to understand how human behaviour may influence cyber resilience. The Protection Motivation Theory is analysed to increase comprehension of the relationship between fear appeals, cognitive evaluations, and beliefs on the motivation to protect and its influence on the attitude towards the behaviour. To increase understanding which cognitive processes take place afterwards, the Theory of Planned Behaviour is examined. As cognitive processes may be subject to mental shortcuts, related theories by Tversky and Kahneman are also investigated.

2.2.2 Protection Motivation Theory

Before recommended responses are brought into action, emotions and cognitive processes take place. Stimulating recommended actional behaviour by appearing to fear as a motivator is described in the Protection Motivation Theory (Maddux & Rogers, 1983; Rogers, 1975). According to this theory, fear is used as an intervention instrument to influence one's motivation towards the attitude of a recommended response. This theory is examined to detect valuable additions to the concept of cyber resilience.

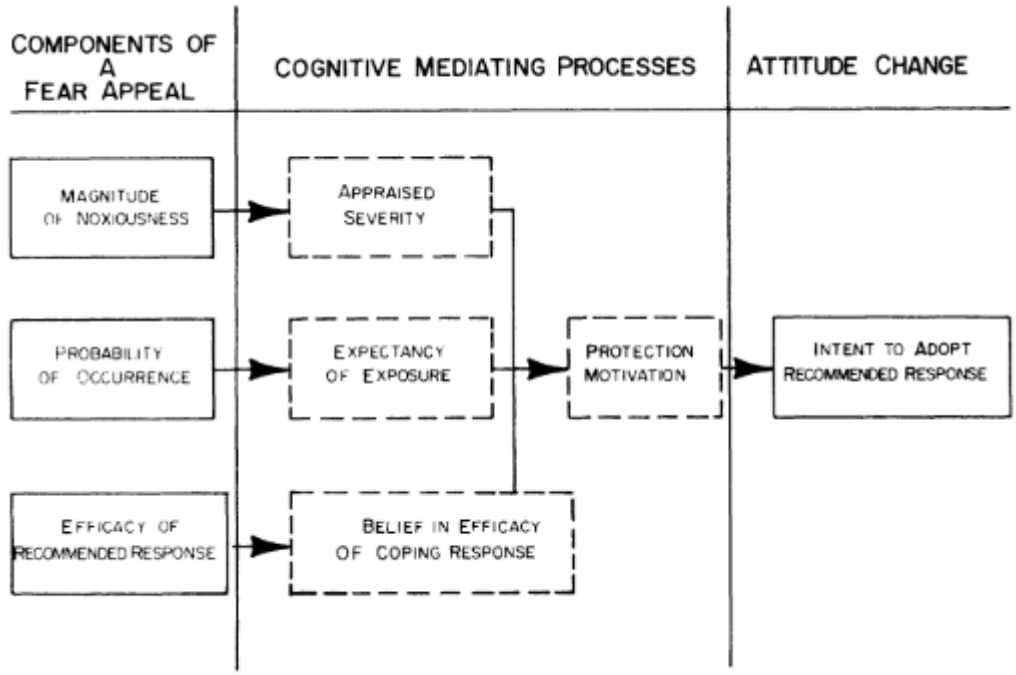

Figure 3. The Protection Motivation Theory Model (Rogers, 1975)

The theory model (see figure 3) starts with three components of fear appeal: the extent of damage, the likelihood of manifestation, and the effectiveness of the recommended actional behaviour. Each component triggers a subsequent mental process. The extent of damage triggers a severity assessment. The likelihood of manifestation activates an assessment of the expected exposure to the event. The effectiveness of the recommended response is assessed against faith in it. If all assessments have a positive outcome, the motivation to protect is initiated with a positive intention to attitude change as outcome.

The influence of emotion such as fear on personal behaviour has been confirmed by other research as well (Hua et al., 2018). Fear appeals to influence behaviour are used in daily life. For example, the

ABN Amro bank publishes real life stories of their own customers who have experienced financial fraud by digitalized banking processes (ABN Amro, 2021).

To illustrate the Protection Motivation Theory, an example is being described. An individual may be socially engineered by a counterfeit bank employee and being persuaded to login into a digital banking website via a provided link. The motivation to protect will rise if the individual believes the situation to be deviant, believes to be targeted, and remembers an appropriate recommended response what to do in such cases. This understanding will lead to awareness of financial loss if the situation continues, recognition that she is currently under target, and assessment to what extent she believes in the recommended response. This may lead to the motivation to protect herself against potential harm, which may trigger the supposed recommended response. In this way, the Protection Motivation Theory may stimulate supportive behaviour towards individual cyber resilience.

Elaborating on this, the motivation to protect does not evolve if a fear appeal component does not occur and/or is assessed as (potentially) unharmful, unlikely to happen or undoubtedly to occur, or the perceived individual competence of applying coping response are assessed as insufficient or ineffective to prevent or limit individual harm. If the described situation is only perceived as aberrant, unlikely to happen or the recommended response is not being remembered, the related cognitive processes and beliefs will not fully evolve. This may result in a lack of motivation to protect.

Also, it may occur that the situation is recognized as potentially harmful, and even a recommended action is being remembered. However, if a person assesses the situation as being harmless or improbable, the motivation to protect will not arise. In this way, the Protection Motivation Theory demonstrates the probability of subversive behaviour towards cyber resilience.

When applied to the concept of cyber resilience, the Protection Motivation Theory has added value by improving understanding how emotion may influence trade-offs, motivations and attitudes before action takes place.

To elaborate on this, focus on action alone may not be efficient if preceding emotions and personal beliefs that influence the motivation and attitude towards the behaviour are disregarded. For example, if communication to perform software updates is limited to this functional, executive instruction, and preceding emotions and beliefs are ignored, the desired action will not entirely take place. However, if attention is given to the secure feeling and beliefs that the action is easy to perform and will protect against attacks, followed by the instruction to update, the intervention will theoretically be more effective.

Cost-benefit calculations regarding threats and harm are attributed to the motivation to protect (Floyd et al., 2000). Individual, cognitive trade-offs may take place to find a balance between response costs and rewards. Response costs will occur when measures are taken to mitigate perceived risks. This may concern costs in terms of time (for example two-factor authentication via an app), reduced pleasure (such as complicated passwords), or money (such as the purchase of anti-virus software) (Bax et al., 2021). Rewards may be experienced if harm does not noticeably occur despite the absence of protection measures against risks. Therefore, beliefs regarding rewards for not taking protection measures may be attributed to subversive behaviour towards cyber resilience. Beliefs in the value of response costs may be supportive to cyber resilience.

Regarding the concept of cyber resilience, the appeal to emotion, and its influence on motivation and attitude are considered to be of added value. Other elements of the Protection Motivation Theory can already be attributed to the predefined concept of cyber resilience. The rational cognitive processes 'appraised severity', 'expectancy of exposure', 'efficacy of an intended response' and rewards-costs trade-offs can be attributed to cost-benefit calculations. Recommended responses can be attributed to supportive action.

2.2.3 The Theory of Planned Behaviour

Although emotion may influence one's attitude towards adopting a recommended response, as substantiated in the Protection Motivation Theory, it may still occur that intended behaviour is not carried out due to personal beliefs. Therefore, increased understanding of the role of beliefs is necessary to detect valuable additions to the concept of cyber resilience.

The Theory of Planned Behaviour (Ajzen, 1991, 2002) explains and predicts the influence on attitudes (behavioural beliefs), norms (normative beliefs) and perceived behavioural control (control beliefs) on intention and human behaviour (see figure 4) to a certain extent in a specific context. Its theoretical basics will be explained and applied to examples in the context of supportive and subversive cyber resilience.

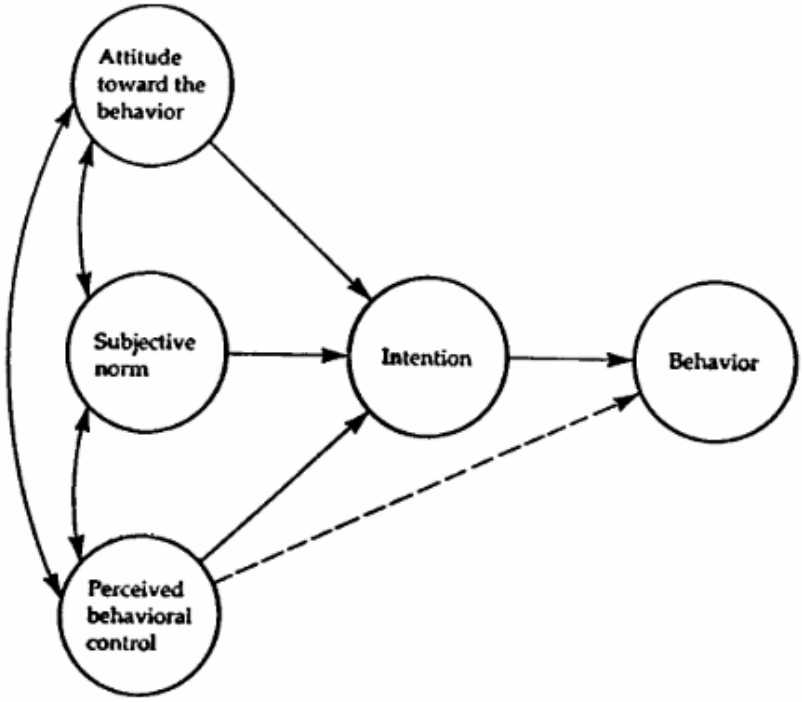

Figure 4. Theory of Planned Behaviour model (Ajzen, 1991).

Attitude towards the behaviour

The first element related to intention is attitude. An individual may have a personal attitude towards specific behaviour. This opinion may be positive, neutral or negative. It may vary and depend on circumstances, and thus be supportive or subversive towards individual cyber resilience. For example, an elderly may have a positive attitude towards a software update of his computer when alone at home and without time restrictions. However, with a family member in the house, the elderly may have a negative attitude towards the update as she might fear being judged for the time and way it will take to do so. In this case, delay of software updates may be subversive to cyber resilience.

According to the theory, behavioural beliefs may change attitudes. For example, if a person has a positive belief to understand how to update the software of his digital doorbell ("I believe I want to know how to update the software"), this will affect the attitude towards the intention in a helpful way ("I want to update the software"). This supports the finding that positive personal beliefs are of added value to the concept of cyber resilience.

Nevertheless, beliefs can be used for good and for bad. For example, an attacker pretending to be a bank employee may influence the beliefs of an elderly to develop a positive attitude towards the behaviour to help with online access to her bank account. The attacker may also influence the beliefs about negative consequences of the behaviour if help is not provided, to influence the elderly's attitude towards the intention to help the attacker and thus undermine cybersecure behaviour. According to the model, attitude towards behaviour may influence subjective norms and perceived behavioural control as well.

Subjective norm

According to the model, beliefs in subjective norms may influence intentions. A person may be individually receptive to the opinions of others who may approve, confirm, or reject specific behaviour. Personal normative beliefs are attributed to the perceived degree of probability of the response by others. The theory postulates that subjective norms may be related to attitude and perceived behavioural control as well. For example, social pressure may be performed to become skilled in two factor authentication. When supported with the assurance that this only requires the entering of an extra code, this may positively influence a person's attitude to want to learn how to apply it. As entering a code may already be a well-controlled activity, the person may be convinced to have the personal capability to control the two factor authentication process.

Perceived behavioural control

The third element related to intention is perceived behavioural control. An individual may have a personal belief to which degree the behaviour will be easy or difficult to effectively perform ("I think I am capable to (not) do it"). This belief may be biased by the degree of individual confidence. It may also vary due to the circumstances as these can change and affect the degree of individual control. According to the theory, perceived behavioural control may be related to attitudes and norms. Personal beliefs in one's ability to control a situation may also be related to perceived behavioural control. For example, when using digitalized processes and devices, control may be related to the attitude and belief to succeed ("I can proof that I am able to make a backup"), social pressure ("I will update the software to prove my digital capabilities to my mocking partner"), and individual beliefs ("If he can change the password of his modem, I can do, too"). Although this may be true in the context of a steady situation, external or internal factors may influence a situation that cannot be controlled by an individual. For example, one may be willing, able and confident to update a smartphone. However, if updates are not being provided anymore due to the end of the smartphone's economic lifespan, one lacks control to solve vulnerabilities in its operating system. Besides, when a person becomes ill, its software might not be updated for weeks or months. Therefore, the theory

points out (Ajzen, 2002, p. 678) that perceived behavioural process control should not only include elements related to self-efficacy, but to controllability as well.

Intention

According to the model, attitude, norms, perceived behavioural control and related beliefs may have impact on a personal intention to perform specific behaviour. As explained by the previous example, the degree to which an element has influence on intention may differ per situation due to external and internal factors. According to the theory, it may be postulated that attention should be paid to the elements contributing to the intention to perform secure behaviour. Therefore, it may be argued that providing only behavioural instructions in awareness campaigns will not structurally change personal behaviour (van Steen et al., 2020). On the contrary, if these elements (attention to the attitudes, norms and perceived behavioural control) are included in the communication, this may support cybersecure behaviour and thus individual resilience. For example, a live hack demonstration of a spectator's smartphone via Bluetooth may offer an effective chance to appeal to beliefs in a cybersecure attitude, subjective norms and perceived behavioural control. The performer might be able to strengthen the spectators' motivation and intention to secure behaviour by turning off the Bluetooth function.

Motivation and intention are mutually related and may affect supportive as well as subversive cybersecure behaviour. For example, two digitally illiterate persons both have the intention to learn how to restore computer software, and both try to do so. The person who is intrinsically motivated to master this activity, is more likely to show persistent behaviour to succeed, than the person who doubts the personal ability to be able to restore computer software.

Behaviour

Having the intention to perform planned behaviour is an important condition. However, this may not be perceived as a guarantee for its execution. The context and preparation may be of influence whether the planned behaviour is carried out to the intended degree. For example, if the intention to buy anti-virus software for the first time is carried out by spontaneously searching on internet, one may be overwhelmed by the variety, functionalities and prices. Therefore, being successful in behaviour is being influenced by specific definition of the intended behaviour and the context (such as time, place and support) in advance. Regarding the anti-virus software example, a person will be more likely to succeed if the computer operating system, budget, perceived effectiveness by the market, level of product support, and support by a relative have been defined in advance. Other measures supporting cyber resilience are the motivation and believe to be able to succeed.

Regarding the concept of cyber resilience, multiple examples explaining the Theory of Planned Behaviour have demonstrated that personal beliefs towards attitude, norms and control can significantly influence the intention, motivation and performance of specific behaviour. Beliefs may evolve over time, influence cost-benefit and effectiveness trade-offs, and affect the motivation to protect and cybersecurity threat perceptions (Li et al., 2019). Beliefs also evidently affect knowledge processing by cybersecurity professionals (Percia David et al., 2020). Beliefs may be supportive or subversive towards cyber resilience, and can be influenced for good or bad intentions. Therefore, significant attention should be paid to the role of beliefs in relation to the concept of cyber resilience.

Other elements of the theory appear to be the outcome of multiple cognitive processes including beliefs. Therefore, they are not of added value towards the predefined concept of cyber resilience.

2.2.4 Heuristics and biases

As argued by the previous behaviour theories and examples, emotion and beliefs influence cognitive processes as well as attitudes and behaviour. Beliefs may be founded on rational considerations, but also be based on mental shortcuts and biases. In this section, the most common shortcuts will be explained and assessed to improve understanding of their added value to the concept of cyber resilience.

In real life, a human being experiences the need to make decisions instinctively quicker rather than rational reasoning beforehand. The human brain will use mental shortcuts (heuristics) when too much information is available in relation to the available or desired time to act. As the amount of information, including cybersecurity information, has grown significantly due to the information technology, the role of heuristics is important to understand (Bellur & Sundar, 2014) as they may influence risk perception (van Schaik et al., 2020).

In case of incomplete information and involvement of risk, heuristics may be applied to perform behaviour that is instinctively good enough. Therefore, human attitudes may be vulnerable to persuasion (Oinas-Kukkonen & Harjumaa, 2008). For example, an individual may be called by an alleged bank employee confirming that her savings are to be transferred abroad, with the intention to initiate a mental shortcut. The risk of losing all savings may be overwhelming and may result in a shock reaction suppressing cognitive signals to verify facts and authenticity. This mental shortcut can be misused by the attacker to offer supposed help to stop the transferral quickly. This may trigger an instinctive response to cooperate with the attacker by allowing access and/or sharing credentials, enabling the attacker to transfer savings. In this way, the natural process of mental shortcuts is

subversive towards cyber resilience. If the mental shortcut would initiate the response to abrupt disconnect the call to be able to contact an acquaintance for advice and help, this may be considered supportive towards cyber resilience.

Mental shortcuts in decision making are closely related to the use of reasoning based on one's individual beliefs (Tversky & Kahneman, 1974) rather than facts and statistics. It is attributed to cognitive dissonance: humans want to be consistent by nature (van Kampen, 2019) and justify their actions for themselves. This explains why an individual may believe to be cyber secure by using passwords and deleting messages from unknown persons without applying software updates.

Such irrational reasoning is called bias. Bias is unconsciously applied behaviour, experienced as logical by the individual at that time, and the root cause of the gap between rational and actual reasoning. Tversky and Kahneman have defined three heuristics and related biases. The most appropriate biases related to the digital environment will be explained below.

Representative heuristic

Humans beings may tend to unconsciously take an initial reference point as basis for the estimated likelihood of another situation assuming that similarity between two situations is more representative than it actually is (Tversky & Kahneman, 1974). In case of digital competences, skills in one domain may vary from abilities in other cognitive domains (Carretero et al., 2017; Pijpers et al., 2020). For example, a grandparent may assume that her grandchild, who spends a lot of time on social media, may be able to perform a software update on her computer. Although both digitalized processes are performed using internet, it may require different knowledge, skills and abilities, such as understanding the difference between required and recommended software updates.

In case of selective perception, an individual may filter information according to its individual preferences of reality. These preferences are taken as a starting point when additional information is being processed. For example, a phishing email proclaims a high chance of winning a brand-new iPad if a simple questionnaire is being filled in at short term. An individual may be tempted to focus on the high probability of winning a valuable device, and filter out the necessity to perform a security check of the link to the questionnaire. As such rational behaviour may hinder the possibility of getting hold of a new iPad, it may therefore be ignored. This may subvert one's cyber resilience. On the contrary, an individual understanding phishing tactics, may be alerted by the time restricted decision to gain a valuable award, and may instantly delete the email message or report it as phishing attempt. Such behaviour will support cyber resilience.

Human beings tend to perceive risks differently (Fagan & Khan, 2018). If a person has never experienced an individual cyberattack, the change of being at risk in cyberspace may be argued as lower than other individuals. This is called the optimism bias (Warkentin et al., 2013). If a cyberattack has never been individually experienced, one may not perceive the necessity to take preventive or recovery measures as no harm is expected. This underestimation of likelihood is called the normalcy bias (Omer & Alon, 1994), and may be perceived as subversive behaviour towards individual cyber resilience.

Availability heuristic

This heuristic is related to judgement after overestimation of the importance of information. It appears to be more comfortable to rely on information received from other people and easy to remember, rather than finding out facts and statistics about the subject in question. Memorizing one simple security solution may be easier than remembering several complex ones. For example, the security measure not to click on links in emails might be easier to remember than procedures how to perform software updates on different smart devices. The availability heuristic may also be related to frequency. For example, internet related incidents extensively discussed in the media may be better recalled than cyber incidents with more impact but less exposed in the media. Also, being individually attacked via internet will have more impact than reading about an attack to an unknown citizen.

Adjustment and anchoring

When a person relies too much on the first information received, and its reliability is not being scrutinized with facts and figures, decisions related to this biased information may lead to misinterpretations (Wall et al., 2019). Such decisions may subvert cyber resilience. Confirmation bias is applicable when the person beliefs the positive confirmation of information already known, and neglects other impressions such as a deviant situation. Outcome bias may occur when focus is only put on the quality of the perceived outcome. The Dunning-Kruger effect (Kruger & Dunning, 1999; Pennycook et al., 2017) is related to overestimation of personal abilities. It is related to the competence to judge how well or worse someone is performing. For example, a person with extended computer and coding knowledge may perceive herself as able to recognize a phishing mail, but may not be sufficiently trained with underperformance as a result. The bandwagon effect refers to the tendency to perform behaviour because other people do so as well (Johnson & Gutzwiller, 2020). The fundamental attribution error (Jones & Harris, 1967) refers to a disproportionate attribution to the behaviour of another person compared to the context influence. For example, one may blame the elderly who lost 800.000 euro of savings after voluntary installing a malicious app (Politie, 2021) without understanding the attacker's professionalism and misuse of biases as described.

Regarding the concept of cyber resilience, it has been demonstrated by multiple examples that information processing is subject to mental shortcuts and biases which may support or undermine cyber resilience. Due to the overwhelming amount of information in society, including the internet, cognitive overload may occur and hamper effective information processing (Fox et al., 2007; Schneider, 1987). As mental shortcuts and biases exist in the subconscious mind, they may hinder logical reasoning attributed to critical thinking (West et al., 2008) and prevent the objectivity of personal views (Pfleeger & Caputo, 2012). In case of cybersecurity information and circumstances, this may affect risk perception and related responses. Therefore, it is argued that mental shortcuts and biases are essential to the concept of cyber resilience.

2.2.5 Discussion

To answer the second sub-question *How may human behaviour influence cyber resilience?*, human behaviour theories have been examined. It has yielded three behavioural characteristics that have been shown by multiple examples to influence cyber resilience. The first characteristic is the appeal to emotion, because it influences motivation and attitude. The second characteristic are beliefs, because they affect intention and motivation. The third characteristic are mental shortcuts (heuristics and biases), because they affect information processing, risk perception, and rational cost-benefit calculations.

It has been demonstrated that these characteristics affect logical reasoning. In the context of cyber resilience, this may result in supportive or subversive behaviour, and thus result in being more or less cyber resilient. In the next section, these findings will be discussed in the context of the predefined concept of cyber resilience, which will result in a theoretical definition of individual cyber resilience.

2.3 Individual cyber resilience

To answer the third sub-question *What is individual cyber resilience?*, the concept of cyber resilience is examined whether its rather rational definition can be improved by making it more personal. Then, the identified behavioural characteristics of added value are used to build up a theoretical definition of individual cyber resilience. The definition aims to provide a framework to increase understanding of the concept of individual cyber resilience. It also provides the basis for data collection to assess its validity.

In section 2.1.3, the concept of cyber resilience has been defined as:

"To continuously look for, recognize and classify specific assets and temporary states of being related to information technology, to evaluate associated cost-benefit calculations, followed by supportive action appropriate to the present tier."

This definition is based on the six conceptual elements process, specific assets, temporary state of being, cost-benefit calculations, action, and tiers. Regarding cyber resilience being relative to specific assets, the definition can be improved by referring to tangible and intangible items of value to an individual. For example, this may include savings, a digital identity, login credentials, and emotional well-being. Therefore, referring to personal valuables instead of specific assets will be more suitable in the context of individual cyber resilience.

It has been substantiated that the identified behavioural characteristics of added value (emotion, beliefs, and mental shortcuts) can support or subvert cyber resilience when an individual performs cost-benefit calculations and takes action. Regarding tiers, it has been argued that each tier has its own degree of accuracy, thoroughness and completeness in risk management, and thus related cognitive processes. Therefore, emotion, beliefs, and heuristics and biases being related to cognitive processes, may vary per tier.

Therefore, the theoretical definition of individual cyber resilience is defined as:

"To continuously look for, recognize and classify personal valuables and temporary states of being related to information technology to evaluate associated cost-benefit calculations. To be aware of the influence of emotion, beliefs, and mental shortcuts on this process of evaluation, and to subsequently take supportive action appropriate to the personal tier."

3 Methodology

In this section, the research methodology and design is explained. The research approach is theory building based on academic literature, reports, and empirical research. Data acquired from qualitative interviews. A case study provided input for qualitative interviews. A discourse analysis is performed to analyse the interview data.

3.1 Literature review and case study

The literature review started with the examination of academic literature related to cybersecurity, resilience, cyber resilience, and the role of human behaviour related to cybersecurity. Also, empirical research was performed, and literature regarding theory building (Swanson & Chermack, 2013; Wacker, 2008) has been studied. The outcome is used to build a concept of cyber resilience and a theory of individual cyber resilience to answer the first three research sub-questions.

To answer the fourth sub-question, a case study of the Dutch Digitalization Strategy and its yearly updates has been performed. Also, related legislation referred to was studied. Data provided by the statistics agencies of the European Union (Eurostat) and the Dutch government (CBS) regarding digitalization has been examined. Supervisory reports evaluating the digitalization of the Dutch society have been examined to detect opposing views and areas of improvement.

3.2 Interviews

Interviews have been primarily conducted to examine which elements of individual cyber resilience the Dutch government focus on, what they aim to achieve and to what extent. Qualitative interviews on top of peer reviewed literature research is recognized as a respected and accepted method to perform academic research within the given time (Aberbach & Rockman, 2002; P. Gill et al., 2008; Kvale, 2011). The findings are used to answer the fifth and sixth sub-question.

Literature (Aberbach & Rockman, 2002; P. Gill et al., 2008; Harvey, 2011; Kvale, 2011) how to design interview questions and prepare, conduct and code qualitative interviews is studied. The interview questions were prepared based on government documents and academic literature, and are listed in table 1. Probing and direct questions are alternated with open questions to explore, lead and counter the answers of the interviewees for validation and saturation purposes. For each question, the

type of question, the relation to a research sub-question (SQ), and the descriptive (D) or explanatory (E) purpose is indicated.

Nr	Question	Type	SQ	D/E
	Opening questions			
1	What is your current role and position in this organization?	Direct	-	D
2	How did you contribute to the content of the document in the way it has been published?	Leading	-	D
3	What were the reasons for the development of the document?	Explore	5	E
	Cybersecurity Risk Assessment 2019			
4	Which skills, attitudes and/or knowledge did you have in mind when you addressed your concerns about the ability to be "kept up to date if threats and security measures develop so fast"?	Explore	5	E
5	Could you elaborate on your opinion about how far you think that the Dutch Digitalization Strategy addresses different aspects of individual resilience?	Explore	6	E
	Dutch Digitalization Strategy			
6	What is the story behind the document?	Explore	-	D
7	Could you elaborate on your opinion how far the document addresses individual cyber resilience?	Explore	5	E
8	Could you elaborate on your opinion if relevant competences have not been (sufficiently) addressed yet?	Explore	6	E
	Personal digital skills			
9	How would you characterize digital skills?	Explore	-	D
10	What are your views about the necessity to develop of individual digital skills? Can you tell me a bit more about that?	Probing	5	E
11	Do you support initiatives by the government to develop digital skills of citizens? Why do you (not) support this? How strongly do you feel about this?	Leading Counter Counter	5	E
12	Do you believe that all Dutch citizens have access and are able to develop personal digital skills, knowledge and attitudes? Why do you (not) support this?	Probing Counter	5	E
	Individual cyber resilience			
13	Could you elaborate on your personal definition of individual cyber resilience?	Explore	5	E
14	What are your views about competences needed to anticipate on a cyberattack?	Explore	5/6	E
15	What are your views about the risk for individuals being attacked via digitalized processes?	Probing	5/6	E

16	Do you believe that each individual knows which skills, knowledge and attitudes are necessary to take to strengthen personal resilience? Why do you (not) support this? How strongly do you feel about this?	Probing Counter Counter	5/6	E
17	Do you agree that an individual should develop personal digital skills to increase its own digital resilience? Why do you (not) support this? How strongly do you feel about this?	Probing Counter Counter	5/6	E
18	How would you describe trust in digitalized processes?	Direct	5	E
19	Do you believe that an individual will sooner or later experience a cyberattack? Why do you (not) support this? How strongly do you feel about this?	Direct Counter Counter	5	E

Table 1. Interview plan

Qualitative, semi-structured interviews with six governmental strategy writers, policy makers and researchers (two females and four males) are performed. The interviews took between 37 and 46 minutes, and were conducted during October to December 2021. All interviewees preferred online interviews due to Covid-19 measures. They agreed beforehand on recording for transcription purposes. During the interviews, additional questions may be asked based on the responses to gain insights in depth. At the request of an interviewee, his individual statements in the context of the thesis are personally verified in advance for approval before for use in the final text. All interviews have been recorded and converted in transcripts. The transcriptions are read multiple times to be well-acquainted with the data. The interview transcripts are included in Appendix A.

3.3 Data analysis

Interview data is analysed by means of discourse analysis to improve understanding of government aims and meaning regarding individual cyber resilience. Related literature has been studied (R. Gill, 2000; Potter, 2004). A discourse analysis has been defined as “a careful, close reading that moves between text and context to examine the content, organization and functions of discourse” (R. Gill, 2000, p. 188). According to Potter (Potter, 2004), it is related to action, situation and construct. Based on these findings, the transcriptions are coded based on the conceptual elements of the individual cyber resilience definition. Then, the data is assessed on deviations, similarities, sentiments, political correctness, and coherence.

Multiple tools are used to support the data collection and analysis. The interviews are recorded by using the Voice Recorder application. The organization Uitgetypt.nl produced professional transcriptions of the interviews. All interview transcripts haven been checked against the recordings and corrected in case of abbreviations and jargon. For the online interviews, Microsoft Teams and Webex software are used. Discourse analysis is supported by Word and Excel software.

3.4 Ethics

To obtain ethically responsible research, risks are identified. The risk to be biased about cybersecurity and cyber resilience theories may occur due to related education and work experiences. The risk to misinterpret human behaviour theories may occur due to absence of thorough psychology education. To minimize these risks, mitigating measures have been taking by being aware of any preliminary assumptions, describing detailed examples, and involving thesis supervisors in the fields of governance and psychology.

Regarding literature review, primarily peer reviewed academic literature from different continents is used. During literature review, counter arguments are searched for, scrutinized and added. Feedback and suggestions of the thesis supervisors is processed. All information used is unclassified.

To prevent biased interview questions, the wording and mutual relation between the predefined questions are peer reviewed. Regarding privacy, none of the interviewees has requested anonymity. One interviewee's claim to review his statements is respected. There is no personal relation with the interviewees or imposed responsibility towards an organization. To prevent miscommunication and unintended qualitative effects during or after interviews, all interviewees are informed in advance by email about the duration, goal, outline and scope of the research. All interviewees pre-approved their consent to record the interview for transcription purposes only. Due to the restrictions of online communication due to Covid-19 measures, nonverbal communication may have been overlooked.

4 The Dutch Digitalization Strategy

To answer the fourth research sub-question, a case study of the government strategy related to strengthen individual cyber resilience is presented. Supervisory reports, statistics and scholars reflect on the effects. The strategy is assessed against the theory of individual cyber resilience.

4.1 Introduction

Digitalization may improve a nation's prosperity and citizens' well-being as it may provide economic and social opportunities (Almeida et al., 2020). It may be postulated that individual citizens may take responsibility to increase cybersecurity competences and perform supportive behaviour to benefit from digitalization. However, security may not only rely on citizens' skills and behaviour alone (Coventry et al., 2014, p. 19). According to the English philosopher Thomas Hobbes, a sovereign state may exist by the grace of its citizens giving consent to allocate part of their power in exchange for security and protection (Chalmers, 2018, Chapter 2). To elaborate on this in the context of this thesis, it may be postulated that citizens need support from the government to increase security and protection against threats and attacks related to digitalization.

Digitalization may affect employment opportunities, and thus citizens' digital competences. In 2017, the Organisation for Economic Cooperation and Development (OECD) published its Skills Strategy Diagnostic Report regarding The Netherlands (OECD, 2017). Compared to other OECD nations, Dutch citizens were reported as strong performers on skills in general. However, the OECD predicted that 35% to 60% of all Dutch jobs were already or would be vulnerable to automation at short term due to the increase of interconnections (OECD, 2017, p. 23). As this could affect a major part of Dutch employment, intervention by the government as the citizens' ultimate national protector seemed unavoidable.

In 2018, the Dutch Digitalization Strategy (Ministerie van Economische Zaken en Klimaat, 2018) was published to ensure a collective, overarching departmental vision on digitalization, including identification and coping strategies regarding common challenges resulting from digitalization. The departmental vision was supported by the government. Digitalization, and increase of confidence by citizens in it, are still perceived conditional for exploitation of economic growth, innovation and new business, as well as supportive to social challenges related to healthcare, transport and nutrition (Ministerie van Economische Zaken en Klimaat, 2018, p. 11). In the context of this thesis, the objective to establishing basic conditions for strengthening individual cyber resilience is explained by the focus areas digitally skilled citizens and their resilience strengthening.

4.2 Digitally skilled citizens

In its first edition in 2018, the Dutch Digitalization Strategy attributed multiple qualifications to digitally skilled citizens. These included the possession of an "adequate level of basic digital skills" so that "everyone can participate in the digital society" (Ministerie van Economische Zaken en Klimaat, 2018, p. 8), lifelong learning (Ministerie van Economische Zaken en Klimaat, 2018, p. 13), and skill support to ensure that no one would stay behind (Ministerie van Economische Zaken en Klimaat, 2018, p. 29). Three groups of citizens were defined to ensure a digital inclusive society: those being part of a school system, employers and their employees, and vulnerable citizens with minor digital skills (Ministerie van Economische Zaken en Klimaat, 2018, pp. 29–30). The latter group is primarily under government attention. Multiple initiatives were started to facilitate their digital skills development. Services at public libraries for digital illiterates were supported. Education budgets became available via local townships. The comprehensibility and user-friendliness of digital government services were reviewed. Also, quantitative and qualitative research is performed to investigate how to respond the best to people's digital needs.

In the 2019 edition, a digital inclusion action plan (Knops, 2018) was introduced to ensure that vulnerable groups would not be digitally locked out of society by means of help with digital skills and explanation of digital opportunities and risks (Ministerie van Economische Zaken en Klimaat, 2019, pp. 21–22).

In 2020, digital illiterates and retired citizens were still directed to local libraries, community centres and social initiatives for help with digital skills development. Research was performed how best to meet citizens' digital needs, including provision of computer hardware to elderly (Ministerie van Economische Zaken en Klimaat, 2020, p. 60). The government concluded (Tweede Kamer, 2020, p. 4) that the Dutch policy regarding digital skills was strongly in line with the updated European Commission's Skills Agenda (European Commission, 2020b).

In 2021, lack of access to computer equipment, connectivity, knowledge, skills, support and awareness of digital risks (Ministerie van Economische Zaken en Klimaat, 2021, pp. 23–24) were identified as vulnerabilities regarding societal participation. Activities regarding comprehensibility, user-friendliness, knowledge, skills and support with digitalized government processes were continued. Activities regarding equipment access and connectivity were not reported. To oppose disinformation risks, the need to improve media literacy was reported. Information desks were opened in local libraries to support digital illiterates with governmental processes and services. Multiple

websites were introduced to educate citizens regarding secure websites, passwords and online payments. Also, a telephone helpline (Digihulplijn) was launched to provide computer help to citizens and information regarding relevant courses.

4.3 Strengthening resilience

In the 2018 edition, the government recognized that a trusted and secure digital society is conditional for the acceptance of digitalization and the usage of digital assets by citizens (Ministerie van Economische Zaken en Klimaat, 2018, p. 38). Three focus tracks were introduced.

The first track aimed at secure use of digital technologies. Resistance to digitalization due to insufficient security measures by citizens was identified as a lurking threat. Their levels of digital resilience, cyberthreat awareness, and protection measures were reported as inadequate (Ministerie van Economische Zaken en Klimaat, 2018, para. 7.1). Citizens were instructed to take appropriate measures to ensure their individual security and cyber resilience, while the government assured to fill in preconditions like crime fight and protection of national security interests. Protection of such intangible values are attributed to cybersecurity (Von Solms & Van Niekerk, 2013). Individual cyber resilience and behavioural change was supported by means of awareness campaigns, specific advice, courses of action and security measures.

The second track was related to increase citizens' trust in online privacy protection and data control. The introduction of the General Data Protection Regulation (GDPR) on May 25, 2018, offered the opportunity to increasingly protect and control individual data.

The third track was related to online purchases protection to support citizens' trust (Ministerie van Economische Zaken en Klimaat, 2018, p. 42).

In 2019, the government reported an increase of the amount and complexity of cyber threats and vulnerabilities, and their concerns to its effect on freedom, security and economic growth (Ministerie van Economische Zaken en Klimaat, 2019, p. 24). As this could hamper digitalization and resilience objectives, new regulations to increase control measures and supervision were reported. The Network and Information Systems Security Act (Dutch Department of Justice and Security, 2018) became effective in November 2018, regulating cybersecurity duty of care and notifications obligation for providers in the digital domain and of critical services. The baseline information security for governmental organizations (Bio-overheid.nl, 2020) was introduced in January 2019, contributing to citizens' trust in the government as a processor of their personal data. European guidelines regarding

the supply of digital content and sale of goods were introduced in April 2019. The European Cyber Security Act (European Union, 2019) was published in June 2019, providing a cybersecurity certification framework and increased supervision by the European Union Agency for Cybersecurity (ENISA). Preparation of new e-privacy regulation was reported. Besides new regulations, cybercrime and cybersecurity awareness campaigns were announced to encourage citizens to implement security measures and change behaviour.

In 2020, main focus was put on implementation of the new regulations within the government, and strengthening the cooperation and resilience of companies with regard to the secure digital society objective. Increased supervision, controls and penalties regarding e-privacy violation to strengthen citizens' rights were implemented. Awareness campaigns for citizens related to software and password updates knowledge were reported (Ministerie van Economische Zaken en Klimaat, 2020, p. 40).

In 2021, digital resilience was explained as the combination of digital security and the ability to adequately anticipate to cyber incidents (Ministerie van Economische Zaken en Klimaat, 2021, p. 33). Digital security was defined as regulation to strengthen the legal position of citizens regarding online platforms, identity protection, online purchases, product safety, and software updates.

4.4 Statistics and supervision

Based on 2019 data, the European Commission (European Commission, 2020a) reports multiple highlights and lowlights regarding Dutch digitalization. Regarding highlights, the overall level of digitalization in The Netherlands has made (after Ireland) the highest progress within the European Union between 2015 and 2020. The Netherlands takes the fourth position of European countries regarding overall digital performance. Dutch citizens take the top positions amongst European citizens with regard to basic software skills (80%), internet use at least once a week (95%), and selling online (38%). Regarding lowlights, nearly 3% of the Dutch population (more than 400.000 citizens) appears to have never used the internet. Amongst them are individuals with no or low education, citizens aged between 55 and 74, and retired and inactive persons. More than 40% of Dutch internet users reported experienced security-related issues. Counterfeit messages (phishing) and attempts to retrieve individual information via falsified websites (pharming) were reported as most common problems. Other statistics may indicate lowlights as well. The European Statistical Office (Eurostat, 2021) reports that the internet access rate by Dutch households has dropped from 98% in 2019 to 97% in 2020, while the Dutch Central Bureau of Statistics (Centraal Bureau voor de Statistiek, 2021) reports

an increase of the amount of Dutch households from 7,9 million in 2019 to 8.0 million in 2020. This may indicate that the amount of households without internet access is increasing. This may undermine the overall Dutch digitalization goals and perceived related benefits on the long term.

Dutch government supervisory agencies have performed qualitative analyses. In 2019, the Dutch Bureau for Economic Policy Analysis (CPB) has assessed digitalization and related cyber risks related to the Dutch society from an economic perspective (Overvest et al., 2019). In general, they forecast an increase of digitalization within society and dependency on digitalized processes, with the risk of digital disruption of society as a result.

Regarding cybersecurity information, the researchers expressed their concerns about diversity, spread and overlap of recommended actions and guidelines (Overvest et al., 2019, p. 3). They assessed that the current governmental approach of cyber risk communication and encouragement of public-private cooperation does not support effective and efficient cybersecurity decision-making by citizens. As a result, civil cyber resilience appears to linger behind compared to businesses. After a cyberattack, nearly 40% of citizens lose confidence in secure digitalized processes (Overvest et al., 2019, p. 6).

Regarding emerging technologies, the researchers consider artificial intelligence (Overvest et al., 2019, p. 13) as a risk to the integrity of information if intentionally used to manipulate images and sounds (deepfake). As a result, citizens may not be able to distinguish reality from manipulated messages. However, if used for better, artificial intelligence can detect deepfakes and therefore be used as a means of protection.

Regarding the NIST functions (Overvest et al., 2019, p. 26), the researchers acknowledge that the government pays much attention to communication towards citizens in the field of cyber risk identification and protection. However, they also conclude that less attention is spend on detection, response and recovery measures. As exposure to an cyberattack will be unavoidable as previously argued, individual competences are required to recognize and anticipate effectively when a cyberattack is being revealed.

In 2019, scholars of the Scientific Council for Government Policy (WRR) published the report ‘Prepare for digital disruption’ (Prins et al., 2019). They perceive that cyberattack goals have changed over time. Although vital infrastructure or critical services can still be attacked, they perceive that cyberattacks seem to increasingly target common facilities such as democratic elections (by manipulation) and general opinions (via disinformation). They imply that the underlying purpose behind such disruptions may be the undermining citizens’ trust in Dutch organizations and digitalized processes with societal and economic harm as a result. They criticize the Dutch government as well as

citizens. They perceive that governmental communication about cyberattacks towards citizens is mainly focused on taking preventive measures, rather than information and behaviour how to cope with digital disruptions. Regarding citizens, they perceive insufficient preparedness to anticipate on disruptions, underestimation of disaster probability, and deficient assessment of the consequences of disruption as being acceptable (Prins et al., 2019, p. 55).

In the perspectives of scholars, the government applies a centralized as well as distributed approach (Shires & Hakmeh, 2020) to improve the cyber resilience of the Dutch society. It also applies institutional and productive cyber-power (Betz & Stevens, 2011). Institutional power is performed to regulate citizens. Productive power is used to define new legislation for basic online protection of its citizens. Besides, dispersed activities are deployed by public-private partnerships, and moral appeals are made to employers and educational organizations.

According to Australian researchers (Third et al., 2014), one of the most effective ways to be individually cyber secure is digital literacy. They refer to abilities to online navigation, adjustment of settings, evaluate the quality and reliability of online information, and, understand social norms in online contexts.

4.5 Discussion

To answer the fourth sub-question 'What is the current government strategy to strengthen individual cyber resilience?', a case study of the Dutch Digitalization strategy and its updates have been presented. Also, the strategy has been assessed against the theory of individual cyber resilience.

Although the Dutch Digitalization Strategy mainly reports in outline as may be expected, it provides a first foundation to assess the application of the conceptual elements of individual cyber resilience. In the 2021 edition, regarding process, the digital transition is explained as an ongoing development requiring continuous navigation (Ministerie van Economische Zaken en Klimaat, 2021, p. 7). Ongoing attention and activities regarding digital skills and strengthening cyber resilience are reported (Ministerie van Economische Zaken en Klimaat, 2021, pp. 73–74 and 79–80). This includes continuous qualitative and quantitative research to meet individual needs, and continuous support to and development of digital and cyber resilience skills to those who reach out for it on own initiative. Therefore, it is argued that the strategy treats cyber resilience as a process.

Regarding individual cyber resilience as a temporary state of being, it is reported at an abstract level that digital conditions change and require different skills and legislation. Individual cyber resilience is

not being referred to as a personal, temporary state of being depending on circumstances and fluctuating over time.

Individual cyber resilience relative to personal valuables is reported in the context of European and national legislation, risk awareness, the protection of smart devices by software updates (Ministerie van Economische Zaken en Klimaat, 2021, p. 35), the provision of mandatory updates and an increased lead time (Ministerie van Economische Zaken en Klimaat, 2021, p. 36), and the protection of personal information (Ministerie van Economische Zaken en Klimaat, 2021, p. 81). The need to identify and protect personal services is not specifically reported.

Individual cyber resilience requiring cost-benefit calculations is mentioned once at an abstract level in the overview section: "[Digitalization as an ongoing development]… requires setting clear goals and making the right considerations. Considerations that sometimes have to be reconsidered due to continuous digitalization in order to maintain a good balance between all different interests." (Ministerie van Economische Zaken en Klimaat, 2021, p. 7). The strategy does not report specific activities to help individuals make personal cost-benefit calculations, nor factors affecting the quality of these considerations such as emotions, beliefs and mental shortcuts.

Individual cyber resilience requiring action is reported in the context of performing software updates of personal digitalized assets. Multiple websites and information points are referred to for tools and help to support personal action. Supportive Initiatives for cybersecurity exercises and tests are reported for employees of government and business organizations (Ministerie van Economische Zaken en Klimaat, 2021, pp. 34–35). No such initiatives are reported for citizens.

Regarding the element of emotion, a fear appeal is indirectly applied by reporting that effective detection and prosecution of malicious parties performing cyberattacks is problematic (Ministerie van Economische Zaken en Klimaat, 2018, p. 38). Individual cyber resilience being relative to tiers, beliefs and mental shortcuts are not specifically reported.

As indicated, this initial assessment is based on a written strategy at an abstract level. To improve understanding of the underlying aims, concerns, and struggles regarding individual cyber resilience strengthening, qualitative interviews are conducted with strategy writers, policy makers and researchers. The results are presented in chapter 5.

5 Results

In this chapter, the interview data and findings are presented per conceptual element by means of a discourse analysis. Strategy writers, policy makers and researchers expand on government and personal aims regarding individual cyber resilience and associated digital skills. Perceived concerns and challenges are also presented. The chapter is concluded with common findings, and the answers to the final research sub-questions.

5.1 Process

Strategy writers have expressed the government aim to continuously examine, test and adjust cybersecurity information to ensure its comprehensibility, findability, completeness, and helpfulness to individuals. Also, policy makers expressed the government aim for citizens to organically grow in cyber resilience maturity reflected in behaviour due to increasing threats in the information world. From the context of their descriptions, and although none of the interviewees directly linked the word 'process' to individual cyber resilience, it can be inferred that these interviewees recognize the necessity for continuous adaptation and growth in cyber resilience as supported by scholars (American Psychological Association, 2012; Fergus & Zimmerman, 2005).

Besides aims, interviewees also expressed concerns and challenges about the continuous process nature. A strategy writer stated: "How do we ensure that it [individual cyber resilience] will have a lasting effect?" This demonstrates the awareness that individual cyber resilience may be achieved with support of the government, and that it is a matter of ongoing attention and effort. This continuous aspect corresponds with the process feature. Another concern related to individual cyber resilience was expressed in the context of continuous improvement. Although lessons learned are applied, doubt remains with a strategy writer: "Where we have good examples, where we see that things work, we try to scale up but that is hard for individual citizens." This demonstrates that continuous effort in applying lessons learned to increase resilience, which is attributed to resilience as a process by scholars (Vandoninck, d'Haenens, et al., 2013).

Based on the findings, it can be concluded that individual cyber resilience being a process is acknowledged by the interviewees.

5.2 Temporary state of being

Discourse analysis shows that, in the context of their explanations, interviewees recognize individual cyber resilience as a temporary state of being. At this point, they have expressed personal aims. A policy maker expressed the aim to establish vigilant citizenship by means of paying close attention to cybersecurity situations. Another policy maker expressed the personal aim to put citizens in a position to be constantly aware of the things around them. A researcher aims that citizens take security measures depending on the context whether it is safe or not, or the degree to which it is safe. All personal aims can be interpret as the need to be aware that, although situations may seem secure, they do not have to be or remain so. This demonstrates resemblance with resilience being temporary of nature (Dunn Cavelty et al., 2015) and related to risk exposure (Rutter, 2012). Although individual cyber resilience as a temporary state of being is personally acknowledged by three interviewees, it may be concluded that this conceptual element is not demonstrated by the interviewees as a strategic government aim to treat individual cyber resilience as such.

5.3 Personal valuables

In the context of individual cyber resilience, the government aim to secure personal valuables such as computers, smartphones and other tangible smart devices is directly expressed by a strategy writer, and indirectly by researchers. A strategy writer acknowledges that these aims mainly focus on laws and regulation regarding software updates to enable citizens to secure their smart devices. Specific government aims expressed are the provision of correct and clear information about the availability of updates by sellers, and to achieve mandatory, automatic and increased lead time of updates. The government aim to apply and securely handling strong passwords by citizens is directly expressed by the strategy writers, and indirectly by researchers and a policy maker. Besides these government aims, a strategy writer and a policy maker expressed personal concerns regarding smart devices in relation to cost-benefit calculations. This will be explained in the next section.

These findings show primary focus on software updates to protect tangible smart devices. It may be postulated that the actual measurability of software updates is the cause. It demonstrates that the government applies its institutional and productive power (Betz & Stevens, 2011) to citizens' systems by regulation. The discourse analysis also shows that personal valuables are related to the conceptual elements action (apply/handle passwords, perform software updates). Despite passwords are mentioned as personal valuables, it may be interpreted that other intangible personal valuables such as data and services (NIST, 2018) are not top of mind among the interviewees. Therefore, it can be

concluded that individual cyber resilience relative to personal valuables as a strategic government aim is partly demonstrated by the interviewees.

5.4 Cost-benefit calculations

Regarding cost-benefit calculations, a strategy writer expressed the government aim to bring secure smart products to the market, so that citizens do not have to think as much about how to secure these products, because "the average person would rather buy a nice product for a nice price than having to pay double for it, while it is more secure." This argument is substantiated by a policy maker's concern about the apparent quality of cost-benefit calculations: "… of course it [a smartphone] is now a thing that can do much more than you think. The same goes for those Alexa devices. Nice speakers, nice sound. That thing will listen, and once it is there, nothing stands in its way." These related insights can be interpreted as an acknowledgement that individual cost-benefit trade-offs may lead to the choice and purchase of a product with security risks undermining personal security interests, thus affecting individual cyber resilience.

Discourse analysis shows that, in the context of their examples and explanations, all interviewees acknowledge that citizens perform cybersecurity related cost-benefit calculations. According to the strategy writers, such calculations are revealed by research data. For example: "…am I going to put in all that effort, do I want to spend all that time, or is it worth it to me that something goes wrong? And then I'll see how I can solve it further." This shows that the respondent makes a trade-off between effort, time, and the value of the impact if risk becomes reality.

All interviewees have revealed personal aims related to cost-benefit calculations made by citizens in the context of individual cyber resilience. They aim to include items such as personal information, social engineering tactics, and published information taken out of context, being misunderstood, or misused for harm. This can be interpret as an appeal to include additional values besides effort, time and money in personal considerations. Disguised as a provocative comment, a policy maker expressed the aim to accept loss of personal information related to online behaviour: "And I think you have to accept that all your movements are digitally used for marketing and commercial purposes. You can fight against that, it makes you tired and it won't work, then you shouldn't be online. ... You are not a flesh-and-blood person who is interesting, you are a digital personality and there is money in it." This demonstrates that the extent to which non-disclosure of personal information can be included in cost-benefit considerations is limited, thus inseparable from being online. One strategy writer expressed the aim to help individuals make the right cost-benefit calculations by the use of nudges. This can be

explained as the aim to unconsciously make an individual more proficient in daily cybersecurity related activities.

A concern expressed by a researcher is related to the cost-benefit calculation to report a cyberattack versus the likelihood of arrest and prosecution: “If you have the idea that the police cannot or will not do anything with it, why would you still file a report?” In the context of the conversation, this may be interpreted as an aim to increase cyber incident reporting, investigation and prosecution to obtain more scientific data about cyberattacks for future analysis and recommendations.

It can be concluded that all interviewees acknowledge the presence of cost-benefit calculations in the context of individual cyber resilience. Also, it is demonstrated that cost-benefits calculations are related to other conceptual elements such as personal valuables (insecure products), mental shortcuts (nudges), action (go online, report or not), and tiers (risk information quality). The government aim that individual cyber resilience requires cost-benefit calculations is indirectly demonstrated by regulation to secure smart products. Despite the recognition of the influence of cost-benefit calculations on individual cyber resilience by all interviewees, no specific government aims are set to assist individuals in making supportive cost-benefit calculations.

5.5 Action

Multiple government aims associated with substantive actions of citizens themselves are expressed, such as making back-ups, using strong passwords, defining in advance where to go to for support, and reporting incidents. If an attack occurs, interviewees personally aim that individuals unplug devices, and seek for support by experts and authorities. Regarding recovery, a policy maker stated: “And yes, limiting damage is of course very good, but eventually you will have to recover until you are back to the old situation and then you can move on.” Those aims may be interpreted as the acknowledgement that individual cyber resilience cannot be achieved without specific actions to secure information, and know what to do and where to go to in case of a cyberattack to limit its lead time and personal harm.

Strategy writers and policy makers express personal aims that individuals should experience their cyber related vulnerabilities, for example by means of training, a live hack demonstration, exercises, vulnerability process checks by professionals, and/or responsible disclosures. Such activities are attributed to resilience by scholars (Boin et al., 2013; Rutter, 2012). A strategy writer links action directly to behaviour: “Of course you can do a lot with information and campaigns, but they also have to experience it. Only then will you influence that behaviour.” These personal aims related to practical experiences can be interpreted as the desire to make individuals aware of what cyber attackers might

see, do, take, and damage. Struggles related to responsible disclosures have also been expressed: “Ideally, it would of course be nice if you have a van driving down a street with ethical hackers who are trying to digitally break into a number of houses. ... Then they experience it. But that's not allowed. The NCSC never agrees to that.” And: “a very large hack in The Netherlands where three quarters of the people cannot use the internet. Yes. But that's not allowed.” This demonstrates that such practical experiences may be subject to political and ethical limitations, and therefore may not be achieved to the desired extent.

A policy maker expressed the aim that individual cyber resilience “is in fact the lead you have over your attacker.” This may be understood as the aim to take action based on a range of prepared responses so that an individual can anticipate to a cyberattack in such a way that the attack is hindered.

Regarding responsibility, two interviewees emphasize that the government can only offer help, but can never take over the responsibility of citizens to take action themselves. This may be understood as the limitation that, no matter how well the government understands and supports individual cyber resilience, it can never be achieved if an individual does not take responsibility for carrying out appropriate actions.

It can be concluded that the interviewees identify multiple government aims related to the conceptual element action. Although the interviewees appear to be passionate about supporting cyber resilience related actions of citizens, they experience difficulty in getting citizens into action due to political, ethical and responsibility issues. Besides, even though the government may offer support to increase individual cyber resilience, it is up to the individual to take responsibility, accept the help offered, and get to work with it.

5.6 Tiers

Discourse analysis shows that no government aims are expressed regarding different tiers, as in different competence levels of risk information related knowledge, management, and activities. On the contrary, all interviewees recognize and describe such tiers and related behaviours without explicitly mentioning. Directly or indirectly, they expressed personal aims and related matters towards an individual basic tier. Regarding risk information knowledge, attributed items are types of attacks on individuals, equipment and software vulnerabilities, technical risk solutions, and authenticity of internet channels. Regarding risk information management, reading skills, filtering and authentication of information, knowledge maintenance, and awareness of the attractiveness and blackmailability of

one's identity are attributed. Regarding risk information activities, attributed items are recognition of attack signals, risk analysis performances, reporting, performance of risk mitigating actions, thoughtful information publication, and distrust against personal information provisioning requests. This enumeration demonstrates that the interviewees recognize different layers in risk-related knowledge, control and activities without explicitly defining them as such.

Regarding challenges, a strategy writer expresses the struggle to what extent cyber incidents should be explained and translated into risk information for individuals. This may be interpreted as an unconscious acknowledgment of different levels of risk awareness, and that connection to those different levels may require different forms of communication.

It can be concluded that all interviewees observe and acknowledge different levels of accuracy, thoroughness and completeness regarding cybersecurity risk information processing without naming it as such. They are able to specify different levels of related knowledge and activities. No government aims related to risk tiers have been revealed. Therefore, it can be concluded that the conceptual element tiers being related to individual cyber resilience is only demonstrated by the interviewees on a personal note.

5.7 Emotion

Discourse analysis reveals three personal notifications by strategy writers referring to specific emotional tensions in the context of ransomware (panic), stories of victims (fear), and cyberattack anticipation (stress). No specific government aims regarding emotion have been directly expressed. One indirect aim, to prevent people from panicking and pay ransom when access is blocked, has been stated. This may indicate that most of the government's attention is primarily focused on rational acts and facts. A strategy writer has expressed the personal aim to apply fear appeal: “Widely share a victim's story. … Yes, that's what they call frightening in communication terms. … At least, that people really feel and also experience what it has been like for someone else and what that has done for that other person and has cost. … Only, communication-wise, people are very reluctant to do that sort of thing. I think it is very unfortunate.” This may be interpreted as meaning that the use of negative emotions to incite the target group to take supportive cybersecurity actions is undesirable by the government.

The interviewee’s assumption that a fear appeal would lead to a personal emotional experience appears to be contrary to the Protection Motivation Theory. According to the theory, a direct fear appeal leads to the assessment of the appraised severity, the expectancy of exposure, and belief in the

efficacy of the recommended response (Maddux & Rogers, 1983; Rogers, 1975). However, in this case, an indirect fear appeal is made by presenting a case of another person. This may be experienced as insufficiently representative of one's own personal situation, and thus be prone to the optimism bias (Warkentin et al., 2013) and/or normalcy bias (Omer & Alon, 1994).

It can be concluded that only strategy writers recognize the conceptual element emotion being related to individual cyber resilience to a limited extent. When mentioned, emotion is related to the conceptual element beliefs (how a situation is perceived) and action.

5.8 Beliefs

Discourse analysis reveals that in their research data, the strategy writers uncovered multiple examples of personal beliefs related to cybersecurity situations and actions. During the interviews, no specific government aims regarding citizens' beliefs have been directly expressed. A strategy writer expresses the personal aim to influence beliefs of citizens in such a way that basic cybersecurity actions in daily practice, such as updates and strong passwords, get into their subconscious mind to move into action more quickly. This shows that the existence of personal beliefs and their possible supportive contribution to individual cyber resilience is recognized by at least one strategy writer, and that it is still unclear how this could be influenced as such.

Another strategy writer acknowledges the struggle to influence personal beliefs: "So people have to be open to it [voluntarily experiencing potential misuse of personal vulnerabilities]. … Influencing behaviour, that's what it's all about. We are struggling with this from various departments … How are we going to change that behaviour in such a way that people feel that they really must do something?" This may be interpreted as a quest for how to intrinsically convince people to believe that action supportive to individual cyber resilience is necessary to perform.

Discourse analysis shows that strategy writers attribute the conceptual element beliefs directly to the conceptual element action. However, according to the Theory of Planned Behaviour (Ajzen, 1991, 2002), beliefs are directly related to intention and motivation, and then to action. This reasoning may indicate that they believe to think in the right direction. However, according to the related theory, they appear to misconstrue possible solutions to the perceived problem.

It can be concluded that strategy writers identify the conceptual element beliefs being relative to individual cyber resilience. Getting beliefs supportive to individual cyber resilience into the minds of citizens is experienced as a challenge. Although it is indicated that multiple departments struggle with

this challenge, no specific government aims regarding personal beliefs supportive to individual cyber resilience have yet been expressed.

5.9 Mental shortcuts

Discourse analysis shows that the interviewees do not refer to specific government aims regarding heuristics and biases (in short: mental shortcuts) have been defined. In the context of their statements, it appears that the strategy writers detect the existence of mental shortcuts from research without specifically referring to the words ‘heuristics’ and ‘biases’. They give examples related to the availability heuristic ("It won't happen to me"), optimism bias ("I am not interesting"), normalcy bias (“There is nothing to get from me”), overestimation of personal abilities known as the Dunning-Kruger effect ("They also rate their knowledge highly, the average Dutch person. But we don't see it reflected in the behaviour"), and selective perception (“The average citizen says: ‘Yes, VDL [an industrial company hit by a cyberattack], that doesn't affect me… I have nothing to do with it. Nice article.’ And then they move forward”). This may be interpreted as noting that mental shortcuts take place, after which they negatively influence the perception of risk, resulting in impediment to take supportive action. It also demonstrates resemblance with related heuristics and biases theories (Fagan & Khan, 2018; Kruger & Dunning, 1999; Omer & Alon, 1994; Tversky & Kahneman, 1974; Warkentin et al., 2013).

In the context of personal information entry, a policy maker expresses the personal aim to create an unconscious mental shortcut at individual level to whether or not leave information behind. This can be interpreted as a search for how to reduce the amount of conscious effort required to verify the secure deposit of personal information while supporting secure behaviour.

In the context of performing software updates, a strategy writer suggests to apply nudges: “But maybe we can bring it in such a way that people are more conscious in doing those updates, or at least in their subconscious more quickly engage in activities.” This may be interpreted as a personal aim to use mental shortcuts for the better by subconsciously lowering the threshold for individuals to take action supportive to their cybersecurity state of being.

It can be concluded that there is coherence between the theories related to heuristics and biases and the interview data. Based on their descriptions, interviewees note that mental shortcuts occur, thus acknowledging the conceptual element of mental shortcuts being relative to individual cyber resilience. It appears that they do not use the common terms (heuristics and biases) to demonstrate this notification. Also, these notifications are not yet converted into specific government aims.

5.10 Common findings

Discourse analysis shows that interviewees express general comments that add value to the findings so far.

During the interview with a strategy writer in the context of individual cyber resilience, the term ‘citizen’ was discussed. The strategy writer indicated to prefer the term ‘consumer’, emphasizing that consumers are perceived within the department as both individuals and businesses, as they all buy products. This may indicate a possible unconscious approach preference from an economic point of view, and a potential risk of reduced nuance regarding insight into details and diversity concerning (individual) cyber resilience from other angles.

Regarding responsibilities, a strategy writer indicates that the Ministry of Justice and Security is primarily responsible for the cyber resilience section within the Dutch Digitalization Strategy. Other departments with partial responsibilities in this field provide passages for this section. Although the strategy writer acknowledges that (individual) cyber resilience is perceived as an increasingly important topic, it is stated that the strategy does not contain much explicit passages about individual cyber resilience strengthening. This may be interpreted as meaning that considerations are made as to which information about strengthening cyber resilience is actually published in the strategy. If so, it may also explain why elements personally expressed as important are not mentioned in the strategy.

Regarding digitalization and related cybersecurity risks, a policy maker states: “Digitalization is a fait accompli and therefore the associated risks are also a fait accompli, otherwise you have to lock yourself in a hut somewhere in the heath.” This may be interpreted as meaning that digitized processes, products and services are permanently embedded in society, and related cybersecurity risks must be accepted and handled accordingly.

The answers to the final sub-questions ‘What do government officials aim to achieve regarding individual cyber resilience?’ and ‘What concerns and challenges do government officials face in achieving these aims?’ are mentioned in this chapter. Multiple government aims as well as personal aims, concerns and struggles are revealed, presented, assessed and interpreted to improve understanding. It can be concluded that the continuous process of strategy development and individual cyber resilience strengthening is permanently challenged by new insights, risks, technologies, attack tactics, different points of view, and different interests. As digitalization will remain within society, learning to deal with these dynamics will be too.

6 Discussion

Digitalized processes, products, and services are here to stay. Dutch citizens are gently but firmly pushed into an increasingly digitalized society. National and commercial interests will lead to a further increase in digitalization. Since 2018, the Dutch government implements its digitalization strategy, aiming to support all interests and mitigate cybersecurity risks.

The main objective of the Dutch Digitalization Strategy is to obtain economic growth and to better meet social challenges by means of digitalization. To support the adoption of and confidence in digitalization, citizens need competences to understand and deal with cybersecurity risks to mitigate personal harm. Government efforts to strengthen this individual cyber resilience have been assessed against the attributed conceptual elements.

The case study of the strategy reveals that the government treats individual cyber resilience as a process by continuously aiming to meet changing individual needs to strengthen individual cyber resilience. This is supported by the interview data. Regarding individual cyber resilience as a temporary state of being, discourse analysis reveals multiple personal aims, although the written strategy does not mention related government aims at all. Reference to this conceptual element in the strategy may be important to acknowledge and emphasize that situations related to information systems are not static, but subject to continuous change so that being individual cyber secure is a temporary status. Acknowledging, explaining and linking this temporary status to other conceptual elements, such as personal valuables and action, may be an important awareness booster. The lack of this could undermine the potential of measures already being taken to strengthen individual cyber resilience.

Regarding individual cyber resilience related to personal valuables, the interview data supports the aims formulated in the strategy regarding the focus on tangible smart devices and personal information. However, intangible personal property, such as bank accounts and digital identities, is not mentioned by the strategy or the interviewees. Reference to this type of personal valuables could provide a more complete understanding of individual cyber resilience being relative to personal valuables.

Regarding the conceptual element cost-benefit calculations, the identified mismatch is surprisingly large. Whereas all interviewees show through the use of their concepts and words that individuals perform cybersecurity related cost-benefit calculations, the strategy does not refer to it in the context of individual cyber resilience. Acknowledgement of this conceptual element in the strategy is important to improve understanding of the reasoning behind decisions by citizens, for this may reveal

root causes of supportive and subversive behaviour towards cybersecurity measures. It may also contribute to the acceptance that reduced individual cyber resilience may be the result of conscious personal choices. As it has been demonstrated that such calculations are directly related to other conceptual elements of individual cyber resilience, it may provide an important opportunity to emphasize their interdependence to improve the quality of such calculations.

Regarding individual cyber resilience requiring action, the interview data partially supports the actions described in the strategy. There is similarity in protective actions, but mismatch in actions to experience vulnerabilities at individual level by means of exercises, demonstrations, and responsible disclosures. Such actions towards individuals are lacking in the strategy. Because it is not a question of if, but when an individual will experience a cyberattack, habituation in taking cybersecurity related actions other than just protective is essential. Absence of government aims and interventions related to individual actions in the field of detection, response and recovery of cyberattacks may unintentionally lead to the impression that taking protective actions may be sufficient to strengthen individual cyber resilience.

Regarding the conceptual element tiers, another mismatch is detected. Whereas discourse analysis reveals extensive and specific understanding of different levels of accuracy, thoroughness and completeness related to risk information and treatment at individual level, there is no reference to such tiers in the strategy. The alleged lack of view on tiers in the strategy may lead to threat intelligence and associated recommended controls and responses being presented at an incorrect level of abstraction. As a result, such efforts may be ineffective and inefficient. Defining tiers for different target groups may be helpful to support the achievement of individual cyber resilience goals in an efficient and effective way.

Individual cyber resilience being related to emotion and beliefs is briefly mentioned in the strategy and by the interviewees. At this point, there is a mismatch between the conceptual theories on the one hand, and the strategy and interview data on the other. It has been demonstrated by literature review that emotions and beliefs can lead to actions supportive or subversive to individual cyber resilience. As strategy writers have seen it reflected in studies and have expressed concerns about it, it may be valuable to increase attention to the role of emotion and beliefs in the context of individual cyber resilience.

Regarding the conceptual element mental shortcuts, the mismatch is substantial. Whereas the strategy writers detect and recognize mental shortcuts and their impact on individual cyber resilience, this conceptual element is not mentioned in the strategy at all. Since it has been demonstrated and substantiated by literature review that heuristics and biases can lead to actions supportive or

subversive to individual cyber resilience, it may be valuable to increase attention for this conceptual element also.

It is noteworthy that the conceptual elements derived from the human behaviour theories seem to be absent from the strategy. It is not yet clear whether this is unintentional, or intentional due to conflict of interest, responsibilities in the strategy text, political correctness, and/or other considerations.

7 Conclusion

Government efforts to strengthen individual cyber resilience can be perceived as a secondary objective to support the primary digitalization objective. This research demonstrates that such a derived goal can lead to deficiencies in the approach to improve individual cyber resilience according to its interrelated conceptual elements.

The conceptual elements process, personal valuables, and action are (partly) reflected in the strategy. The elements temporary state of being, cost-benefit calculations, tiers, emotion, beliefs, and mental shortcuts are not sufficiently reflected in the strategy, although interviewees have substantiated its existence and expressed concerns about it.

The answer to the first part of the main research question ‘To what extent is individual cyber resilience strengthened by the Dutch government, and how may individual cyber resilience be improved at individual and government level?’ is formulated as supportive in one way, but far from sufficient in another way. The answer to the second part of the questions is attributed to the application of all conceptual elements identified. At individual level, taking personal responsibility for developing related competences and action is required. At government level, suggestions for improvement have been substantiated in the Discussion chapter 6.

Limitations

Due to the limited available research time, not all available academic literature related to (cyber) resilience topic is examined. Therefore, focus is put on peer reviewed articles and researchers frequently referenced. Qualitative interviews are limited due to the restricted amount of strategy writers and policy makers within the two departments who contributing to the individual cyber resilience sections in the Dutch Digitalization Strategy. To obtain data from a different perspective,

governmental researchers of a supervisory agency who examined cybersecurity threats and events of digitalization are interviewed as well.

Interview discourse can be seen as the result of an ongoing orientation of the interviewees to construct and express the context as they interpret it (R. Gill, 2000, p. 175). The discourse is also related to the occasion where an external researcher asks questions about a government strategy to which they contribute substantively or reflectively. As the discourse analysis is an interpretation by the researcher, there may be other ways of understanding the texts. Despite this risk, a discourse analysis is a valuable way of understanding the construct of text (R. Gill, 2000; Wacker, 2008). It is worth noting that the performed discourse analysis is principally meant to improve understanding of the concept of individual cyber resilience.

Recommendations

The fact that digitalization may also entail personal risks for citizens may be a difficult message to convey. Citizens may wonder why they should accept such risks arising from digitalization aims at national level. To secure national interests, it may be conditional to continuously involve citizens in understanding why digitalization is important, necessary and valuable, and how its benefits may outweigh any possible drawbacks. Therefore, a joint focus on common interests may be supportive to individual cyber resilience.

At present, individual cyber resilience is a derived objective of digitalization. It could be the subject of future research to investigate the impact on the adoptation of digitalization if individual cyber resilience is set as the main goal.

Extended automation and additional regulation may be necessary to prevent citizens from being burdened with security and financial consequences of the fact that the economic lifespan of smart devices is currently shorter than their technical lifespan.

In the government's definition of cyber resilience (NCTV, 2021, p. 14) the term 'prevention' is attributed to cyber incidents. However, cyber resilience scholars and theories do refer to this term at all. It has been argued that cyber incidents and cyberattacks cannot be prevented. Prevention of cyberattacks may only occur if the government is able to prohibit cyber attackers from continuing their activities by law enforcement (Nam, 2019). Therefore, it is suggested to use the commonly used term 'protection' instead of 'prevention' as it may better indicate what is probably meant.

References

Aberbach, J. D., & Rockman, B. (2002). Conducting and Coding Elite Interviews. *PS: Political Science and Politics*, *35*, 673–676.

ABN Amro. (2021). *Fraudeverhalen*. https://www.abnamro.nl/nl/prive/abnamro/veilig-bankieren/fraudeverhalen/index.html

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. *Journal of Applied Social Psychology*, *32 (4)*, 665–683.

Almeida, F., Duarte Santos, J., & Augusto Monteiro, J. (2020). The Challenges and Opportunities in the Digitalization of Companies in a Post-COVID-19 World. *IEEE Engineering Management Review*, *48*(3), 97–103. https://doi.org/10.1109/EMR.2020.3013206

American Psychological Association. (2012). *Building your resilience*. https://www.apa.org/topics/resilience

Andriole, S. J. (2018). Skills and Competencies for Digital Transformation. *IT Professional*, *20*(6), 78–81. https://doi.org/10.1109/MITP.2018.2876926

Banken.nl. (2013). *NVB: Nieuwe campagne veilig bankieren van start*. Banken.Nl. https://www.banken.nl/nieuws/1655/nvb-nieuwe-campagne-veilig-bankieren-van-start

Bax, S., McGill, T., & Hobbs, V. (2021). Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. *Computers & Security*, *106*, 1–15. https://doi.org/10.1016/j.cose.2021.102278

Bellur, S., & Sundar, S. S. (2014). How Can We Tell When a Heuristic Has Been Used? Design and Analysis Strategies for Capturing the Operation of Heuristics. *Communication Methods and Measures*, *8*(2), 116–137. https://doi.org/10.1080/19312458.2014.903390

Betz, D. J., & Stevens, T. (2011). Chapter One: Power and cyberspace. *Adelphi Series*, *51*(424), 35–54. https://doi.org/10.1080/19445571.2011.636954

Bio-overheid.nl. (2020). *Baseline Informatiebeveiliging Overheid (BIO) v1.04zv* (p. 76).

Boin, A., Kuipers, S., & Overdijk, W. (2013). Leadership in times of crisis: a framework for assessment. *International Review of Public Administration*, *18*(1), 79–91.

Brighi, A., Mameli, C., Menin, D., Guarini, A., Carpani, F., & Slee, P. T. (2019). Coping with cybervictimization: The role of direct confrontation and resilience on adolescent wellbeing. *International Journal of Environmental Research and Public Health*, *16*(24). https://doi.org/10.3390/ijerph16244893

Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers and Security*, *88*, 1–13. https://doi.org/10.1016/j.cose.2019.101607

Bryant, R. (2001). What Kind of Space is Cyberspace? *Minerva - An Internet Journal of Philosophy*, *5*, 138–155.

Bryant, W. D. (2015). Resiliency in Future Cyber Combat. *Strategic Studies Quarterly*, *9*(No. 4 (Winter)), 87–107. https://www.jstor.org/stable/26271279

Carretero, S., Vuorikari, R., & Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens. With eight proficiency levels and examples of use. In *Joint Research Centre*. Publications Office of the European Union. https://doi.org/10.2760/38842

Centraal Bureau voor de Statistiek. (2021). *Huishoudens nu*. https://www.cbs.nl/nl-nl/visualisaties/dashboard-bevolking/woonsituatie/huishoudens-nu

Chalmers, S. (2018). The concept of law. In *Liberia and the Dialectic of Law* (1st ed., pp. 23–37). Birkbeck Law Press. https://doi.org/10.4324/9781351000277

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. In *URN GS/14/835*. https://nrl.northumbria.ac.uk/id/eprint/23903/1/14-835-cyber-security-behavioural-insights.pdf

Dunn Cavelty, M., Kaufmann, M., & Søby Kristensen, K. (2015). Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue*, *46*(1), 3–14. https://doi.org/10.1177/0967010614559637

Dutch Department of Justice and Security. (2018). Wet beveiliging netwerk- en informatiesystemen. *Staatsblad*, 1–11.

Edwards, C. (2009). Resilient nation. In *Demos*. https://apo.org.au/sites/default/files/resource-files/2009-04/apo-nid12895.pdf

European Commission. (2008). The European Qualifications Framework for Lifelong Learning (EQF). In *Office for Official Publications of the European Communities*. https://doi.org/10.2766/14352

European Commission. (2020a). Digital Economy and Society Index (DESI) 2020: Thematic chapters. In *European Commission*. https://ec.europa.eu/digital-single-market/en/desi

European Commission. (2020b). European Skills Agenda for Sustainable Competitiveness , Social Fairness and Resilience. *OECD Publishing*, 1–23. https://ec.europa.eu/social/main.jsp?catId=1223&langId=hr

European Union. (2019). *Cybersecurity Act*. European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN#d1e40-15-1

European Union. (2021). *The history of the European Union*. https://europa.eu/european-union/about-

eu/history_en

Eurostat. (2021). *Level of internet access - households*. https://ec.europa.eu/eurostat/databrowser/view/tin00134/default/table?lang=en

Fagan, M., & Khan, M. M. H. (2018). To Follow or Not to Follow: A Study of User Motivations around Cybersecurity Advice. *IEEE Internet Computing*, *22*(5), 25–34.

Fergus, S., & Zimmerman, M. A. (2005). Adolescent Resilience: A Framework for Understanding Healthy Development in the Face of Risk. *Annual Review of Public Health*, *26*, 399–419. https://doi.org/10.1146/annurev.publhealth.26.021304.144357

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407–429.

Fox, J. R., Park, B., & Lang, A. (2007). When available resources become negative resources: The effects of cognitive overload on memory sensitivity and criterion bias. *Communication Research*, *34*(3), 277–296. https://doi.org/10.1177/0093650207300429

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal*, *204*(6), 291–295. https://doi.org/10.1038/bdj.2008.192

Gill, R. (2000). Discourse Analysis. In M. W. Bauer & G. Gaskell (Eds.), *Qualitative Researching with Text, Image and Sound: A Practical Handbook* (Vol. 1, pp. 172–190). SAGE.

Harvey, W. S. (2011). Strategies for conducting elite interviews. *Qualitative Research*, *11*(4), 431–441. https://doi.org/10.1177/1468794111404329

Herrington, L., & Aldrich, R. (2013). The future of cyber-resilience in an age of global complexity. *Politics*, *33*(4), 299–310. https://doi.org/10.1111/1467-9256.12035

Hua, J., Chen, Y., & Luo, X. (Robert). (2018). Are we ready for cyberterrorist attacks?—Examining the role of individual resilience. *Information and Management*, *55*(7), 928–938. https://doi.org/10.1016/j.im.2018.04.008

Johnson, C. K., & Gutzwiller, R. S. (2020). *A Cyber-Relevant Table of Decision Making Biases and their Definitions*. *December*. https://doi.org/10.13140/RG.2.2.14891.87846

Jones, E. E., & Harris, V. A. (1967). The attribution of attitudes. *Journal of Experimental Social Psychology*, *3*(1), 1–24. https://doi.org/10.1016/0022-1031(67)90034-0

Knops, D. R. W. (2018). *Kamerbrief digitale inclusie* (pp. 1–18). Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Kruger, J., & Dunning, D. (1999). Unskilled and Unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments. *Journal of Personality and Social Psychology1*, *77*(6), 1121–1134. https://doi.org/10.1037/0022-3514.77.6.1121

Kvale, S. (2011). Interview Quality. *Doing Interviews*, 79–91.

https://doi.org/10.4135/9781849208963.n7

Lazarus, R. S., & Folkman, S. (1984). *Stress, Appraisal, and Coping* (1984th ed.). Springer Publishing Company, Inc. https://www.academia.edu/37418588/_Richard_S_Lazarus_PhD_Susan_Folkman_PhD_Stress_BookFi_

Lederer, V., Loisel, P., Rivard, M., & Champagne, F. (2014). Exploring the diversity of conceptualizations of work (dis)ability: A scoping review of published definitions. *Journal of Occupational Rehabilitation*, *24*(2), 242–267. https://doi.org/10.1007/s10926-013-9459-4

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*(November 2018), 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Lorenz, B., Kikkas, K., & Osula, K. (2018). Development of Children's Cyber Security Competencies in Estonia. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10925 LNCS*, 473–482. https://doi.org/10.1007/978-3-319-91152-6_36

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Makdoun, I., Rahhal, I., Mezzour, G., Kassou, I., & Carley, K. M. (2021). Skill mismatch evidence for cybersecurity skills in Morocco. *Procedia Computer Science*, *184*(2018), 941–946. https://doi.org/10.1016/j.procs.2021.03.117

Marron, J., Gopstein, A., Bartol, N., & Feldman, V. (2019). *Cybersecurity Framework Smart Grid Profile*. https://doi.org/10.6028/NIST.TN.2051

Mäses, S., Randmann, L., Maennel, O., & Lorenz, B. (2018). Stenmap: Framework for Evaluating Cybersecurity-Related Skills Based on Computer Simulations. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10925 LNCS*, 492–504. https://doi.org/10.1007/978-3-319-91152-6_38

Ministerie van Economische Zaken en Klimaat. (2018). Nederlandse Digitaliseringsstrategie. *Tweede Kamer*. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2018Z11577&did=2018D34352

Ministerie van Economische Zaken en Klimaat. (2019). Nederlandse Digitaliseringsstrategie 2.0. *Tweede Kamer*, 1–45. https://www.rijksoverheid.nl/documenten/kamerstukken/2021/02/03/tk-uitkomsten-verkenning-wettelijke-bevoegdheden-digitale-weerbaarheid-en-beleidsreacties-

wodc-rapporten

Ministerie van Economische Zaken en Klimaat. (2020). *Nederlandse Digitaliseringsstrategie 2020*. 78. https://www.rijksoverheid.nl/documenten/rapporten/2020/06/25/nederlandse-digitaliseringsstrategie-2020

Ministerie van Economische Zaken en Klimaat. (2021). *Nederlandse Digitaliseringsstrategie 2021*. https://www.rijksoverheid.nl/documenten/rapporten/2020/06/25/nederlandse-digitaliseringsstrategie-2020

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*(May 2018), 1–10. https://doi.org/10.1016/j.techsoc.2019.03.005

NCTV. (2021). Cybersecuritybeeld Nederland 2021. In *Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)*.

NIST. (2018). Framework for improving critical infrastructure cybersecurity. In *National Institute of Standards and Technology* (p. 55). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

NIST. (2019). *Cybersecurity Framework V1-1 Presentation* (p. 12). National Institute of Standards and Technology. https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.nist.gov%2Fsystem%2Ffiles%2Fdocuments%2F2019%2F10%2F30%2Fcybersecurity_framework_v1-1_presentation.pptx&wdOrigin=BROWSELINK

OECD. (2014). *PISA 2012 Results: Creative Problem Solving: Students' Skills in Tackling Real-Life Problems: Vol. V*. https://doi.org/10.1787/9789264208070-en

OECD. (2017). *OECD Skills Strategy Diagnostic Report: The Netherlands*.

Oinas-Kukkonen, H., & Harjumaa, M. (2008). Towards deeper understanding of persuasion in software and information systems. *Proceedings of the 1st International Conference on Advances in Computer-Human Interaction, ACHI 2008*, *March*, 200–205. https://doi.org/10.1109/ACHI.2008.31

Omer, H., & Alon, N. (1994). The Continuity Principle: A Unified Approach to Disaster and Trauma. *American Journal of Community Psychology*, *22*(2), 273–287. https://www.proquest.com/docview/1295916811/fulltextPDF/B1D0953B0C1E4799PQ/1?accountid=12045

Overvest, B., Non, M. C., Dinkova, M., El-Dardiry, R. G. S., & Windig, R. J. (2019). *Cyber Security Risk Assessment for the Economy 2019*.

Oxford Advanced Learner's Dictionary. (2021a). *Definition of citizen*. Oxford University Press. https://www.oxfordlearnersdictionaries.com/definition/english/citizen

Oxford Advanced Learner's Dictionary. (2021b). *Definition of government*. Oxford University Press. https://www.oxfordlearnersdictionaries.com/definition/english/government?q=government

Panter-Brick, C., & Leckman, J. F. (2013). Editorial commentary: Resilience in child development - Interconnected pathways to wellbeing. *Journal of Child Psychology and Psychiatry and Allied Disciplines*, *54*(4), 333–336. https://doi.org/10.1111/jcpp.12057

Pennycook, G., Ross, R. M., Koehler, D. J., & Fugelsang, J. A. (2017). Dunning–Kruger effects in reasoning: Theoretical implications of the failure to recognize incompetence. *Psychonomic Bulletin and Review*, *24*(6), 1774–1784. https://doi.org/10.3758/s13423-017-1242-7

Percia David, D., Keupp, M. M., & Mermoud, A. (2020). Knowledge absorption for cyber-security: The role of human beliefs. *Computers in Human Behavior*, *106*(January). https://doi.org/10.1016/j.chb.2020.106255

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers and Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Pijpers, R., Heitink, M., Meelissen, M., Luyten, H., & Veldkamp, B. (2020). Leerlingmonitor Digitale Geletterdheid. In *Kennisnet*. https://www.kennisnet.nl/artikel/7743/leerlingmonitor-grote-verschillen-tussen-leerlingen-in-digitale-geletterdheid/

Potter, J. (2004). Discourse Analysis. In M. Hardy & A. Bryman (Eds.), *Handbook of Data Analysis* (1st ed., pp. 607–624). SAGE Publications, Ltd. https://doi.org/10.4135/9781848608184

Prins, P. mr. J. E. J., Schrijvers, D. E. K., Passchier, M. dr. R., & Visser, P. dr. M. de. (2019). *Voorbereiden op digitale ontwrichting*.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rutter, M. (2006). Implications of Resilience Concepts for Scientific Understanding. *Annals of the New York Academy of Sciences*, *1094*, 1–12. https://doi.org/10.1196/annals.1376.002

Rutter, M. (2012). Resilience as a dynamic concept. *Development and Psychopathology*, *24*(2), 335–344. https://doi.org/10.1017/S0954579412000028

Schneider, S. C. (1987). Information overload: Causes and consequences. *Human Systems Management*, *7*(2), 143–153. https://doi.org/10.3233/HSM-1987-7207

Schneier, B. (2000). *Semantic Attacks: The Third Wave of Network Attacks*. https://www.schneier.com/crypto-gram/archives/2000/1015.html#1

Shires, J. (2019). Family Resemblance or Family Argument? Three Perspectives on Cybersecurity and their Interactions. *St Antony's International Review*, *15*(1), 18–36.

Shires, J., & Hakmeh, J. (2020). Is the GCC Cyber Resilient? In *Chatham House* (p. 20). The Royal Institute of International Affairs.

Simanjuntak, T. (n.d.). *NIST CyberSecurity Framework: An Overview*. SlideShare. Retrieved

December 28, 2021, from https://www.slideshare.net/tandhy/simanjuntaktandhynistcybersecurityframework-v3/32

SLO. (2021). *Vakportaal digitale geletterdheid*. SLO. https://www.slo.nl/vakportalen/vakportaal-digitale-geletterdheid/

Southwick, S. M., Bonanno, G. A., Masten, A. S., Panter-Brick, C., & Yehuda, R. (2014a). Resilience definitions, theory, and challenges: Interdisciplinary perspectives. *European Journal of Psychotraumatology*, *5*, 1–14. https://doi.org/10.3402/ejpt.v5.25338

Southwick, S. M., Bonanno, G. A., Masten, A. S., Panter-Brick, C., & Yehuda, R. (2014b). Resilience definitions, theory, and challenges: interdisciplinary perspectives. *European Journal of Psychotraumatology*, *5*, 10.3402/ejpt.v5.25338. https://doi.org/10.3402/ejpt.v5.25338

Spöttl, G., & Windelband, L. (2021). The 4th industrial revolution–its impact on vocational skills. *Journal of Education and Work*, *34*(1), 29–52. https://doi.org/10.1080/13639080.2020.1858230

Stouffer, K., Zimmerman, T., Tang, C., Lubell, J., Cichonski, J., & McCarthy, J. (2019). Cybersecurity Framework Manufacturing Profile. In *NIST Internal Report*. https://doi.org/10.6028/NIST.IR.8183

Swanson, R. A., & Chermack, T. J. (2013). *Theory building in applied disciplines* (1st ed.). Berrett-Koehler Publishers. https://web-p-ebscohost-com.ezproxy.leidenuniv.nl/ehost/ebookviewer/ebook/ZTAwMHh3d19fNTgxODY2X19BTg2?sid=3eec738e-4282-4a4e-b632-69793b2bc2f5@redis&vid=0&format=EB&rid=1

The MITRE Corporation. (2022). *MITRE ATT&CK*. https://attack.mitre.org/

Third, A., Forrest-Lawrence, P., & Collier, A. (2014). *Addressing The Cyber Safety Challenge: From Risk to Resilience* (Issue June). https://researchdirect.westernsydney.edu.au/islandora/object/uws:28267/datastream/PDF/view

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and Biases. *Science*, *185 (4157)*, 1124–1131. https://doi.org/10.1126/science.185.4157.1124

Tweede Kamer. (2020). *Fiche 2: Europese Vaardighedenagenda* (pp. 1–8). https://www.rijksoverheid.nl/documenten/rapporten/2020/09/04/europese-vaardighedenagenda

van den Berg, J. (2018). Cybersecurity for Everyone. In M. Bartsch & S. Frey (Eds.), *Cybersecurity Best Practices* (pp. 571–583). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21655-9_40

van Kampen, H. S. (2019). The principle of consistency and the cause and function of behaviour. *Behavioural Processes*, *159*(November 2018), 42–54. https://doi.org/10.1016/j.beproc.2018.12.013

van Schaik, P., Renaud, K., Wilson, C., Jansen, J., & Onibokun, J. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers and Security*, *90*.

https://doi.org/10.1016/j.cose.2019.101651

van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity*, *6*(1), 1–8. https://doi.org/10.1093/CYBSEC/TYAA019

Vandoninck, S., d'Haenens, L., & Roe, K. (2013). Online Risks. *Journal of Children and Media*, *7*(1), 60–78. https://doi.org/10.1080/17482798.2012.739780

Vandoninck, S., D'Haenens, L., & Roe, K. (2013). Online Risks. *Journal of Children and Media*, *7*(1), 60–78. https://doi.org/10.1080/17482798.2012.739780

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Vuorikari, R., Punie, Y., Carretero, S., & Van Den Brande, L. (2016). DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: The Conceptual Reference Model. In *Jrc-Ipts* (Issue June). Publication Office of the European Union. https://doi.org/10.2791/11517

Wacker, J. G. (2008). A conceptual understanding of requirements for theory-building research: Guidelines for scientific theory building. *Journal of Supply Chain Management*, *44*(3), 5–15. https://doi.org/10.1111/j.1745-493X.2008.00062.x

Walklate, S., Mythen, G., & McGarry, R. (2012). States of Resilience and the Resilient State. *Current Issues in Criminal Justice*, *24*(2), 185–204. https://doi.org/10.1080/10345329.2012.12035954

Wall, E., Blaha, L., Paul, C., & Endert, A. (2019). A Formative Study of Interactive Bias Metrics in Visual Analytics Using Anchoring Bias. In D. Lamas, F. Loizides, L. Nacke, H. Petrie, M. Winckler, & Panayiotis Zaphiris (Eds.), *Human-Computer Interaction – INTERACT 2019* (1st ed., Vol. 1, pp. 555–575). Springer International Publishing. https://doi.org/10.1007/978-3-030-29384-0

Warkentin, M., Xu, Z., & Mutchler, L. A. (2013). I'm Safer than You: The Role of Optimism Bias in Personal IT Risk Assessments. *International Conference on Information Systems Proceedings*, *October*, 1–32. http://aisel.aisnet.org/icis2005/

Weil, T., & Murugesan, S. (2020). IT Risk and Resilience-Cybersecurity Response to COVID-19. *IT Professional*, *22*(3), 4–10. https://doi.org/10.1109/MITP.2020.2988330

West, R. F., Toplak, M. E., & Stanovich, K. E. (2008). Heuristics and Biases as Measures of Critical Thinking: Associations with Cognitive Ability and Thinking Dispositions. *Journal of Educational Psychology*, *100*(4), 930–941. https://doi.org/10.1037/a0012842

Wilding, N. (2016). Cyber resilience: How important is your reputation? How effective are your people? *Business Information Review*, *33*(2), 94–99. https://doi.org/10.1177/0266382116650299

Zebrowski, C. R. (2013). The nature of resilience. *Resilience*, *1*(3), 159–173. https://doi.org/10.1080/21693293.2013.804672

Zhang, D. J. (2010). Integrating Cyber Security Into Nuclear Digital I&C Safety Systems. *ASME Conference Proceedings 18th International Conference on Nuclear Engineering (ICONE18)*, 1–5. https://doi.org/10.1.1.658.3444

Appendix A. Interview transcripts

Due to the extent, the interview transcripts are available in a separate document and available to the thesis supervisors.